

# **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.

Bureau of Justice Assistance U.S. Department of Justice

## **Table of Contents**

Table of Contents	i
Introduction	
Purpose and Scope	1
Test Result Summary	1
Test Assertions	2
Testing Environment	2
Test Computer	2
Support Software Used	4
Additional Information	4
Test Results	5
Report Notes	51
Additional References	51
Glossary	51

### 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**

- 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	<b>Date</b> : 23 July 200						
Description:	<b>Description</b> : To determine if XYZ does ABC							
Tester Name:		JShmoe	Test Machine:	Dave1				
Assertions Tes	sted:	XYZ does A						
		XYZ does B						
		XYZ does C						
<b>Unique Setup</b>		Non-Universal Stuff. New partition	scheme, etc. Cou	ld also inclu	ude pre-hash			
Information:		values, etc.						
Results By		XYZ does A		As Expected				
Assertion:								
		XYZ does B		As Expected				
		XYZ does C			alies Detected			
Tester Notes:		Any additional information the test	er wants to addp	robably in	Paragraph form.			
	Could include hash information.							
			1					
Overall Succes	ss:	As Expected or Anomalies Detected						

## **Test Results**

Test Name:	Runn	erTest001			<b>Date</b> : 26 August 2009	
Description:	Runni	ng a COFEE	generated thumb o	drive with the NW3C Volat	ile Data Profile (SP3)	
Tester Name:		JWykes		Test Machine:	Abe	
Assertions Te	sted:	2. Red dri 3. Exe (Fil 4. Exe (Re	Il programs identified in the profile were executed. esults of the tools were properly stored on the investigator's thumb rive. executing runner.exe did not cause any direct writes to the suspect drive File System). executing runner.exe did not cause any direct writes to the suspect drive Registry). he tools executed were run from the thumb drive, not from the suspect's hachine.			
Unique Setup				osoft Windows XP Service	Pack 3.	
Information:		1GB PNY A	ttaché Thumb Driv cess Monitor.		ile Data" profile loaded, as	
Results By			. •	ed in the profile were	As Expected	
Assertion:		2. Res	estigator's thumb			
			_	did not cause any direct drive (File System).	As Expected	
			ecuting runner.exe ites to the suspect	did not cause any direct	Anomaly Detected	
		5. The	•	ere run from the thumb	As Expected	
Tester Notes:		booting to navigated t Once Proce	Windows. After the to the thumb drive	ne thumb drive drivers fini and started Process Moni , and had begun capturing	_	
		Start Time:	tart Time: 9:42 am End Time: 9:43 am			
		Monitor ca examined l	pture and saved th	etion of runner, the tester ne log file to the thumb dr the assertions listed above	ive. The log file was	
			ation of the thumb	drive's file system indicat platile Data profile were su	ed that all of the programs accessfully 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).

 ${\tt HKLM} \verb|SOFTWARE| Microsoft| Cryptography| RNG| Seed$ 

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

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

	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:	Runne	rTest002			Date:	26 August 2009
Description:			generated thumb of	rive with the NW3C	Incident Resp	onse Profile (SP3)
Tester Name:	JW	/ykes		Test Machine:	Abe	
<ol> <li>Assertions         <ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's thum</li> <li>Executing runner.exe did not cause any direct writes to the suspect File System.</li> <li>Executing runner.exe did not cause any direct writes to the suspect Registry.</li> </ol> </li> <li>The tools executed were run from the thumb drive, not from the sum achine.</li> </ol>						e suspect drive's
Unique Setup Information:	1G as	B PNY Atta	ché Thumb Drive w cess Monitor.	ft Windows XP Servion with the "NW3C – Incident of the FDVRWBUS3LJO200	dent Respons	se" profile loaded,
Results By Assertion:		execu 2. Resulinvest	ts of the tools were tigator's thumb driv	properly stored on t		
		writes 4. Execuments 5. The to drive,	s to the suspect driving runner.exe dictions to the suspect driving executed were not from the suspe	ve (File System). I not cause any direct ve (Registry). run from the thumb ect's machine.	Anoma	ly Detected
Tester Notes:	bo na Or	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."				
	Im cal tes	pture and s sting of the sertion 1: examination sociated with sk.	after the completio aved the log file to assertions listed at on of the thumb drith the NW3C-Incide on of the Process Mth the NW3C-Incide	end Time: 9:26 am n of runner, the teste the thumb drive. The tove. The results of t ve's file system indicates and Response profile went Response profile	e log file was he analysis an ated that all o were succession	examined later for re detailed below:  of the programs fully copied to the

