COFEE v1.1.2 – Runner & NW3C Profiles

Validation Study

9/29/2009

Written and Tested By:

Justin Wykes, CFCE

Computer Crime Specialist, NW3C

Additional Testing By:

Mark Bowser, CFCE

Computer Crime Specialist, NW3C

NW3C

NW3C, Inc., d/b/a the National White Collar Crime Center, is a 501c3 non-profit corporation under the United States Internal Revenue Tax code, incorporated in the Commonwealth of Virginia. NW3C has more than a 30-year history in serving State, Local, and Tribal Law Enforcement.

NW3C's no-cost membership, training, and services are extended to all Law Enforcement, regulatory and prosecutorial agencies. NW3C is governed by a Board of Directors elected from member law enforcement agencies. The Board establishes strategic direction in accordance with the NW3C corporate bylaws, grant conditions, and other appropriate guidelines, such as applicable Office of Management and Budget (OMB) circulars and the OJP *Financial Guide*.

What NW3C Does

NW3C's primary area of service to justice agencies is training, and since 1996 has been the nation's leading provider of no-cost Investigative and Forensics Computer Crime and Digital Evidence training to State, Local, and Tribal Law Enforcement. Through a combination of training and critical support services, NW3C equips state and local law enforcement agencies with skills and resources they need to tackle emerging economic and cyber crime problems.

For the general public, NW3C provides information and research so they too may become proactive in the prevention of economic and cyber crime. Victims of crimes can rely on NW3C to help them register Internet crime complaints through their website at **www.ic3.gov** and notify the appropriate authorities at local, state, and federal levels promptly, accurately, and securely.

A congressionally funded non-profit organization, NW3C has been continuously funded for the past 28 years in support of state and local enforcement efforts. NW3C is a national program with a presence in all 50 states.

Membership in NW3C is free and open to federal, state, local and international law enforcement; regulatory and prosecution agencies; as well as duly constituted permanent task forces. Neither individuals nor private companies are eligible for membership.

This project was supported by Grant No. 2008-CE-CX-0001 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

Table of Contents

Introduction

The purpose of this report is to document the validation of Computer Online Forensic Evidence Extractor's (COFEE) generated thumb drives which were created using the two NW3C collection profiles: "NW3C – Volatile Data" and "NW3C – Incident Response."

Tool Tested:	Computer Online Forensic Evidence Extractor
Version:	1.1.2
Run Environments:	Windows XP Service Pack 2 and Windows XP Service Pack 3
Supplier:	Microsoft & NW3C

Purpose and Scope

This validation study was conducted, in conjunction with the validation study titled "COFEE GUI CONSOLE," to verify that the COFEE suite functions properly. This document focuses on the validation of the COFEE generated thumb drives.

COFEE's primary purpose is to create a thumb drive which contains a pre-determined set of applications which are set to run on a suspect's live machine. Upon connecting a COFEE generated thumb drive to a suspect's machine, the investigator executes *runner.exe* (a program located on the thumb drive) which, in turn, executes all of the programs specified by COFEE, and stores the data collected on the investigator's thumb drive.

The programs placed on the generated thumb drives are identified by a "profile" loaded into COFEE. While any user can create their own profile, this validation study will focus only on the profiles created by NW3C: "NW3C – Volatile Data" and "NW3C – Incident Response."

This validation study was conducted to ensure that when *runner.exe* is executed: all of the programs identified by the profile are executed, that the collected data is stored on the investigator's thumb drive, that no applications were run from the suspect's machine, and that no unacceptable writes were made to the suspect's machine.

COFEE is currently only supported on the Microsoft Windows XP operating system. No other operating system was tested during this validation study.

Test Result Summary

Overall Result

Testing conducted on Runner and the NW3C profiles verified that both the *runner.exe* application, as well as the selected programs, functioned as expected and are well within acceptable practices for data collection on a live system.

NW3C – Volatile Data Profile

There were no writes to the suspect drive's file system using this profile.

There were updates made to the Windows Registry on the suspect's machine, however none of the registry updates were of obvious forensic value. For specific information on what keys were written to, see "Test Results."

NW3C – Incident Response Profile

This profile caused three writes to the suspect drive's file system. All three writes were caused by the program *handle.exe* and were made to the file "PROCEXP100.sys." The reference to the file PROCEXP100.sys is hard-coded into *handle.exe*, a product of Sysinternals, and as such it is not possible to restrain *handle.exe* from writing to this file. However, this file is specifically written as part of the Sysinternals' toolset and is not of evidentiary interest.

There were also updates made to the Windows Registry on the suspect's machine, however none of the registry updates were of obvious forensic value. For specific information on what keys were written to, see "Test Results."

During the testing of the Incident Response Profile, one test (RunnerTest012) fell outside of normal parameters. During this test, *handle.exe* did not write to the file PROCEXP100.sys, or any registry entries related to PROCEXP100. This anomaly occurred during only one test, and as it caused even fewer writes, does not affect the overall outcome of this validation.

Test Assertions

The following assertions were based upon the listed features of COFEE, as well as adherence to accepted forensic practices on a live machine.

1. All programs identified in the profile were executed.
2. Results of the tools were properly stored on the investigator's thumb drive.
3. Executing runner.exe did not cause any direct writes to the suspect drive (file system).
4. Executing runner.exe did not cause any direct writes to the suspect drive (registry).
5. The tools executed were run from the thumb drive, not from the suspect's machine.

