Harrison Group White Paper:

Genuine Microsoft Products Vs. Pirated Counterparts

Prepared by:
Case Braskamp
Jake Soffronoff

Date:
August 26, 2011

Sponsored By:
# Table of Contents

IN THIS WHITE PAPER .......................................................................................................................... 3

EXECUTIVE SUMMARY .......................................................................................................................... 4
- Counterfeit Users Make Significant Sacrifices .................................................................................. 5

METHODOLOGY .................................................................................................................................... 6

RESULTS ................................................................................................................................................. 7
- Security .................................................................................................................................................. 7
  - Viruses, Worms and Trojans Found in Pirated Versions ................................................................. 7
  - Vulnerability Regardless of Channel ................................................................................................. 8
- Pirated Software Often Unable to Download Updates ....................................................................... 8

PERFORMANCE & PRODUCTIVITY ....................................................................................................... 8
- Genuine Microsoft Users Experience Superior Performance than Users of Counterfeit Products ....... 8
- Genuine Microsoft Windows Boots Faster ......................................................................................... 9
- Genuine Microsoft Office is More Efficient to Use ........................................................................... 9
- Genuine Microsoft Provides Superior Intranet Performance .......................................................... 9
- Genuine Microsoft is Faster When Loading Popular Text-and-Graphics Heavy Web Pages ............. 9

POWER CONSUMPTION & BATTERY LIFE ......................................................................................... 9
- Genuine Microsoft is More Energy Efficient When Performing Processor-Intensive Tasks .......... 10
- Genuine Microsoft is More Energy Efficient Both in and Coming out of Sleep Mode ................. 10
- Genuine Microsoft Machines Enjoy Longer Battery Life ............................................................... 10

IN SUMMARY: IMPLICATIONS FOR COUNTERFEIT USERS ................................................................ 11
- How to Recognize Counterfeit Software ......................................................................................... 11
- Support for Windows XP and Office 2003 is in the Process of Being Phased Out ......................... 11
- Conclusion ....................................................................................................................................... 12

APPENDICES ....................................................................................................................................... 12
- Appendix I: Methodologies for Performance & Productivity Tests ................................................ 13
- Appendix II: Methodologies for Security Tests ............................................................................... 16
- Appendix III: Methodologies for Power Consumption Tests ........................................................ 17
- Appendix IV: Hardware Configurations ......................................................................................... 19
- Appendix V: Software Configurations ........................................................................................... 20
In This White Paper

This white paper presents the results of a series of independently-run tests that were designed to discover differences between genuine and counterfeit installations of Microsoft software. It describes the variation in levels of security, performance and power consumption that were found between genuine and pirated Microsoft software, and provides some discussion of the implications that these findings have for business and everyday users alike.
Executive Summary

Despite the fact that, excluding price, people rank reliability and protection against viruses and malicious code as the most valuable software attributes, millions of everyday users and businesses entrust their virtual worlds to software that they obtained from unaccountable resources.

Many users may believe that the risks associated with using counterfeit software are isolated to programs acquired from the web, but studies demonstrate that is not the case. In fact, users obtain problematic counterfeit software through a number of channels, including from hardware retailers that pre-install it on the machines that they sell, or from purchases made at unauthorized retailers, street markets or through online auctions or suppliers.

Sources of Improperly Licensed Software

In order to investigate the potential ramifications of using pirated software, the Harrison Group contracted an independent technology benchmarking firm to run and collect data on a series of comparison tests between genuine Microsoft software and counterfeit versions that had been obtained from the web, from hardware retailers and from street market stalls. That data was then analyzed by the Harrison Group in order to identify any security, performance, functionality or resource consumption differences that existed between the various software packages.

Genuine users enjoy a safer experience than counterfeit users

Our findings confirm that users of counterfeit software are, in fact, opening themselves up to risk of infection by worms, Trojans and viruses. 24% of the machines running counterfeit software in our study either became infected at installation, or independently downloaded and installed malicious software upon connection to the internet. Further, we received malicious software from each of the three popular distribution channels we tested – peer-to-peer downloads, purchases from street markets, and purchases from hardware retailers that fail to use genuine Microsoft products. Our results indicated that the level of risk involved in using pirated software is considerable, and that the risk of exposure remains high regardless of the software’s source.

