

Georgia State University College of Law

From the Selected Works of Jack F. Williams

May 27, 2008

Manipulating and Hiding Terrorist Content on the Internet: Legal and Tradecraft Issues

Jack F Williams, *Georgia State University*



Available at: https://works.bepress.com/jack_williams/1/

MANIPULATING AND HIDING TERRORIST CONTENT ON THE INTERNET: LEGAL AND TRADECRAFT ISSUES

Jack F. Williams
Professor, Georgia State University College of Law
Middle Eastern Institute
President
VIAPAB, LLC
Jwilliams@gsu.edu

Marisa Urgo
Executive Vice President for Strategic Research and Intelligence Analysis
VIAPAB, LLC

Tony Burns, JD
Georgia State University

ABSTRACT

The global war on terror ("GWOT") is being fought on many levels. In addition to traditional terror and counterterror activity, both sides are engaged in a public relations and propaganda war, employing the media, willingly and unwillingly, to support their positions. Hovering over these war campaigns are information technologies, which include the Internet. This article provides an introduction to various online content concealing practices that have been employed by those seeking to conceal or limit access to information on the Internet, including terrorist organizations. Further, there is a discussion on tracking and monitoring of website visitors. After reviewing open source information and websites, this article examines techniques and technologies that are easily available to terrorist organizations -- foreign and domestic -- whose structure can be obtained through Internet websites. The article then turns to a discussion of the legal issues posed by active and passive website monitoring techniques. To those who may assert that this article teaches the enemies of the United States new tactics and countermeasures, we note that the topics discussed in this article are culled from open-source information and are well-publicized and well-known tactics and measures. For obvious reasons, we have purposefully excluded certain tactics and countermeasures that may not be as well known.

TABLE OF CONTENTS

INTRODUCTION	4
I. DISSEMINATING INFORMATION.....	6
II. CONCEALING INFORMATION	12
A. Source Code.....	12
B. Concealed Messages in Source Code	13
C. Hidden Links	14
D. Disguised Images.....	16
E. Orphaned Sections	17
F. Meta Refreshes	17
G. Example Page	18
III. SITE SEARCHING.....	21
A. Crawlers and Spiders	21
B. Site Mirroring	22
C. Tracking and Statistical Services.....	23
D. “Bug” Tracking.....	25
E. Hijacking.....	29
F. Location Filtering	31
G. Log File Information.....	32
IV. SITE SPOOFING	33
V. EXAMPLE WEBSITE.....	34
A. Scenario One.....	36
B. Scenario Two	39
C. Scenario Three	42
D. Scenario Four.....	44
E. Alternate Port.....	49
F. Alternate Page Extension (<i>i.e.</i> , .jack).....	51
VI. LEGAL IMPLICATIONS	52
Conclusion	60

INTRODUCTION

Information technologies shrink our world, bringing together families, friends, businesses, and governments. These same technologies have also brought terrorists closer to their intended victims and to themselves for purposes of community, recruiting, fundraising, and training. The dissemination of information over the Internet is most often straightforward and transparent; however, it is possible to conceal content while freely distributing information around the world with a wide variety of implementation options. These options for concealing content can often be achieved with little technical skill or effort. Thus, a terrorist organization may engage in asymmetrical activity in an effective manner by leveraging activity through prudent and covert Internet use.

The ability to track a website's visitors and their habits concerning a target site is another aspect of the Internet. Gathering statistics about site visitors is a common practice and an integral part of doing business on the Internet. The ability to track and trace visitors depends on the ability to manipulate and control various aspects of the site, in addition to the ability to fund such endeavors. Site components include the domain name, domain name servers, site hardware, content and webserver software, and dynamic elements, *etc.* With administrative authority over the components, one can control the content and content dissemination; one can also gather detailed information regarding each visitor. This detailed information may include the following: who visited (as tracked by IP address), the geographic location of the visitor, length of the visit, and the frequency of visits.

On August 1, 2005, while inspecting user logs on an Internet server popular among cyber-jihadists, Vladimir, the purveyor of InfoVlad.net, came across an image file of a well-

dressed, middle class teenager, sporting cool shades, and using an Internet service provider (“ISP”) located in Jordan.¹ In the seven years since September 11, 2001 al Qaida and its affiliate groups and sympathizers have exploited the boundless nature of the Internet, repackaging themselves as slick technologically savvy fighters for Allah, employing every digital tool available to maintain a stream of young men ready to kill and die.

Al Qaida’s long-term communications strategy includes a simple goal: maintain the hearts and minds of enough young Muslim men to sustain the global jihad until it has accomplished its goal of ridding the Muslim world from Western cultural and geo-political influence, and to expand the Muslim community and world through dawa or a religious “call to faith.” One putative “reformed jihadi” told Saudi TV in 2005 that, “The brothers in Afghanistan wanted to build an army of 12,000 fighters who would constitute the core of Islam, to whom Allah would grant victory.”² This “core of radical and militaristic Islam” is allegedly drawn from a long Islamic military history – endlessly retold by today’s Salafist-Jihadist ideologues – and includes many examples of small armies of Muslim men winning strategic battles against larger, stronger enemies. One such story involves the Battle of Badr, where Mohammed and a small group of companions defeated the ruling pagan tribes of Mecca. Bin Laden has attempted to maintain a similar cadre of young men willing to die

¹ Infovlad.net, Ecce Homo, <http://www.infovlad.net/?p=253> (last visited December 24, 2007).



² Middle East Media Research Institute. “Saudi Al-Qaeda Terrorists: We Meant to Build a 12,000-Strong Army,” Clip No. 966, December 13, 2005. http://www.memritv.org/clip_transcript/en/966.htm (last visited May 26, 2008)

often described as a “vanguard.” They are a new generation of “companions” to Bin Laden’s leadership.

The Internet has become the pulsing lifeblood of the “core of Jihadi Islam,” developing and maintaining community cohesion across languages and borders. Active Salafist-Jihadists all over the world rely on Internet forums for news and information. They build friendships and form their own “brigades.” Further, they share ideas on everything from how to tell their mothers they are going to fight jihad, to jihadi tactics, such as a video showing creative use of a sheep carcass as Improvised Explosive Device (“IED”) camouflage³ and a recent video showing a simple but sophisticated recipe for the manufacture of nitroglycerin.

I. DISSEMINATING INFORMATION

Jihadists are comfortable and proficient in employing modern information and telecommunication technologies. For instance, insurgents sent emails and posted messages to forums from Fallujah during Marine operations there in November 2004.⁴ Younis Tsouli, a notorious cyber jihadi arrested in the United Kingdom in October 2005, was a prolific jihadi forum participant, going by the *nom de guerre*, irhabi007 (translated as terrorist007).⁵ Rabei Osman Sayed Ahmed, also known as Mohammed the Egyptian and suspected of being the

³ Di. Rusty Shackleford, *Terrorists Using Sheep IED in Iraq*, THE JAWA REPORT, Feb. 21, 2006, <http://mypetjawa.mu.nu/archives/159773.php>.

⁴ *Through the Eyes of the Mujahideen*, JANES.COM, Dec. 1, 2004, http://www.janes.com/security/international_security/news/jiaa/jiaa041201_1_n.shtml. (last visited December 24, 2007)

⁵ See Rita Katz & Michael Kern, *Terrorist 007, Exposed*, WASHINGTON POST, Mar. 26, 2006, at B01, available at <http://siteinstitute.org/bin/articles.cgi?ID=inthenews10206&Category=inthenews&Subcategory=0> (discussing the exposure of Terrorist007 by intelligence services).

mastermind of the Madrid 3/11 bombings,⁶ spent late nights surfing jihadi forums. He was a “stateless” Arab, who illegally traversed the European Union, maintaining his connections to the jihadi movement through the Internet. Italian officials believe Ahmed downloaded hundreds of files and used them for recruitment⁷. Closer to home, U.S. officials have accused Marwan El-Hindi of registering for a “basic training” course on a secure jihadist website. According to the Federal indictment, he and two other young men in Ohio planned to integrate Internet-based paramilitary training videos into a real-world course for young American men willing to go to Iraq to fight for the insurgents.⁸

The enemy is always on the vanguard of new technology. They were early adopters of satellite communications, the only means of reaching their families and fellow jihadists while moving in the high mountain regions of Pakistan and Afghanistan. Further, they were also early adopters of video and print technology. Early Salafist-Jihadist leaders like Sheik Abdullah Azzam, who co-founded Al Qaida with Osama bin Laden, videotaped sermons, speeches, and press conferences. Azzam’s disciples are digitizing this material and making it available to participants on today’s jihadi forums and websites.⁹

Necessity continued to drive innovation throughout the 1990s. Many Arab leaders of the Afghan-Soviet War, who had settled in countries like Kuwait and Pakistan, were forced to move after the first Gulf War. Some returned to their home countries, while others fled west and settled in the U.S., Spain, and the United Kingdom. They founded large, thriving radical

⁶ Elaine Sciolino, *On Trial in Milan: New Kind of Enemy*, INT’L HERALD TRIB., Nov. 18, 2005, <http://www.iht.com/articles/2005/11/18/europe/web.milan.php>. (last visited, December 24, 2007)

⁷ After a lengthy trial in Madrid in 2007, Ahmed was acquitted of all charges, due to lack of strong evidence on October 31, 2007. See <http://www.foxnews.com/story/0,2933,306577,00.html> (last visited, December 24, 2007)

⁸ Indictment Against Amawi, El-Hindi, and Mazloun, http://www.usdoj.gov/opa/documents/indictment_22006.pdf (last visited December 24, 2007).

⁹ Questions and Answers Regarding Jihad – Sheikh Abdullah Azzam, <http://www.archive.org/details/azzam-qa-jihad> (last visited Sept. 5, 2006).

Salafist-Jihadist communities, and maintained contact with their movements in the Middle East through the Internet. Many of the first Salafist-Jihadist websites dedicated to jihad against the West date from the mid-1990s.

After some early web experimentations in 2002, Al Qaida's current digital media began as a public relations effort in Saudi Arabia after the May 2003 attacks on four housing compounds in Riyadh. Average Saudis did not support the attacks, and Al Qaida ground commanders decided the group needed a way to quickly voice their justifications to counter the Saudi government's spin on the issue. The first issue of *Voice of Jihad* magazine was published and posted on a popular jihad forum in October 2003.¹⁰ The *Al Battar Training Camp* magazine followed in January 2004. As its name implies, the magazine explained paramilitary skills once taught in the Afghan training camps: how to clean a gun, how to create camouflage, who to target for kidnapping and assassination. Both magazines were produced regularly until their chief editors and designers were eliminated by the Saudi government.

The adoption of digital technology came as a response to mainstream Arab media's reluctance to accommodate Al Qaida's request to broadcast their unabridged audio and videotapes. Al Qaida leaders and ground commanders began to make their own media, distributing it through Internet forums where most of their core followers access them with no extraneous editorial hindrances. It is a challenge-response pattern that displays the group's resilience in addition to the sheer power of using networking technology to sustain a borderless, global community.

In a parallel development, the accessibility of cheap, light-weight digital video cameras and easy-to-use movie production software, allowed terrorists in Iraq to take the print

¹⁰ Reuven Paz, *Sawt al-Jihad* (Oct. 27, 2003), <http://www.ladlass.com/intel/archives/007049.html>.

idea and turn it into video. Soon after September 11, 2001, Osama Bin Laden and Ayman al-Zawahiri began producing audio and videotapes through a front organization, As-Sahab. The early videos were not much better than amateur home videos, but production values quickly improved. After switching to digital audio and video files distributed over the Internet, the production quality mimics that of any Arab news show, using logos, credits, and even commercials. By 2004, many, if not all, operations against U.S. forces in Iraq had a video component. The cameraman became just as important as the gunmen and IED builders. In the succeeding eighteen months, Iraq became a terrorist “Bollywood” complete with genres and celebrities such as martyr profiles of suicide bombers, and named “stars” of sniper videos showing insurgents firing at American soldiers. A 2006 As-Sahab video, commemorating London bombers Mohammad Siddiqui Khan and Shahzad Tanweer, also included in-house animations and event re-creations.

One media adaptation shows the speed of Al Qaida’s response to traditional media challenges. Tired of not seeing Arab language news channels cover the issues they find important, Al Qaida began producing its own news show: Voice of the Caliphate. Airing in September 2005, the first episode included a lone masked man sitting at a table reading from a piece of paper.¹¹ One episode included a one-on-one interview with Saif al-Kinani, the “head of the public relations office” of the Global Islamic Media Front, Al Qaida’s media company. Al Qaida is not the only group using the news broadcast format. Ansar al-Sunnah, an Iraqi based insurgency group, produced an hour-long news magazine show with masked “anchors”

¹¹ “New Al-Qaeda Weekly Internet News Broadcast Celebrates U.S. Hurricanes and Gaza Pullout, Reports on Al-Zarqawi's Anti-Shiite Campaign and Chemical Mortar Shells in Iraq,” MEMRITV, Special Dispatch Series - No. 993. <http://www.memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP99305> (last visited December 24, 2007).

reading the news and a masked “reporter” visiting a school in Iraq.¹² Experiments in the format continue to show up in the regular streams of information.

As the leading group in the global Salafist-Jihadist movement, it has laid the ground work for a single, global knowledge base that is defining the movement. Today, every major Salafist-Jihadist group produces periodicals and videos distributed through their forums on assorted methods of mayhem and destruction. Using digital print, video, and communication techniques, Al Qaida has become so adept at framing events that it is able to morph its operational failures into strategic successes within hours. Its failed attack on a key Saudi Arabian oil refinery is a perfect example. The mujahedeen teams failed to inflict significant damage to the facility, but within 24 hours, Al Qaida claimed it as a success, and responded directly to claims that the operation was a failure, stating, “We direct your particular attention to the erroneous media broadcast claiming that the operation was foiled when the two vehicles exploded at the gate.”

Contemporary jihadi websites are more than just an outlet for Cold War-era style propaganda. They are communities built around a core identity, often the work of a specific religious authority, charismatic leader, ideologue, or regional Salafist-Jihadist movement. Any young man drawn to the movement would need to acquire a jihadi identity by building a deeper religious and ideological understanding of the movement. Thousands of articles, fatawa, sermons, reports, and even PowerPoint presentations are available to build and disseminate the terror masters’ understanding of jihad in word and deed. Far from being just outlets of information, as educational programming, websites and forums act as individual

¹² *The Lions of the Nomads in the City of al-Ramadi - A Video Presented by the Media Department of Ansar al-Sunnah Army*, SITE INST. (Mar. 15, 2006), <http://siteinstitute.org/bin/articles.cgi?ID=publications156606&Category=publications&Subcategory=0>. (last visited December 24, 2007)

pathways toward jihad. Some young men grow bored and drop out, but others are drawn closer into the community. These young men form what the terror masters call the “core of Islam,” and it is these young men who represent the next generation of terrorists.