Testing Environment

Test Computer

1. Gateway 600YG2 Laptop ("Abe")
    a. Serial Number: 0029567634
    b. Intel Pentium 4 – Mobile 2.00 GHz
    c. 512 MB RAM
    d. PATA 2.5" Hard Drive

        i. IBM IC25N030ATCS04-0 30GB Hard Drive
        ii. Serial Number: DAH4W0AB
        iii. Contained 1 Primary Partition which was reported at 27.94 GB
    e. Integrated Network Card
2. Dell Latitude D820 Laptop ("Eli")
    a. Intel Centrino Duo T2500 2.00GHz
    b. 2 GB RAM
    c. SATA 2.5" Hard Drive
        i. Seagate Momentus 60GB 5400 RPM
        ii. Serial Number: 5PJ3J3FR
        iii. Contained 1 Primary Partition which was reported at 55.88 GB
    d. Integrated Network Card
3. Dell Latitude D820 Laptop ("Jenny")
    a. Intel Centrino Duo T2500 2.00GHz
    b. 2GB RAM
    c. SATA 2.5" Hard Drive
        i. Seagate Momentus 60GB 5400 RPM
        ii. Serial Number: 5PJ31XJM
        iii. Contained 1 Primary Partition which was reported at 55.88 GB
    d. Integrated Network Card
4. Digital Intelligence Forensic Recovery of Evidence Device (FRED) Tower ("Jim")
    a. Serial Number: F0039002127
    b. Intel Pentium 4 2.4 GHz
    c. 1 GB RAM
    d. PATA 3.5" Hard Drive
        i. Maxtor DiamondMax Plus 9 80GB
        ii. Serial Number: Y2B7HYVE
        iii. Contained 1 Primary Partition which was reported at 76.33 GB
    e. Integrated Network Card
5. Gateway 600YG2 Laptop ("Pat")
    a. Serial Number: 0029567607
    b. Intel Pentium 4 – Mobile 2.00 GHz
    c. 512 MB RAM
    d. PATA 2.5" Hard Drive
        i. IBM IC25N030ATCS04-0 30GB
        ii. Serial Number: DAH4VJNB
        iii. Contained 1 Primary Partition which was reported at 27.94 GB
    e. Integrated Network Card
6. Digital Intelligence Forensic Recovery of Evidence Device (FRED) Tower ("Paul")
    a. Serial Number: F0039002132
    b. Intel Pentium 4 2.4 GHz
    c. 1 GB RAM

d. PATA 3.5” Hard Drive
    i. Maxtor DiamondMax Plus 9 80GB
    ii. Serial Number: Y2B7KF6E
    iii. Contained 1 Primary Partition which was reported at 76.33 GB
e. Integrated Network Card

Support Software Used

1. Process Monitor was used to record all processes and writes made during the testing of the generated thumb drives. Process Monitor is a free Windows Sysinternals tool written by Mark Russinovich and Bryce Cogswell. This software was downloaded from: http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx
2. Microsoft Excel 2007 was used for analysis of the log files created by Process Monitor. The copy of Microsoft Office used is licensed to NW3C.

Additional Information

The operating system was not listed in the descriptions above as they were a unique part of testing. While all the machines were running Windows XP, they were not all running on the same service pack. The service pack used on any given test will be listed on the specific test page.

Test Results

This section contains details on all tests conducted during the validation study.

Test Results Report Key

Test Results Report Key				
Test Name:	0001		**Date**:	23 July 2009
Description:	To determine if XYZ does ABC			
Tester Name:	JShmoe	**Test Machine**:	Dave1	
Assertions Tested:	XYZ does A XYZ does B XYZ does C			
Unique Setup Information:	Non-Universal Stuff. New partition scheme, etc. Could also include pre-hash values, etc.			
Results By Assertion:	XYZ does A XYZ does B XYZ does C		As Expected As Expected Anomalies Detected	
Tester Notes:	Any additional information the tester wants to add…probably in Paragraph form. Could include hash information.			
Overall Success:	As Expected or Anomalies Detected			

Test Results

Test Name:	RunnerTest001	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP3)		
Tester Name:	JWykes	**Test Machine**:	Abe
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. 1GB PNY Attaché Thumb Drive with the "NW3C – Volatile Data" profile loaded, as well as Process Monitor. Internal ID#: VOL3 Drive SN# 9VQRE66HNQD8RB16		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected As Expected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 9:42 am End Time: 9:43 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the		

disk.

An examination of the Process Monitor logs indicates that all of the programs associated with the NW3C-Volatile Data profile were successfully run during the testing period.

Assertion 2:
An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.

Assertion 3:
An examination of the Process Monitor logs indicates that there were no direct writes made to the suspect drive by Runner or any of its processes (to include all of the programs within the selected profile). This test was done by filtering the Process Monitor log results to show only Filesystem information, and searching for any "WriteFile" operation.

Assertion 4:
An examination of the Process Monitor logs indicates that there were 135 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.