Sources of Improperly Licensed Software

- Came with the computer: 12.2%
- Bought in a store, from a street market, or from an online auction/supplier: 9.1%
- Downloaded from a peer-to-peer network or web site: 71.5%
- Transferred from another computer or borrowed from a friend: 7.2%

n=550
Base = People known to respondents to use pirated software

Genuine Microsoft Products Vs. Pirated Counterparts

**Genuine users enjoy superior performance and productivity than counterfeit users**
While few might be surprised to learn that using pirated products comes with an increased risk of exposure to worms, Trojans and viruses, counterfeit users may not realize that they risk sacrificing performance by failing to use genuine software.

In a recent study, IDC found that 36% of consumers had installed software on their machines that had slowed their computer so much that it had to be uninstalled, and 34% reported installing software that would not run at all*. Our study reinforces these findings, confirming that genuine Microsoft users tend to enjoy superior performance in the form of faster boot times, faster print times, faster document loading times, faster loading times when visiting popular text-and-graphics-heavy websites, and faster intranet page loading times than users of counterfeit products. The reduction in wait time for all of these common tasks adds up to a more dynamic, productive and satisfying experience for users of genuine Microsoft products.

**Genuine users get power consumption benefits compared to counterfeit users**
Another sacrifice that counterfeit users may not realize they are making is in energy efficiency. We found that computers installed with genuine Microsoft products tend to consume less energy when performing processor-intensive tasks, when in sleep mode, and when coming out of sleep mode than their pirated counterparts, all of which adds up to longer battery life, reduced environmental impact, and lower energy costs for consumers and businesses alike.

**Counterfeit users make significant sacrifices**
In total, our results indicate that counterfeit users pay a high cost for the low price of counterfeit software. Users of pirated software are opening themselves up to the potential for both catastrophic security breaches and significant losses in productivity and performance, regardless of the platform they use, and regardless of whether the counterfeit software’s source is the web, a street market stall, or an unprincipled hardware retailer.

Genuine Microsoft Products Vs. Pirated Counterparts

**Methodology**

The Harrison Group contracted an independent technology benchmarking firm to perform a number of tests and collect data comparing genuine and pirated Microsoft products. That data was then analyzed by the Harrison Group to discover any variations in the levels of security, performance, functionality and resource consumption that might exist between genuine and pirated Microsoft products.

The tests for this study were performed in May and June, 2011, by trained personnel using a variety of genuine and counterfeit Windows and Office software. The different versions of Windows XP, Windows 7, Office 2003 and Office 2007 that were used came from some of the most popular channels of pirated software distribution, including peer-to-peer file sharing, independent hardware dealers, and street market stalls, and originated from a wide geographical area, including China and Eastern Europe. The software was installed on a variety of computer models manufactured by a representative group of popular brands in order to mitigate the effects that using any specific hardware configuration might have on the results.

More detail on the specific hardware and software configurations, as well as on the testing methodologies that were employed for this study, can be found in Appendices I-VI of this document.
Genuine Microsoft Products Vs. Pirated Counterparts

Results
In a recent global survey of 25,000 computer users, 36% of consumers reported that they had needed to uninstall software they had obtained in the past two years because it made their machines too slow, 34% reported installing software that wouldn’t run, 16% reported finding viruses on their computers, and 15% reported having pop-up ads overrun their machines. Our test results corroborate what these users report, and even indicate that the potential risks of using counterfeit software may be greater than some users believe.

Security
Counterfeit users put themselves at risk by using pirated software, regardless of whether their software is obtained through Peer-to-Peer file sharing, from a street market, or from a hardware retailer that fails to install genuine Microsoft products on the machines they sell.

Price excluded, the attribute that users value the most in their software is protection against viruses and hackers*, yet millions of consumers and businesses still choose to install potentially-infected counterfeit software on their computers. Computer users are aware of the risks they’re taking: in a recent poll, 53% of consumers said that they believe that pirated software is either much less secure or dangerously less secure than properly licensed software, and further said that they believe that 55% of pirated software web sites and 53% of pirated software from peer-to-peer sharing posed a security risk if used*. Despite these well-known risks, 4 in 10 software installations today are still improperly licensed*.