The potential was recognized early by Salafist-Jihadist ideologue, Abu Mu’sab al-Suri. In his 1,600 page strategic document, “A Call for Global Islamic Resistance,” he describes a “jihad of individualized terrorism,”¹³ where self-identified movement members educate themselves on Salafist-Jihadist ideology and paramilitary tactics, and then commit acts of terrorism based on information drawn from the vast knowledgebase available on the Internet.

None of this activity goes on under the cloak of state secrets. Unlike our enemies of the past like the Soviet Union, Al Qaida and the associated movement does not maintain a bureaucracy of information controllers. Instead, it relies on the power of distributed numbers, trusting that if information is worth sharing, it will be shared for the improvement of the entire movement, regardless of who else reads it. In this way, the Internet is just as important as sanctuary, funding, and state support. The Internet is the lifeline of the movement, because it keeps the message fresh and relevant to the young men who find instruction, camaraderie, and a certain kind of entertainment in real-life hyper-violence.

Osama Bin Laden, as leader of the global Salafist-Jihadist movement, repeatedly remind their followers that Allah will protect them and guide them to victory as long as they follow Islamic law. There is nothing in that law that prevents them from using the Internet or any other technology to gain global dominance. They need only keep in God’s good grace and survive to fight another day. As Abu Mu’sab al-Suri once wrote, “The power will be

¹³ BRYNJAR LIA, THE AL-QAIDA STRATEGIST ABU MUS’AB AL SURI: A PROFILE (2006), http://www.mil.no/multimedia/archive/00076/_The_Al-Qaida_strate_76568a.pdf.

greatly unbalanced between us and the enemy, so the only choice is that we will have to be patient and to sacrifice. However, the duty of jihad is a must until the end of days.”¹⁴

II. CONCEALING INFORMATION

This portion of the paper presents a limited discussion about the techniques used to openly disseminate information *via* the Internet while, at the same time, limiting access to certain components of the site to informed users. The following are specific techniques used to conceal information, which are included in an example Web page (“page”) at the end of this section, referred to as “example.html.”

A. *Source Code*

All Web browsers (“browsers”), such as Internet Explorer (IE), Netscape, Firefox, Opera, and Safari, use the source code (“source”) of a page as instructions on how to display or render the page for the visitor (*i.e.*, text, background color, text size, text color, page layout, image sizes, *etc.*). While text and images are often displayed to visitors, there is always underlying source code not displayed to a visitor, unless the visitor actually sought to view the source code. Generally, the more advanced the page design, the more non-displayed source code that exists. A plethora of source code components and instructions are not directly displayed, including comments, JavaScript, includes, stylesheets, table formats, and more.

Although owners of content may implement JavaScript to block browsers from displaying the source, a determined visitor still may gain access to the source code. The visitor can save the page locally then view the source through Microsoft Notepad or a similar

¹⁴ “A Quote from a Jihadist,” Political Yen/Yang Blog, (August 3, 2005) <http://poli-yy.blogspot.com/2005/08/quote-from-jihadist.html> (last visited May 27, 2007)

text editor. Additionally, some lesser known and less popular browsers, such as Lynx, do not respect or recognize an attempt to block source code viewing.

Almost all structured HTML pages at a minimum contain the following structure, while most pages contain significantly more.

```
<HTML>  
    <HEAD> </HEAD>  
    <BODY> </BODY>  
</HTML>
```

B. Concealed Messages in Source Code

The general perception is that a public site publishes its content for public consumption and the world is invited to access and digest the information on the site. However, some sites make information available around the world but conceal or restrict certain information to those identified as proper users. Both the general information and the special information exist together on the site. Without knowing the proper access protocol, however, any attempt by the general public to access the special information is highly unlikely but far from impossible. This game of virtual “hide and seek” is similar to the struggle between governments and counterfeiters. For example, the United States uses disguised words and symbols on U.S. currency, which to the untrained eye appear to be decoration or images, if detectable at all. Nonetheless, those who are trained, look for the disguised words, watermarks, and other symbols to validate the authenticity of the currency.

As discussed previously, a page has two views. The first view is rendered (presented or displayed) to the visitor via their browser. The second is the source used by the browser as the instructions for rendering the page. The browser does not display the entire source, although it is always delivered with each page. To view source in mainstream browsers, such as IE, Netscape, and Firefox, click on “View” from the menu bar, then select “Page Source”

or “Source.” Once selected, a new window will appear displaying the source of the page being viewed through the browser.

In an effort to obscure content, one common technique is to instruct a browser not to display certain content by commenting out the content. If text is within comment tags, the browser will not display the comments, unless one actually views the source code. For HTML pages, comment tags are “<!--” and “-->” where the beginning tag is “<!--” and the ending tag is “-->.” These tags must be in this order. As stated above, any content located within the comment tags is not presented via the browser. By using a comment tag, terrorist organizations may direct key users to additional sites by embedding words or symbols that harbor links to other pages. The specific directions may be transferred by word-of-mouth, a prior communication, or agreed-upon procedures. The following comment example is from the example.html page below:

```
<!--  
  Beginning of comments that are not rendered by the browser.  
  (1) Confidential info. Is located at  
  http://example.com/notlinked/secret.html  
  (2) The word "Hidden", in the parentheses, links to another site.  
  (3) The second word 'LINK' is also a link to another site.  
  (4) The 5TH period ".", is a link to another page.  
  (5) The meta refresh takes the visitor to another page after 20  
  minutes (1200 seconds).  
  Thus, if the visitor does nothing for 20 min, the page will  
  automatically take the visitor elsewhere.  
-->
```

C. Hidden Links

Links are universally used portals to different web locations. Links are convenient, easily usable, and efficient mechanisms to share additional information and resources with site visitors. Without a link, a visitor has to know the specific URL and manually insert it into the address bar.

Most sites provide links to different pages or sites. Standard procedure provides that links are usually identified by a contrasting color and an underline or other clear indication of

their status as a link. This contrasting convention is done so both the link and the ordinary text may be easily identifiable. This convention may be easily exploited by a terrorist organization. For example, a terrorist organization may seek to hide information in the “open” by providing a link, but disguising or otherwise concealing the link to prevent ordinary visitors from accessing hidden information.

With minimal effort and expertise, a link can be instructed to appear just like all other text on a webpage, including matching link text color with standard text color, removing underlines, and any other clear indication of its status as a link. Using this technique in example.html below, the following is displayed in the browser: “The next 'LINK' word at the end of this sentence is a non-underlined LINK, which takes the user to another site.” The source code that enables this is as follows:

```
The next 'LINK' word at the end of this sentence is a non-underlined
<a style="text-decoration: none" href=http://dod.gov target=
"_blank"><font color=black>LINK</font></a>, which takes the user to
another site. <br><br>
```

With little additional effort or expertise, a link’s color may be set to the background color of the page itself, thus, making the link invisible. Therefore, a visitor would have to know of the link’s existence, carefully search the source code for these types of links, or stumble across the link. In the example.html page, the following is displayed in the browser: “The following parentheses contain a concealed link (), which could be hidden anywhere on a page.” The source that enables this is as follows:

```
The following parentheses contain a concealed link
(<a href="http://www.mitre.org" target= "_blank"><font
color=#CCCCC>Hidden</font></a>), which could be hidden anywhere on a
page.<br><br>
```

In the example.html page below, the fifth period on the document is a link to a different site. The following is rendered via the browser: “This sentence’s period is a link

and below this line are hidden messages in the source.” The source that enables this is as follows:

```
<u>This sentence's period is a link and below are concealed messages  
in the source<a href="http://www.dhs.gov" target=  
"_blank">.</a></u><br><br>
```

D. *Disguised Images*

For practical purposes, an image may contain an unlimited variety of content and content types, including pictures, maps, text, and even one pixel white space (*i.e.*, the smallest footprint available). The one-pixel white space gif is discussed in more detail later under “Bug” Tracking. This portion of the paper discusses display manipulation of images.

In the example.html page below, the same image (.jpg file) is displayed four different times. The first image displayed is clear and easily identified, while the last is smaller than a period and is easily overlooked or mistaken for a smudge on the monitor. However, each image is the same (*i.e.*, ../img/mapimage.jpg). The only difference is how the image is instructed to be displayed. The third image appears to be a period, and could be placed as a period, but it is in reality an image of a map (or picture, graph, *etc.*).

At this stage it is important to distinguish between the “period as a link” example described in Section C with the “picture as a period” example described in this Section. A major difference between the two content manipulators is that with the “period as a link” example, a visitor could actually stumble across the period and trigger a cursor link indicator. That is, with the “period as a link” example, if a visitor were to mouse-over the period, the cursor would indicate a link. However, in the case where one uses the “picture as a period” example, a mouse-over would not indicate a link. Thus, the tell-tale sign of a link could not be accidentally triggered.

In order to view the “picture as a period” image, a user could “right click” over the image and select “properties.” The dialogue box displayed contains the address of the image. By copying the location (i.e., <http://example.com/pdf-img/oblp11.jpg>) and pasting the URL in the browser’s location bar, the full image will be displayed. The user could also search the source for images not displayed on the page, but this could be a difficult task if done manually depending on size of the page and number of images.

The following is the source that includes and displays the first and fourth image. Notice the only difference is the settings for width, height, and border.

```
<center>(1) </center><br>
<center>(4) </center><br><br>
```

E. Orphaned Sections

If a page or section of pages (“section”) is not linked from the home page or other linked pages, the page or section does not exist for practical purposes to the average visitor or for search engines (e.g., Google™). The visitor would have to know that the unlinked page or section exist and manually enter the URL into the browser’s address bar (i.e., <http://example.com/orphaned/message.html>). Many mainstream sites use this technique to test functionality, new content, designs, and layouts prior to public launches.

F. Meta Refreshes

A common technique used by many sites is an automatic refresh of the page after the visitor has viewed the page for a specified amount of time. Often a meta refresh is the technique used to attain the automatic refresh. The refresh is often applied to pages that change fairly frequently. For example, news and sporting sites may refresh their news or

scoring pages automatically every minute or so in order to keep visitors abreast of current events and scores.

When the refresh is implemented, it is possible to instruct the browser to refresh to a different site or location within the current site. Further, the interval for refresh is configurable based on the site's preferences (*e.g.*, 10, 20, 60 minutes, *etc.*), so that a patient and informed visitor would know to wait for the page to refresh and take the visitor to the predetermined alternate location. A visitor may also view the source and see the refresh destination because the meta refresh is another non-displayed instruction. Unlike finding a commented image, the meta refresh rate is easy to identify in the source. By setting the refresh rate to an extended period of time, the average visitor is excluded from this refresh function, as an ordinary visitor does not pause on a page for an extended period of time. However, the risk may be deemed unacceptable as an unintended user may leave the page up while tending to other matters.

The `example.html` page has a refresh rate of twenty minutes (1,200 seconds) that is enabled as follows:

```
<meta http-equiv="refresh"
content="1200;url=http://example.com/redirected/directory/index-
redirect.html" />
```

G. Example Page

We constructed the following page, [example.html](#), so that it contains an example of each technique described above for concealing content on a publicly accessible page. The displayed page looks like the following:

VI. Example.html -- Concealing Content - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://example.com/example.html Go


This simple page has concealed content and links. Several examples follow:





The following parentheses contain a concealed link (), which could be hidden anywhere on a page.

The next 'LINK' word at the end of this sentence is a non-underlined LINK, which takes the user to another site.

This sentence contains a 'bug', which cannot be seen by site visitors.

The next four images are the same image. The only difference between the images are the display characteristics relating to size.



(1)  (2)  (3)  (4) 

This sentence's period is a link and below are concealed messages in the source.

My Computer

The source code for the page above is as follows:

[illegible]

III. SITE SEARCHING

The ability to search and reproduce content from sites is important. Search engines, such as Google™ and Yahoo!™ enable the Internet to be a prevalent communication channel available practically around the world. Search engines base their knowledge of the Internet's content on the ability to electronically search, copy, and/or index a wide-range of information contained on publicly available Internet sites.

Sites are often comprised of many apparently unrelated pages, links, and pages grouped by theme or topic ("sections"). Therefore, a detailed manual (human) search of sites is impractical, if not impossible, where multiple sites are involved and where the content changes frequently. However, technology provides many helpful techniques and tools in order to search and keep track of site content. For example, one can use a "crawler" or "spider" to index target sites or to save information about target sites to the spider's local computer or network. A variation of a searching script is a mirror script, which creates a copy of the site on the spider's local computer or network.

A. *Crawlers and Spiders*

A spider or crawler is a form of robot ("bot") that is an extremely useful tool for indexing and searching sites on the Internet. The spiders are computer scripts with the ability to search, save, and index information relating to target sites at a speed that is exponentially faster than that of humans and error free. A robot is defined as a "program that runs automatically without human intervention."¹⁵ Usually, "a robot is endowed with some

¹⁵ Webopedia: How Web Search Engines Work, <http://www.webopedia.com/DidYouKnow/Internet/2003/HowWebSearchEnginesWork.asp> (last visited Feb. 14, 2007).

artificial intelligence so it can react to different situations it may encounter.”¹⁶ One common type of robot is the “spider.”¹⁷ A spider is defined as a “program that automatically fetches Web pages. Spiders are used to feed pages to search engines. Since most Web pages contain links to other pages, a spider can start almost anywhere. As soon as it sees a link to another page, it goes off and fetches it.”¹⁸ Further,

[c]rawler-based engines send crawlers, or spiders, out into cyberspace. There, crawlers visit a Website, read the information on the actual site, read the site’s meta tags, and follow the links to which the site connects. The crawler returns all that information back to a central repository where the data is indexed. The crawler will periodically return to the sites to check for any information that has changed[.]¹⁹

The most notorious users of spiders or crawlers are search engines (*e.g.*, Google™ and Yahoo!™). A search engine returns a list of URLs with a description of the link based on the visitor’s inquiry. For example, the visitor enters a search string (*e.g.* “Atlanta law schools”), then the search engine applies a search algorithm to its database, which contains information about sites around the world.

B. Site Mirroring

While a bot searches a site, other tools attempt to reproduce complete copies (mirror images) of the target site on the mirror’s local computer or network. As with most situations, the level of success is based on the configuration and design of the target site and the script

¹⁶ Webopedia: Robot, <http://webopaedia.com/TERM/robot.html> (last visited Sept. 5, 2006).

¹⁷ *Id.*

¹⁸ Webopedia: Spider, <http://webopaedia.com/TERM/spider.html> (last visited Sept. 5, 2006).