There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: ipconfig.exe (8), nbtstat.exe (0), net.exe (8), netstat.exe (16), pslist.exe (2), psloggedon.exe (0), quser.exe (1), sclist.exe (1), showgrps.exe (1), systeminfo.exe (8), whoami.exe (0), cmd.exe (52), and runner.exe (8).

```
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
```

In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:

```
HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\
                    TrapPollTimeMilliSecs
```

In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\7644\DEBUG\Trace Level
```

In addition to any writes listed above, *ipconfig.exe* made one write to each of the following registry keys:

	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\Guid HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\CategoryCount HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\TypesSupported In addition to any writes listed above, *pslist.exe* also made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\ Performance\Error Count

	HKLM\System\CurrentControlSet\Services\PerfProc\ Performance\Error Count Assertion 5: An examination of the Process Monitor logs indicates that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern, in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the registry, the writes were unavoidable in attempting to retrieve the desired information, and as such, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest002	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP3)		
Tester Name:	JWykes	**Test Machine**:	Abe
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. 1GB PNY Attaché Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor. Internal ID#: IR3 Drive SN#FDVRWBUS3LJO20CP		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected Anomaly Detected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 9:21 am End Time: 9:26 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Incident Response profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs associated with the NW3C-Incident Response profile were successfully run during the testing period.		

Assertion 2:
An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.

Assertion 3:
An examination of the Process Monitor logs indicates that there were three direct writes made to the suspect's hard drive. This test was done by filtering the Process Monitor log results to show only file system information, and searching for any "WriteFile" operation. The results indicate that the program *handle.exe* made three writes to the file C:\WINDOWS\system32\drivers\PROCEXP100.sys

A reference to the file PROCEXP100.sys is hard-coded within handle.exe, and as such it appears that it is not possible to restrain handle.exe from writing to this file. However, this file is specifically written as part of the Sysinternals' tool and would not be of evidentiary interest.

Assertion 4:
An examination of the Process Monitor logs indicates that there were 277 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.

There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: arp.exe (8), at.exe (0), autorunsc.exe (8), getmac.exe (8), handle.exe (0), hostname.exe (8), ipconfig.exe (8), msinfo32.exe (8), nbtstat.exe (0), net.exe (9), netdom.exe (0), netstat.exe (16), openfiles.exe (1), psfile.exe (0), pslist.exe (2), psloggedon.exe (0), psservice.exe (1), pstat.exe (0), psuptime.exe (8), quser.exe (1), route.exe (0), sc.exe (2), sclist.exe (1), showgrps.exe (1), srvcheck.exe (0), tasklist.exe (8), whoami.exe (0), cmd.exe (133), and runner.exe (8).

```
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
```

In addition to any writes listed above, *arp.exe* also made one write to the following registry key:

```
HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\
          Parameters\TrapPollTimeMilliSecs
```

In addition to any writes listed above, *autorunsc.exe* also made one write to each of the following registry keys:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
          {3c4fbd00-9243-11de-9ad6-00e0b8534d66}\BaseClass
```

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{923d6cc2-90ab-11de-9ad0-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{923d6cc3-90ab-11de-9ad0-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{c64021c7-90aa-11de-a515-806d6172696f}\BaseClass

In addition to any writes listed above, *handle.exe* also made one write to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\PROCEXP100

HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum

HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl

HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath

HKLM\System\CurrentControlSet\Services\PROCEXP100\Start

HKLM\System\CurrentControlSet\Services\PROCEXP100\Type

In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:

HKLM\SOFTWARE\Microsoft\ESENT\Process\6344\DEBUG\Trace Level

In addition to any writes listed above, *ipconfig.exe* also made one write to each of the following registry keys:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\traceIdentifier\Guid

	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\Guid HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryCount HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\TypesSupported In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key: HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\ Parameters\TrapPollTimeMilliSecs In addition to any writes listed above, *pslist.exe* made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\Performance\Error Count Assertion 5: An examination of the Process Monitor logs indicates that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern, in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the drive and registry, the writes were either specific to a program run (handle.exe) or were unavoidable in attempting to retrieve the desired information, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest003	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP2)		
Tester Name:	MBowser	**Test Machine**:	Eli
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 2. 1GB PNY Attaché Thumb Drive with the "NW3C – Volatile Data" profile loaded, as well as Process Monitor. Internal ID#: VOL2 Drive SN# 02KDC41B09G1H205		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected As Expected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 10:07 am End Time: 10:08 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk.		

	An examination of the Process Monitor logs indicates that all of the programs associated with the NW3C-Volatile Data profile were successfully run during the testing period.
	
	Assertion 2:
	An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.
	
	Assertion 3:
	An examination of the Process Monitor logs indicates that there were no direct writes made to the suspect drive by Runner or any of its processes (to include all of the programs within the selected profile). This test was done by filtering the Process Monitor log results to show only Filesystem information, and searching for any "WriteFile" operation.
	
	Assertion 4:
	An examination of the Process Monitor logs indicates that there were 117 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.
	
	There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: ipconfig.exe (8), nbtstat.exe (0), net.exe (8), netstat.exe (16), pslist.exe (2), psloggedon.exe (0), quser.exe (1), sclist.exe (1), showgrps.exe (1), systeminfo.exe (8), whoami.exe (0), cmd.exe (52), and runner.exe (8).
	
	`HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed`
	
	In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	
	In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\ESENT\Process\4597\DEBUG\Trace Level`
	
	In addition to any writes listed above, *ipconfig.exe* made one write to each of the following registry keys:
	
	`HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryCount`

	HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\TypesSupported In addition to any writes listed above, *pslist.exe* also made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\ Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\ Performance\Error Count Assertion 5: An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern, in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the registry, the writes were unavoidable in attempting to retrieve the desired information, and as such, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest003	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP2)		
Tester Name:	MBowser	**Test Machine**:	Eli
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 2. 1GB PNY Attaché Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor. Internal ID#: IR2 Drive SN#4311RZBJVSAHWWDV		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected Anomaly Detected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 9:55 am End Time: 9:57 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Incident Response profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs associated with the NW3C-Incident Response profile were successfully run during the testing period.		

