Office of the Attorney General
High Tech Crimes Bureau
Regional Computer Forensic Lab - Chicago

RCFL Case Number:	HTCB-06-01-1028
Case Agent:	Detective William Martin Schiller Park Police Department
Forensic Examination Performed by:	Shahna G. Monge, EnCE Senior Computer Evidence Recovery Technician Illinois Attorney General's Office High Tech Crime Bureau Chicago, IL 60601
Case Classification:	Computer Tampering
Suspect (Case Name):	Annabel Melongo
High Tech Crimes Bureau:	A.A.G. David Haslett, Bureau Chief Deputy Chief of Investigations Daniel Ferraro Deputy Chief Michael Sullivan – ICAC Coordinator A.A.G. Abigail Abraham, Prosecutor A.A.G. Kyle French, Prosecutor A.A.G. Elizabeth Lepic, Prosecutor

Forensic Procedure Summary:

The hard drive from the computer system relating to this case was locked (write-protected) via the use of the Encase Fast Bloc IDE to SCSI imaging device. The hard drive was then imaged to a separate hard drive within the forensic computer. The ZIP media was imaged to the same hard drive within the forensic computer, and a separate file was created for each ZIP disk. The ZIP media was acquired though Encase's network acquisition and the ZIP drive was locked to prevent writing to the media through Encase in DOS mode before the acquisition was begun. The CD media was imaged to the same hard drive within the forensic computer, and a separate file was created for each CD. The forensic CD drive does not have writing capabilities. The USB thumb drive was imaged to the same hard drive within the forensic computer. The thumb drive was write-blocked by the use of a Windows registry change that prohibits any writes being made to any media connected via USB.

This imaging process entailed the creation of an evidence file (disk image) in which the hard drive/ZIP/CD/USB thumb drive were recreated sector by sector in a forensic environment utilizing forensic software licensed and registered to Shahna G. Monge, Senior Computer Evidence Recovery Technician and/or the Illinois Attorney General.

This process allowed the forensic examination to proceed without altering any of the original files from the suspect media, and also preserved File, Disk and Volume Slack. This also allowed the unallocated sectors of the disk to be searched and examined. The process detailed above also allowed for forensic examination of RAM Slack.

Forensic Report Summary:

I reviewed the case files provided by Detective Martin, Schiller Park Police Department. After review of the search warrant, it was determined that I would attempt to recover any information that would constitute evidence of the offense Computer Tampering and also determine ownership/control and/or dominion over the data.

The forensic examination was completed and forensic reports are listed under their respective names and were provided as separate documents (files) to Detective Martin.

During the course of the examination I observed the following:
Please refer to the included Forensic Report for detailed information regarding the following.

- Two link files were found in the Recycle Bin for a network connection to Save A Life Foundation.
- Log files for the program Go To My PC were discovered. Go To My PC is a program that allows remote access to another computer.
- A log file for the Jakarta service were discovered that contained entries for the specific date and time of the intrusion. Jakarta is a project to create an open-source java-based server.
- Connection settings were found in the Microsoft network connections phonebook resident on the laptop computer.
- Within a restore point “snapshot” that was automatically created by the computer, there was a text document discovered named “domain.txt” that contains information relating to a computer on the domain savealifefou.
- A cookie file containing IP information for comcast server with IP 24.15.202.102 was discovered. File last written 04/28/06 09:43:13hrs.
- Several instances of the IP 24.15.202.102 were discovered on the evidence. Please see the forensic report for further details.
- The URL f·t·p·:·/·/·7·0·.·1·4·2·.·2·5·1·.·2·4·2·/·· was found in the registry in the folder "TypedURLs" for Windows user Administrator. It also shows that an FTP session (or file transfer protocol) session was initiated by the Windows user Administrator for the IP 70.142.251.242.

- The IP shown of 24.15.202.102 was located in the registry in the folder "TypedURLs". It is shown as it was typed by the Windows user Administrator.
- The URL h·t·t·p·:·/·/·w·w·w·.·g·o·t·o·m·y·p·c·.·c·o·m·/··· was found in the registry in the folder "TypedURLs" by the Windows user Administrator.
- The URL h·t·t·p·:·/·/·m·a·i·l·.·s·a·l·f·.·o·r·g·/··· was found in the registry in the folder "TypedURLs" for Windows user Administrator.
- What appears to be user name and password (carol@salf.org:herman·) for the website www.salf.org:2095/Webmail. was found in the Protected Storage System Provider folder for SID (System ID) that corresponds to Windows user Administrator.
- s·g·h·o·l·a·r·@·s·a·l·f·.·o·r·g···s·g·h·o·l·a·r·8·8·9·9··· appears to be information typed in at URL shown of http://70.142.251.241/
- The URL of f·t·p·:·/·/·7·0·.·1·4·2·.·2·5·1·.·2·4·2·/·d·o·c·u·m·e·n·t·s··· was found in the registry in the folder "TypedURLs" for Windows user Administrator. It also shows that an FTP session (or file transfer protocol) session was initiated by the Windows user Administrator for the IP 70.142.251.242 and the folder "documents"
- The executable file for the setup of the program Go To My PC, which allows remote access to other computers, was discovered under the Administrator account on the laptop computer.
- The executable file for the program Go To My PC, which allows remote access to other computers, was discovered under the Administrator account on the laptop computer.
- Several web pages (.htm) files were discovered that showed emails associated with melongo_Annabel@yahoo.com and what appears to be Annabel Melongo's Roosevelt University email account that contain references to different individuals with Save A Life Foundation. Please see the forensic report for more detailed information. These pages can also be viewed separately and can be found in the folder named "Email".
- One Word document was discovered that contained the name "Saquan Gholar"
- Connection information for "scantron" was discovered shown in a java script page contained within a folder named "new version", located on a USB thumbdrive.
- A URL was discovered for http://70.236.105.150 that was titled Scantron System.
- A URL was discovered for http://70.142.251.241 that was titled SALF Scantron System.
- Several different files that appear to relate to ID cards for various SALF employees were discovered. This information was found in a folder on a USB thumbdrive named "TMP".
- Several images that appear to be parts of a website associated with Save A Live Foundation were discovered. These images were found in a folder named "IMAGES", which was located on a USB thumbdrive.
- Several different files were discovered that appear to be database items from Save A Life Foundation.
- Several images, documents and one web page were discovered that contain information relating to ownership/control and/or dominion over the data.
- The Recycle Bin report is also included that shows files that were contained in the recycle bin before it was emptied.

The Media Report can be found here and it contains information pertaining to the evidence that was turned over to our lab for analysis.

The Duplicate Digital Evidence (DDE), created on CD, will remain in the ESR until termination of this investigation. The DDE created on the forensic computer hard drive will be erased in preparation for future unrelated examinations.

The original evidence is to be returned to Detective Martin for retention.

Appendix A

Appendix B

Reporting Examiner: Shahna G. Monge, EnCE
Senior Computer Evidence Recovery Technician
Office of the Illinois Attorney General – High Tech Crime Bureau
188 W. Randolph, Chicago, IL