Our findings support the suspicion that users feel about the safety of counterfeit software: nearly one in four (24%) of the pirated operating systems in our study either became infected at installation, or independently downloaded and installed malicious software upon connection to the internet. Further, we found worms, Trojans and viruses across both Windows XP and Windows 7 installations, indicating that no pirated platform was safe from threat, and across all of the distribution channels that we investigated, indicating that paying for a piece of counterfeit software from a market stall or hardware retailer does not guarantee its safety.

Viruses, Worms and Trojans Found in Pirated Versions
The viruses that we found in counterfeit Microsoft software ranged from simple worms to annoying Trojans to particularly malicious and fast-spreading viruses. Some of the specific threats found in pirated Microsoft installations included:

- **Helompy.A**, a worm that spreads itself from machine to machine by either copying itself to removable media, or by attaching itself to emails sent from the user’s account. Worms like Helompy.A reduce computer performance and put those in contact with the user’s digital world at risk of infection.

- **Deeterohms.A**, also known as Generic3_c.HHQ, a Trojan that downloads and installs adware on an infected computer while masquerading as legitimate software. This adware attempts to take over the machine’s User Account Controls while downloading any of a number of pieces of

Genuine Microsoft Products Vs. Pirated Counterparts

software to the machine without the user’s knowledge or consent. Ultimately, Trojans like Helompy.A serve as an obtrusive drag on performance while opening users up to potential threats through downloading unwanted software from the internet.

- Generic16.CJLD, a virus that deletes important files from any machine it infects while hijacking the OS and its network tools. Once infected, the virus opens a network back door through which hackers can access any data on computer, including personal and financial information. The virus then uses the backdoor to spread readily through local area networks and infect other machines that are then open to the same risks.

While the level of harm inflicted by each threat varies, the existence of an unknown threat across all platforms and channels of distribution should give users pause when deciding whether or not to test their luck with an unknown source.

**Vulnerability Regardless of Channel**

Those who purchase pirated software may feel that their seller has a vested interest in ensuring that the software they buy is safe, but our results do not support that theory. While it would not come as a shock to most that we found viruses and Trojans in our study’s peer-to-peer downloads, we also received infected software through purchases at street markets, and pre-installed on hardware that was sold by retailers who failed to use genuine Microsoft products.

This work leads us to conclude that the level of risk involved in using pirated software is considerable, and that the risk of exposure remains high regardless of the software’s source.

**Pirated Software Often Unable to Download Updates**

Regularly downloading updates for the software that users employ is a vital part of maintaining a secure and efficient computing experience. One in four of the counterfeit versions of Microsoft software tested in our study was unable to download automatic Windows and Office updates, and one in five was also unable to manually install Windows updates. As with the risk of virus exposure, the inability to download automatic updates was found across all platforms, and was found both in software that had been downloaded for free and in software that had been purchased from a street market or hardware retailer.

The inability to download updates affects users by preventing them from patching any security vulnerabilities that may exist in their software, by preventing them from incorporating updated features that have been made available to paying customers, and eventually by leaving them with software that is out of date and prone to attack. By choosing to download or purchase counterfeit software, both consumers and businesses may be choosing to work in a less efficient computing environment that simultaneously opens them up to additional security risks.

**Performance & Productivity**

*Genuine Microsoft Users Experience Superior Performance than Users of Counterfeit Products*

Waiting for your PC to boot, waiting for documents to open, waiting for the printer to receive your documents, waiting for a web page to load – whether it comes in the form of one long wait or thousands of smaller ones, it all adds up to lost productivity and a less elegant user experience. Genuine Microsoft users enjoy faster boot times, smoother MS-Office performance, faster load times when visiting popular text-and-graphics-heavy websites, and faster intranet page load times than users of counterfeit products, which all adds up to a more dynamic, productive and satisfying user experience.
Genuine Microsoft Windows Boots Faster
Perhaps the most universal and annoying wait of all is the time spent waiting for a computer to boot. In boot time tests, genuine Windows machines outperformed those with pirated installations 60% of the time by an average of 56%. Recapturing this time on a daily basis at work and at home would be a boon for most users. Less time spent waiting is more time spent being productive, connecting with friends and family, or having fun on your PC.