Assertion 2:
An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.

Assertion 3:
An examination of the Process Monitor logs indicates that there were three direct writes made to the suspect's hard drive. This test was done by filtering the Process Monitor log results to show only file system information, and searching for any "WriteFile" operation. The results indicate that the program *handle.exe* made three writes to the file C:\WINDOWS\system32\drivers\PROCEXP100.sys

A reference to the file PROCEXP100.sys is hard-coded within handle.exe, and as such it appears that it is not possible to restrain handle.exe from writing to this file. However, this file is specifically written as part of the Sysinternals' tool and would not be of evidentiary interest.

Assertion 4:
An examination of the Process Monitor logs indicates that there were 261 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.

There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: arp.exe (8), at.exe (0), autorunsc.exe (8), getmac.exe (8), handle.exe (0), hostname.exe (8), ipconfig.exe (8), msinfo32.exe (8), nbtstat.exe (0), net.exe (9), netdom.exe (0), netstat.exe (16), openfiles.exe (1), psfile.exe (0), pslist.exe (2), psloggedon.exe (0), psservice.exe (1), pstat.exe (0), psuptime.exe (8), quser.exe (1), route.exe (0), sc.exe (2), sclist.exe (1), showgrps.exe (1), srvcheck.exe (0), tasklist.exe (8), whoami.exe (0), cmd.exe (133), and runner.exe (8).

```
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
```

In addition to any writes listed above, *arp.exe* also made one write to the following registry key:

```
HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\
        Parameters\TrapPollTimeMilliSecs
```

In addition to any writes listed above, *autorunsc.exe* also made one write to each of the following registry keys:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
        {44596dc1-923f-11de-9e16-806d6172696f}\BaseClass
```

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{dfb5a3d0-9247-11de-9e17-0015c5a7cb2f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{feaef4c4-616a-11de-93cb-806d6172696f}\BaseClass

In addition to any writes listed above, *handle.exe* also made one write to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\PROCEXP100

HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum

HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl

HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath

HKLM\System\CurrentControlSet\Services\PROCEXP100\Start

HKLM\System\CurrentControlSet\Services\PROCEXP100\Type

In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:

HKLM\SOFTWARE\Microsoft\ESENT\Process\1785\DEBUG\Trace Level

In addition to any writes listed above, *ipconfig.exe* also made one write to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryCount

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\TypesSupported

In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:

HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs

In addition to any writes listed above, *pslist.exe* made two writes to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count

HKLM\System\CurrentControlSet\Services\PerfProc\Performance\Error Count

	Assertion 5: An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern, in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the drive and registry, the writes were either specific to a program run (handle.exe) or were unavoidable in attempting to retrieve the desired information, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest005	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP3)		
Tester Name:	JWykes	**Test Machine**:	Jenny
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. 1GB PNY Attaché Thumb Drive with the "NW3C – Volatile Data" profile loaded, as well as Process Monitor. Internal ID#: VOL2 Drive SN# 02KDC41B09G1H205		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected As Expected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 9:14 am End Time: 9:15 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs		

associated with the NW3C-Volatile Data profile were successfully run during the testing period.

Assertion 2:
An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.

Assertion 3:
An examination of the Process Monitor logs indicates that there were no direct writes made to the suspect drive by Runner or any of its processes (to include all of the programs within the selected profile). This test was done by filtering the Process Monitor log results to show only Filesystem information, and searching for any "WriteFile" operation.

Assertion 4:
An examination of the Process Monitor logs indicates that there were 127 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.

There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: ipconfig.exe (8), nbtstat.exe (0), net.exe (8), netstat.exe (16), pslist.exe (2), psloggedon.exe (0), quser.exe (1), sclist.exe (1), showgrps.exe (1), systeminfo.exe (8), whoami.exe (0), cmd.exe (52), and runner.exe (8).

```
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
```

In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:

```
HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\
                    TrapPollTimeMilliSecs
```

In addition to any writes listed above, *ipconfig.exe* made one write to each of the following registry keys:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\4597\DEBUG\Trace Level

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
          Tracing\Microsoft\eappcfg\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
       Tracing\Microsoft\eappcfg\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
     Tracing\Microsoft\eappcfg\LogSessionName
```

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappcfg\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappcfg\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\traceIdentifier\Guid

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\CategoryCount

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\CategoryMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\EventMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\TypesSupported

In addition to any writes listed above, *pslist.exe* also made two writes to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\PerfOS\
Performance\Error Count

HKLM\System\CurrentControlSet\Services\PerfProc\
Performance\Error Count

Assertion 5:
An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive.

	Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern, in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the registry, the writes were unavoidable in attempting to retrieve the desired information, and as such, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest006	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP3)		
Tester Name:	JWykes	**Test Machine**:	Jenny
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. 1GB PNY Attaché Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor. Internal ID#: IR2 Drive SN# 4311RZBJVSAHWWDV		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.	As Expected As Expected Anomaly Detected Anomaly Detected As Expected	
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 9:01 am End Time: 9:03 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Incident Response profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs		

associated with the NW3C-Incident Response profile were successfully run during the testing period.

