Procedure for Windows Incident Response

Scope: The purpose of this document is to assist the assigned investigator when a Request for Computer Forensic Examination(link) is submitted to the SIRT. If it is determined to be a Windows based system that needs to be investigated, this document provides the tools and procedures for gathering the information needed to analyze and resolve the incident.

Initial Steps: The Request for Computer Forensic Examination should give the investigator a summary of the type of incident as stated by the requestor. Provided with this information the investigator should plan for the correct response that will yield the information needed to fully understand the scope of the incident. The investigator should be equipped with the necessary tools and be able to tailor them to meet the needs of each individual incident.

In any type of incident the investigator should be focused on obtaining the following information:

1. System date and time
2. Who is logged in to the system (including remote-access users, if applicable)
3. Open network ports
4. Applications associated with the open ports
5. All running processes
6. Timestamps and checksums on all files
7. Systems that have current or had recent connections to the system
8. System event logs
9. Possible forensic duplication of system hard drive and/or physical memory

It is very important to preserve and not destroy or alter any evidence obtained during the initial response. While it is preferred that no changes occur to the system, depending on the tools that are used, there are times when footprints are left by the investigator. Complete documentation of the steps taken must be kept in order to verify the data that was obtained.

Tools: There are many different tools that can be used to perform the initial response in order to gather sufficient information. The investigator has the option to build their own toolkit or use a preconfigured kit or script that will perform the response. It is generally recommended to have a hybrid collection of tools containing utilities and trusted commands that can be used in various circumstances. Below are some links to utilities that could be beneficial while performing incident response:

Helix 3: A live-response forensic suite that can be run from CD or USB
http://www.e-fense.com/helix3-download.php

Sysinternals: Utilities to help you troubleshoot and diagnose your Windows systems and applications.
http://live.sysinternals.com/

MIR-ROR is a security incident response specialized, command-line script that calls specific Windows Sysinternals tools, as well as some other useful tools, to provide live capture data for investigation.
http://mirror.codeplex.com/

Windows Examination Checklist

Main role of the system :
□ Workstation □ Domain Controller(AD) □ DNS Server □ DHCP Server □File Server
□ Mail Server □ Web/Application Server(IIS, ASP.NET) □ Print Server □ Terminal Server

□	Windows version documented
□	Last boot time documented
□	Last shutdown time documented
□	“Local” vs. “real” date/time delta identified and resolved
□	File system partitions examined and documented
□	Examine log and event files
□	Check for new/odd user accounts and groups
□	Check startup application and services at boot
□	Check network configuration and activity
□	Check for unauthorized processes
□	Check for unauthorized shares
□	Examine jobs run by the scheduler service
□	Look for unusual or hidden files
□	Check system binaries for changes
□	Check for altered permissions on files or registry keys
□	Forensic duplication of the hard drive from the system
□	Summary of findings/report/conclusions/opinion written

The following is a list of tools and a description of the function they perform:

Tool	Description
cmd	The command prompt
loggedon, psloggedon, logonsessions	A utility that shows all users connected locally and remotely
netstat	Enumerates all listening ports and all current connections to those ports
arp	Shows the MAC addresses of the systems that the target machine has been communicating with, within the last minute
srvinfo, psinfo	Displays system information
showacls	Displays the access control list
tasklist	Resolves processes that run in the context of another service
psfile	Shows what files are opened remotely
autoruns	See what programs are configured to startup automatically when your system boots and you login.
listDLLs	List all the DLLs that are currently loaded, including where they are loaded and their version numbers.
psfile	shows a list of files on a system that are opened remotely
psloglist	lets you dump the contents of an Event Log on the local or a remote computer.
psservice	displays the status, configuration, and dependencies of a service
md5sum	Calculates and verifies hashes of files
dd	Provides byte-exact copy of data

Conclusion: The initial information gathering will provide assistance to determine the severity of the incident and form the basis for the level of response that is needed. While performing the response you should use this document and the Incident Response Checklist(link) to record your initial findings. The checklist and any notes taken should be sufficient enough to then fill out a Security Incident Report(link) and continue the incident response process defined by the UCF SIRT.