GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

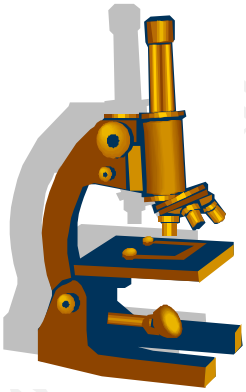
Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at http://www.giac.org/registration/gcfa

CC Terminals Computer Forensics Analysis Report

CC Terminals Computer Forensics Analysis of Suspect Flash Drive For Investigation Into Employee Harassment Claims

© SANS Institute 200 ,nor retains full rights.



Investigator: George Do
Date Submitted: March 16, 2005

© SANS Institute 2000 - 2005 Author retains full rights.

TABLE OF CONTENTS

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

EXECUTIVE SUMMARY

CC Terminals corporate security has received a harassment complaint from employee Leila Conlay levied against employee Robert Lawrence. What follows in this report is a summary of the evidence gathered, subsequent data analysis, and account of events as submitted by the corporate security team.

On the afternoon of October, 29th, CC Terminals employee Leila Conlay reported a potential harassment incident to corporate security. It was reported that employee Robert Lawrence made numerous attempts to meet Ms. Conlay both during and outside of work. On the evening of the night before, October 28th, Ms. Conlay reported seeing Mr. Lawrence at a local coffee shop while there with a friend. This last encounter prompted Ms. Conlay to report this to Corporate Security.

Ms. Conlay also reported that Mr. Lawrence contacted her through her personal email address and that the content of the emails have become increasingly aggressive in nature.

CC Terminals Corporate Security responded by investigating Ms. Conlay's claims. A search of Mr. Lawrence's cubicle turned up a USB Flash Drive device used for storing information. Mr. Mark Mawer of Corporate Security took custody of this evidence for further investigation.

A subsequent computer forensics examination of this device revealed several key pieces of evidence that corroborates Ms. Conlay's claims. Key evidence gathered during the examination included:

- Copies of text / email that confirms Ms. Conlay's harassment claims
- A network capture log which indicates that Mr. Lawrence used wire-tapping to eavesdrop on Ms. Conlay's computer activities
- Network eavesdropping software and tools that suggest Mr. Lawrence actively and maliciously eavesdropped on Ms. Conlay to garner information for his personal use
- An image file of a map of a local coffee shop as where in Ms. Conlay claimed that Mr. Lawrence tracked her
- A timeline of events established via file time stamps that support Ms. Conlay's claims

Given the evidence and circumstances, it is recommended that CC Terminals / Corporate Security take appropriate steps as outlined in established company policies to respond to this harassment charge as soon as possible.

© SANS Institute 2000 - 2005 Author retains full rights.

EXAMINATION DETAILS

Mr. Mark Mawer of Corporate Security took the USB Flash Drive device into custody as evidence. Strict chain of custody procedures was observed to protect the integrity of the evidence as well as employee privacy. The USB Flash Drive was tagged into evidence as:

- Date and Time: October 29th, 2004 @ 9PM
- Location: Robert Lawrence's Cubicle at CC Terminals HQ
- Investigator / Evidence Collector: Mark Mawer – October 29th @9:00PM
- Investigator / Forensics Analyst: Signed for by George Do - October 29th @9:30PM
- Tag #: USBFD-64531026-RL-001
- Description: 64M Lexar Media JumpDrive
- Serial #: JDSP064-04-5000C
- Image: USBFD-64531026-RL-001.img
- MD5: 338ecf17b7fc85bbb2d5ae2bbc729dd5

Mr. George Do of Corporate Security served as the primary computer forensics investigator for this incident. Mr. Do signed for and took custody of the evidence from Mr. Mawer at 9:30PM on October 29th.

Step 1: Evidence Collection and Integrity

Computer forensics is made much simpler by working with image files rather than physical devices. Image files represent a true bit-for-bit representation of the actual physical device. Image files are also easier to work with in that they are easily transferable from system to system as well can be taken as input for a variety of forensics tools. The volatility of computer evidence is rather high as systems tend to modify files/directories thereby tainting the evidence. To mitigate this, evidence integrity is maintained using mathematical checksums (MD5). This provides assurance that the evidence will maintain its integrity throughout the investigation.

A bit-for-bit image copy of the physical drive was created using the "dd" utility. An MD5 hash was generated on the output image file once created to track integrity.

- GCFAPractical2.0-USBImageAndInfo.img
- MD5 Hash: 338ecf17b7fc85bbb2d5ae2bbc729dd5

Using the "mmls" utility on this image reveals partition table information:

```
DOS Partition Table
Units are in 512-byte sectors

Slot        Start        End          Length       Description
00:  -----  0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----  0000000001   0000000031   0000000031   Unallocated
02:  00:00  0000000032   0000121950   0000121919   DOS FAT16 (0x04)
```

There are 3 discreet partitions discovered on the image as revealed above from

© SANS Institute 2000 - 2005 Author retains full rights.

the “mmls” output with a basic 512-byte sector size. The “mmls” utility also reports the start and end sectors for each partition which allows us to “cut” out these partitions. Using the “dd” utility a second time, these 3 separate partitions were extracted into individual partition image files. MD5 hashes were generated on the extracted partitions to once again maintain evidence integrity:

1st Partition - GCFAPractical2.0 USBImageAndInfo.partit MD5 HASH: 5bf1cea807dec8655ed18b9bbf2ee918 2nd Partition - GCFAPractical2.0-USBImageAndInfo.unalloc MD5 HASH: 51596dda30fc38f0df3556d6f115256d 3rd Partition - GCFAPractical2.0 USBImageAndInfo.fat16 MD5 HASH: 5f830a763e2144483f78113a8844ad52

The 1st partition is the sector that contains the partition table - “GCFAPractical2.0 USBImageAndInfo.partit “. The 2nd partition is unallocated space, 31 sectors in length – “GCFAPractical2.0-USBImageAndInfo.unalloc”. The 3rd partition is a FAT16 partition that contains the most relevant data/evidence. The focus for the investigation was placed on the “GCFAPractical2.0 USBImageAndInfo.fat16” image as it represents the “actual data” part of the physical device.

All 3 images were loaded into the Autopsy Forensics Browser for examination. Autopsy is an open-source and free forensics tool. It is basically a web frontend that uses backend unix-based utilities for data analysis. It parses output data and displays it to the forensics investigator for examination. Autopsy was used as the primary forensics investigative tool. More information on Autopsy binaries and source code is available at http://www.sleuthkit.org/autopsy/index.php

Step 2: Timeline Creation

Autopsy was used to compile a timeline of all files and directories on the images. A timeline provides the investigator with MAC (Modified, Access, Change) times for all files/directories on the system, which aids tremendously in tracking the activities on the system. The completed timeline is attached for reference in **Appendix A**.

Although malicious users can modify timeline evidence, it nevertheless reports the last time files/directories were modified, accessed, or changed on the tools that modified the MAC times. Most often however, MAC times are not changed and thus provide a good basis for all system activities.

Step 3: Timeline Analysis and Data Recovery

© SANS Institute 2000 - 2005 Author retains full rights.

Crafted Email / Messages

Analysis of the timeline suggests that on October 25th and 26th, Mr. Lawrence crafted messages to Ms. Conlay in the form of 2 Microsoft Word formatted documents that support her claims against him. Below is a fragment of the timeline that supports this assertion.