Genuine Microsoft Office is More Efficient to Use
Throughout your workday, you probably experience many small waits. Waiting for documents to load, waiting for your work to be sent to the printer – in the course of a normal workday, these small waits can add up to a lot of time. In a series of tests designed to measure these waits, we found significant advantages for genuine users when performing a number of everyday tasks in Microsoft Office.

PCs running genuine Windows and MS-Office products outperformed their pirated counterparts 75% of the time by an average of 52% when opening the kinds of multiple-sheet Excel documents that businesses use every day. Further, in tests measuring the time it takes to print 500kb or 1mb Word documents, genuine machines were faster than their pirated counterparts in half (48%) of the test configurations by an average of 56%. Considering the frequency with which these tasks are completed, over the long term these advantages can mean significant productivity gains for businesses and consumers alike.

Genuine Microsoft Provides Superior Intranet Performance
Whether it’s sharing calendars or large-scale data sources, many modern businesses provide significant amounts of information over intranet websites. In a series of tests measuring load times for intranet websites, genuine Windows products demonstrated far superior performance than their pirated counterparts – 67% of the time the genuine Microsoft products were an average of 100% faster. Aside from the peace of mind that using genuine products provides, this advantage could mean very large productivity gains for enterprises for whom the use of internal websites is key to productivity.

Genuine Microsoft is Faster When Loading Popular Text-and-Graphics Heavy Web Pages
As websites have evolved over time to include more graphics and information, users have been subjected to regular waits that can last from milliseconds to minutes. In a test measuring the time it took to load popular Internet web pages that were heavy with text and graphics, PCs running genuine Windows outperformed their pirated counterparts 59% of the time by an average of 46%. By shortening these waits, genuine users save a significant amount of time – and businesses gain worker productivity – as they surf the net.

Power Consumption & Battery Life
Computers installed with genuine Windows and Office software are more energy efficient than their pirated counterparts, which leads to lower energy costs for users, longer battery life for genuine Laptops, and a more environmentally friendly experience for everyone.

Whether you are a road warrior who depends on that extra bit of battery life, or you are just trying to control costs, energy efficiency is an area of concern due to its ramifications on battery life, energy costs, and the environmental impact of computing. A majority of the PCs installed with genuine Microsoft Windows and Office software in our study consumed less energy and exhibited superior battery life than their pirated counterparts.
Genuine Microsoft Products Vs. Pirated Counterparts

**Genuine Microsoft is More Energy Efficient When Performing Processor-Intensive Tasks**
The genuine Microsoft installations in our study demonstrated significantly superior energy efficiency than their pirated counterparts while performing processor-intensive operations.

In a test measuring how much power is consumed while running processor-intensive programs for an hour, genuine Windows machines outperformed pirated operating systems 60% of the time by an average of 20%. In a test measuring how much power is consumed when watching a high definition movie, half (47%) of the genuine-installed machines in our study consumed an average of 25% less power than their pirated counterparts. These drains add up to significant additional energy costs (and adverse environmental impact) over the life of a computer and would negatively affect laptop users’ battery life, which is a particular concern business and media-inclined road warriors looking to squeeze every ounce of performance from their machines while travelling or working in the field.

**Genuine Microsoft is More Energy Efficient Both in and Coming out of Sleep Mode**
Genuine Microsoft products are consistently more energy efficient than their pirated counterparts when either in or coming out of sleep mode.

In a test measuring how much power is consumed by a computer when the operating system is in sleep mode with no programs running, the machines installed with genuine Microsoft software outperformed those with pirated installations more than half (62%) of the time by an average of nearly 8%. When coming out of sleep mode, the genuine-installed machines consumed an average of 17% less power over half (53%) of the time. Considering that many people routinely leave their machines in sleep mode instead of shutting down at the end of a session, these numbers can add up to a significant increase in energy efficiency for genuine users over the life of an average computer.

