

IS 6323
Lab 1
Don Franke
08 February 2006

Table of Contents

Table of Contents.....	2
1. Introduction.....	3
2. Approach/Techniques Used.....	4
Macintosh.....	4
Windows 2003 Server.....	4
3.Observations.....	6
4.Conclusions.....	6
Appendix.....	7

1. Introduction

This lab aims to demonstrate familiarity with the logging options of a computer. The computers I used for this lab are:

Macintosh
2GHz Dual Core
512 MB RAM
Mac OS X 10.4.4

AMD 2100
1.83 GHz
1.28 GB RAM
Windows 2003 Server

These computers are attached to a local network.

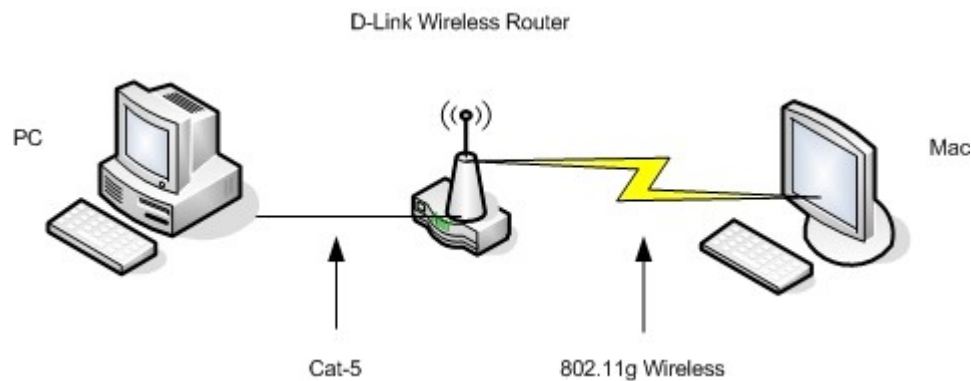


Figure 1: Network Overview

The tools I used for this lab are:

- Mac Console version 2.2
- Microsoft Notepad

I chose these two tools because the lab was to demonstrate a basic understanding of computer logging, and these two tools are general purpose log readers and fit the needs for this lab.

The IP addresses at the time of this lab are:

Mac 192.168.0.101
PC 192.168.0.102

The Macintosh runs a version of Apache httpd called Personal Web Server. It's setup is nearly identical to that of a Linux or UNIX installation. On Windows 2003 Server IIS 6.0 is running.

2. Approach/Techniques Used

Macintosh

I wanted to get more familiar with the web server logging of both Windows 2003 and Mac OS X. To start on the Mac, I deleted the following web server log files:

```
/var/log/httpd/error_log  
/var/log/httpd/access_log
```

Then I started the Personal Web Server. Starting the web server immediately created the two files again.

At the root of this web server I had a simple file: index2.html This file displays "Hello World." On the PC I called up the Mac's IP address in Internet Explorer and got Hello World.

Refreshing the Console, the access_log now had the following entry:

```
192.168.0.102 - - [05/Feb/2006:12:52:53 -0600] "GET / HTTP/1.1"  
200 524
```

I then tried to call up index0.html, which doesn't exist. "Page cannot be found" displayed in Internet Explorer, and this entry was added to access_log:

```
192.168.0.102 - - [05/Feb/2006:12:55:45 -0600] "GET /index0.html  
HTTP/1.1" 404 302
```

And this was added to error_log:

```
[Sun Feb 5 12:55:45 2006] [error] [client 192.168.0.102] File  
does not exist: /Library/WebServer/Documents/index0.html
```

Next I thought I'd play with the permissions a little. I changed the permissions to index2.html from -rw-r--r-- to ---x--x-- and tried the page on the PC. "You don't have permission to access /index2.html on this server." Was the response, and in the error_log file was the entry:

```
[Sun Feb 5 12:59:37 2006] [error] [client 192.168.0.102]  
(13)Permission denied: file permissions deny server access:  
/Library/WebServer/Documents/index2.html
```

I issued chmod 644 index2.html to restore the file to its default permission settings.