Mon Oct 25 2004 00:00:00	19968 .a. -/-rwxrwxrwx 0	0	3	E:\her.doc
Mon Oct 25 2004 08:32:06	19968 ..c -/-rwxrwxrwx 0	0	3	E:\her.doc
Mon Oct 25 2004 08:32:08	19968 m.. -/-rwxrwxrwx 0	0	3	E:\her.doc
Tue Oct 26 2004 00:00:00	19968 .a. -/-rwxrwxrwx 0	0	4	E:\hey.doc
Tue Oct 26 2004 08:48:06	19968 ..c -/-rwxrwxrwx 0	0	4	E:\hey.doc
Tue Oct 26 2004 08:48:10	19968 m.. -/-rwxrwxrwx 0	0	4	E:\hey.doc

These documents – "her.doc" and "hey.doc" were recovered from the image using Autopsy and are referenced in complete form in **Appendices B and C** respectively. These documents support Ms. Conlay's claims that Mr. Lawrence has made contact with her outside of work as well as other inappropriate actions that may be perceived as harassment.

Network Eavesdropping Tools Discovered

Following the sequence of events established by the timeline - 2 files were accessed, modified, and created on October 27th. The timeline indicates that these files were compiled and created on this date. These files are "WinDump.exe" and "WinPcap_3_1_beta_3.exe". "WinDump" is a windows version of TCPDump (Unix), a common network protocol analyzer. "WinDump" requires a "libpcap"-compatible library in order to run under the win32 platform. "WinPcap_3_1_beta_3.exe", the 2nd file discovered, provides these libraries. More information on WinDump and its capabilities and functions can be found at http://windump.polito.it/

"WinDump.exe" was shown to be "accessed" or executed on October 28th at midnight as indicated by the timeline:

Thu Oct 28 2004 00:00:00 450560 .a. -/-rwxrwxrwx 0 0 14 E:\WinDump.exe (_INDUMP.EXE) (deleted)

Eavesdropping Evidence Discovered

In addition to the WinDump eavesdropping tool, a network capture log file was also discovered on the image – "_apture". Ethereal, an industry-common GUI protocol analyzer was used to view and analyze the contents of this file. Further analysis with Ethereal on this log file revealed that it contained Ms. Conlay's email communication to a personal friend to meet at a coffee shop. Because the capture file is in "raw" format and email communications were conducted over

© SANS Institute 2000 - 2005 Author retains full rights.

the HTTP protocol via hotmail.com email services, the actual output of the email content is not in friendly-readable format. The raw log file was sanitized into an easy to read friendly-format and summarized in the following table. A full snapshot of this conversation in raw HTTP format (extracted from the network capture log) is attached in **Appendix D** for reference.

login=flowergirl96(@hotmail.com) to=SamGuarillo@hotmail.com subject=coffee Sure coffee sounds great. Let's meet at the coffee shop on the corner Hollywood and McCadden. It's a nice out of the way spot. See you at 7pm -Leila

This log file contains network traffic captures that proves that Ms. Conlay's email communication was compromised. This evidence further supports Ms. Conlay's assertion that Mr. Lawrence has contacted her at her personal email address as her personal (hotmail) email address is contained in the compromised email message. The timestamp associated with the email was October 28th at 11:10AM according to the network capture file. This further indicates that Mr. Lawrence obtained this information at approximately this time and had plenty of time to intercept Ms. Conlay and her friend at the coffee shop that evening as reported by Ms. Conlay.

Given the discovery of WinDump and this log file, it is clear that Mr. Lawrence has violated established corporate security/privacy policies and possibly civil/federal wiretapping laws.

Exploitation Evidence

An image file was also recovered during the examination – "_ap.gif". Autopsy was used to recover this file:

This image is a map showing the location of the coffee shop as referenced in

© SANS Institute 2000 - 2005 Author retains full rights.

Ms. Conlay's email. This is clear evidence that Mr. Lawrence exploited the information that he was able to obtain while eavesdropping on Ms. Conlay's email communications.

IMAGE DETAILS

File Listing of All Files on Image:

r/r 3:	her.doc
r/r 4:	hey.doc
r/r * 7:	WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 10:	WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 12:	WinDump.exe (_INDUMP.EXE)
r/r * 14:	WinDump.exe (_INDUMP.EXE)
r/r * 15:	_apture
r/r * 16:	_ap.gif
r/r * 17:	_ap.gif
r/r 18:	coffee.doc

True Name of Programs / Files Used by Mr. Lawrence (as proven by MD5 hash value comparisons):

"WinDump.exe"	- Windows-based sniffer binary executable program
"WinPcap_3_1_beta_3.exe"	- Windows Packet Capture Libraries

An MD5 hash was computed for the "WinDump.exe" file discovered on the image as well as the official program executable available from http://windump.polito.it and they were found to match exactly.

79375b77975aa53a1b0507496107bff7	WinDump.exe (File from image)
79375b77975aa53a1b0507496107bff7	WinDump.exe (File downloaded from http://windump.polito.it)

Modified / Accessed / Change Times for all files on image:

See **Appendix A**.

File Sizes in Bytes:

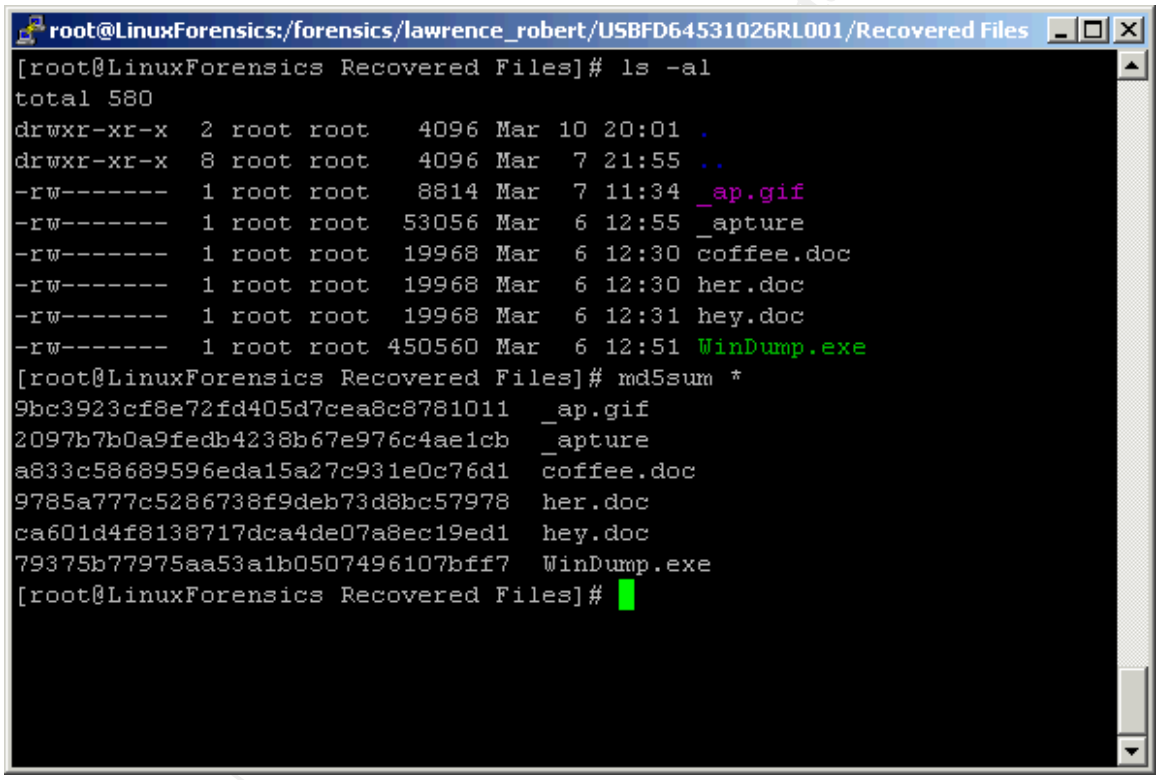
her.doc	19968
hey.doc	19968
WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)	0 (Deleted)
WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)	4858100
WinDump.exe (_INDUMP.EXE)	0 (Deleted)
WinDump.exe (_INDUMP.EXE)	450560
_apture	53056