¹⁹ Webopedia: How Web Search Engines Work, <http://www.webopedia.com/DidYouKnow/Internet/2003/HowWebSearchEnginesWork.asp> (last visited Sept. 5, 2006).

implemented. The easiest and most effective implementation is achieved when the mirrorer has unfettered access (full access and permissions) to the target site. Typically, however, a mirrorer has limited access to the site as though it was an ordinary visitor. Thus, the mirrorer can only copy files linked from the home page, or a page linked from a page linked from the home page, and so on. For example, a mirrorer could reproduce any page linked to another page linked to the home page or is otherwise explicitly given to the bot. Therefore, an orphaned directory or page will not be detected by a spider. A basic method for site mirroring is:

“`wget --mirror <domain>`”, as exemplified by “`wget --mirror www.mitre.org`”

C. Tracking and Statistical Services

Site audits seek to catalogue who is visiting what site, what is viewed at the site, when it is visited, and where the visitor comes from.

The ability to know statistical information (Web analytics) regarding site visitors is important, particularly for Internet businesses. Statistical information reveals how a site is used as well as the characteristics and habits of the site’s visitors. Often the statistical information includes, who visited (IP address), their habits, what pages are viewed, and the rough duration spent on the site and/or individual pages. With the appropriate budget, tools, access, and control of the target site’s hardware and software, a myriad of detailed information about the site’s usage and visitors can be gathered, sorted, reported, and graphed.

In the market place, several companies provide Web analytics. The services provide varying information from geographic location of visitors (*i.e.*, city and/or nation of origin), bandwidth of the visitor (*i.e.*, dial-up or broadband), type of browser, and length of time spent at various pages of the site.

To enable a third-party service to gather the information about visitors, a block of code must be embedded on each page of the target site that is to be tracked. The block of code required varies depending on the service provider. This block of code is not rendered by the browser and thus not visible to the visitor, unless the source is viewed.

Below are examples of code blocks used by Fireclick™, Omniture™, and StatCounter™ for Web analytics. Fireclick™ and Omniture™ are cost based services used by several large corporations, while StatCounter™ is a free service. These are only a few of the companies providing these services.

Fireclick™ block of code for creating Web analytics:

```
<!-- Fireclick Netflame -->
<script language="javascript">
function handle(){return true;}
window.onerror=handle;
var fc_host='www.example.com';
document.write('<scr'+ 'ipt '
+'src="'+((location.protocol=='http:')?'http://a644.g.akamai.net/f/644
/67/3h/':'https://a248.e.akamai.net/f/248/67/3h/ssl-')
+'hints.netflame.cc/service/sc'+ 'ript/'+fc_host+'"></scr'+ 'ipt>');
function fcce(){if (typeof(fcnf)!="undefined") fcnf();}
var fcnf=window.onload;
function fcco(){window.setTimeout("fcce();", 100);fcfn();}
window.onload= null==fcfn ? fcce:fcco;
</script>
<!-- Fireclick Netflame -->
```

Omniture™ block of code for creating Web analytics:

```
<!-- SiteCatalyst code version: G.1.
Copyright 1997-2003 Omniture, Inc. More info available at
http://www.omniture.com --><script language="JavaScript"><!--
/* You may give each page an identifying name, server, and channel on
the next lines. */
var s_pageName="We Know"
var s_server=""
var s_channel="We Know"
var s_pageType=""
var s_prop1=""
var s_prop2=""
var s_prop3=""
var s_prop4=""
var s_prop5=""
/***** INSERT THE DOMAIN AND PATH TO YOUR CODE BELOW *****/
/***** DO NOT ALTER ANYTHING ELSE BELOW THIS LINE! *****/
var s_code=' '//--></script>
<script language="JavaScript"
src="http://www.example.com/Includes/s_code.js"></script>
```

```
<script language="JavaScript"><!--
var s_wd=window,s_tm=new Date;if(s_code!=' '){s_code=s_dc(
'examplecom');if(s_code)document.write(s_code)}else
document.write('<im'+ 'g
src="http://examplecom.112.207.net/b/ss/examplecom/1/G.1--
FB/s'+s_tm.getTime()+'?[AQB]'
+'&pageName='+escape(s_wd.s_pageName?s_wd.s_pageName:(s_wd.pageName?s_
wd.pageName:'))
+'&server='+escape(s_wd.s_server?s_wd.s_server:(s_wd.server?s_wd.serve
r:'))
+'&ch='+escape(s_wd.s_channel?s_wd.s_channel:(s_wd.channel?s_wd.channe
l:'))
+'&[AQE]" height="1" width="1" border="0" /><br />')
//--></script><script language="JavaScript"><!--
if(navigator.appVersion.indexOf('MSIE')>=0)document.write(unescape('%3
C')+ '!'-'+'-')
//--></script><noscript><br /></noscript><!--/DO NOT
REMOVE/-->
<!-- End SiteCatalyst code version: G.1. -->
```

StatCounter™ block of code for creating Web analytics:

```
<!-- Start of StatCounter Code -->
<script type="text/javascript" language="javascript">
var sc_project=330669;
var sc_partition=1;
</script>

<script type="text/javascript" language="javascript"
src="http://www.statcounter.com/counter/counter.js"></script><noscript>
<a href="http://www.statcounter.com/free_web_stats.html"
target="_blank"></a></noscript>
<!-- End of StatCounter Code --></p>
```

D. “Bug” Tracking

Depending on the circumstances, the use of a third-party service for statistical and informational tracking may be impractical or impossible. For example, inadequate budget, the desire to maintain a small footprint (minimal addition to source), stealth, or the desire for control by maintaining the service in-house, may lead one to embrace a different, not off-the-rack approach. There are simple alternatives that can be implemented without a third-party service. The alternatives also provide extensive information regarding site visitors, their patterns, general geographic location, and ISP.

One of the simplest, yet most effective tools, is referred to as a “bug.” Bug tracking is achieved by inserting “an include” on the target site’s page(s), which call a predetermined file (*e.g.*, one pixel image) from the destination server that would be maintained and controlled by the site tracker.

If you have continuous access and authority over the target site, there is no need to implement the bug, you merely mine the log files directly. Nonetheless, once the bug is on the desired page(s), the page(s) can be tracked without the need for constant access to the site’s content, hardware, or software. However, if the target page is updated, the bug may have to be re-included, requiring access to the content.

The following contains a description of a bug scenario and an example of a bug source. If example.com/index.html, has an include for <http://report.tracking.com/pixel.gif>, when the visitor goes to the target page (*i.e.*, example.com/index.html), the visitor’s browser retrieves [pixel.gif](http://report.tracking.com/pixel.gif) from ‘report.tracking.com’. This file is invisible to a human visitor. Further, if [pixel.gif](http://report.tracking.com/pixel.gif) fails to load, there is no inhibition to the browser’s ability to render the page, thus no noticeable affect by the visitor.

When the call to ‘report.tracking.com’ is made, that webserver gains information concerning the visitor from example.com. The information about the visitor is written to the access log, which contains the visitor’s IP address, pages requested, referring page, and the time of each request, all of which can be used to determine general geographic location and the ISP of each visitor.

If monitoring of the webserver(s)’ access log is possible, a script can take each IP and run a reverse DNS lookup (*e.g.*, arnit.net) to determine the ISP, and also a “traceroute” (tracert on Windows machines) to determine more specific information regarding the visitor’s access

point on the Internet. The traceroute begins looking for the target IP from the searcher's computer by tracing the hops through the various routers around the world until it finds the visitor's IP or is blocked by the target's ISP.

A reverse DNS lookup (arin.net) response looks like this:

Search results for: 66.91.65.167

OrgName: Road Runner
OrgID: [RRWE](#)
Address: 13241 Woodland Park Road
City: Herndon
StateProv: VA
PostalCode: 20171
Country: US

ReferralServer: rwhois://ipmt.rr.com:4321

NetRange: [66.91.0.0](#) - [66.91.255.255](#)
CIDR: 66.91.0.0/16
NetName: [ROADRUNNER-HAWAII2](#)
NetHandle: [NET-66-91-0-0-1](#)
Parent: [NET-66-0-0-0-0](#)
NetType: Direct Allocation
NameServer: DNS1.RR.COM
NameServer: DNS2.RR.COM
NameServer: DNS3.RR.COM
NameServer: DNS4.RR.COM
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 2001-03-29
Updated: 2003-02-11

TechHandle: [ZS30-ARIN](#)
TechName: ServiceCo LLC
TechPhone: +1-703-345-3416
TechEmail: abuse@rr.com

OrgAbuseHandle: [ABUSE10-ARIN](#)
OrgAbuseName: Abuse
OrgAbusePhone: +1-703-345-3416
OrgAbuseEmail: abuse@rr.com

OrgTechHandle: [IPTEC-ARIN](#)
OrgTechName: IP Tech
OrgTechPhone: +1-703-345-3416
OrgTechEmail: abuse@rr.com

The traceroute output for the same target IP address is pasted below. In the example, the traceroute made hops to routers in Hawaii before, presumably, being blocked by the routers. Some ISPs block traceroutes to IP addresses under their authority. However, once the traceroute was blocked, if the last top level domain of the router is taken and a “whois” is run, one learns the domain is owned by “rr.com,” RoadRunner™, whose administrative contact is located in Herdon, Va. However, this does not indicate the visitor’s location was Virginia. The whois output is located below the following traceroute output:

```

traceroute to 66.91.65.167 (66.91.65.167), 30 hops max, 38 byte packets
 1 msfc-rtr-intprod (10.189.224.3) 0.270 ms 0.202 ms 0.190 ms
 2 10.189.252.22 (10.189.252.22) 0.298 ms 10.189.252.26 (10.189.252.26) 0.322 ms
10.189.252.22 (10.189.252.22) 0.227 ms
 3 rt-xxx-b-g2-16 (10.188.191.78) 0.308 ms rt-xxx-b-g1-15 (10.188.191.74) 0.325 ms rt-
xxx-b-g2-16 (10.188.191.78) 0.325 ms
 4 lst-int-rtr (10.188.122.139) 0.625 ms 0.532 ms 0.601 ms
 5 h-64-236-241-254.aoltw.com (64.236.241.254) 1.018 ms 1.449 ms 1.005 ms
 6 pop2-atl-P1-0.atdn.net (66.185.145.117) 1.402 ms 1.110 ms 0.967 ms
 7 bb1-atm-P5-0.atdn.net (66.185.136.18) 1.601 ms 1.113 ms 1.033 ms
 8 bb1-hou-P7-0.atdn.net (66.185.152.185) 22.378 ms 21.668 ms 21.614 ms
 9 bb2-hou-P1-0.atdn.net (66.185.152.153) 22.735 ms 23.049 ms 23.276 ms
10 bb2-pho-P7-0.atdn.net (66.185.152.107) 53.133 ms 54.194 ms 53.112 ms
11 bb1-pho-P1-0.atdn.net (66.185.152.36) 58.726 ms 185.499 ms 201.880 ms
12 bb1-las-P7-0.atdn.net (66.185.152.26) 172.143 ms 208.761 ms 216.938 ms
13 bb2-las-P2-0.atdn.net (66.185.152.25) 62.330 ms 63.223 ms 62.273 ms
14 bb2-hon-P2-1.atdn.net (66.185.152.8) 111.842 ms 112.649 ms 111.851 ms
15 pop1-hon-P0-1.atdn.net (66.185.137.51) 112.221 ms 112.477 ms 112.059 ms
16 RR-Mililani.atdn.net (66.185.137.62) 112.410 ms 112.374 ms 112.357 ms
17 srp5-0-oahuhikane-gsr1.hawaii.rr.com (24.25.224.68) 113.334 ms 113.383 ms
113.398 ms
18 pos1-0-oahuhikane-ubr2.hawaii.rr.com (24.25.225.214) 113.703 ms 114.141 ms
113.514 ms
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

```

The output from the whois command returns a few key points of information, such as who registered the domain, how to contact the registered owner of the domain, and the authoritative Name Servers for the given domain. The following is a sample of the whois output from a generic Linux box.

```
Domain Name: RR.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: DNS1.RR.COM
Name Server: DNS2.RR.COM
Name Server: DNS3.RR.COM
Name Server: DNS4.RR.COM
Status: REGISTRAR-LOCK
Updated Date: 22-oct-2004
Creation Date: 01-oct-1996
Expiration Date: 30-sep-2010
```

```
>>> Last update of whois database: Sat, 23 Oct 2004 07:04:51 EDT <<<
```

```
Registrant:
Road Runner HoldCo, LLC (RR6-DOM)
13241 Woodland Park Rd
Herndon, VA 20171
US
```

```
Domain Name: RR.COM
```

```
Administrative Contact, Technical Contact:
Road Runner HoldCo LLC (XGUKSSRMIO)      abuse@RR.COM
13241 Woodland Park Rd
Herndon, VA 20171
US
703-345-3416 fax: 703-345-3607
```

```
Record expires on 30-Sep-2010.
Record created on 01-Oct-1996.
Database last updated on 23-Oct-2004 15:23:48 EDT.
```

E. Hijacking

In this context, the term “hijacking” refers to switching the Web hosting service from an owner’s hosting service to machines controlled by the hijacker. If a person has the authority or ability to manipulate the DNS for the target site’s domain, the domain’s IP

address may be changed, thus pointing the domain to an IP address served by web servers under the hijacker's control.

To reduce the risk of being discovered, the hijacker needs to maintain a complete and accurate copy of the content of the target site on the hijacker's web servers. If this route is desired, the content should be updated regularly. Without regular updates, the risk of detection is increased, as another party may realize the content is not accurate and the investigation may discover the hijack (*i.e.*, their Web hosting provider no longer serves the site). If discovered, intentional misleading might be initiated.

A less complicated avenue is to move the DNS to the hijacker's servers and serve a page resembling a 404 page (*i.e.*, "Page Not Found"), service down page, or other generic error message. Regardless of the page served, all visits are logged.

Another option for hijacking is to implement caching servers controlled by the hijacker to front the target site. In general, if the content is static or if dynamic aspects can be identified, the hijacker could use caching servers to front the target site so that all page requests to the target site are actually served by the caching servers, which obtain the content directly from the target site. As a result of the caching servers serving content to the public, the cache servers' logs contain information about those visiting the site, as discussed previously. This method reduces the risk of missing content updates and being discovered because the cache servers make requests to the target site. Squid and Apache are open source methods frequently implemented, though other methods are available. There is a risk in that if the target site employs Web analytics, the target owner may discover a drop in traffic and may notice all requests come from a few IP addresses. This is because only the cache servers are making requests to the target site and thus are the only ones making hits on the site. The

caching hijacker may be able to mitigate this risk by varying the IP addresses used and location of the caching servers. This method, like the others under the hijacking theme, requires the ability to manipulate the DNS records to move the sites' domains to the caching servers.

F. Location Filtering

Webservers and their plugins provide the ability to treat users differently based on certain characteristics. For example, it is possible for "[example.com](#)" to block users from the U.S., or only allow users from the U.S., and block the rest of the world. Another option is to present different content depending on the geographic location of the visitor. For example, if the user comes from Pakistan, then Pakistani related content is displayed; otherwise the website displays the default content. Aside from geographic location, the same techniques can be used based on IP class, subnet, and specific IP address.