Assertion 2:
An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.

Assertion 3:
An examination of the Process Monitor logs indicates that there were three direct writes made to the suspect's hard drive. This test was done by filtering the Process Monitor log results to show only file system information, and searching for any "WriteFile" operation. The results indicate that the program *handle.exe* made three writes to the file C:\WINDOWS\system32\drivers\PROCEXP100.sys

A reference to the file PROCEXP100.sys is hard-coded within handle.exe, and as such it appears that it is not possible to restrain handle.exe from writing to this file. However, this file is specifically written as part of the Sysinternals' tool and would not be of evidentiary interest.

Assertion 4:
An examination of the Process Monitor logs indicates that there were 276 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.

There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: arp.exe (8), at.exe (0), autorunsc.exe (8), getmac.exe (8), handle.exe (0), hostname.exe (8), ipconfig.exe (8), msinfo32.exe (8), nbtstat.exe (0), net.exe (9), netdom.exe (0), netstat.exe (16), openfiles.exe (1), psfile.exe (0), pslist.exe (2), psloggedon.exe (0), psservice.exe (1), pstat.exe (0), psuptime.exe (8), quser.exe (1), route.exe (0), sc.exe (2), sclist.exe (1), showgrps.exe (1), srvcheck.exe (0), tasklist.exe (8), whoami.exe (0), cmd.exe (133), and runner.exe (8).

```
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
```

In addition to any writes listed above, *arp.exe* also made one write to the following registry key:

```
HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\
        Parameters\TrapPollTimeMilliSecs
```

In addition to any writes listed above, *autorunsc.exe* also made one write to each of the following registry keys:

	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\ {4961381b-90f6-11de-919c-806d6172696f}\BaseClass HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\ {843fd392-9240-11de-91a3-0015c5aa5641}\BaseClass HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\ {feaef4c4-616a-11de-93cb-806d6172696f}\BaseClass In addition to any writes listed above, *handle.exe* also made one write to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PROCEXP100 HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath HKLM\System\CurrentControlSet\Services\PROCEXP100\Start HKLM\System\CurrentControlSet\Services\PROCEXP100\Type In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key: HKLM\SOFTWARE\Microsoft\ESENT\Process\1785\DEBUG\Trace Level In addition to any writes listed above, *ipconfig.exe* also made one write to each of the following registry keys: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappcfg\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

	Tracing\Microsoft\QUtil\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\Guid HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryCount HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\TypesSupported In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key: HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\ Parameters\TrapPollTimeMilliSecs In addition to any writes listed above, *pslist.exe* made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\Performance\Error Count Assertion 5: An examination of the Process Monitor logs indicates that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern, in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the drive and registry, the writes were either specific to a program run (handle.exe) or were unavoidable in attempting to retrieve the desired information, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest007	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP3)		
Tester Name:	JWykes	**Test Machine**:	Jim
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. 1GB PNY Attaché Thumb Drive with the "NW3C – Volatile Data" profile loaded, as well as Process Monitor. Internal ID#: VOL1 Drive SN# 0XRVIMHLKSVVY0X8		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected As Expected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 8:31 am End Time: 8:33 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs		

	associated with the NW3C-Volatile Data profile were successfully run during the testing period.
	
	Assertion 2:
	An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.
	
	Assertion 3:
	An examination of the Process Monitor logs indicates that there were no direct writes made to the suspect drive by Runner or any of its processes (to include all of the programs within the selected profile). This test was done by filtering the Process Monitor log results to show only Filesystem information, and searching for any "WriteFile" operation.
	
	Assertion 4:
	An examination of the Process Monitor logs indicates that there were 132 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.
	
	There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: ipconfig.exe (8), nbtstat.exe (0), net.exe (8), netstat.exe (16), pslist.exe (2), psloggedon.exe (0), quser.exe (1), sclist.exe (1), showgrps.exe (1), systeminfo.exe (8), whoami.exe (0), cmd.exe (52), and runner.exe (8).
	
	`HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed`
	
	In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	
	In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\ESENT\Process\6898\DEBUG\Trace Level`
	
	In addition to any writes listed above, *ipconfig.exe* made one write to each of the following registry keys:
	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\Active`
	
	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\ControlFlags`

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappcfg\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappcfg\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappcfg\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\eappprxy\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Tracing\Microsoft\QUtil\traceIdentifier\Guid

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\CategoryCount

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\CategoryMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\EventMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\
Application\ESENT\TypesSupported

In addition to any writes listed above, *pslist.exe* also made two writes to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\PerfOS\
Performance\Error Count

HKLM\System\CurrentControlSet\Services\PerfProc\
Performance\Error Count

	Assertion 5: An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern, in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the registry, the writes were unavoidable in attempting to retrieve the desired information, and as such, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest008	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP3)		
Tester Name:	JWykes	**Test Machine**:	Jim
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. 1GB PNY Attaché Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor. Internal ID#: IR1 Drive SN#FAV3RW6Q0RP0L3M7		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.	As Expected As Expected Anomaly Detected Anomaly Detected As Expected	
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 8:43 am End Time: 8:51 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Incident Response profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs		

	associated with the NW3C-Incident Response profile were successfully run during the testing period.
	
	Assertion 2:
	An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.
	