© SANS Institute 2000 - 2005 Author retains full rights.

_ap.gif	0 (Deleted)
_ap.gif	8814
coffee.doc	19968

MD5 (Message Digest) Hashes of All Files:

9bc3923cf8e72fd405d7cea8c8781011	_ap.gif
2097b7b0a9fedb4238b67e976c4ae1cb	_apture
a833c58689596eda15a27c931e0c76d1	coffee.doc
9785a777c5286738f9deb73d8bc57978	her.doc
ca601d4f8138717dca4de07a8ec19ed1	hey.doc
79375b77975aa53a1b0507496107bff7	WinDump.exe



Key Words Associated With Program File:

windump.exe
winpcap.exe
_apture (capture)
_ap.gif (map.gif)

FORENSICS DETAILS

A suspected Windows-based sniffer program was discovered on the image – "WinDump.exe". This file was recovered and its MD5 hash computed. A

© SANS Institute 2000 - 2005 Author retains full rights.

comparison with the MD5 hash value of the official program downloaded from http://windump.polito.it showed both files to be identical.

It has been proven that Mr. Lawrence used "WinDump.exe" as an eavesdropping tool for his own advantages. Timeline analysis shows that this program was executed on October 28th at precisely midnight. In addition, WinDump requires packet capture libraries in order to function. "WinPcap_3_1_beta.exe" provides these libraries and was also found on the analyzed image.

Both WinDump and WinPcap was downloaded and installed on a VMWare WindowsXP Forensics workstation for further analysis. WinPcap (packet capture libraries) needed to be installed before WinDump can be executed.

WinPcap installs its files in "C:\Program Files\WinPcap". Within this directory, there is an "INSTALL.LOG" log file that shows the actions that the installer took during installation. A portion of this log file is included below to show some of the actions of the installation:

```
[SharedFiles]
C:\Program Files\WinPcap\Uninstall.exe=

[PreRunApp]
0='C:\Program Files\WinPcap\npf_mgm.exe','-u','C:\Program Files\WinPcap',0,'',1,0
1='C:\Program Files\WinPcap\daemon_mgm.exe','-u','C:\Program Files\WinPcap',0,'',1,0

[CreateKeys]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst=

[CreateDirs]
C:\Program Files\WinPcap=

[CopyFiles]
C:\WINDOWS\system32\drivers\npf.sys=
C:\WINDOWS\system32\packet.dll=
C:\WINDOWS\system32\wanpacket.dll=
C:\WINDOWS\system32\wpcap.dll=
C:\WINDOWS\system32\pthreadVC.dll=
C:\Program Files\WinPcap\npf_mgm.exe=
C:\Program Files\WinPcap\daemon_mgm.exe=
C:\Program Files\WinPcap\rpcapd.exe=
C:\Program Files\WinPcap\NetMonInstaller.exe=
```

The above log file reveals install directories, registry keys created, and files copied. Some of these files / libraries are no doubt accessed when WinDump is executed. Furthermore, this log file gives additional information that can be used for analyzing Mr. Lawrence's computer system(s). Existence of these directories / files on Mr. Lawrence's system(s) can be considered the "smoking gun" in this investigation.

In addition to support these assumptions, a network capture log file was discovered on the image – "_apture". Using Ethereal for analysis, this capture

© SANS Institute 2000 - 2005 Author retains full rights.

log revealed network traffic, which contained an email sent from Ms. Conlay to a friend via the hotmail.com email service. The content of the email contained the address location and time of their scheduled meeting. The fact that Ms. Conlay reported that she encountered Mr. Lawrence at this specific location at the time of her scheduled appointment further proves that Mr. Lawrence purposely used the eavesdropped information for tracking her.

PROGRAM IDENTIFICATION

Program used by Mr. Lawrence has been identified as WinDump and WinPcap. Both can be downloaded in both binary format and source code at http://windump.polito.it

The "WinDump.exe" file recovered from the image and the "WinDump.exe" file downloaded from http://windump.polito.it were found to be identical. This is evident by the matching computed MD5 hashes below:

79375b77975aa53a1b0507496107bff7	WinDump.exe (File from image)
79375b77975aa53a1b0507496107bff7	WinDump.exe (File downloaded from http://windump.polito.it)

It is clear from the hash and timeline evidence that Mr. Lawrence used the pre-compiled binary executable.

LEGAL IMPLICATIONS

The Federal Wiretap Act – Title 18 U.S.C. 2510-22 and Title 18 U.S.C. 3121-27

"The Wiretap Act broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies." [1]

Given all the evidence, it has been proven that Mr. Lawrence has violated the Federal Wiretap Act (Title 18 U.S.C. 2510-22) [2]. Although there are numerous exceptions to this statute such as being a "provider" or obtaining user "consent" for monitoring, Mr. Lawrence being a mere member of the Sales team does not qualify for any of these exceptions. The evidence of the network capture log file along with network eavesdropping software proves without a doubt that Mr. Lawrence is in violation of this statute.

Mr. Lawrence may have also violated Title 47 U.S.C. 223(a) [3], which covers threats and harassment. The evidence recovered from Mr. Lawrence's flash drive, namely the 2 MS Word documents with content supporting Ms. Conlay's claim of harassment and a digital map of the coffee shop meeting place both can be deemed as harassment. If Ms. Conlay did indeed receive these messages via her personal email, this further proves intent to harass or annoy which clearly violates this law.

© SANS Institute 2000 - 2005 Author retains full rights.

Violations of the Wiretap Act carry penalties of fines and a prison sentence of up to 5 years. Violations of Title 47 U.S.C. 223(a) carry penalties of fines and a prison sentence of up to 2 years.

In addition to possible violations of federal law, Mr. Lawrence has also violated CC Terminals Acceptable Use Policy (AUP) which clearly states that employees are forbidden to use company resources including any and all company equipment including the computer network for personal or non-work related use. Mr. Lawrence has also violated CC Terminals Corporate Security Policy which specifies that only authorized company personnel such as those within the Security group with written approval from the CIO (Chief Information Officer) may monitor employees' computer and network activities. In addition, Mr. Lawrence has also used the company network in a manner that constitutes employee misconduct.