There are several ways to implement location or IP filtering. As with statistical tracking (web analytics), there are fairly sophisticated third-party services available as well as less costly alternatives. Digital Envoy™ is an example of a third-party solution that can, for the most part, determine a visitor's geographic origin. These geographic ("geo") identifying services base their determination on the visitor's reported IP address, and/or the router serving that IP address.

Each request to a webserver contains the visitor's IP address. As mentioned above, less sophisticated filtering can be implemented based on the IP class, subnet of IP address, or specific IP address(es).

Thus, based on IP or geographic location, a webserver can be configured to create multiple virtual sites. One site may provide confidential information to specified visitors, or,

in the alternative, send a segment of the Internet (IP based) or geographic location as decoy content.

G. *Log File Information*

Webservers are almost always configured to write “access” and “errors” logs. The access logs contain information regarding who visited by IP address, what was requested, what referred the visitor to the requested page, and how long they stayed. The following is a very brief sample of a webserver’s access log:

```
24.184.176.67 Gcf1947fb-23287-1052175586-2 - [20/Oct/2004:10:08:47 -0400]
"GET /games/worldtour/menu.swf HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705; MSN 6.1; MSNbDELL; MSNmen-
us; MSNc0z; v5m)" www.example.com
```

- Log breakdown:
 - Visitor IP 24.184.176.67
 - Cookie header Gcf1947fb-23287-1052175586-2 –
 - Request Date [20/Oct/2004:10:08:47 -0400]
 - Item Requested "GET /games/worldtour/menu.swf
 - Html standard HTTP/1.1
 - Response Code 304
 - Referrer "-"
 - Browser MicroSoft’s (MS) Internet Explorer (IE) Version 6.0
 - OS Windows NT Version 5.1
 - Misc. info NET CLR 1.0.3705; MSN 6.1; MSNbDELL; MSNmen-us; MSNc0z; v5m
 - Domain www.example.com

```
68.186.187.235 Gcf1947fb-970341-1061044710193-1 - [20/Oct/2004:10:08:47 -0400]
"GET /tools/img/ad_cell_lft.gif HTTP/1.1" 304 -
"http://www.example.com/tv_shows/index.html" "Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1)" www.example.com
```

- Log breakdown:
 - Visitor IP 68.186.187.235
 - Cookie header Gcf1947fb-970341-1061044710193-1
 - Request Date 20/Oct/2004 @ 10:08:47
 - Item Request /tools/img/ad_cell_lft.gif
 - Html standard HTTP/1.1
 - Response Code 304
 - Referrer: http://www.example.com/tv_shows/index.html
 - Browser MS’s Internet Explorer Version 6.0.
 - OS Windows NT 5.1

- Misc. Info. SV1
- Domain www.example.com
- Not Found – 404 Example
- net.comcast.nj.clmntn01.pcp09681194pcs.68.39.112.56 Gaa5116-1333068321-1061848650281-1 - [20/Oct/2004:10:08:47 -0400] "GET /section/site_exclude.html HTTP/1.1" 404 6777 "-" "Mozilla/4.0 (compatible; MSIE 5.22; Mac_PowerPC)" "www.example.com"
- Google Referred Example
- 66.50.249.183 - - [20/Oct/2004:10:08:48 -0400] "GET /tools/js/mnfinder.js HTTP/1.1" 200 3609 "http://www.google.com.pr/search?q=cache:hWkH1MbQ3A0J:www.example.com/+&hl=en" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" www.example.com

IV. SITE SPOOFING

Among the first types of Internet law cases focused on the practice known as cyber-squatting. The practice worked as follows: A person would buy domain names that would be associated with well known companies or entities, such as PETA.com, Panavision.com, EddieBauer.com, hoping the company would pay a premium for the domain name matching its corporate name. An alternative method was to purchase domain names that were similar to the company or entity, such as a common misspelling, typical typing errors (substituting an ‘F’ with a ‘G’ because of their location on the keyboard). Site-spoofers would create alternative domain names for a variety of reasons, such as to get traffic to their site, or express opinions regarding the company. For example, if expressing an opinion, a person might buy Pepsi-sucks.com and then create a site expressing that opinion.

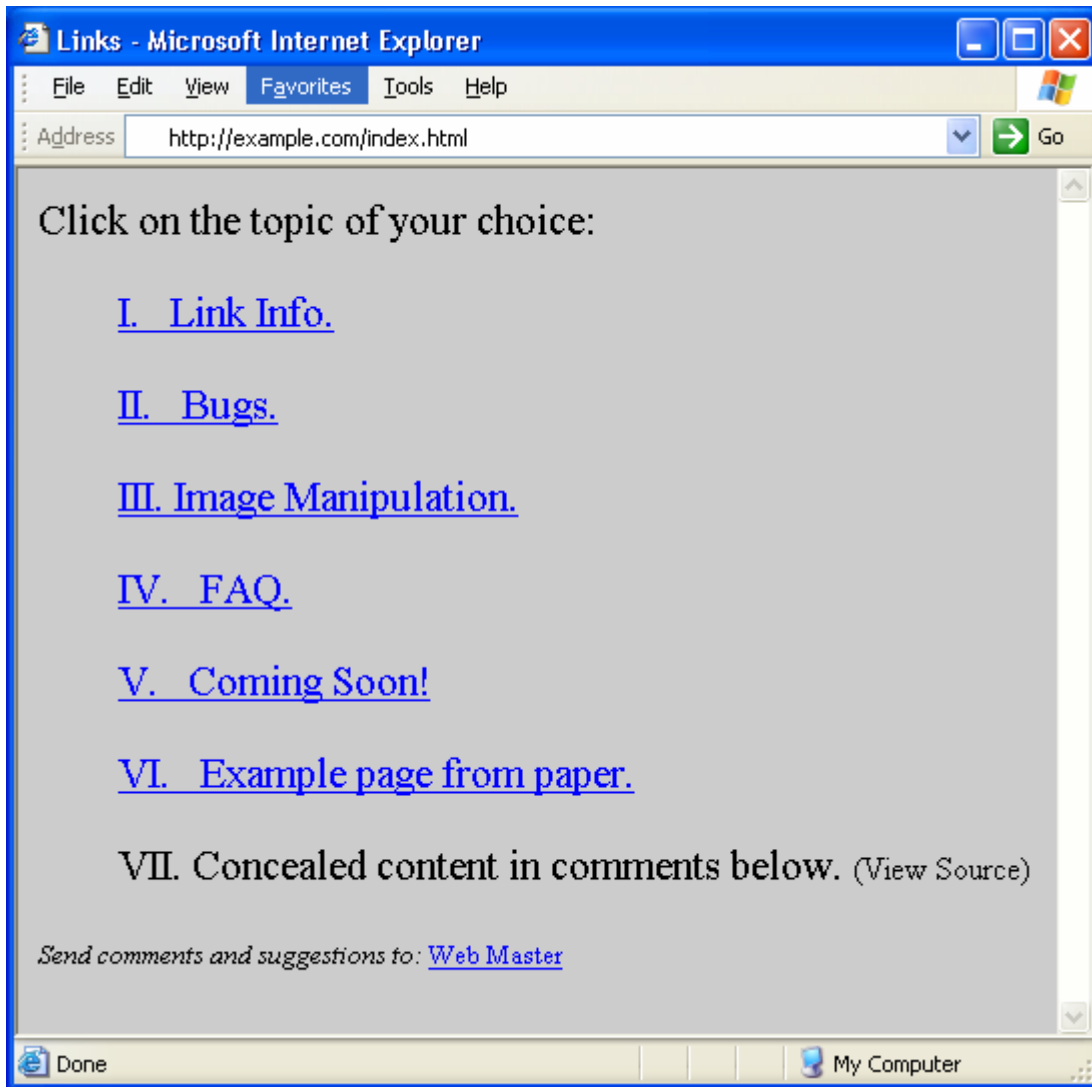
If one desires information about who visits or attempts to visit a certain site, a domain could be purchased that is nearly identical to the target domain name (*e.g.*, leave off an “s,” add an extra “o,” *etc.*). Further, the .org and/or .net version of the domain could be purchased. Although crude, this method captures the traffic generated when a potential visitor mistypes

the desired domain while allowing the spoofing site to analyze the resulting statistical information.

V. EXAMPLE WEBSITE

This example site implements several previously discussed techniques, including concealed links, comments, embedded hints, and meta refreshes. Also included are alternative techniques, for example alternative ports and non-traditional page extensions (*i.e.*, .jack).

Each section (*i.e.*, Link, Bugs, FAQ, Coming Soon), including the home page, has at least one concealed message, instruction, or image. The home page for the example site (example.com) is [index.html](#) on the document-root directory of the webserver. This page also contains comments in the source giving direction to a concealed page, not intended for the general population. This page also has a meta refresh that takes the visitor to another site.



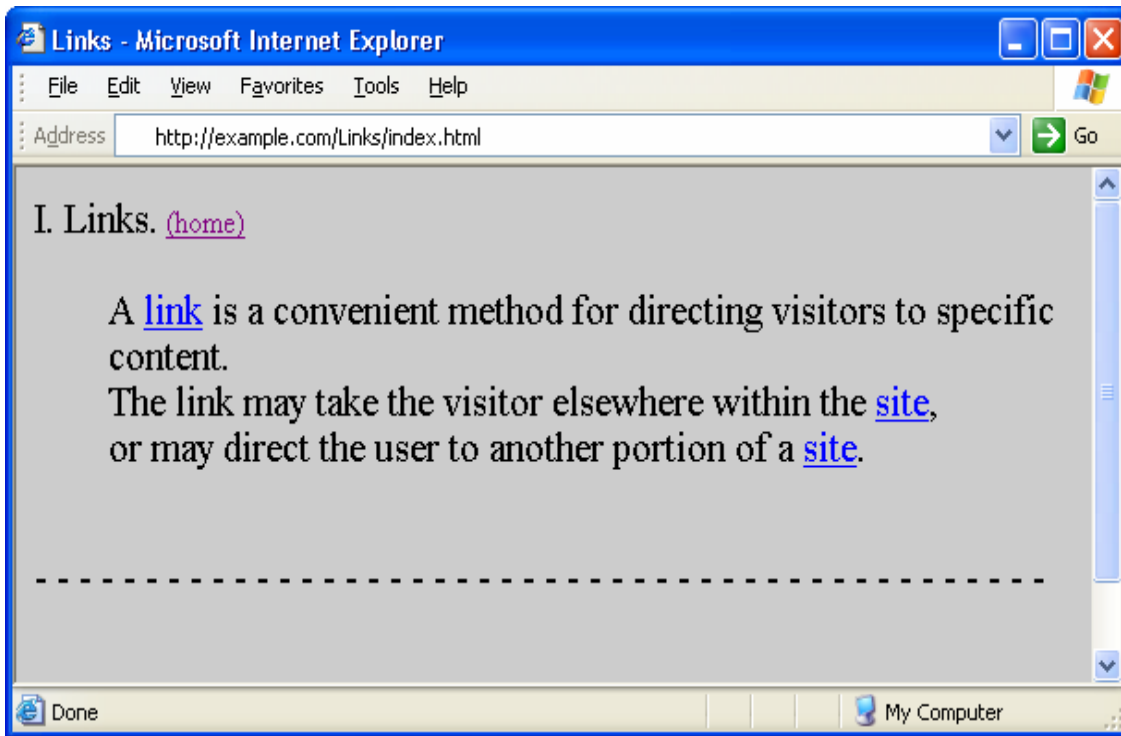
Source:

```
<HTML>
<HEAD>
  <TITLE>Links</TITLE>
  <meta http-equiv="refresh" content="1200;url=http://law.gsu.edu" />
  <META NAME="description" CONTENT="Search engines key on this entry.">
</HEAD>
<BODY style="font-size:16pt" bgcolor=#CCCCCC>
Click on the topic of your choice:<br><br>
  <ul>
    <a href="./Links/index.html" title="Links.">I.   &nbsp; Link Info.</a>
    <br><br>
    <a href="./Bug/index.html" title="Bugs.">II.   &nbsp; Bugs.</a> <br><br>
    <a href="./Image/index.html" title="Image Manipulation">III.   Image
Manipulation.</a>       <br><br>
    <a href="./Faq/index.html" title="Frequently Asked Questions">IV.
&nbsp; FAQ.</a> <br><br>
    <a href="./Soon/index.html" title="Coming Soon">V.   &nbsp; Coming
Soon!</a> <br><br>
```

```
<a href="./Ex/example.html" title="Example.html">VI.  &nbsp; Example  
page from paper.</a> <br><br>  
VII.    Concealed content in comments below. <font size=3>(View  
Source) </font>  
</ul>  
<!-- Beginning of comments that are not rendered by the browser.  
(1) For confidential information go to -- ./message.html  
(2) The meta refresh above takes the visitor to another page after 20  
minutes (1200 seconds).  
Thus, if the visitor does nothing for 20 min, the page will  
automatically take the visitor elsewhere.  
-->  
<font size=2><i>Send comments and suggestions to:</i>  
<a href="mailto:jwilliams@gsu.edu" style="text-decoration:underline;"  
class="onwhite">Web Master</a></font>  
</BODY>  
</HTML>
```

A. *Scenario One*

This scenario for finding concealed pages is accomplished by two techniques on two different pages. The first page involved is entitled “Links.” Links purports to provide basic information about Web links. However, below the dotted line there is a blended link that loads a new page with the hidden file name in the address bar. The address bar reads <http://example.com/<p1>/mission.html>. This says one directory (p1) is missing but once that directory is determined the file “[mission.html](#)” should be placed in the URL to access the concealed page. Second, the comments instruct one to open “[../Msg/errno2.html](#)”, which is discussed below.