	Assertion 3:
	An examination of the Process Monitor logs indicates that there were three direct writes made to the suspect's hard drive. This test was done by filtering the Process Monitor log results to show only file system information, and searching for any "WriteFile" operation. The results indicate that the program *handle.exe* made three writes to the file C:\WINDOWS\system32\drivers\PROCEXP100.sys
	
	A reference to the file PROCEXP100.sys is hard-coded within handle.exe, and as such it appears that it is not possible to restrain handle.exe from writing to this file. However, this file is specifically written as part of the Sysinternals' tool and would not be of evidentiary interest.
	
	Assertion 4:
	An examination of the Process Monitor logs indicates that there were 277 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.
	
	There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: arp.exe (8), at.exe (0), autorunsc.exe (8), getmac.exe (8), handle.exe (0), hostname.exe (8), ipconfig.exe (8), msinfo32.exe (8), nbtstat.exe (0), net.exe (9), netdom.exe (0), netstat.exe (16), openfiles.exe (1), psfile.exe (0), pslist.exe (2), psloggedon.exe (0), psservice.exe (1), pstat.exe (0), psuptime.exe (8), quser.exe (1), route.exe (0), sc.exe (2), sclist.exe (1), showgrps.exe (1), srvcheck.exe (0), tasklist.exe (8), whoami.exe (0), cmd.exe (133), and runner.exe (8).
	
	`HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed`
	
	In addition to any writes listed above, *arp.exe* also made one write to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	
	In addition to any writes listed above, *autorunsc.exe* also made one write to each of the following registry keys:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{02bb35ea-1621-11da-840f-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{02bb35eb-1621-11da-840f-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{02bb35ec-1621-11da-840f-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a958b38f-9106-11de-b151-000d6137076a}\BaseClass

In addition to any writes listed above, *handle.exe* also made one write to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\PROCEXP100

HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum

HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl

HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath

HKLM\System\CurrentControlSet\Services\PROCEXP100\Start

HKLM\System\CurrentControlSet\Services\PROCEXP100\Type

In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:

HKLM\SOFTWARE\Microsoft\ESENT\Process\1785\DEBUG\Trace Level

In addition to any writes listed above, *ipconfig.exe* also made one write to each of the following registry keys:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\LogSessionName

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\BitNames

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\Active

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\ControlFlags

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

	Tracing\Microsoft\eappprxy\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\eappprxy\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\Active HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\ControlFlags HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\LogSessionName HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Tracing\Microsoft\QUtil\traceIdentifier\Guid HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryCount HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\TypesSupported In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key: HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\ Parameters\TrapPollTimeMilliSecs In addition to any writes listed above, *pslist.exe* made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\Performance\Error Count Assertion 5: An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern; in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due

	to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the drive and registry, the writes were either specific to a program run (handle.exe) or were unavoidable in attempting to retrieve the desired information, the overall rating for this test will be listed “As Expected.”
Overall Success:	As Expected

Test Name:	RunnerTest009	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP2)		
Tester Name:	MBowser	**Test Machine**:	Pat
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 2. 1GB PNY Attaché Thumb Drive with the "NW3C – Volatile Data" profile loaded, as well as Process Monitor. Internal ID#: VOL3 Drive SN# 9VQRE66HNQD8RB		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected As Expected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 10:31 am End Time: 10:32 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs		

	associated with the NW3C-Volatile Data profile were successfully run during the testing period.
	
	Assertion 2:
	An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.
	
	Assertion 3:
	An examination of the Process Monitor logs indicates that there were no direct writes made to the suspect drive by Runner or any of its processes (to include all of the programs within the selected profile). This test was done by filtering the Process Monitor log results to show only Filesystem information, and searching for any "WriteFile" operation.
	
	Assertion 4:
	An examination of the Process Monitor logs indicates that there were 112 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.
	
	There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: ipconfig.exe (8), nbtstat.exe (0), net.exe (8), netstat.exe (16), pslist.exe (2), psloggedon.exe (0), quser.exe (1), sclist.exe (1), showgrps.exe (1), systeminfo.exe (8), whoami.exe (0), cmd.exe (52), and runner.exe (8).
	
	`HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed`
	
	In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	
	In addition to any writes listed above, *ipconfig.exe* made one write to each of the following registry keys:
	
	`HKLM\SOFTWARE\Microsoft\ESENT\Process\6898\DEBUG\Trace Level`
	
	`HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryCount`
	
	`HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile`
	
	`HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile`

	HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\TypesSupported In addition to any writes listed above, *pslist.exe* also made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\ Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\ Performance\Error Count Assertion 5: An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern; in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the registry, the writes were unavoidable in attempting to retrieve the desired information, and as such, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest010	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP2)		
Tester Name:	MBowser	**Test Machine**:	Pat
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 2. 1GB PNY Attaché Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor. Internal ID#: IR3 Drive SN#FDVRWBU53LJO20CP		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected Anomaly Detected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 10:39 am End Time: 10:43 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Incident Response profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs		

	associated with the NW3C-Incident Response profile were successfully run during the testing period.
	
	Assertion 2:
	An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.
	
	Assertion 3:
	An examination of the Process Monitor logs indicates that there were three direct writes made to the suspect's hard drive. This test was done by filtering the Process Monitor log results to show only file system information, and searching for any "WriteFile" operation. The results indicate that the program *handle.exe* made three writes to the file C:\WINDOWS\system32\drivers\PROCEXP100.sys
	
	A reference to the file PROCEXP100.sys is hard-coded within handle.exe, and as such it appears that it is not possible to restrain handle.exe from writing to this file. However, this file is specifically written as part of the Sysinternals' tool and would not be of evidentiary interest.
	