#### 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\
{923d6cc2-90ab-11de-9ad0-806d6172696f}\BaseClass

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

 $\label{local-condition} HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\\ \left\{c64021c7-90aa-11de-a515-806d6172696f\right\}\BaseClass$ 

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

 ${\tt HKLM} \setminus {\tt System} \setminus {\tt CurrentControlSet} \setminus {\tt Services} \setminus {\tt PROCEXP100} \setminus {\tt Type}$ 

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\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\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:	Runne	erTest003 <b>Date</b> : 26 August 2009				
Description:	Runni	ng a COFEE generated thumb drive with the NW3C Volatile	e Data Profile (SP2)			
<b>Tester Name:</b>		MBowser Test Machine: Eli				
Assertions Te	red. nvestigator's thumb ites to the suspect drive ites to the suspect drive ve, not from the suspect's					
Unique Setup Information:		System was loaded with Microsoft Windows XP Service P.  1GB PNY Attaché Thumb Drive with the "NW3C – Volatile well as Process Monitor.  Internal ID#: VOL2 Drive SN# 02KDC41B09G1H205				
Results By Assertion:		<ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's thumb drive.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive (File System).</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive (Registry).</li> <li>The tools executed were run from the thumb drive, not from the suspect's machine.</li> </ol> As Expected As Expected Anomaly Detected As Expected Anomaly Detected				
Tester Notes:		The thumb drive was first connected to the machine afte booting to Windows. After the thumb drive drivers finish navigated to the thumb drive and started Process Monitor.  Once Process Monitor loaded, and had begun capturing of 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 st Monitor capture and saved the log file to the thumb drive examined later for testing of the assertions listed above. analysis are detailed below:  Assertion 1:  An examination of the thumb drive's file system indicated associated with the NW3C-Volatile Data profile were succedisk.	opped the Process  The log file was The results of the			

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:

 ${\tt HKLM} \verb|SOFTWARE| Microsoft| ESENT| Process| 4597| DEBUG| Trace Level|$ 

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\CategoryMessageFile

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

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

#### 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: 2	26 August 2009			
Description:	Running a COFEE generated thumb drive with the NW3C Incident Respons	se Profile (SP2)			
Tester Name:					
Assertions Tested:	<ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's</li> <li>Executing runner.exe did not cause any direct writes to the sur</li> </ol>	ools were properly stored on the investigator's thumb drive.			
	File System.  4. Executing runner.exe did not cause any direct writes to the sur Registry.  The tools executed were run from the thumb drive, not from the surplication.				
	5. The tools executed were run from the thumb drive, not from t machine.	tile suspect s			
Unique Setup	System was loaded with Microsoft Windows XP Service Pack 2.				
Information:	1GB PNY Attaché Thumb Drive with the "NW3C – Incident Response"   as well as Process Monitor. Internal ID#: IR2 Drive SN#4311RZBJVSAHWWDV	profile loaded,			
Results By	1. All programs identified in the profile were  As Expecte	ed ed			
Assertion:	executed.				
	<ol> <li>Results of the tools were properly stored on the investigator's thumb drive.</li> </ol>	ed			
	3. Executing runner.exe did not cause any direct writes to the suspect drive (File System).	Detected			
	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 were run from the thumb drive, not from the suspect's machine.				
Tester Notes:	The thumb drive was first connected to the machine after the system booting to Windows. After the thumb drive drivers finished loading, to navigated to the thumb drive and started Process Monitor.				
	Once Process Monitor loaded, and had begun capturing data, the testo the thumb drive and ran "runner.exe."	er navigated to			
	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 associated with the NW3C-Incident Response profile were successfully disk.				
	An examination of the Process Monitor logs indicates that all of the prassociated with the NW3C-Incident Response profile were successfully 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).