Source:

```
<HTML>
<HEAD> <TITLE>Links</TITLE> </HEAD>
<BODY style="font-size:16pt" bgcolor=#CCCCCC>
I. Links.<font size=3pt>
  <a href=" ../index.html" title="Home.">(home)</a></font> <br><br>
  <ul>
    A <a href="http://www.webopaedia.com/TERM/L/link.html">link</a>
    is a convenient method for directing visitors to specific content.<br>
    The link may take the visitor elsewhere within the
    <a href=" ../Bug/index.html">site</a>,<br>
    or may direct the user to another portion of a
    <a href="http://www.whitehouse.gov/president/" target=
    "_blank">site</a>.
  </ul>
  <br><!--
  (1) For P1 hint go to -- ../Msg/errno2.html
  (2) The blank link "P2" gives the file name of a orphaned page.
  (3) Within the line below (---) there is a link to a different site. -
  -->
  ---
  <a style="text-decoration: none" href="http://law.gsu.edu" target=
  "_blank"><font color=black>-- --</font></a>
  ---
  <br><a href=" ../p1/mission.html" target= "_blank"><font
  color=#CCCCCC>P2</font></a>
  <br><br>
</BODY>
</HTML>
```

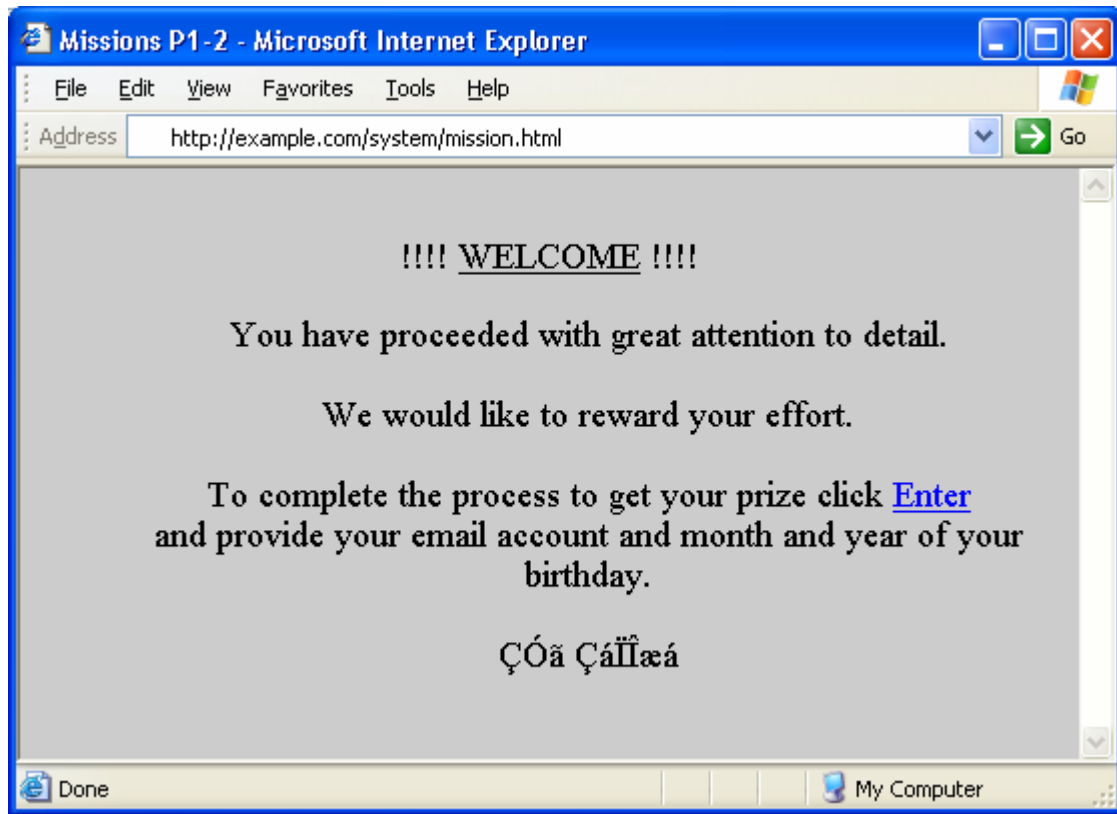
The file [errno2.html](#) provides a hint by the error reported. The error represents the orphaned directory, “system”, which represents the directory name for the first orphaned directory.



Source:

```
<HTML>
<HEAD> <title>ERROR-P1</title> </HEAD>
<BODY bgcolor=#CCCCCC>
  <b>ERROR ENCOUNTERED:</b><br><br>
  The application returned the following output:  handling protocol
  errno: system; Part1 <br><br>
</BODY>
</HTML>
```

With the above file name “[mission.html](#)” and the directory from [errno2.html](#), “system,” you have the location of a concealed page. The following URL is created, <http://example.com/system/mission.html>. This page is intentionally deceptive. In the event some curious and observant visitor finds the page, the owner does not want to draw attention to the page. The prize processing form could be a password validation prompt but disguised as email and birth date form. Those who have passwords will be allowed in, while those entering emails will be ignored or tracked.



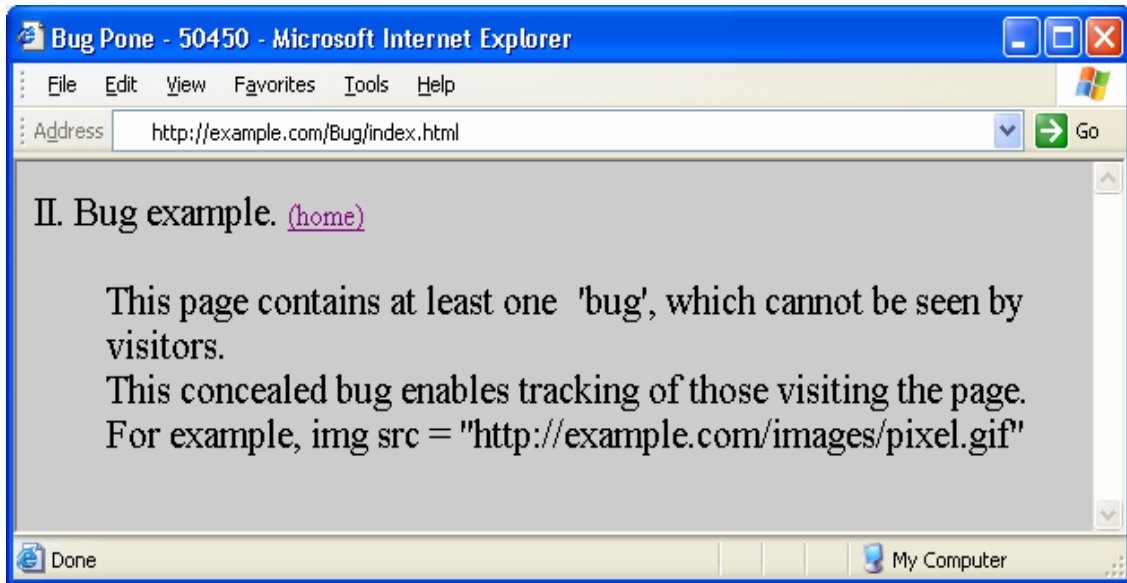
Source:

```
<HTML>
<HEAD> <title>Missions P1-2</title> </HEAD>
<BODY bgcolor=#CCCCCC>
  <br><center><font size=4pt>!!!! <u>WELCOME</u> !!!!<br>
  <ul>
    You have proceeded with great attention to detail. <br><br>
    We would like to reward your effort. <br><br>
    To complete the process to get your prize click
    <a href="./submission.html" title="Enter">Enter</a><br>
    and provide your email account and month and year of your
    birthday.<br>
    <br>ÇÓã Çáĭġæá<br>
  </font></ul>
</BODY>
</HTML>
```

B. Scenario Two

This scenario has two concealed hints to find another orphaned page on the example.com site. Both hints are on this single page. The first hint is in the window's title bar (blue bar across top of page) says "bug pone – 50450." Pone represents the orphaned

directory. The ptwo hint for file name, [message.html](#), is located in the comment in the middle of the page.

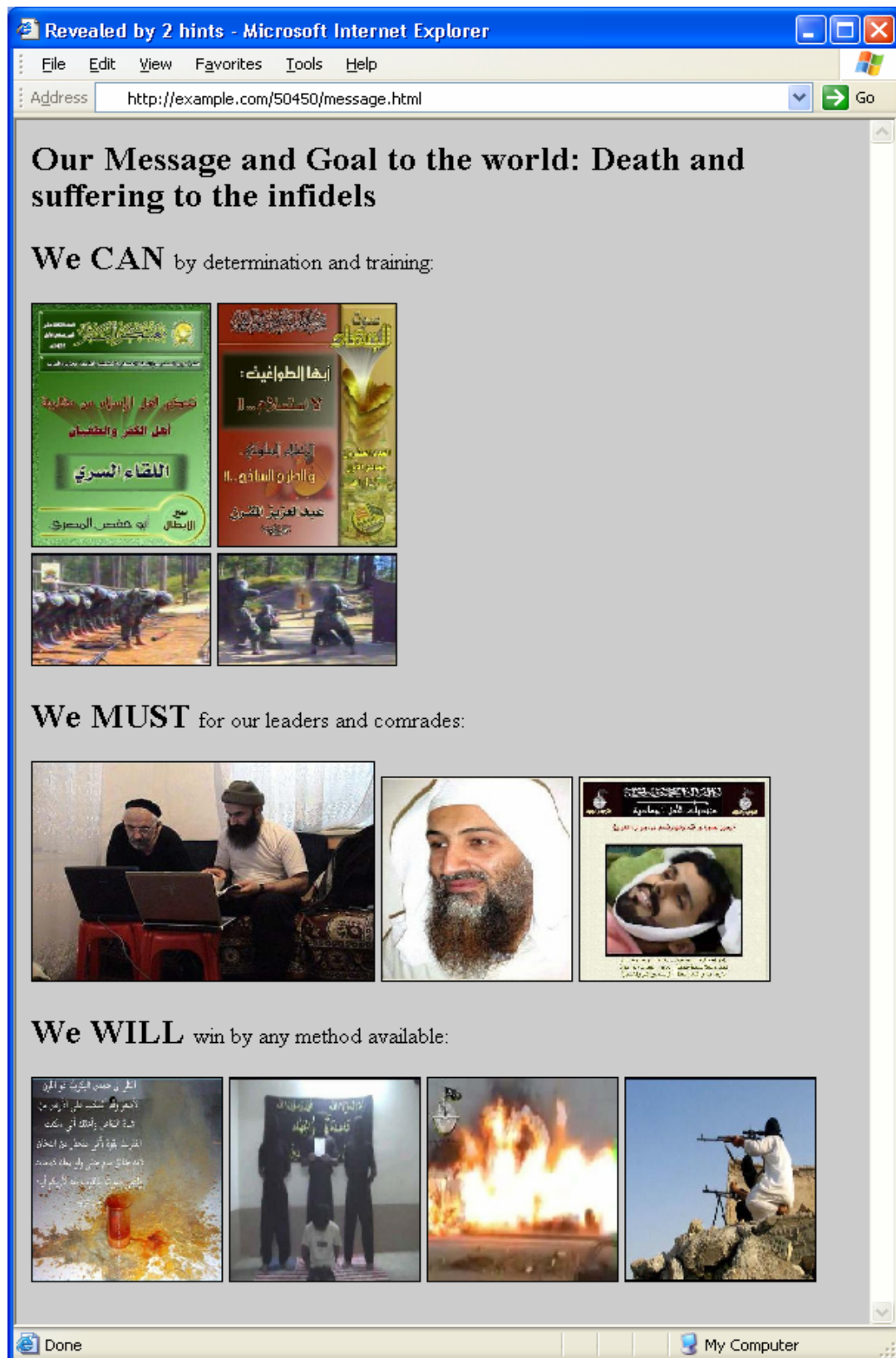


Source:

```
<HTML>
<HEAD> <TITLE>Bug Pone - 50450</TITLE> </HEAD>
<BODY style="font-size:16pt" bgcolor=#CCCCCC>

II. Bug example. <font size=3pt>
  <a href="../../index.html" title="Home.">(home)</a></font> <br><br>
  <ul>
    This page contains at least one  'bug',
    which cannot be seen by visitors.<br>
    This concealed bug enables tracking of those visiting the page.<br>
    <!-- notes for this page Ptwo ../<pone>/message. -->
    For example, img src = "http://example.com/images/pixel.gif" <br><br>
  </ul>
</BODY>
</HTML>
```

This page was the combination of two hints located on the same page. While these were fairly simple and located on the same page, there are many ways by which to implement these results, including the use of multiple pages.



Source:

```
<HTML>
<HEAD Aasir = Can/training; Mahir = Must/planning; Zadeer = Will/Operations
<title>Revealed by 2 hints</title> </HEAD>
<BODY bgcolor=#CCCCC>

    <b><font size=5pt> Our Message and Goal to the world:  Death and
suffering to the infidels</font></b><br><br>
    <b><font size=5pt> We CAN </font></b> by determination and
training:<br><br>
    
     <br>
    
     <br><br>
    <b><font size=5pt> We MUST </font></b> for our leaders and
comrades:<br><br>
    
     <br><br>
    <b><font size=5pt> We WILL </font></b> win by any method
available:<br><br>
    

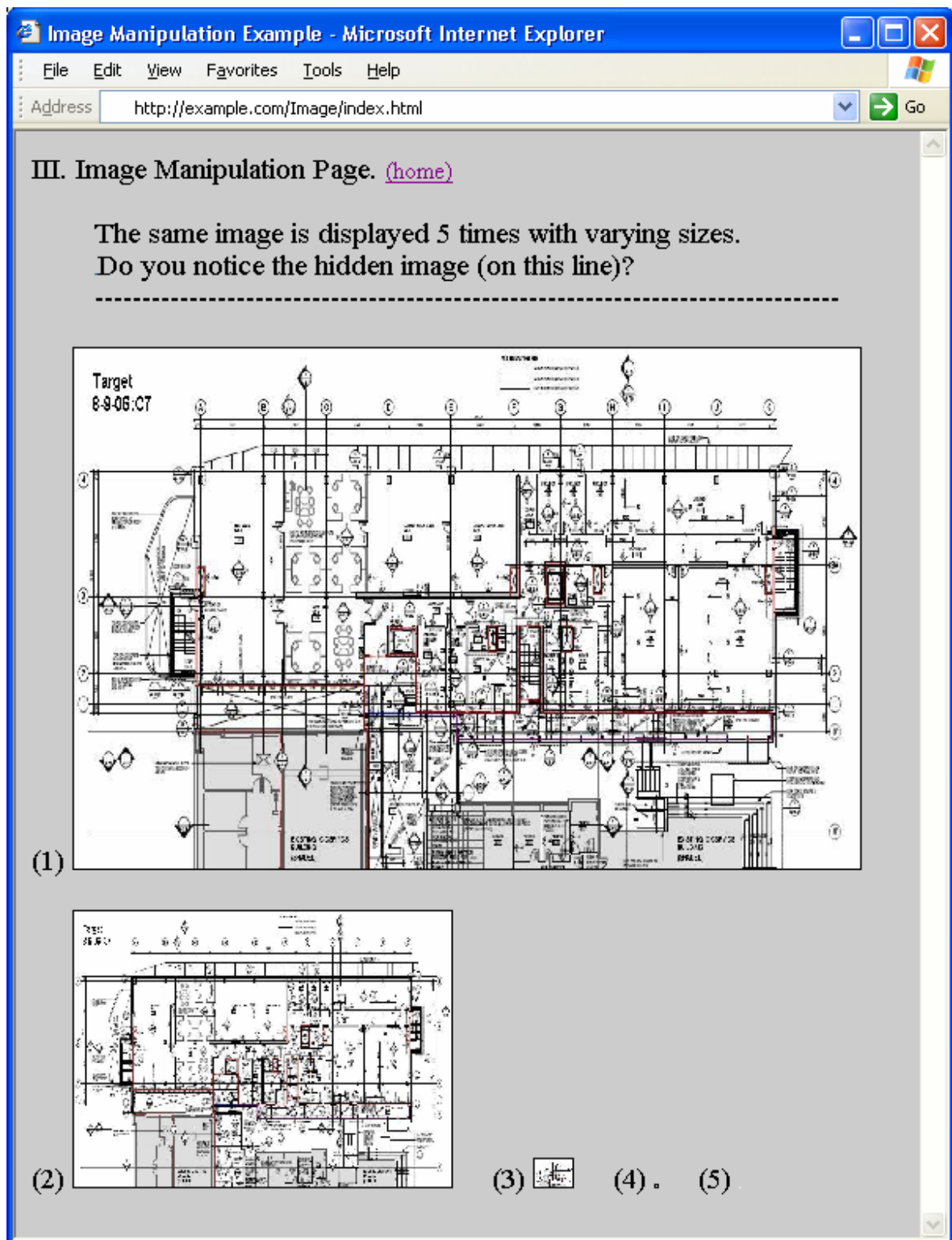
     <br>
      <!-- use your basic User ID to
access privilege areas of the site.
Reference training manual #1 for instructions -->

</BODY>
</HTML>
```