RECOMMENDATIONS

Given the evidence discovered thus far in this investigation, it is recommend that the following steps be taken in order to build a criminal case against Mr. Lawrence. It is recommended that CC Terminals take the following steps:

1. Gather more evidence – Conduct a wiretap on Mr. Lawrence's network and computer activities (allowed as an exception under the Wiretap Act – "Written Consent". All CC Terminals employees once hired are required to sign a waiver giving up their expectation of privacy along with an acknowledgement that CC Terminals may at any time and without consent monitor employee activities via company-owned computers and networks. Wiretaps may yield additional evidence for possible prosecution.

2. Conduct a full forensics analysis on Mr. Lawrence's computer system(s). An image of the computer can be taken covertly after hours and without Mr. Lawrence's knowledge. Forensics analysis may yield more evidence that will help in prosecution. This is also allowed as an exception under the "Written Consent" clause.

3. Once enough evidence is gathered, notify HR, Legal, and Mr. Lawrence's manager of the investigation into these harassment claims and the evidence against him. Company policies regarding harassment should be observed and followed. This may include employee conduct probation and up to termination of employment.

4. Contact Law Enforcement – CC Terminals should contact local law enforcement to begin a case file on Mr. Lawrence. Evidence gathered thus far can already be used by law enforcement to build a case for prosecution.

© SANS Institute 2000 - 2005 Author retains full rights.

ADDITIONAL INFORMATION

WinDump and WinPcap - *http://windump.polito.it*

WinDump and WinPcap are a windows-based protocol analyzer (network sniffer) and packet capture libraries respectively. Additional information can be found for WinDump and WinPcap at the above URL. This includes source code, binary, and syntactical use and functions of the program.

TCPDump and Libpcap - *http://www.tcpdump.org/*

TCPdump is the original protocol analyzer on Unix platforms. It is open source. It uses Libpcap as its packet capture libraries. WinDump and WinPcap are "windows-ports" of TCPDump and Libpcap. The link above provides for source code and binary distributions of TCPDump and Libpcap.

The Sleuthkit / Autopsy Forensics Tools - *http://www.sleuthkit.org/*

The Sleuthkit / Autopsy were the primary forensics tool used for analysis in this investigation. Autopsy is basically a compilation of trusted and proven unix-based forensics tools with a web frontend for easy navigation. It is open source and free. It simply executes the unix commands, parses the output, and displays it via a web browser for analysis.

Ethereal Protocol Analyzer - *http://www.ethereal.com/*

Ethereal is a software-based protocol analyzer (network sniffer) with a GUI (graphical user interface). Ethereal can be used to view network capture log files such as those collected from TCPDump and WinDump. Ethereal can also be used to "sniff" network traffic. It is available for both the Unix and Windows platforms. Ethereal is also open source and free.

United States Code - *http://www.law.cornell.edu/*

The Legal Information Institute is a portal dedicated to providing easy access to federal laws and statutes. It is hosted at Cornell University and maintained by the Cornell School of Law. This portal is an excellent site for searches for federal statutes and United States Code and was used in this investigation to identify the laws violated.

© SANS Institute 2000 - 2005 Author retains full rights.

LIST OF REFERENCES

[1] Lee, Rob. SANS Institute. Track 8 – System Forensics Investigation & Response. Volume 8.5. SANS Press, 2004: 30

[2] Legal Information Institute. Federal Wiretap Act (Title 18 U.S.C. 2510-22). Cornell University. School of Law, Cornell University, 2005: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002511----000-.html

[3] Legal Information Institute. Title 47 U.S.C. 223(a). Cornell University. School of Law, Cornell University, 2005: http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000223----000-.html

APPENDICIES

Appendix A – Complete Timeline

```
Mon Oct 25 2004 00:00:00    19968 .a. -/-rwxrwxrwx 0       0       3       E:\her.doc
Mon Oct 25 2004 08:32:06    19968 ..c -/-rwxrwxrwx 0       0       3       E:\her.doc
Mon Oct 25 2004 08:32:08    19968 m.. -/-rwxrwxrwx 0       0       3       E:\her.doc
Tue Oct 26 2004 00:00:00    19968 .a. -/-rwxrwxrwx 0       0       4       E:\hey.doc
Tue Oct 26 2004 08:48:06    19968 ..c -/-rwxrwxrwx 0       0       4       E:\hey.doc
Tue Oct 26 2004 08:48:10    19968 m.. -/-rwxrwxrwx 0       0       4       E:\hey.doc
Wed Oct 27 2004 00:00:00        0 .a. -rwxrwxrwx 0       0       12      <GCFAPractical2.0-USBImageAndInfo.fat16-_INDUMP.EXE-dead-12>
                450560 .a. -/-rwxrwxrwx 0       0       12      E:\WinDump.exe (_INDUMP.EXE) (deleted)
                    0 .a. -rwxrwxrwx 0       0       7       <GCFAPractical2.0-USBImageAndInfo.fat16-_INPCA~1.EXE-dead-7>
                485810 .a. -/-rwxrwxrwx 0       0       7       E:\WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:50   485810 m.. -/-rwxrwxrwx 0       0       10      E:\WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                485810 m.. -rwxrwxrwx 0       0       10      <GCFAPractical2.0-USBImageAndInfo.fat16-_INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:54        0 ..c -rwxrwxrwx 0       0       7       <GCFAPractical2.0-USBImageAndInfo.fat16-_INPCA~1.EXE-dead-7>
                485810 ..c -/-rwxrwxrwx 0       0       10      E:\WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                485810 ..c -/-rwxrwxrwx 0       0       7       E:\WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                485810 ..c -rwxrwxrwx 0       0       10      <GCFAPractical2.0-USBImageAndInfo.fat16-_INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:56   485810 m.. -/-rwxrwxrwx 0       0       7       E:\WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                    0 m.. -rwxrwxrwx 0       0       7       <GCFAPractical2.0-USBImageAndInfo.fat16-_INPCA~1.EXE-dead-7>
Wed Oct 27 2004 16:24:02   450560 m.. -rwxrwxrwx 0       0       14      <GCFAPractical2.0-USBImageAndInfo.fat16-_INDUMP.EXE-dead-14>
                450560 m.. -/-rwxrwxrwx 0       0       14      E:\WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:04   450560 ..c -/-rwxrwxrwx 0       0       12      E:\WinDump.exe (_INDUMP.EXE) (deleted)
                    0 ..c -rwxrwxrwx 0       0       12      <GCFAPractical2.0-USBImageAndInfo.fat16-_INDUMP.EXE-dead-12>
                450560 ..c -/-rwxrwxrwx 0       0       14      E:\WinDump.exe (_INDUMP.EXE) (deleted)
                450560 ..c -rwxrwxrwx 0       0       14      <GCFAPractical2.0-USBImageAndInfo.fat16-_INDUMP.EXE-dead-14>
Wed Oct 27 2004 16:24:06        0 m.. -rwxrwxrwx 0       0       12      <GCFAPractical2.0-USBImageAndInfo.fat16-_INDUMP.EXE-dead-12>
                450560 m.. -/-rwxrwxrwx 0       0       12      E:\WinDump.exe (_INDUMP.EXE) (deleted)
Thu Oct 28 2004 00:00:00     8814 .a. -/-rwxrwxrwx 0       0       16      E:\_ap.gif (deleted)
                 8814 .a. -/-rwxrwxrwx 0       0       17      E:\_ap.gif (deleted)
                450560 .a. -/-rwxrwxrwx 0       0       14      E:\WinDump.exe (_INDUMP.EXE) (deleted)
                 19968 .a. -/-rwxrwxrwx 0       0       18      E:\coffee.doc
                 53056 .a. -rwxrwxrwx 0       0       15      <GCFAPractical2.0-USBImageAndInfo.fat16-_apture-dead-15>
                485810 .a. -/-rwxrwxrwx 0       0       10      E:\WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                485810 .a. -rwxrwxrwx 0       0       10      <GCFAPractical2.0-USBImageAndInfo.fat16-_INPCA~1.EXE-dead-10>
                 53056 .a. -/-rwxrwxrwx 0       0       15      E:\_apture (deleted)
                  8814 .a. -rwxrwxrwx 0       0       17      <GCFAPractical2.0-USBImageAndInfo.fat16-_ap.gif-dead-17>
                    0 .a. -rwxrwxrwx 0       0       16      <GCFAPractical2.0-USBImageAndInfo.fat16-_ap.gif-dead-16>
                450560 .a. -rwxrwxrwx 0       0       14      <GCFAPractical2.0-USBImageAndInfo.fat16-_INDUMP.EXE-dead-14>
Thu Oct 28 2004 11:08:24    53056 ..c -rwxrwxrwx 0       0       15      <GCFAPractical2.0-USBImageAndInfo.fat16-_apture-dead-15>
                 53056 ..c -/-rwxrwxrwx 0       0       15      E:\_apture (deleted)
Thu Oct 28 2004 11:11:00    53056 m.. -rwxrwxrwx 0       0       15      <GCFAPractical2.0-USBImageAndInfo.fat16-_apture-dead-15>
                 53056 m.. -/-rwxrwxrwx 0       0       15      E:\_apture (deleted)
Thu Oct 28 2004 11:17:44     8814 ..c -/-rwxrwxrwx 0       0       16      E:\_ap.gif (deleted)
                  8814 ..c -rwxrwxrwx 0       0       17      <GCFAPractical2.0-USBImageAndInfo.fat16-_ap.gif-dead-17>
                  8814 ..c -/-rwxrwxrwx 0       0       17      E:\_ap.gif (deleted)
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
                    0 ..c -rwxrwxrwx 0       0       16      <GCFAPractical2.0-USBImageAndInfo.fat16-_ap.gif-dead-16>
Thu Oct 28 2004 11:17:46    8814 m.. -rwxrwxrwx 0       0       17      <GCFAPractical2.0-USBImageAndInfo.fat16-_ap.gif-dead-17>
                    8814 m.. -/-rwxrwxrwx 0       0       17      E:\/_ap.gif (deleted)
                       0 m.. -rwxrwxrwx 0       0       16      <GCFAPractical2.0-USBImageAndInfo.fat16-_ap.gif-dead-16>
                    8814 m.. -/-rwxrwxrwx 0       0       16      E:\/_ap.gif (deleted)
Thu Oct 28 2004 19:24:46    19968 ..c -/-rwxrwxrwx 0       0       18      E:\/coffee.doc
Thu Oct 28 2004 19:24:48    19968 m.. -/-rwxrwxrwx 0       0       18      E:\/coffee.doc
```