 ${\tt HKLM \backslash SOFTWARE \backslash Microsoft \backslash Cryptography \backslash RNG \backslash Seed}$ 

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:

 $\label{local-bound} $$HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\ {dfb5a3d0-9247-11de-9e17-0015c5a7cb2f}\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

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

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

 ${\tt HKLM} \\ {\tt System} \\ {\tt CurrentControlSet} \\ {\tt Services} \\ {\tt PerfOS} \\ {\tt Performance} \\ {\tt Error} \\ {\tt Count} \\ {\tt System} \\ {\tt CurrentControlSet} \\ {\tt Services} \\ {\tt PerfoS} \\ {\tt Performance} \\ {\tt Error} \\ {\tt Count} \\ {\tt System} \\ {\tt CurrentControlSet} \\ {\tt Services} \\ {\tt PerfoS} \\ {\tt Performance} \\ {\tt Error} \\ {\tt Count} \\ {\tt System} \\ {\tt System$ 

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

Ar	ssertion 5: n 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.
W we ru th	dditional Tester Notes: /hile there were several writes to the system's registry, the registry keys modified ere not of any evidentiary concern, in addition, the modifications were a result of inning these tools on a live machine, and could not be avoided. In addition, due to be nature of the registry, determining if the registry changes were actually written to the drive is difficult.
sp	/hile there were slight changes to the drive and registry, the writes were either pecific 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:	Runne	rTest005	Da	<b>te</b> : 26 August 2009	
Description:	Runni	ng a COFEE generated thumb drive wit	h the NW3C Volatile D	ata Profile (SP3)	
Tester Name:		JWykes <b>T</b>	Test Machine: Jenny	У	
Assertions Tes	sted:	<ol> <li>All programs identified in the</li> <li>Results of the tools were properties.</li> <li>Executing runner.exe did not (File System).</li> <li>Executing runner.exe did not (Registry).</li> <li>The tools executed were run machine.</li> </ol>	cause any direct write cause any direct write cause any direct write from the thumb drive,	estigator's thumb s to the suspect drive s to the suspect drive not from the suspect's	
Unique Setup		System was loaded with Microsoft W	indows XP Service Pacl	k 3.	
Information:		1GB PNY Attaché Thumb Drive with the well as Process Monitor. Internal ID#: VOL2 Drive SN# 020	he "NW3C – Volatile D KDC41B09G1H205	ata" profile loaded, as	
Results By		1. All programs identified in the	profile were	As Expected	
Assertion:		executed.  2. Results of the tools were propinvestigator's thumb drive.		As Expected	
		<ol><li>Executing runner.exe did not writes to the suspect drive (Fig. 1)</li></ol>	ile System).	As Expected	
		<ol><li>Executing runner.exe did not writes to the suspect drive (R</li></ol>	egistry).	Anomaly Detected	
		<ol><li>The tools executed were run drive, not from the suspect's</li></ol>		As Expected	
Tester Notes:		The thumb drive was first connected booting to Windows. After the thumb navigated to the thumb drive and star Once Process Monitor loaded, and hat to the thumb drive and ran "runner.e	b drive drivers finished rted Process Monitor. Id begun capturing dat	l loading, the tester	
		Start Time: 9:14 am End Time: 9:15 am			
		Immediately after the completion of a Monitor capture and saved the log file examined later for testing of the asse analysis are detailed below:	e to the thumb drive.	The log file was	
		Assertion 1: An examination of the thumb drive's associated with the NW3C-Volatile Dadisk.	•		
		An examination of the Process Monito	or logs indicates that a	III 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).