**Genuine Microsoft Machines Enjoy Longer Battery Life**
In light of our results on power consumption, it was not surprising to find that laptops installed with genuine Windows operating systems demonstrated significantly longer battery life in over half (56%) of the test configurations in our study. On average, these laptops experienced nearly 26 extra minutes of computer use per charge, which would be a very nice pick up for those who need their machines to stay “alive” while working remotely in order to remain productive, or for those who simply want to get the most out of their machines.
In Summary: Implications for Counterfeit Users

Users of pirated Microsoft software open their digital worlds to threatening security vulnerabilities while running the risk of sacrificing performance, productivity and energy efficiency. Our study demonstrates that, regardless of the software configuration employed, and regardless of whether the counterfeit software’s source is the web, a street market stall or an unprincipled hardware retailer, the low price of using counterfeit software comes at a high cost.

How to Recognize Counterfeit Software

Our research makes it clear that the risks run by those using pirated software are both real and potentially costly. There are several cues that can help those who are unsure about the legitimacy of their Microsoft software to recognize counterfeit versions:

Source: 8-in-10 of the users running improperly licensed software obtained it online through a website or peer-to-peer network, purchased it through an online auction or supplier, or purchased it through a street market or store. In order to be sure that users obtain genuine software, they should instead purchase it either directly from Microsoft, or from an authorized Microsoft retailer.

Activation: Genuine Microsoft software requires activation and validation at installation. If a user is not required to enter a genuine Microsoft product key at installation, the chances are that they are installing counterfeit software.

Updates: Users running genuine Microsoft software receive automatic security and feature updates. If a piece of software is unable to receive automatic updates, there is a good chance that it is not genuine and that it is therefore vulnerable to sacrificed performance and security threats.

Labeling: Genuine Microsoft discs are labeled with a hologram and come with a certificate of authenticity. Counterfeiters are now able to convincingly replicate Microsoft’s sophisticated labeling, however, so the presence of a hologram should not be used as the sole indicator of a piece of software’s validity.

Support for Windows XP and Office 2003 is in the Process of Being Phased Out

All users should be aware that in April, 2009 Microsoft moved the Windows XP and Office 2003 software platforms from Mainstream to Extended support. While users are still able to receive monthly security updates, they are no longer able to make warranty claims or receive free technical support. Further, In April, 2014 all Windows XP and Microsoft Office 2003 support, including security updates and security-related hot-fixes, will be terminated. This will leave anyone still using Windows XP and Office 2003 vulnerable to performance and security threats, and those most at risk will be those whose pirated software has left their machines the longest unprotected.

Conclusion
Given the risks identified in this study, all users – particularly businesses with long-term deployment timeframes – would be well served to upgrade to genuine Microsoft Windows and Office products. Employing genuine software allows users to protect the performance they experience and the security of their personal and professional information. All users should verify that the software that they run is genuine, and if it’s not they should acquire an upgrade either from Microsoft directly, or from an authorized Microsoft retailer.
**Appendix I: Methodologies for Performance & Productivity Tests**

<table>
<thead>
<tr>
<th>Test Measuring…</th>
<th>Testing Method</th>
</tr>
</thead>
</table>
| Average time to open a multipage Excel spreadsheet. | **Preconditions:**  
  - Put the test file on the desktop.  
  - Set Excel Macro security to low.  
  - Select Auto Scroll in Procmon’s edit menu.  
  - Select Always on Top under Procmon Options.  
  **Procmon filters added:**  
  - Process name: EXCEL.EXE.  
  - Operation: Process Start.  
  - Operation: CloseFile.  
  **Testing method:**  
  1. Open Procmon.  
  2. Open multipage excel spreadsheet.  
  3. When data stops scrolling for 5+ seconds record time reading from last entry.  
  4. Subtract the process start time from the last entry time and record the result.  
  5. Repeat the test 5 times and record the average result. |
| Average time to print a 500kb Word document. | **Preconditions:**  
  - Add a local printer.  
  **Procmon filters added:**  
  - Operation: Create File.  
  - Operation: Close File.  
  - Path Contain: xxtestprintxx.  
  **Testing method:**  
  1. Open Procmon.  
  2. Open 500kb Word document (“xxtestprintxx”).  
  4. Click on “Ok” to print.  
  5. Subtract the process start time from the end time and record the result.  
  6. Repeat the test 5 times and record the average result. |
### Appendix I: Methodologies for Performance & Productivity Tests, Cont’d

<table>
<thead>
<tr>
<th>Test Measuring...</th>
<th>Testing Method</th>
</tr>
</thead>
</table>
| **Average time to print a 1mb Word document.** | **Preconditions:**  
  o Add a local printer.  