	Assertion 4:
	An examination of the Process Monitor logs indicates that there were 262 total writes/updates/deletions were made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.
	
	There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: arp.exe (8), at.exe (0), autorunsc.exe (8), getmac.exe (8), handle.exe (0), hostname.exe (8), ipconfig.exe (8), msinfo32.exe (8), nbtstat.exe (0), net.exe (9), netdom.exe (0), netstat.exe (16), openfiles.exe (1), psfile.exe (0), pslist.exe (2), psloggedon.exe (0), psservice.exe (1), pstat.exe (0), psuptime.exe (8), quser.exe (1), route.exe (0), sc.exe (2), sclist.exe (1), showgrps.exe (1), srvcheck.exe (0), tasklist.exe (8), whoami.exe (0), cmd.exe (133), and runner.exe (8).
	
	`HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed`
	
	In addition to any writes listed above, *arp.exe* also made one write to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	
	In addition to any writes listed above, *autorunsc.exe* also made one write to each of the following registry keys:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{ab7c3e54-924c-11de-83b1-00e0b8534ba4}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e727fc90-921e-11de-b2a5-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e727fc91-921e-11de-b2a5-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e727fc92-921e-11de-b2a5-806d6172696f}\BaseClass

In addition to any writes listed above, *handle.exe* also made one write to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\PROCEXP100

HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum

HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl

HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath

HKLM\System\CurrentControlSet\Services\PROCEXP100\Start

HKLM\System\CurrentControlSet\Services\PROCEXP100\Type

In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:

HKLM\SOFTWARE\Microsoft\ESENT\Process\6344\DEBUG\Trace Level

In addition to any writes listed above, *ipconfig.exe* also made one write to each of the following registry keys:

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryCount

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile

HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\TypesSupported

In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:

HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs

In addition to any writes listed above, *pslist.exe* made two writes to each of the

	following registry keys:
	`HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count`
	
	`HKLM\System\CurrentControlSet\Services\PerfProc\Performance\Error Count`
	
	Assertion 5:
	An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive.
	
	Additional Tester Notes:
	While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern; in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult.
	
	While there were slight changes to the drive and registry, the writes were either specific to a program run (handle.exe) or were unavoidable in attempting to retrieve the desired information, the overall rating for this test will be listed "As Expected."

Overall Success:	As Expected

Test Name:	RunnerTest011	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP2)		
Tester Name:	MBowser	**Test Machine**:	Paul
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 2. 1GB PNY Attaché Thumb Drive with the "NW3C – Volatile Data" profile loaded, as well as Process Monitor. Internal ID#: VOL1 Drive SN# 0XRVIMHLKSVVY0X8		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected As Expected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 9:43 am End Time: 9:44 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs		

	associated with the NW3C-Volatile Data profile were successfully run during the testing period.
	
	Assertion 2:
	An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.
	
	Assertion 3:
	An examination of the Process Monitor logs indicates that there were no direct writes made to the suspect drive by Runner or any of its processes (to include all of the programs within the selected profile). This test was done by filtering the Process Monitor log results to show only Filesystem information, and searching for any "WriteFile" operation.
	
	Assertion 4:
	An examination of the Process Monitor logs indicates that there were 117 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.
	
	There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: ipconfig.exe (8), nbtstat.exe (0), net.exe (8), netstat.exe (16), pslist.exe (2), psloggedon.exe (0), quser.exe (1), sclist.exe (1), showgrps.exe (1), systeminfo.exe (8), whoami.exe (0), cmd.exe (52), and runner.exe (8).
	
	`HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed`
	
	In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	
	In addition to any writes listed above, *ipconfig.exe* also made two writes to the following registry key:
	
	`HKLM\SOFTWARE\Microsoft\ESENT\Process\6898\DEBUG\Trace Level`
	
	In addition to any writes listed above, *ipconfig.exe* made one write to each of the following registry keys:
	
	`HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryCount`
	
	`HKLM\System\CurrentControlSet\Services\Eventlog\`

	Application\ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\TypesSupported In addition to any writes listed above, *pslist.exe* also made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\ Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\ Performance\Error Count Assertion 5: An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern; in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the registry, the writes were unavoidable in attempting to retrieve the desired information, and as such, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Test Name:	RunnerTest012	**Date**:	26 August 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP2)		
Tester Name:	MBowser	**Test Machine**:	Paul
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 2. 1GB PNY Attaché Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor. Internal ID#: IR1 Drive SN#FAV3RW6Q0RP0L3M7		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		As Expected As Expected As Expected Anomaly Detected As Expected
Tester Notes:	The thumb drive was first connected to the machine after the system had finished booting to Windows. After the thumb drive drivers finished loading, the tester navigated to the thumb drive and started Process Monitor. Once Process Monitor loaded, and had begun capturing data, the tester navigated to the thumb drive and ran "runner.exe." Start Time: 9:24 am End Time: 9:26 am Immediately after the completion of runner, the tester stopped the Process Monitor capture and saved the log file to the thumb drive. The log file was examined later for testing of the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Incident Response profile were successfully copied to the disk. An examination of the Process Monitor logs indicates that all of the programs associated with the NW3C-Incident Response profile were successfully run during the testing period.		