Windows 2003 Server

For IIS 6.0 on my PC, the web server log file is stored at D:\Windows\System32\LogFiles\W3SVC1\ex060205.log The filename is the date the file was created. I deleted the log files from this directory and started the web server.

The home directory of the web server on this PC is D:\inetpub\wwwroot In this directory I created a simple web page using Visual Studio 2005. This created the file

Default.aspx in this directory. On my Mac I called up the address <http://192.168.0.102/Default.aspx> in my Safari web browser and got a "Hello World" message, which is the content of this web page. Opening the log file I saw that the following entry was added:

```
2006-02-05 20:03:26 W3SVC1 192.168.0.102 GET
/Default.aspx - 80 - 192.168.0.101
Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X;+en)+AppleWebKit/417.9+
(KHTML,+like+Gecko)+Safari/417.8
200 0 0
2006-02-05 20:03:26 W3SVC1 192.168.0.102 GET
/favicon.ico - 80 - 192.168.0.101
Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X;+en)+AppleWebKit/417.9+
(KHTML,+like+Gecko)+Safari/417.8
404 0 2
```

Deciphered: the web page Default.aspx came up OK (code 200), but the file favicon.ico did not (code 404, file not found.) I have more of this in the Observations section.

Next I tried to call up Default2.aspx from my Mac. The web browser predictably displayed "HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable." The log file recorded the following:

```
2006-02-05 20:20:37 W3SVC1 192.168.0.102 GET
/Default2.aspx - 80 - 192.168.0.101
Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X;+en)+AppleWebKit/417.9+
(KHTML,+like+Gecko)+Safari/417.8
404 0 0
2006-02-05 20:20:37 W3SVC1 192.168.0.102 GET
/favicon.ico - 80 - 192.168.0.101
Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X;+en)+AppleWebKit/417.9+
(KHTML,+like+Gecko)+Safari/417.8
404 0 2
```

Code 404 was the result of both requests.

Next I changed the permissions for the Default.aspx file for the IIS_WPG user to Deny to the Read and Write permissions it previously had. Calling up the page now I get the error:

"Error message 401.3: You do not have permission to view this directory or page using the credentials you supplied (access denied due to Access Control Lists). Ask the Web server's administrator to give you access."

The log file had the new entry:

```
2006-02-05 20:35:37 W3SVC1 192.168.0.102 GET
/Default.aspx - 80 - 192.168.0.101
Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X;+en)+AppleWebKit/417.9+
(KHTML,+like+Gecko)+Safari/417.8
401 5 0
2006-02-05 20:35:37 W3SVC1 192.168.0.102 GET
```

```
/favicon.ico - 80 - 192.168.0.101
Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X;+en)+AppleWebKit/417.9+
(KHTML,+like+Gecko)+Safari/417.8
404 0 2
```

3.Observations

I noticed that it seems that entries for the IIS log file are only written to after an event occurs—an event, such as a page request or shutting down the server, writes the logger memory to the file it seems. Until an event occurs, the most recent event stays in memory and does not display in the file. I needed to stop and restart the web service in order to get the most recent event to show up in the file. On the Mac, however, the event occurrence and it being recorded in the log file seemed nearly instantaneous. It seems to me that how Windows logs its web server events may cause headaches, since entries in memory rely on an event in order to be committed to the log file.

Opening the log file I saw that the following entry as added:

```
2006-02-05 19:53:44 W3SVC1 192.168.0.102 GET
/favicon.ico - 80 - 192.168.0.101
Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X;+en)+AppleWebKit/417.9+
(KHTML,+like+Gecko)+Safari/417.8
404 0 2
```

What I noticed right away is that the entry for Mac→Windows is about twice in size. I looked at the entry carefully and saw that two entries were made in the log file as a result of my single page request. Different from Microsoft's Internet Explorer, Apple's Safari requested both the page (which resulted in code 200 or OK) as well as the file favicon.ico, which resulted in code 404 or Not Found.) According to Wikipedia:

"favicon (short for "Favorites icon"), also known as a page icon, is an [icon](#) associated with a particular [website](#) or [webpage](#). A web designer can create such an icon, and many graphical [web browsers](#)—such as recent versions of [Internet Explorer](#), [Firefox](#), [Mozilla](#), [Opera](#), [Safari](#), and [Konqueror](#)—can then make use of them. Browsers that support favicons may display them in the browser's [URL bar](#), next to the site's name in lists of [bookmarks](#), and next to the page's title in a [tabbed document interface](#)."