  **Procmon filters added:**  
  o Operation: Create File.  
  o Operation: Close File.  
  o Path Contain: xxtestprintxx.  

  **Testing method:**  
  1. Open Procmon.  
  2. Open 1mb Word document (“xxtestprintxx”).  
  4. Click on “Ok” to print.  
  5. Subtract the process start time from the end time and record the result.  
  6. Repeat the test 5 times and record the average result. |
| **Average time to print a 5mb Word document.** | **Preconditions:**  
  o Add local printer.  

  **Procmon filters added:**  
  o Operation: Create File.  
  o Operation: Close File.  
  o Path Contain: xxtestprintxx.  

  **Testing method:**  
  1. Open Procmon.  
  2. Open 5mb Word document (“xxtestprintxx”).  
  4. Click on “Ok” to print.  
  5. Subtract the process start time from the end time and record the result.  
  6. Repeat the test 5 times and record the average result. |
| **Average time to load an intranet web page.** |  
  2. Clear browsing history and cache before each test.  
  3. Repeat the test 5 times and record the average result. |
### Appendix I: Methodologies for Performance & Productivity Tests, Cont’d

<table>
<thead>
<tr>
<th>Test Measuring…</th>
<th>Testing Method</th>
</tr>
</thead>
</table>
| Average time to load an intranet web page heavy with text. | 1. Use http://www.numion.com/Stopwatch/index.html to open and close an intranet web page and record the time.  
2. Clear browsing history and cache before each test.  
3. Repeat the test 5 times and record the average result. |
| Average time to load an intranet web page heavy with graphics. | 1. Use http://www.numion.com/Stopwatch/index.html to open a graphic intranet web page and record the time to a log file.  
2. Clear browsing history and cache before each test.  
3. Repeat the test 5 times and record the average result. |
2. Clear browsing history and cache before each test.  
3. Repeat the test 5 times and record the average result. |
## Appendix II: Methodologies for Security Tests

<table>
<thead>
<tr>
<th>Test Measuring...</th>
<th>Testing Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to install automatic</td>
<td>1. Set operating system to check for automatic updates.</td>
</tr>
<tr>
<td>Microsoft OS updates.</td>
<td>2. Check for automatic download of updates.</td>
</tr>
<tr>
<td>Ability to install manual</td>
<td>1. Search for manual updates on the Microsoft website.</td>
</tr>
<tr>
<td>Microsoft OS updates.</td>
<td>2. Download and run the manual updates.</td>
</tr>
<tr>
<td>Ability to install manual</td>
<td>3. Check for download and installation of manual updates.</td>
</tr>
<tr>
<td>Microsoft OS updates.</td>
<td></td>
</tr>
</tbody>
</table>

**Preconditions:**
- Fresh install of OS under test.
- Install manufacturer’s hardware drivers.
- Run all windows recommended updates.
- No third party applications installed.
- System configured to boot into windows without logon screen.

**Testing method:**
1. Add a shortcut to notepad in windows startup.
2. Launch Procmon.
3. Select Options > Enable Boot Logging and select OK.
4. Restart computer.
5. Launch Procmon.
6. Save the boot log to the desktop.
7. Open the boot log file.
8. Record the time of the first process start and the start time of notepad.exe.
9. Calculate boot time by subtracting the first boot time from the start time of notepad.
10. Repeat the test 5 times and record the average result.

| Presence of viruses.               | 1. Run AVG full virus scan.                                                                                                                   |
|                                   | 2. Monitor network traffic and analyze results to find irregularities.                                                                    |
## Appendix III: Methodologies for Power Consumption Tests