C. Scenario Three

This page openly demonstrates the size and presentation manipulation of an image. However, the comments contain phrases that are cryptic hints. This example contains two corporation names as illustrations (*e.g.*, Akamai and Tivoli). These two names, if read backwards, are phonetically pronounced “I am a.k.a.” (also known as) and “I love it.” In addition, to hiding hints within words themselves, there is an example of hiding content using a period. The period after “...size characteristic” is not a period, but is, in fact, a small image

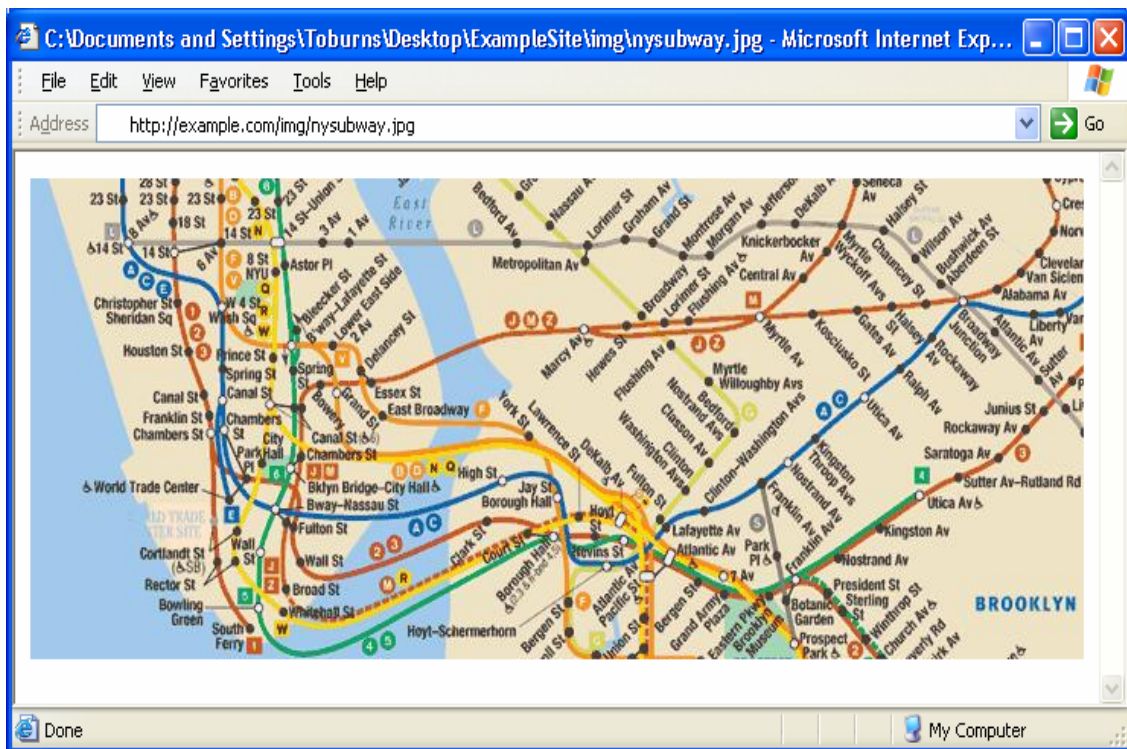
that could represent a map, schematics to a system, blueprints to a building, contact names, security plans, *etc.*



Source:

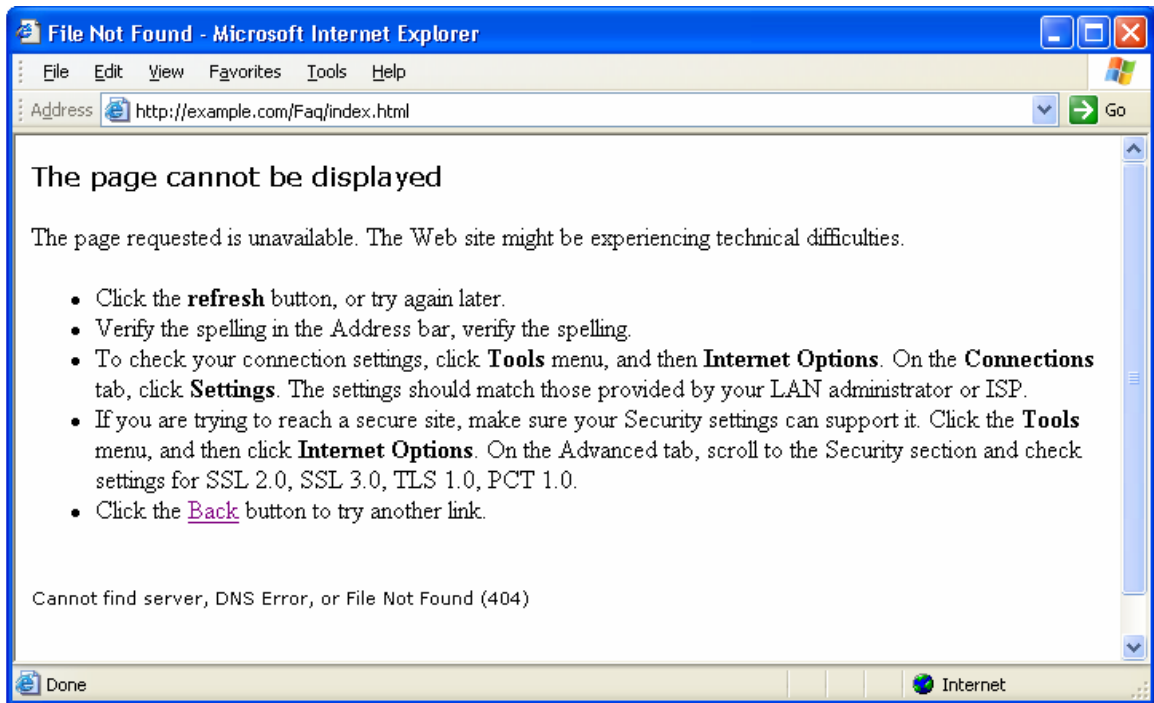
```
<HTML>
<HEAD> <TITLE>Image Manipulation Example</TITLE> </HEAD>
<BODY style="font-size:14pt" bgcolor=#CCCCCC>
III. Image Manipulation Page.
<font size=3pt><a href=" ../index.html" title="Home.">(home)</a></font> <br><br><ul>
The same image is displayed 5 times with varying sizes.<br>
Do you notice the hidden image (on
this line)?<br>-----<br><br></ul>
(1)  &nbsp; &nbsp; <br><br>
(2)  &nbsp; &nbsp; &nbsp;
(3)  &nbsp; &nbsp; &nbsp;
<!-- available spot for hidden information. Iamalsoknownas and Iloveit -->
(4)  &nbsp; &nbsp; &nbsp;
(5) 
</BODY>
</HTML>
```

While the image appear as a period, when they are right clicked and “Properties” is selected, the location of the image is presented as a URL. A copy of this image URL can be placed in a browser’s address bar. The hidden image from the page above is presented below at its normal size.



D. Scenario Four

This scenario uses three pages to gather enough information to find the next orphaned page. The first page is “FAQ,” and here there are two hints to the PI hint page. The first is the period after “...verify the spelling.” The period is a link that takes the visitor to another page ([../Msg/errno1.html](http://example.com/Msg/errno1.html)) that contains the next hint.



Source:

```
<HTML>
<HEAD> <title>File Not Found</title> </HEAD>
<BODY>

  <h1 style="COLOR: black; FONT: 13pt/15pt verdana">The page
  cannot be displayed</h1>

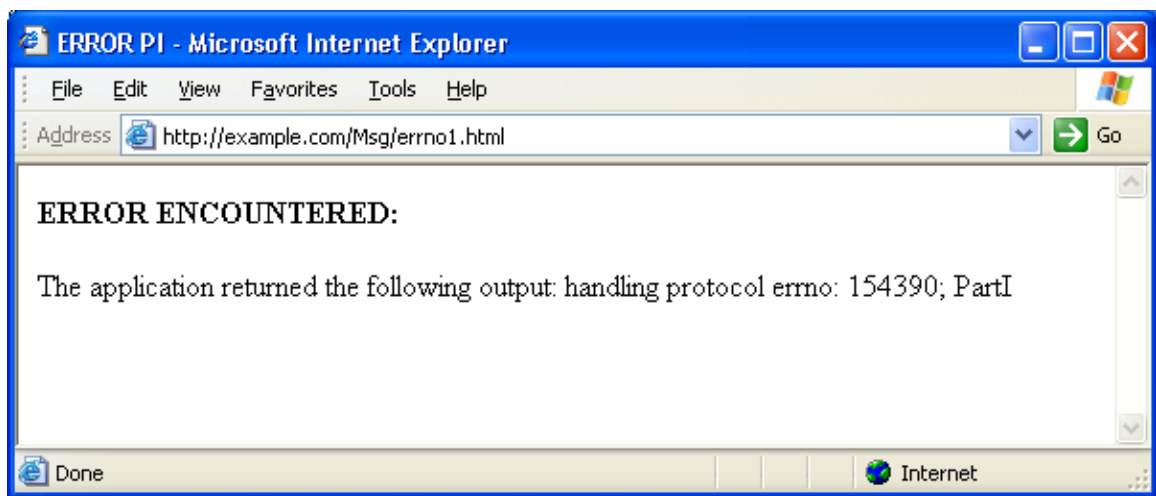
  The page requested is unavailable. The Web site might be
  experiencing technical difficulties. <br><br>

  <ul>
  <li> Click the <b>refresh</b> button, or try again
  later.</li><br>
  <li> Verify the spelling in the Address bar, verify the
  spelling<a style="text-decoration: none"
  href="http://example.com/Msg/errno1.html"><font color=black>.</font></a>
  </li> <br>
  <li> To check your connection settings, click <b>Tools</b> menu,
  and then <b>Internet Options</b>.
  On the <b>Connections</b> tab, click <b>Settings</b>.
  The settings should match those provided by your LAN
  administrator or ISP. </li><br>
  <li> If you are trying to reach a secure site, make sure your
  Security settings can support it.
```

```
Click the <b>Tools</b> menu, and then click <b>Internet
Options</b>.
On the Advanced tab, scroll to the Security section and check
settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0. </li> <br>
<li> Click the <a href="../index.html" title="Back">Back</a>
button to try another link.</li>
</ul><br>

<h2 style="font:8pt/11pt verdana; color:black">Cannot find
server, DNS Error, or File Not Found (404) <br><br>
<a href="../Msg/errno1.html"> <font
color=FFFFFF>test</font></a><br><br>
</h2>
</BODY>
</HTML>
```

This page, [errno1.html](#), contains an erroneous error code (154390; PartI), which is a key for the PI directory (154390). Therefore, once the file is determined, if necessary, the next orphaned page will be accessible via the URL. At the moment, <http://exampel.com/154390> is an orphaned directory.

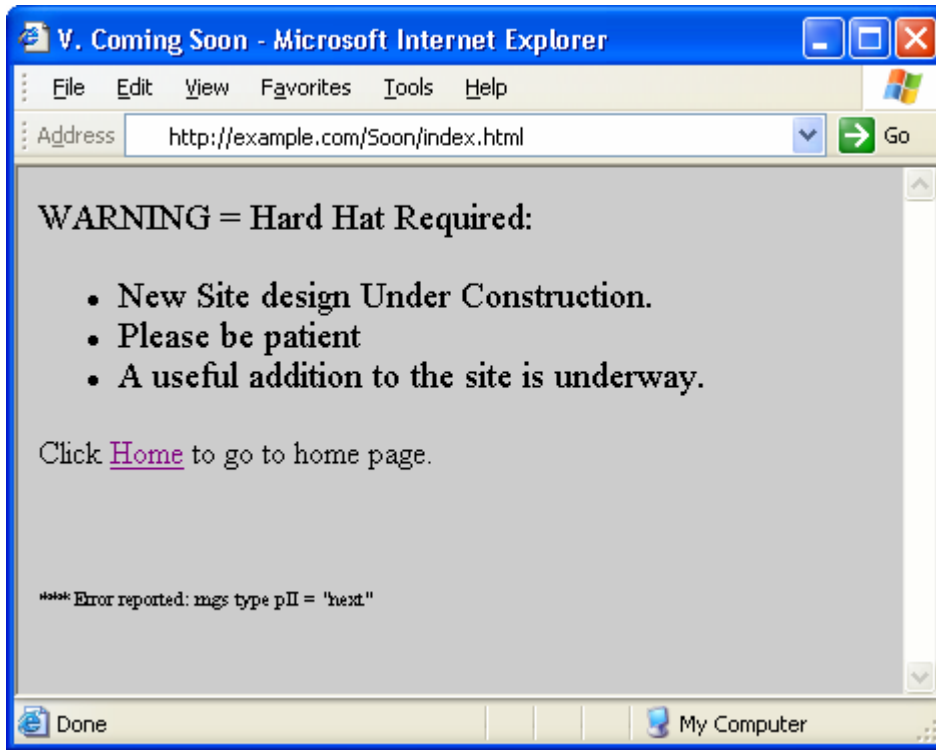


Source:

```
<HTML><HEAD> <title>ERROR PI</title> </HEAD>
<BODY>
<b>ERROR ENCOUNTERED:</b><br><br> The application returned the
following output:  handling protocol errno: 154390; PartI <br><br>
</BODY>
</HTML>
```

The next step in finding the orphaned page is by accessing the “Coming Soon” page. The page suggests that it is a placeholder for a new section on the site. However, at the end of