Appendix B – Contents of Recovered MS Word file "her.doc"

```
Hey I saw you the other day.  I tried to say "hi", but you
disappeared???  That was a nice blue dress you were wearing.  I heard
that your car was giving you some trouble.  Maybe I can give you a
ride to work sometime, or maybe we can get dinner sometime?

Have a nice day
```

Appendix C – Contents of Recovered MS Word file "hey.doc"

```
Hey!  Why are you being so mean?  I was just offering to help you out
with your car!  Don't tell me to get lost!  You should give me a
chance.  I'm a nice guy just trying to help you out, just because I
think you're cute doesn't mean I'm weird.  Perhaps coffee would be
better, when would be a good time for you?
```

Appendix D – Email Network Capture in Raw Format

```
POST /cgi-bin/premail/2452 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, */*
Referer: http://by12fd.bay12.hotmail.msn.com/cgi-
bin/compose?&curmbox=F000000001&a=27d6f510deac1bac5415e72029263cd9
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: by12fd.bay12.hotmail.msn.com
Content-Length: 576
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: MC1=V=3&GUID=49A9B22A05294A1A81F11881BF3C264B; y=1;
MSPAuth=5Qr3f0LU3B54zQBmCG3iUtdaiAo608EFiBYmrtzv6oAL1cQ1ayApRce4N7XCEkk%2aa5e9H9c
WS5x%21xBTivKy%2aSEwg%24%24;
MSPProf=5e1XcTCShGOf1gQhcCITXJM67JMAbywIG67BmEwf%2aNbKWq2vOyMjJTO2P1%2aaU%2av
iMTcr8nestOX6uJi5QYv9nb%21V3ReGZPm3yhrewvAYzs3vjyK4rdsGyuC2UGGRIga01ksxgsOTye%2aN6
x6RSiEoVSY1B7nwcTwqlcErZoYBZYceDYvmlHy2W1RBkki3tMoJtq2IN4ZFwblNM%24;
PIM=1%2clang%2cEN%2ctabstyle%2c4%2c
cluster%2cby12fd%252ebay12%252ehotmail%252emsn%252ecom%2ctimestamp%2c1098692237%2c
section%2cpersonal%2csubsection%2cInvalidSubSection; mid=29ede1b79f320aa332327a4460;
HMSatchmo=0; HMP1=1;
HMSC0899=224flowergirl96%40hotmail%2ecomrEM%2a5jEHcXVGV4%2aAWzQ6w%2a0KAj39KgAbJw
M3dx89O12eFCP8QpvDRxtOmG0LfDW%2azTT3QAp7%2aslY6H2QtQ5HQXNkLZglQmXIy9iEXRtDjJoz
9OYjoxLF3Ma%2axDVQGszV4go%2au43pw8jYIglxM0UW%21z0ldqqhUN1TQ4ctSsc5TvwyIbDyDgcRpT
SWI4a5eks5
ccQVXfG4uV1JekTVpqRyBUcsm9mPtf5j55s7ZhD82ttArNKHEJD92eufZJ8AVnTljxVkdfoHs%2aAyv%2a4
```

© SANS Institute 2000 - 2005 Author retains full rights.