Downloading two files for each page request seems like some overhead I could do without. I have started looking into how to disable automatic favicon.ico file downloading in Safari.

4.Conclusions

These tools allow for basic log reading. However, do any in-depth mining, more sophisticated tools would be needed. It would be very difficult to find entries of interest in log files that are megabytes in size (for this lab I was able to start from scratch and only had to keep my eye on the latest entries.) There are various Perl scripts available that allow for search for patterns and entries and generate reports. There are also several third-party tools available, both free (many open source) and software for sale.

For risk assessment, yes, these basic log readers could be used, but it would be very tedious.

Appendix

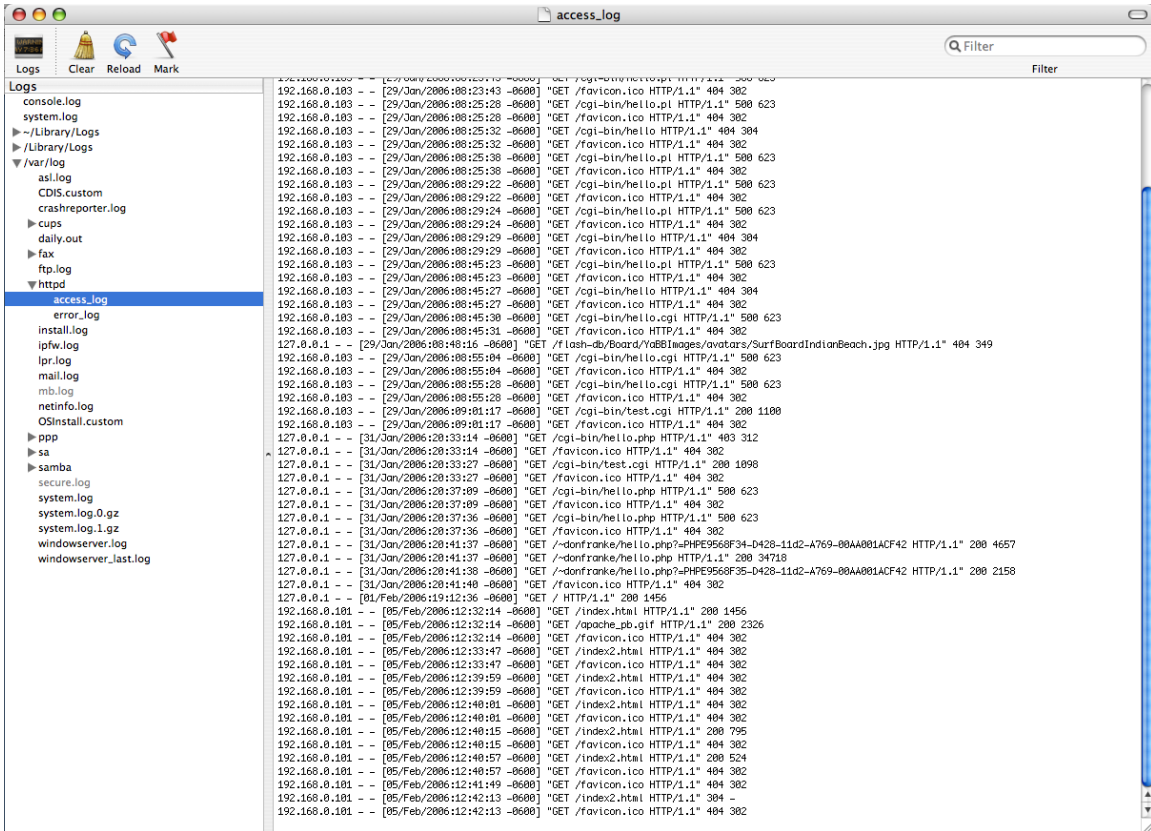
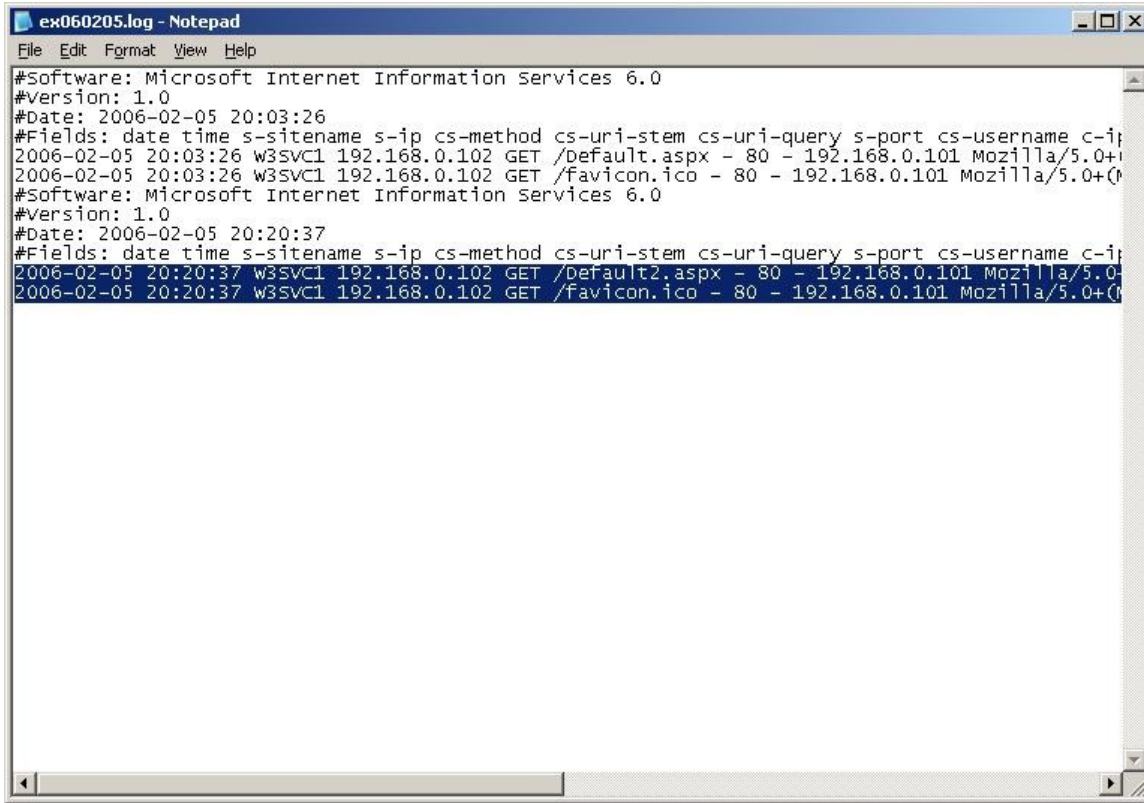


Figure 2: Screen Shot of Mac Console



```
ex060205.log - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2006-02-05 20:03:26
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip
2006-02-05 20:03:26 w3svc1 192.168.0.102 GET /default.aspx - 80 - 192.168.0.101 Mozilla/5.0+
2006-02-05 20:03:26 w3svc1 192.168.0.102 GET /favicon.ico - 80 - 192.168.0.101 Mozilla/5.0+
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2006-02-05 20:20:37
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip
2006-02-05 20:20:37 w3svc1 192.168.0.102 GET /Default2.aspx - 80 - 192.168.0.101 Mozilla/5.0+
2006-02-05 20:20:37 w3svc1 192.168.0.102 GET /favicon.ico - 80 - 192.168.0.101 Mozilla/5.0+
```

Figure 3: Screen shot of ex060205.log