<table>
<thead>
<tr>
<th>Test Measuring...</th>
<th>Testing Method</th>
</tr>
</thead>
</table>
| Battery life      | 1. Ensure that battery is fully charged.  
2. Configure Windows Media Player to loop playback.  
3. Disconnect the laptop from non-battery power supply and record time.  
4. Play a looping HD AVI movie.  
5. Ping computer being tested from a second computer every 30 seconds, then record time when the ping test fails.  
6. Subtract the start time from the end time to get total battery life. |
| Time to recharge its battery. | 1. Ensure that the battery is dead.  
2. Start a stopwatch.  
3. Plug in the machine to charge the battery.  
4. Stop the stopwatch when the computer's battery is fully charged, record time. |
| Power consumption while running processor intensive programs for an hour. | 1. Ensure that the laptop is sitting idle and that the battery is at least charged to 75%.  
2. Calibrate JouleMeter software.  
3. Start Internet Explorer.  
4. Enter the names of the program executable to run (iexplore.exe).  
5. Save the data to a file.  
6. Click "Start Saving"  
7. Play video from the Microsoft website to completion.  
8. Stop saving when the video has completed.  
9. Record power consumption.  
10. Repeat the test 5 times and record the average result. |
| Power consumption during sleep mode. | 1. Remove the battery from the laptop.  
2. Connect the machine to a "Kill a Watt" measuring device.  
3. Boot the computer and let it go into sleep mode.  
4. Record the reading on the "Kill a Watt" device each minute for the next 5 minutes.  
5. Repeat the test 5 times and record the average result. |
| Power consumption when coming out of sleep mode. | 1. Remove the battery from the laptop.  
2. Connect the machine to a "Kill a Watt" measuring device.  
3. Boot the computer and let it go into sleep mode.  
4. Wake the computer up by pressing the power button.  
5. Record the highest "Kill a Watt" reading over the next minute.  
6. Repeat the test 3 times and record the average. |
### Appendix III: Methodologies for Power Consumption Tests, Cont’d

<table>
<thead>
<tr>
<th>Test Measuring...</th>
<th>Testing Method</th>
</tr>
</thead>
</table>
| Power consumption when playing an HD Movie. | 1. Remove the battery from the laptop.  
2. Connect the machine to a "Kill a Watt" measuring device.  
3. Boot up a high quality video and skip forward to the 30 minute mark.  
4. Play the movie in full screen mode.  
6. Record the reading on the "Kill a Watt" device each minute for the next 5 minutes.  
5. Repeat the test 5 times and record the average result. |
## Appendix IV: Hardware Configurations

<table>
<thead>
<tr>
<th>Processor</th>
<th>RAM/Hard Drive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Core 2 Duo 2.10</td>
<td>3gb/250gb</td>
</tr>
<tr>
<td>AMD II 2.29</td>
<td>3gb/250gb</td>
</tr>
<tr>
<td>Turion II 560 Dual 2.5</td>
<td>3gb/300gb</td>
</tr>
<tr>
<td>Pentium R 2.13</td>
<td>2gb/300gb</td>
</tr>
<tr>
<td>Intel Core 2 Duo 2.20</td>
<td>3gb/500gb</td>
</tr>
<tr>
<td>AMD II 2.19</td>
<td>1.74gb/300gb</td>
</tr>
</tbody>
</table>
**Appendix V: Software Configurations**

<table>
<thead>
<tr>
<th><strong>Windows OS Versions Tested</strong></th>
<th><strong>MS-Office Versions Tested</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 Professional SP1 VL</td>
<td>Office Pro 2010 FPP</td>
</tr>
<tr>
<td>Windows 7 Professional SP1</td>
<td>Office Pro Plus 2010 VL</td>
</tr>
<tr>
<td>Windows 7 Ultimate SP1</td>
<td>Office Pro Plus 2010</td>
</tr>
<tr>
<td>Windows 7 Ultimate Themed Installation</td>
<td>Office Pro Plus 2010 FPP</td>
</tr>
<tr>
<td>Windows 7 Ultimate</td>
<td>Office Pro 2010</td>
</tr>
<tr>
<td>Windows 7 Ultimate SP1 VL</td>
<td>Office Pro 2010 VL</td>
</tr>
<tr>
<td>Windows 7 Ultimate VL</td>
<td>Office Pro 2010</td>
</tr>
<tr>
<td>Windows 7 Ultimate VL Minimal Installation</td>
<td>Office Pro 2003 FFP</td>
</tr>
<tr>
<td>Windows 7 Ultimate VL Themed Installation</td>
<td>Office Pro 2003 VL</td>
</tr>
<tr>
<td>Windows XP Professional SP3</td>
<td></td>
</tr>
<tr>
<td>Windows XP Professional SP3 Themed Installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>