HRUpaX5MT3RkmxfvaHdNIXwLGY3eGw2iYFxTBWHxOhAZMfocojMk6YQHaSLzEp4ueB3Cq0fUl29ndIe
9jfW71zZRlTOxLaRk0LgudQuu%2aGGwyJX%21WH%2aUfLO%2aeKlnyxDTIY35xVxy0LwJQ7wGI7fxd%
2aTBu%2apX7tNZYmw6n4bzSUMtIXi6f

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl9
6&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec29119
6189c78555223c_1098692452&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&en
codedbcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc
=&bcc=&subject=RE%3A+coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coff
ee+shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A
%0D%0ASee+you+at+7pm%21%0D%0A%0D%0A-Leila
HTTP/1.1 100 Continue

HTTP/1.1 200 OK
Connection: close
Date: Thu, 28 Oct 2004 19:10:54 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Cache-Control: private
Content-Type: text/html
X-XFS-Error: 600
HMServer: H: BAY12-F42.phx.gbl V: WIN2K3 09.09.00.0054 i D: Oct 19 2004 12:10:04 S: 0

<html><head><script language="JavaScript">
IsNotBulkEnabled=IStatus=IsPrintEnabled=NewMenu=Junk=PutInFldr=Attach=Tools="";
_UM = "curmbox=F000000001&a=ffe029b28282c8a187f262742182d9db";
</script><title>MSN Hotmail - Sent Message Confirmation</title><link rel="stylesheet" href="/cgi-
bin/dasp/EN/hotmail___9080050023.css"><script language="JavaScript" src="/cgi-
bin/dasp/EN/helppane___9080000001F.js"></script><script language="JavaScript" src="/cgi-
bin/dasp/EN/hotmail___90900000014.js"></script></head><!----><body bgcolor=#336699 ><a
name="top"><table border=0 cellpadding=0 cellspacing=0 width=100%><tr valign=top><td width=450
style="padding-top:3px;"><table border=0 cellpadding=0 cellspacing=0><tr><td nowrap> <a
href="http://g.msn.com/8HMBEN/7341??PS=9621" class="F" target="_top">MSN
Home </td><td>|</td><td nowrap> <a
href="http://g.msn.com/8HMBEN/7342??PS=9621" class="F" target="_top">My
MSN </td><td>|</td><td
nowrap> Hotmail </td><td>|</td><td nowrap> <a href="http://g.msn.com/8HMBEN/7345??PS=9621"
class="F" target="_top">Shopping </td>.<td>|</td><td
nowrap> <a href="http://g.msn.com/8HMBEN/7346??PS=9621" class="F"
target="_top">Money </td><td>|</td><td
nowrap> <a
 href="http://g.msn.com/8HMBEN/7347??PS=9621" class="F" target="_top">People &
Chat </td></tr></table></td><td> </td><td><a
href="http://by12fd.bay12.hotmail.msn.com/cgi-
bin/logout?curmbox=F000000001&a=ffe029b28282c8a187f262742182d9db&t=1098692544&loru=&id=
2&fs=1&cb=_lang%3dEN%26country%3dUS&ct=1098692544"><img border=0
src="http://64.4.55.109/crs_918.gif" alt="Sign out of .NET Passport sites" width="66"
height="19"></td><td> </td><td nowrap valign=middle><label for="q">Web Search:</label></td><td><span
style="width:6px;"> </td><td width=100% nowrap valign=middle><form method="GET"
name="websearch" action="http://search.msn.com/results.asp" style="margin-bottom:0px;margin-
bottom:0px;"><input type="Hidden" name="RS" value="CHECKED"><input type="Hidden" name="Form"
value="HM"><input type="Hidden" name="cp" value="1252"><input type="Hidden" name="v"

© SANS Institute 2000 - 2005, Author retains full rights.

value=1><input type="text" id="q" n
ame="q" size=14 accesskey="S" style="WIDTH:65%"><input
type="submit" value="Go" size=4></form></td></tr></table><table border=0 cellpadding=0 cellspacing=0
width=100%><tr><td><img src="http://64.4.55.109/spacer.gif" width=1 height=5></td></tr><tr><td
width=100% align=center></td></tr></table><table border=0 cellpadding=0 cellspacing=0 width=100%
><tr><td colspan=2><img src="http://64.4.55.109/spacer.g
if" height=1 width=779></td></tr><tr><td><table border=0 cellpadding=0 cellspacing=0 width=100%><tr>
<td rowspan=2 background="http://64.4.55.109/tab.bg.dln.gif"><a
href="http://g.msn.com/1HMCEN/141??PS=9621" target="_top"><img
src="http://64.4.55.109/lgo_msn_118x35.gif" width=118 height=35 border=0 alt="go to MSN"></td><td
rowspan=2 background="http://64.4.55.109/tab.bg.dln.gif" nowrap>Hotmail</td><td
rowspan=2><img src="http://64.4.55.109/tab.slide.hm.li.gif"></td><td colspan=12 height=13
bgcolor=#336699></td></tr><tr><td><img src="http://64.4.55.109/tab.separator.off.gif"></td><td
background="http://64.4.55.109/tab.bg.off.gif" nowrap>   <a href="javascript:G('/cgi-
bin/hmhome?');" tabindex=120 class="E">Today   </td><td><img
src="http://64.4.55.109/tab.separator.on.l.gif"></td><td background="http://64.4.55.109/tab.bg.on.gif"
nowrap>   <a href="/cgi-
bin/HoTMaiL?curmbox=F000000001&a=ffe029b28282c8a187f262742182d9db" tabindex=121 clas
s="E">Mail   </td><td><img src="http://64.4.55.109/tab.separator.on.r.gif"></td><td
background="http://64.4.55.109/tab.bg.off.gif" nowrap>   <a
href="http://calendar.msn.com/calendar/isapi.dll" tabindex=122
class="E">Calendar   </td><td><img
src="http://64.4.55.109/tab.separator.off.gif"></td><td background="http://64.4.55.109/tab.bg.off.gif"
nowrap>   <a href="jav
ascript:G('/cgi-bin/addresses?');" tabindex=123
class="E">Contacts   </td><td><img
src="http://64.4.55.109/tab.separator.end.gif"></td><td background="http://64.4.55.109/tab.bg.sln.gif"
width=100%> </td></tr></table></td><td valign=bottom><table border=0 cellpadding=0
cellspacing=0 width=100%><tr><td background="http://64.4.55.109/tab.bg.sln.gif"><img
src="http://64.4.55.109/spacer.gif" width=1 height=35></td><td
background="http://64.4.55.109/tab.bg.sln.gif" nowrap align=right><a href="/cgi-
bin/options?section=mail&subsection=&curmbox=F000000001&a=ffe029b28282c8a187f262742182d9d
b" class="G">Options | <a
href="javascript:CPH('PIM_SentMessageConf');"
class="G">Help   </td></tr></table></td></tr></table><table border=0
cellpadding=0 cellspacing=0 width="100%"><tr bgcolor="#4791C5"><td colspan=3><img
src="http://64.4.55.109/spacer.gif" height=1 width=779></td></tr><tr bgcolor="#4791C5"><td
style="padding-left:10px;height:
20px;border-bottom"><table border=0 cellpadding=0 cellspacing=0 width="100%"><tr><td width=100%
align="left" valign="middle">flowergirl96@hotmail.com</td></tr></table></td><td
align=right style="padding-left:10px;height:20px;border-bottom"><table border=0 cellpadding=0
cellspacing=0><tr><td align="right" valign="middle"><a href="http://g.msn.com/8HMBEN/9848??PS=9621"
class="G" target="_top">Free Newsletters | <a href="http://g.msn.com/8HMBENUS/9851??PS=9621"
class="G" target="_top">MSN Featured Offers </td></tr></table></td></tr></table><iframe
id="Hfrm" class="NN"></iframe><table border=0 cellpadding=0 cellspacing=0 width=100% class="N"
style="border-bottom:1px solid #FFFFFF" id="HMTB"><tr><td colspan=2><img
src="http://64.4.55.109/spacer.gif" height=1 width=266></td></tr><tr><td><table border=0 cellpadding=0
cellspacing=0 width=100% class="O"><tr><td style="width:8px"><img src="http://64.4.55.109/spacer.gif"
height=1 width=8></td><td class="P" nowrap onmouseover="MO()" onmouseout="MU()" onclick="G('/cgi-
bin/compose?');"><img src="http://64.4.55.109/i.p.writenew.gif" border=0 align=absmiddle hspace=1
alt="New"> New
Message</td><td class="LL">|</td><td class="P" nowrap onmouseover="MO()" onmouseout="MU()"
onclick="G('http://calendar.msn.com/calendar/isapi.dll?request=view&operation=new&uicode1=ad
dappointment');"><img src="http://64.4.55.109/i.p.cal.gif" border=0 align=absmiddle hspace=1
alt="Calendar"> <a href="#"
onclick="G('http://calendar.msn.com/calendar/isapi.dll?request=view&operation=new&uicode1=addappoint
ment');return false;" tabindex=1>New Appointment</td><td class="LL">|</td><td class="P" nowrap