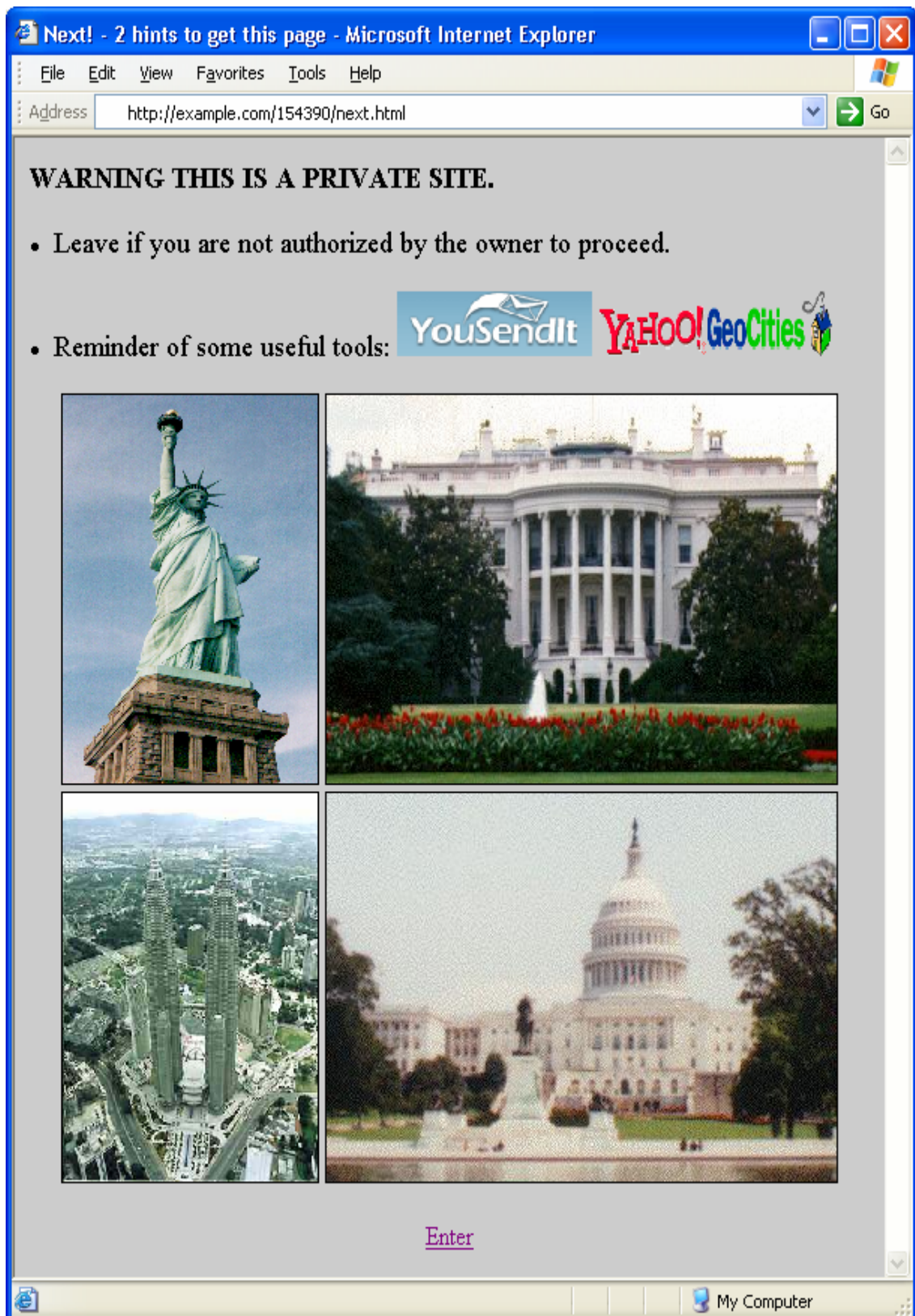
the page it provides the hint “msg type pII = next”. While it appears to be a system or application error the word “next” is the file corresponding to the directory above (154390).



Source:

```
<HTML>
<HEAD> <title>V. Coming Soon</title> </HEAD>
<BODY bgcolor=#CCCCCC>
<font size=4pt>WARNING = Hard Hat Required:<br>
<ul><li>New Site design Under Construction. <br>
<li>Please be patient <br>
<li>A useful addition to the site is underway.<br> </ul></font>
Click <a href="../index.html" title="Home page">Home</a>
to go to home page. <br><br><br><br>
<font size=1pt> *** Error reported: mgs type pII = "next" </font>
</BODY>
</HTML>
```

The following page is the result of placing “154390/next.html” in the URL for <http://example.com>. This difficult to find page may provide sensitive information in a public but obscure location.

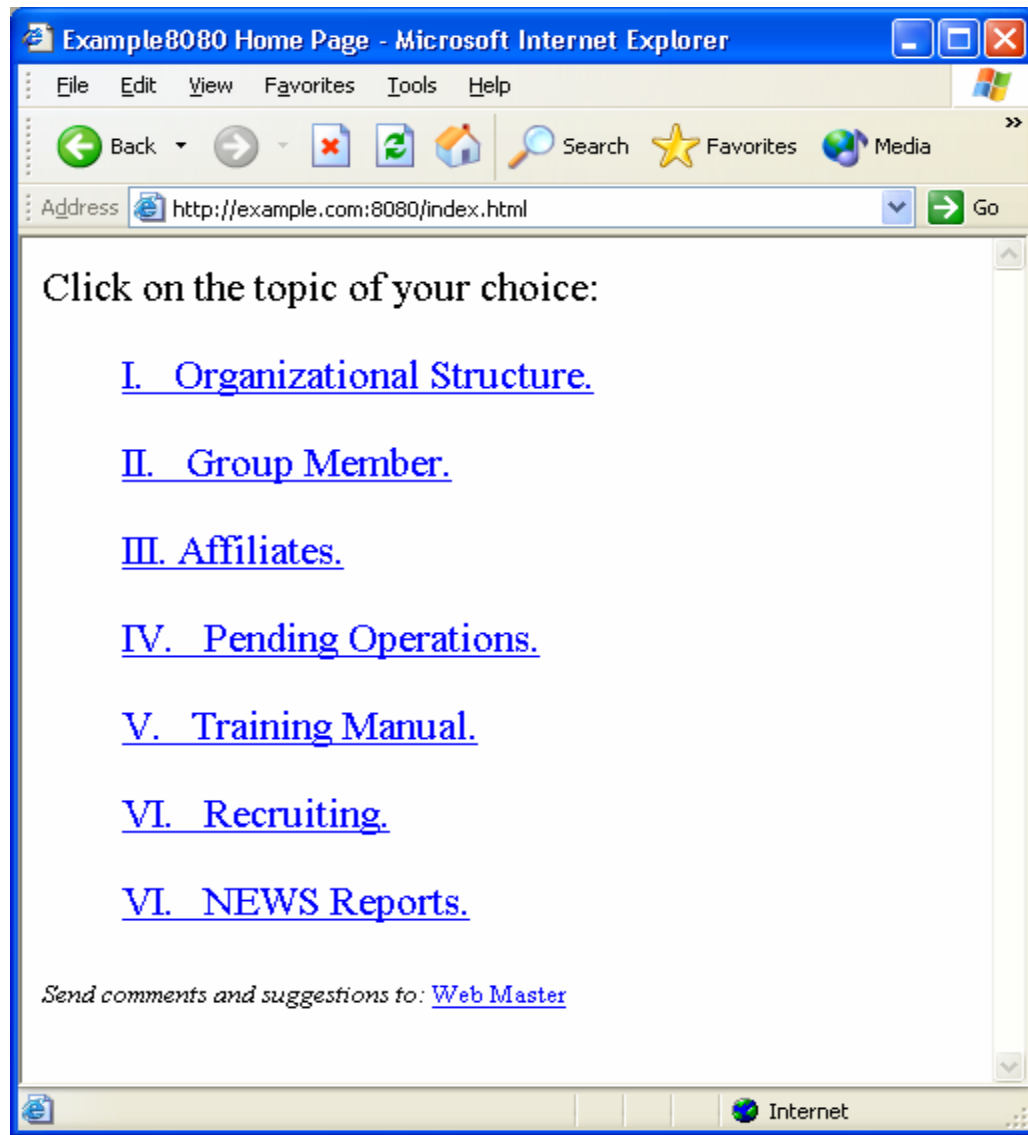


Source:

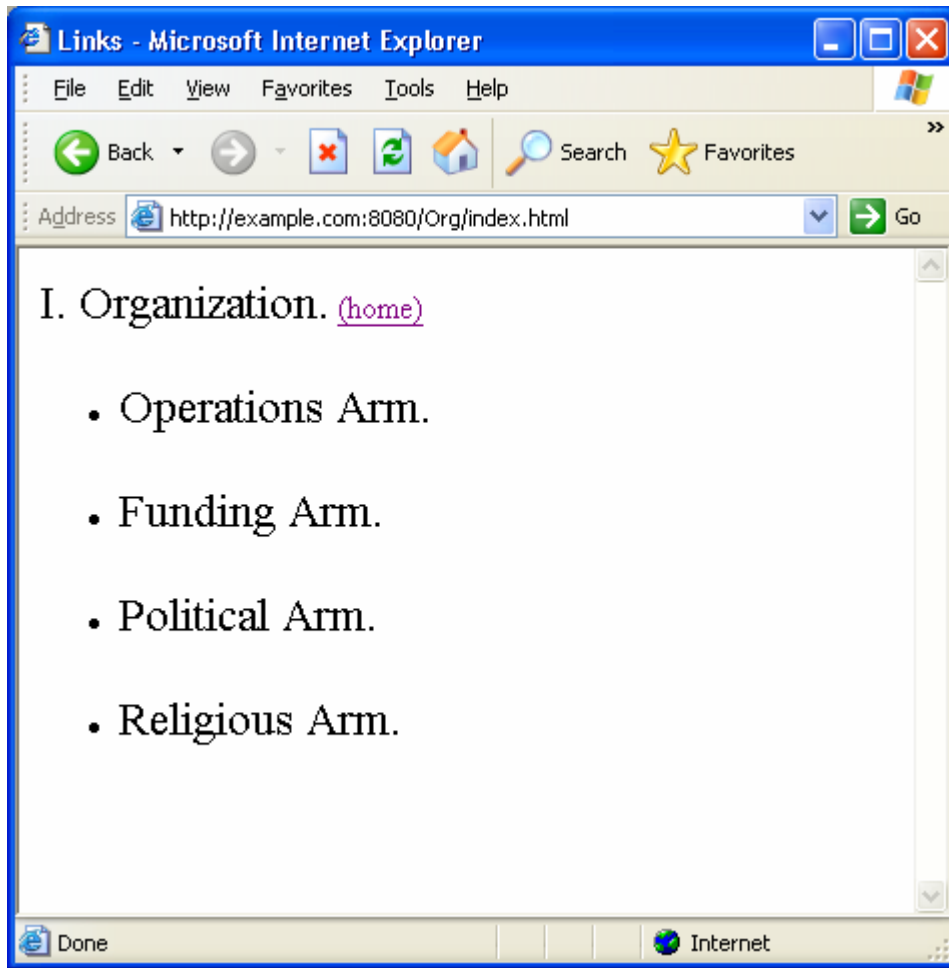
```
<HTML>
<HEAD> <title>Next! - 2 hints to get this page </title> </HEAD>
<BODY bgcolor=#CCCCC>
  <b><font size=4pt>WARNING THIS IS A PRIVATE SITE.</b><br><br>
  <li>Leave if you are not authorized by the owner to proceed. <br><br>
  <li>Reminder of some useful tools:
    <a href="http://www.yousendit.com"></a>
    <a href="http://geocities.yahoo.com"></a>
    <br>
  </font><br>
  <center>
    
    <br>
    
    <br><br>
    <a href="../index.html" title="Enter">Enter</a>
  </center>
</BODY>
</HTML>
```

E. Alternate Port

The next example is only accessible when the visitor manually enters :8080 after the domain name (*i.e.*, <http://example.com:8080>). The port 8080 is rather arbitrary and could be substituted for another port. This is only an example to help illustrate the idea. Besides being a non-standard port, there is nothing magical with this, although this technique could be very useful. Note the difference between the [index.html](#) here and the [index.html](#) in the example provided prior to Scenario One. These files are different but are served from the same domain and hosts. An additional note for this technique is that the visitor must include ‘http://’ in the address bar for the page to render. For example, ‘example.com:8080’ will not display the page, where ‘http://example.com:8080’ will return the page. This subtle difference is important, as most users do not manually add ‘http://’ to their page request because when using the standard port (*i.e.*, port 80), the browser does this automatically. A port scan against the site may determine the ports that are accessible from the Internet.



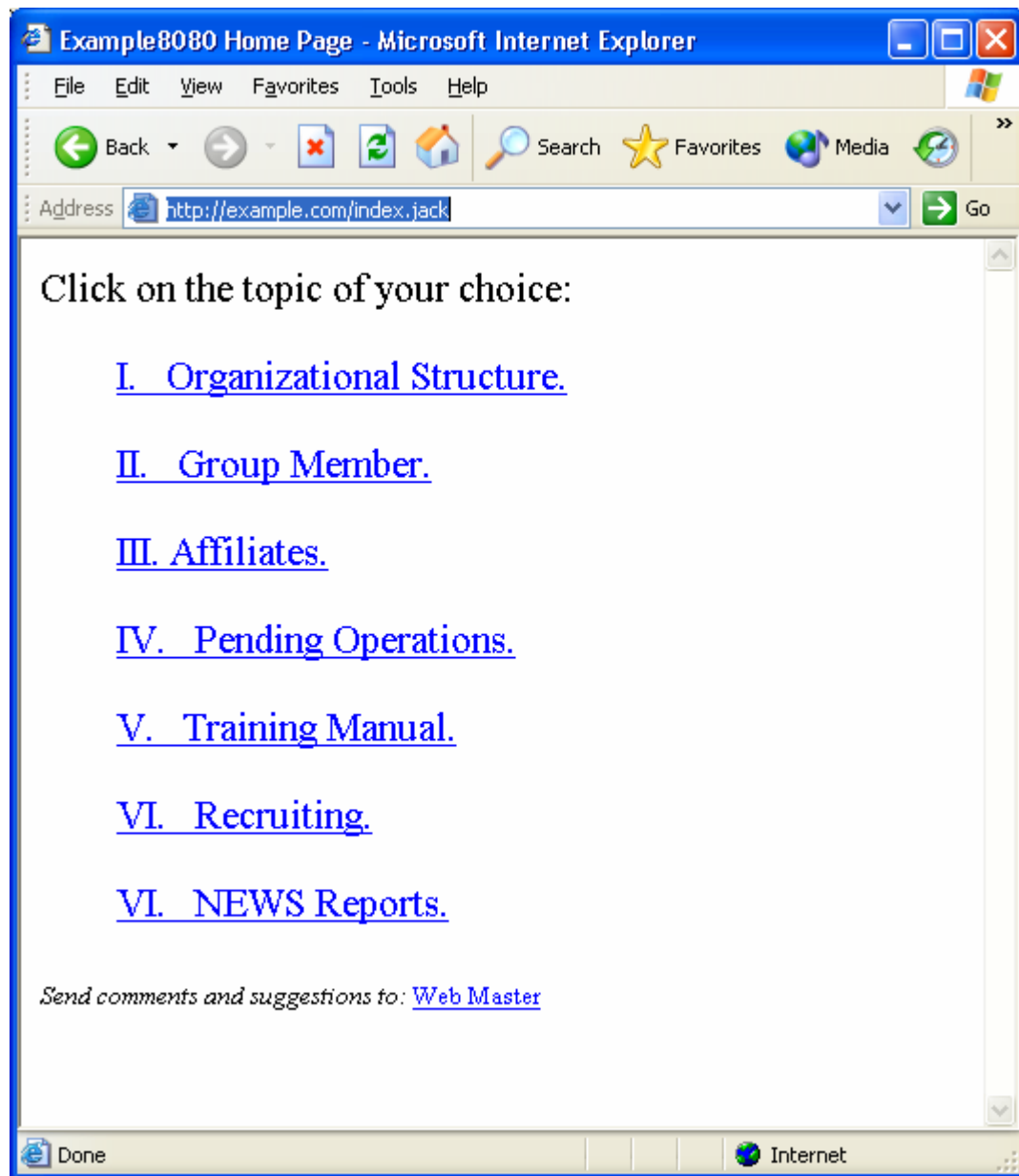
There is actually nothing of note in the source code; the concealing aspect is in the non-standard port. Next is a sample page utilizing an alternative port (*i.e.*, 8080).