Assertion 2:
An examination of the contents of the thumb drive indicates that *runner.exe* successfully saved the output files on the thumb drive, and in the appropriate directories.

Assertion 3:
An examination of the Process Monitor logs indicates that there were no direct writes made to the suspect drive by Runner or any of its processes (to include all of the programs within the selected profile). This test was done by filtering the Process Monitor log results to show only Filesystem information, and searching for any "WriteFile" operation.

Assertion 4:
An examination of the Process Monitor logs indicates that there were 277 total writes/updates/deletions made to the registry by Runner and its processes (to include all of the programs within the selected profile). These results will also include attempts to change that were not allowed (i.e., an attempt to delete a key that doesn't exist). This test was done by filtering the Process Monitor log results to show only Registry information, and searching for any "RegSetValue," "RegDeleteValue," or "RegDeleteKey" operation. For simplicities sake, any change made to the registry will be listed as a write below.

There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key is as follows: arp.exe (8), at.exe (0), autorunsc.exe (8), getmac.exe (8), handle.exe (0), hostname.exe (8), ipconfig.exe (8), msinfo32.exe (8), nbtstat.exe (0), net.exe (9), netdom.exe (0), netstat.exe (16), openfiles.exe (1), psfile.exe (0), pslist.exe (2), psloggedon.exe (0), psservice.exe (1), pstat.exe (0), psuptime.exe (8), quser.exe (1), route.exe (0), sc.exe (2), sclist.exe (1), showgrps.exe (1), srvcheck.exe (0), tasklist.exe (8), whoami.exe (0), cmd.exe (133), and runner.exe (8).

```
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
```

In addition to any writes listed above, *arp.exe* also made one write to the following registry key:

```
HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\
        Parameters\TrapPollTimeMilliSecs
```

In addition to any writes listed above, *autorunsc.exe* also made one write to each of the following registry keys:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
      {02bb35ea-1621-11da-840f-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
      {02bb35eb-1621-11da-840f-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
      {02bb35ec-1621-11da-840f-806d6172696f}\BaseClass
```

	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\ {c583de36-925c-11de-b154-000d6119d38a}\BaseClass In addition to any writes listed above, *ipconfig.exe* also made one write to each of the following registry keys: HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryCount HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\Eventlog\Application\ ESENT\TypesSupported In addition to any writes listed above, *netstat.exe* also made two writes to the following registry key: HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\ Parameters\TrapPollTimeMilliSecs In addition to any writes listed above, *pslist.exe* made two writes to each of the following registry keys: HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\Performance\ Error Count Assertion 5: An examination of the Process Monitor logs indicate that the programs run as part of the profile were run from the thumb drive, and not from the suspect's hard drive. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were not of any evidentiary concern; in addition, the modifications were a result of running these tools on a live machine, and could not be avoided. In addition, due to the nature of the registry, determining if the registry changes were actually written to the drive is difficult. While there were slight changes to the registry, the writes were unavoidable in attempting to retrieve the desired information, and as such, the overall rating for this test will be listed "As Expected."
Overall Success:	As Expected

Report Notes

This validation was conducted to test the functionality of the two NW3C profiles as they would run on a suspect's system. This is not a validation of the full COFEE "suite."

Additional References

Leo Dorrendorf, Z. G. (2007). *Cryptanalysis of the Windows Random Number Generator.* The Hebrew University of Jerusalem.

Bowser, M & Wykes, J. (2009). *COFEE GUI CONSOLE.* National White Collar Crime Center.

Glossary

Entropy: Random data –mouse position, processor statistics, local time, etc.—collected by an application or operating system for use in cryptography.

File System: In relation to this document, file system refers to active files on the suspect's system.

Incident Response: The actions and approaches taken to a network security breach (such as a system being hacked).

Registry: The registry consists of a number of separate hive files which store various types of information. When a system is powered on, the operating system "combines" these hive files in RAM to create the registry. When changes are made to the registry, the changes are made to the registry that is located in RAM. The point at which these changes are actually written to the hive files on the disk varies depending upon a number of factors; therefore it is difficult to determine if any of the changes made to the registry by the profiles discussed in this report would actually affect the data stored on the suspect's hard drive. For example, if the investigator removes power from the suspect's machine (by pulling the power cord) immediately after running the Volatile Data profile, it is possible that none of the changes made to the registry would have actually been stored to the suspect's disk.

Volatile Data: Any data that is lost when power is removed from the system.

Windows Random Number Generator: A pseudo-random number generator (PRNG) that uses collected entropy from a Windows machine to establish cryptographic keys. Each Windows process has its own copy of a WRNG instance. Entropy collected is used to generate an RC4 key that is stored in its internal state for random number generation. Each instance of the WRNG uses eight RC4 streams. Entropy collection occurs when an RC4 stream is initialized or it reaches the 16KB threshold. The entire 3584 bytes of collected entropy are hashed to produce an 80-byte digest which is then fed into an RC4 algorithm as a key. The key is used to encrypt the clear text contained in the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed` registry key. This key contains the latest seeded value obtained from Windows entropy sources and is used by all instances of the WRNG run on the machine. The result is another 80-byte digest that is again fed into an RC4

algorithm that is used to encrypt a 256-byte entropy source read from a Windows device driver. The result of the final encryption is used as a key for the RC4 instance that is used in the WRNG internal state. (Leo Dorrendorf, 2007)