© SANS Institute 2000 - 2005 Author retains full rights.

```
onmouseover="MO()" onmouseout="MU()" onclick="G('/cgi-
bin/doaddresses?strUsrFltr=&strUsrView=&strAlphNav=&_HMaction=
Create')"><img src="http://64.4.55.109/i.p.cont.individual.gif" border=0 align=absmiddle hspace=1
alt="Contact"> <a href="#" onclick="G('/cgi-
bin/doaddresses?strUsrFltr=&strUsrView=&strAlphNav=&_HMaction=Create');return false;"
tabindex=1>New Contact</a></td><td width=100%> </td></tr></table></td><td
style="CURSOR:auto"><table border=0 cellpadding=0 cellspacing=0 width=100% class="O"><tr><td
width=100%> </td></tr></table></td></tr><tr><td colspan=2><img
src="http://64.4.55.109/spacer.gif" height=1 width=779></td></tr></table><script language="JavaScript">
function subForm()
{
var trkChk=0;
if (frm && frm != "undefined")
{
for(i=0; i < frm.length; i++)
{
if (frm.elements[i].type == 'checkbox')
{
if (frm.elements[i].checked)
trkChk++;
}
}
if (trkChk>0)
return true;
else
{
Err("150995871");
return false;
}
}
}
</script><table border=0 cellpadding=0 cellspacing=0 width=100% bgcolor=#FFFFFF><tr><td valign=top
width=173 bgcolor=#DBEAF5><table border=0 cellspacing=0 cellpadding=0 width=100%><tr><td width=1
00% valign=top bgcolor=#87b3d0 style="padding:10px;border-bottom:1px solid #FFFFFF"><table
border=0 cellspacing=0 cellpadding=0 width=100%><tr><td valign=top><font class="BB">Today on
MSN</font></td></tr><tr><td valign=top><table border=0 cellpadding=2 cellspacing=0><tr><td><img
src='http://64.4.55.109/i.p.white.b.gif' align='absmiddle'></td><td><a
href="http://g.msn.com/0US!s6.470_6199/95.a38/1??cm=ConfTodayOnMSN??PS=9621" target="
_top">Download Shania's greatest...</a></td></tr><tr><td><img src='http://64.4.55.109/i.p.white.b.gif'
align='absmiddle'></td><td><a
href="http://g.msn.com/0US!s6.470_6199/95.c38/2??cm=ConfTodayOnMSN??PS=9621" target="_top">8
ways to win at work</a></td></tr><tr><td><img src='http://64.4.55.109/i.p.white.b.gif'
align='absmiddle'></td><td><a
href="http://g.msn.com/0US!s6.470_6199/95.c38/3??cm=ConfTodayOnMSN??PS=9621"
target="_top">Are you bitter about love?</a></td></tr><tr><td><img src='http://64.4.55.109/i.p.white.b.gif'
align='absmiddle'></td><td><a
href="http://g.msn.com/0US!s6.470_6199/95.b38/4??cm=ConfTodayOnMSN??PS=9621"
target="_top">Romantic places to dine</a></td></tr></table></td></tr><tr><td valign='top' style='padding-
top:6px;'><a href="http://g.msn.com/0US!s7.471_6199/7.c39/2??cm=ConfSmallPic??PS=9621"><img
border=0 src="http://sc.msn.com/@K/-IGIS_RKU32KYBNJDJEA3.jpg" alt="Man and woman holiday
shopping (. Andreas Pollok/Getty Images)" width="68" align="left"></a><font class="BB"
color=#B73032>On
ly on MSN</font><br><a
href="http://g.msn.com/0US!s7.471_6199/7.c39/1??cm=ConfSmallPic??PS=9621" target="_top">Win a
$100 holiday shopping spree</a></td></tr></table></td></tr><tr><td height=33 valign=bottom><IFRAME
FRAMEBORDER=0 SCROLLING=NO MARGINHEIGHT=0 MARGINWIDTH=0 WIDTH=109 HEIGHT=23
SRC="http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=HOTA43?SC=LG?HM=0450474d554b105157
56564b414671700a4f6f511634520d5d525d51470c32530d606a?LOC=I?
```

© SANS Institute 2000 - 2005, Author retains full rights.