F. Alternate Page Extension (i.e., .jack)

The next example is using a non-traditional file extension. Webservers are typically configured to recognize file extensions such as [.html](#), [.jsp](#), [.xml](#), *etc.* However, any extension may be used if there are instructions for the webserver on how to deliver the alternative extension. Therefore, once again, a visitor would have to be knowledgeable about the alternative extension to utilize it. Note that an alternative port is not required, and the [index.html](#) in the example prior to Scenario One does not display. This is yet another way to conceal content from the general public while distributing it around the world to those who

know what to look for on the site. As with the Alternative Port example, the source for the page is not interesting. The power comes from the non-standard page extension.



VI. LEGAL IMPLICATIONS

The GWOT has pitted law enforcement and military personnel against the Jihadist and his supporters and comrades. As Jihadist organizations increase their presence on websites

throughout the world, difficult issues of jurisdiction, free speech and association, privacy, and the like are becoming even more pressing. Initially, Jihadist activity on the web, particularly that activity mounted by al Qaida, its affiliates, and those free radicals that seek an alliance with al Qaida, pose the question of the proper metaphor by which to gauge this conflict. Al Qaida and its alliances have made clear that they are at war with the United States and the West. Although under International law, traditionally nation states declare war on nation states, the territorial influences of nation-state paradigms have been outdistanced by technology that has largely freed itself of the moorings of territory. There is no conceptual limit that should inherently constrain the United States from executing war against non-nation state actors. Of course, embracing a war paradigm does not mean laws do not apply. International and national laws and customs of war still provide a robust matrix by which actions should be judged in prosecuting the GWOT; however, application of standing laws to nonstate actors does press issues of enemy identification, rights to access to federal courts, detention length, and the like. This is far from an academic issue. For example, if we embrace a war metaphor for our conflict with Jihadist organizations, we speak in terms of proximate, and not specific, culpability; we gather intelligence and not evidence; military courts are the rule and not the exception; there is a legal distinction as to treatment among civilians, enemy combatants, prisoners of war, etc.; extradition laws are generally inapplicable; the full panoply of individual rights granted and guarded in our criminal justice process are generally inapplicable; and various rights of all individuals within the theater of operations may be curtailed or suspended.

The question of privacy on the internet is difficult largely because both advocates and critics of monitoring and surveillance tend to be one-eyed prophets that fail to see the other

side of the privacy issue. On one hand, this country strongly values privacy; it has created a constitutional right to it; and it has comparatively some of the most aggressive protectionary laws securing people from unreasonable searches and seizures. On the other hand, neither the legislature nor the courts have suggested that a privacy right is absolute. For example, the Federal Wiretap Act²⁰ which protects against interception and disclosure of wire, oral, or electronic communications, has an exception which states “It shall not be unlawful ... for any person ... to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.”²¹ The courts have also carved out exceptions to the right to privacy by holding in some instances that no reasonable expectation of privacy exists in private chat room communications²², instant messages²³, or in email messages²⁴. In fighting the GWOT, the federal government must engage in surveillance of potential threats. These threats could include terrorists, their financiers, nation-states that support them, and organizations that help them fund raise and recruit. The difficulty is that the government must balance the individual rights of unindicted people under suspicion against a fundamental duty to protect its citizens from terrorist attack. To protect effectively, the government must have broad but not limitless authority to engage in surveillance for national security purposes.

There are currently two different forms of authority that can be invoked in order to justify surveillance: (1) intelligence authority under the Foreign Intelligence Surveillance Act (FISA); and (2) authority to pursue a criminal investigation under a variety of federal statutes. Enacted in 1978, FISA created authority to conduct searches and surveillance of foreign

²⁰ [18 USCA §§ 2510–2520](#)

²¹ 18 U.S.C. § 2511(2)(g)(i)

²² See *U.S. v. Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997)

²³ See *State v. Turner*, 805 N.E.2d 124 (2d Dist. Montgomery County 2004).

²⁴ See *U.S. v. Lifshitz*, 369 F.3d 173 (2d Cir. 2004).

agents or foreign governments with the goal of gaining intelligence information and not the building and prosecution of a case against a particular defendant. There are several key differences between a FISA intercept order obtained under intelligence authority and an intercept order obtained under authority to investigate criminal matters. For example, in order to obtain a FISA order, the federal government need not show probable cause for a FISA search, requirement for the issuance of a search warrant in a criminal investigation. Second, there is no requirement of notice for a FISA search. The target of a FISA search cannot obtain discovery of the FISA court order application. As a result, the target of a FISA search cannot effectively challenge a wiretap or search conducted under FISA authority. Third, FISA investigations could be used only when foreign intelligence gathering was the “primary purpose.”

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the “Patriot Act”)²⁵ was enacted on October 26, 2001. Among other things, the Patriot Act significantly broadens the scope of situations where FISA intelligence authority can be invoked in an effort to combat terrorism.²⁶ For example, under the Patriot Act, FISA surveillance authority may be used so long as the primary purpose is a criminal investigation. Thus, intelligence gathering need only be a “significant” purpose and not the primary purpose that was once required. After enactment of the Patriot Act, the federal government may invoke FISA to conduct a parallel criminal investigation despite an

²⁵ H.R. 3162

²⁶ Patriot Act §802 creates a definition for the crime of ‘domestic terrorism.’ It is an extremely broad definition under which any crime that ‘appears to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, affect the conduct of a government...’ now falls under the heading of ‘domestic terrorism.’ Thus, given the broad scope of the offense, broad latitude is created for investigation of possible terrorism activities, making it easier for government investigators to obtain private information in pursuit of such an investigation. Similarly, USAPA §808 adds to the list of offenses that comprise the ‘federal crime of terrorism.’ Of interest is the addition of new computer crimes to the list. Again, this increases the scope of permissible government investigations.

inability to make a showing of probable cause. Moreover, if the federal government is monitoring electronic communications used exclusively between foreign powers and when it is unlikely that communications to which a U.S. person is a party will be intercepted, there is no immediate FISA order requirement and the government may conduct surveillance for up to a year without a court order. One concern is that the government may use FISA to circumvent Fourth Amendment protections and conduct more aggressive domestic surveillance not necessarily involving the threat of terrorism.

The Patriot Act condones an aggressive governmental monitoring program of individuals in order to obtain private information. For example, the Act permits increased monitoring of financial transactions, creation for a DNA bank to identify terrorists and other violent offenders, required disclosure to the CIA and FBI of information obtained during grand jury proceedings, changes in the scope of search warrants for electronic information, and greatly increased CIA and FBI powers to monitor individuals.

Government web surveillance generally clusters on four methods. These methods include wiretaps, search warrants, pen/trap orders, and subpoenas. The Patriot Act recognizes these time-tested tools of surveillance and expands the government's power to use them. Several of these tools, however, pose their own privacy issues that warrant further discussion.

Prior to the Patriot Act, law enforcement involved in intelligence investigations may obtain a "pen register" or "trap and trace" order (pen/trap order) through which the government may access numbers dialed and received by a particular phone. In order to obtain a pen/trap order, law enforcement had to show that the information that it sought (1) was "relevant to an ongoing criminal investigation" and (2) that the suspect that they were tracking was "in communication with" someone involved in international terrorism or intelligence

activities. This standard is much less exacting than the probable cause standard employed in criminal investigations. The Patriot Act²⁷ reduced the standard even further. Under the Act, the second requirement was deleted.²⁸ Thus, law enforcement must simply show that the information they are seeking is relevant to an ongoing criminal investigation. It appears that under §216 of the Patriot Act, when law enforcement requests a pen/trap order from a court, the court *must* issue it. The judge has no discretion to refuse.

Moreover, under §216 of the Act, the scope of information that may be obtained using a pen/trap order has been increased. Traditionally, pen/trap orders could only be used to obtain telephone numbers dialed and received. However, under §216 of the Act, law enforcement may now have access to “dialing, routing and signaling” information. The reference to “routing” information refers specifically to internet use — for either email or browsing. The Patriot Act expressly states that “contents” of communications may not be obtained with trap/trace orders, but USAPA does not define the term.

The concern is that government agents may, under this low standard, obtain internet routing information that would show what websites a suspect visited and what they did while on those websites. Unlike a telephone call, where the numbers dialed and received can easily be separated from the content of the phone call, this is not currently the case with a packet-switched network like the internet. Under the new standards for trap/trace orders, because the government is authorized to obtain only the numbers dialed/received, the authorities do not have permission to listen to the content. However, content cannot easily be separated from internet routing information. As a result, in order to obtain an email address, for example, law enforcement must be given access to the entire email packet (which includes content). Law

²⁷ USAPA §§ 214 and 216.

²⁸ USAPA §214.

enforcement is then entrusted with viewing only the address and deleting the content without viewing it. Moreover, with internet browsing, content cannot easily be separated from internet routing information. Furthermore, §216 of the Act authorizes pen/trap orders to be served on any ISP. In effect, a federal judge or magistrate in one jurisdiction can issue a ‘blank’ pen/trap order that does not name the ISP that is subject to the search. That order theoretically may be used to search any ISP in the United States. Like the provision allowing search warrants to be executed in any district, this encourages forum shopping on the part of law enforcement, and also limits the ability of the ISP to challenge the pen/trap order.²⁹

Under prior law, the government could use a subpoena to compel an ISP or website to release the following information about their subscribers: customer’s name, address, length of service, and method of payment (specifically, whether the payment was by credit card, direct withdrawal from bank account. etc.). The government could *not* get credit card numbers, bank account numbers, or other more specific identifying information via a subpoena. Under §210 of the Act, the government may now use a subpoena to obtain credit card numbers and bank account numbers. Law enforcement successfully argued that this is essential information as many people register with websites using false names; thus credit card and bank information is the only way to get a positive identification of a suspect.

Prior to the passage of the Act, government access to stored email communications was governed by the Electronic Communications Privacy Act³⁰ and government access to stored voice mail communications was governed by the federal wiretap statute.³¹ This difference is due to the distinction between stored electronic data (email) and stored wire communications (voice mail). Under the federal wiretap statute, wiretap orders were required

²⁹ Patriot Act §216 does not have a sunset provision.

³⁰ 28 USC §2703.

³¹ 18 USC §2510(1).

in order to access voice mail that was stored by a third party provider (i.e. voice mail stored by the telephone service provider). But, a search warrant could be used to gain access to and confiscate an answering machine from inside a residence or office. The procedure for obtaining a wiretap order is more complex and time consuming than the procedure for obtaining a search warrant. As a result, law enforcement officers often claimed that their investigations were hampered by the need to obtain the wiretap orders. Moreover, as technology progressed and MIME (Multipurpose Internet Mail Extensions) technology became more common, problems for this statutory scheme arose more frequently. MIME allows emails to contain attachments that may include voice recordings. Thus, to obtain unopened email both a search warrant and wiretap order were required. Section §209 of the Act modifies the workings of the wiretap statute and ECPA. Thus, stored wire communications are governed by the same rules as stored electronic data and both can be obtained with a search warrant (*i.e.*, wiretap order not needed).³² Furthermore, §202 of the Act adds to the list of crimes for which law enforcement may use wiretaps to investigate. Thus, law enforcement may now obtain a wiretap order for violations of the Computer Fraud and Abuse Act, for example.³³

Section 212 of the Patriot Act allows for voluntary disclosure on the part of ISPs of private information including customer records as well as content of electronic transmissions. ISPs are given broad latitude to make such disclosures. The provision states that ISPs may choose to voluntarily disclose private customer information if there is a ‘reasonable belief’ that it relates to an ‘emergency involving immediate risk of death or serious bodily injury to any person.’ Thus, ISPs are given authority to disclose private information about their

³² This provision, initially set to sunset December 31, 2005, has been extended.

³³ 18 U.S.C. §1030. This provision, set to expire on December 31, 2005, was also extended.

subscribers in order to assist in criminal investigations. However, the provision is for *voluntary* disclosure - ISPs are not required to disclose information unless it is known that it relates to criminal matters. This minimizes the possibility that ISPs will be induced to monitor transmissions for criminal data as there is no incentive to do so.

Conclusion

Terrorists have used the Internet in a myriad of ways, including fundraising, propaganda, “swarming,” recruitment, deception, denial, and communications. This paper has focused on ways a terrorist organization may utilize the power, accessibility, scalability, ubiquitous nature, and ease of use of the Internet to manage content. By the use of the techniques identified above, terrorist organizations can manipulate content, manage information, increase disinformation and deception, and limit access in what otherwise would be considered a public domain. There are terrorist organizations that have spoken about, written on, or virtually chatted over the varying techniques discussed in this paper. Further, there are terrorist organizations engaged in the use of techniques to mine information about those that access their websites, as described in this paper. By the use of these techniques, a terrorist organization’s command and control functions may operate with little likelihood of detection, content may be managed, and accessibility can be limited to specific visitors – all with our eyes wide shut!

Terrorist activity on the web, however, invites government surveillance. With heightened surveillance, our society runs the risk of a serious erosion of fundamental rights. Traditional tools of surveillance, including search warrants, pen orders, and intercepts provide ample opportunity for governmental abuse. However, these tools are effective at monitoring potential terrorists and terror groups. As we continue to engage the enemy in the GWOT, we

will continue to struggle with striking an appropriate balance between an individual's privacy rights and the government's duty to protect the public from terrorist activity. Striking an appropriate balance is difficult; the struggle to get it right will continue. But the struggle itself, with the opportunity to reflect on our choices and the concerns of too much governmental power, catapults us well beyond our enemy, an enemy unconcerned with the niceties of individual rights and human dignity.