TF=adframe?ID=000600008EAA48DA?UC=100?PS=8307?PI=44364?AP=1447" tabindex="-1"></IFRAME></td></tr><tr><td height=33 valign=bottom><IFRAME FRAMEBORDER=0 SCROLLING=NO MARGINHEIGHT=0 MARGINWIDTH=0 WIDTH=109 HEIGHT=23 SRC="http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=HOTB43?SC=LG?HM=0450474d554b10515756564b414671700a4f6f511634520d5d525d51470c32530d606a?LOC=I?TF=adframe?ID=000600008EAA48DA?UC=100?PS=8307?PI=44364?AP=1447" tabindex="-1"></IFRAME></td></tr><tr><td height=33 valign=bottom><IFRAME FRAMEBORDER=0 SCROLLING=NO MARGINHEIGHT=0 MARGINWIDTH=0 WIDTH=109 HEIGHT=23 SRC="http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=HOTC43?SC=LG?HM=0450474d554b10515756564b414671700a4f6f511634520d5d525d51470c32530d606a?LOC=I?TF=adframe?ID=000600008EAA48DA?UC=100?PS=8307?PI=44364?AP=1447" tabindex="-1"></IFRAME></td></tr><tr><td height=33 valign=bottom><IFRAME FRAMEBORDER=0 SCROLLING=NO MARGINHEIGHT=0 MARGINWIDTH=0 WIDTH=109 HEIGHT=23 SRC="http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=HOTD43?SC=LG?HM=0450474d554b10515756564b414671
700a4f6f511634520d5d525d51470c32530d606a?LOC=I?TF=adframe?ID=000600008EAA48DA?UC=100?PS=8307?PI=44364?AP=1447" tabindex="-1"></IFRAME></td></tr><tr><td height=10></td><tr></table></td><td style="padding:10px;" valign=top><table border=0 cellspacing=0 cellpadding=0 width=100%><form method=POST name="addtoAB" onsubmit="javascript:return subForm();" action="/cgi-bin/domsgaddresses" style="margin:0px;"><input type="hidden" name="curmbox" value="F000000001">
<input type="hidden" name="HrsTest" value="">
<input type="hidden" name="type" value=""><input type="hidden" name="msg" value=""><input type="hidden" name="soid" value=""><input type="hidden" name="wcid" value=""><input type="hidden" name="from" value="premail"><input type="hidden" name="action" value="ModifyConfirmSend"><input type="hidden" name="allbox"><tr><td style="padding:5" bgcolor=#A0C6E5 nowrap width="100%"><img src="http://64.4.55.109/i.p.send.gif">Your message has been sent to:</td><td bgcolor=#A0C6E5 align=center style="width:60px;">Save
Address:</td></tr><style>
.TName.{border-bottom:1px solid #DBEAF5;padding:4px;}
.TStat.{border:1px solid #A0C6E5;border-top:none;padding:4px;}
</style><tr><td colspan=3> <table border=0 cellpadding=0 cellspacing=0 width=100% id="RecpTab"><tr><td width=100% bgcolor=#A0C6E5></td><td bgcolor=#A0C6E5><img src="http://64.4.55.109/spacer.gif" height=1 width=60></td></tr><tr><td cl
ass="TName">SamGuarillo@hotmail.com</td><td class="TStat" align=center bgcolor=#DBEAF5><input tabindex="1" type="checkbox" onclick="javascript:CCA(this);doThisTD(this);" name="ADDRSamGuarillo@hotmail.com" value="ADDRSamGuarillo@hotmail.com" title="save address "></td></tr></table> </td></tr><tr><td style="padding:5" nowrap> </td><td bgcolor="#DBEAF5" align=center style="padding:7" class="TStat"><input tabindex="2" type="submit" name="save" value="Save" class="A"></td></tr><tr><td></td><td><img src="http://64.4.55.109/spacer.gif" height=1 width=61></td></tr><tr><td colspan=3 style="padding-top:10px;padding-bottom:23px;">Return to Inbox</td></tr></form></table><table border=0 cellpadding=5 cellspacing=0 width=100% bgcolor=#FFFFFF style="border:1px solid #87b3d0"><tr><td colspan=2 bgcolor=#DBEAF5>Send larger photos and other attachments </td></tr><tr><td colspan=2>With MSN Hotmail Plus, you can send attachments up to 20MB in size for only $19.95 per year. </td></tr>.<tr><td><img src="http://ads.msn.com/ads/pronws/HM010804mailbox.gif" border=0 width=49 height=49></td><td width=100% valign=top><table border=0 cellpadding=0 cellspacing=0 width=100%><tr><td valign=top><img src="http://64.4.55.109/i.p.black.b.gif" vspace=5 hspace=5 border=0></td><td valign=top><a href="
http://g.msn.com/8HMBENUS/8283??PS=9621" target="_top">Includes an increased inbox limit of 2GB</td></tr><tr><td valign=top><img src="http://64.4.55.109/i.p.black.b.gif" vspace=5 hspace=5 border=0></td><td valign=top>And Web e-mail with no graphical ads. </td></tr></table></td>.</table></td><td style="padding-top:10px;" valign=top><IFRAME FRAMEBORDER=0 SCROLLING
=NO MARGINHEIGHT=0 MARGINWIDTH=0 WIDTH=300 HEIGHT=250

© SANS Institute 2000 - 2005 Author retains full rights.

```
SRC="http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=HOTM44?SC=PP?HM=0450474d554b105157
56564b414671700a4f6f511634520d5d525d51470c32530d606a?LOC=H?TF=_NEW?ID=000600008E
AA48DA?UC=100?PS=9621?PI=44364?AP=1089" tabindex="-1"></IFRAME></td><td
width=100%></td></tr><tr><td bgcolor=#DBEAF5><img src="http://64.4.55.109/spacer.gif" height=1
width=173></td><td><img src="http://64.4.55.109/spacer.gif" height=1 width=306></td><td><img
src="http://64.4.55.109/spacer.gif" height=1 width=300></td><td></td></tr></table><script
language="javascript">
var frm = document.addtoAB;
function doThisTD(sm_cb)
{
if (sm_cb.parentElement.parentElement.className=='H')
sm_cb.parentElement.style.backgroundColor = '#C1CDD8';
else
sm_cb.parentElement.style.backgroundColor = '';
}
</script><table border=0 cellpadding=0 cellspacing=0 width=100%><tr><td height=24
colspan=2>   <a href="http://g.msn.com/8HMBEN/9853??PS=9621" class="HH">Get
the latest updates from MSN</a>...</td><
/tr><tr><td height=24><table border=0 cellpadding=0 cellspacing=0><tr><td nowrap>  <a
href="http://g.msn.com/8HMBEN/7341??PS=9621" class="F" target="_top">MSN
Home</a>  </td><td><font class="G">|</font></td><td nowrap>  <a
href="http://g.msn.com/8HMBEN/7342??PS=9621" class="F" target="_top">My
MSN</a>  </td><td><font class="G">|</font></td><td nowrap>  <font
class="F">Hotmail</font>&
#160; </td><td><font class="G">|</font></td><td nowrap>  <a
href="http://g.msn.com/8HMBEN/7344??PS=9621" class="F"
target="_top">Search</a>  </td>.<td><font class="G">|</font></td><td
nowrap>  <a href="http://g.msn.com/8HMBEN/7345??PS=9621" class="F"
target="_top">Shopping</a>  </td>.<td><font class="G">|</font></td><td
nowrap>  <a href="http://g.msn.com/8HMBEN/7346??PS=9621" class="F"
target="_top">Money</a>  </td><td><font class="G">|</font></td><td
nowrap>  <a href="http://g.msn.com/8HMBEN/7347??PS=9621" class="F"
target="_top">People & Chat</a>  </td></tr></table></td><td nowrap align=right><a
href="http://g.msn.com/0nwenus0/A9/23??PS=9621&DI=9621" class="G"
target="_NEW">Feedback</a>  <font class="G">|</font>  <a
href="javascript:CPH('PIM_SentMessageConf');"
class="G">Help</a>   </td></tr><tr><td height=20 style="BORDER-TOP:1px solid
#87b3d0" nowrap colspan=2> <font class="G">&copy
```

```
; 2004 Microsoft Corporation. All rights reserved.</font> <a
href="http://g.msn.com/8HMBEN/12264??PS=9621" target="_top" class="G">TERMS OF
USE</a>  <a href="http://g.msn.com/1HMCENUS/164??PS=9621" target="_top"
class="G">Advertise</a>  <a href="http://g.msn.com/8HMBEN/12263??PS=9621"
target="_top" class="G">TRUSTe Approved Privacy Statement</a>  <a
href="http://g.msn.com/0nwenus0/A7/24??PS=9621" class=
```

```
"G">Anti-Spam Policy</a></td></tr><tr><td colspan=2><img src="http://64.4.55.109/spacer.gif" height=1
width=779></td></tr></table><IMG
SRC="http://h.msn.com/c.gif?RF=http%3a%2f%2fby12fd%2ebay12%2ehotmail%2emsn%2ecom%2fcgi%
2dbin%2fcompose%3f%26curmbox%3dF000000001%26a%3d27d6f510deac1bac5415e72029263cd9&
PI=44364&DI=7474&PS=9621" width=1 height=1></body></html><!-- H: BAY12-F42.phx.gbl -->
<!-- V: WIN2K3 09.09.00.0054 i -->
<!-- D: Oct 19 2004 12:10:04-->
<!-- S: 0-->
```

© SANS Institute 2000 - 2005 Author retains full rights.