 ${\tt HKLM} \\ {\tt SOFTWARE} \\ {\tt Microsoft} \\ {\tt Cryptography} \\ {\tt RNG} \\ {\tt Seed} \\$ 

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

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\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\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\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\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\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:	Runn	nerTest006			Date:	26 August 2009
Description:	Runn	ing a COFEE	generated thumb o	rive with the NW3C	Incident Resp	onse Profile (SP3)
Tester Name:		JWykes		Test Machine:	Jenny	
<ol> <li>Assertions Tested:         <ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's thur drive.</li> <li>Executing runner.exe did not cause any direct writes to the suspect File System.</li> <li>Executing runner.exe did not cause any direct writes to the suspect Registry.</li> <li>The tools executed were run from the thumb drive, not from the smachine.</li> </ol> </li> </ol>						he suspect drive's
<b>Unique Setup</b>		System was	loaded with Micro	soft Windows XP Ser	vice Pack 3.	
Information:			vell as Process Mor	e with the "NW3C – In nitor. SN# 4311RZBJVSAHW	·	nse" profile
Results By			•	d in the profile were	As Expe	cted
Assertion:		2. Res the	investigator's thun			
		writ	tes to the suspect o	did not cause any dire drive (File System). did not cause any dire		ly Detected
		5. The	tes to the suspect of tools executed we re, not from the sus	ere run from the thun	nb As Expe	ected
Tester Notes:		The thumb booting to Nonavigated to Once Procesto the thum Start Time:  Immediately Monitor capexamined laare detailed Assertion 1: An examina associated withe disk.	drive was first conf Windows. After the o the thumb drive a ass Monitor loaded, ab drive and ran "ru 9:01 am y after the complet oture and saved the ater for testing of the ater for testing of the tion of the thumb of with the NW3C-Inci	nected to the maching thumb drive drivers and started Process Nand had begun capto	s finished load Monitor.  uring data, the  ster stopped to b drive. The le bove. The res  dicated that alle were succes	the Process og file was sults of the analysis

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:

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

 $\label{local-continuous} HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\ {843fd392-9240-11de-91a3-0015c5aa5641}\BaseClass$ 

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

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\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\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

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:	Runn	rTest007		Date:	26 August 2009
Description:	Runni	ng a COFEE generated t	thumb drive with the NW3C Volati	le Data F	Profile (SP3)
Tester Name:		JWykes		m	
Assertions Tes	sted:	<ol> <li>Results of the drive.</li> <li>Executing rung (File System).</li> <li>Executing rung (Registry).</li> <li>The tools executing.</li> </ol>	dentified in the profile were exect tools were properly stored on the ner.exe did not cause any direct were.exe did not cause any direct were turn from the thumb direct were run from the thumb direct were run from the thumb direct were run from the thumb direct.	rites to trites to trites to trites to trive, not f	the suspect drive
Unique Setup		System was loaded wi	th Microsoft Windows XP Service	Pack 3.	
Information:		1GB PNY Attaché Thur well as Process Monito Internal ID#: VOL1	mb Drive with the "NW3C – Volati or. Drive SN# 0XRVIMHLKSVVY0X8	le Data"	profile loaded, as
Results By			dentified in the profile were	As Exp	pected
Assertion:		investigator's		As Exp	pected
		writes to the s	ner.exe did not cause any direct suspect drive (File System).		pected
		writes to the s	ner.exe did not cause any direct suspect drive (Registry).		aly Detected
			cuted were run from the thumb methods the suspect's machine.	As Exp	pected
Tester Notes:		booting to Windows. navigated to the thum	first connected to the machine aft After the thumb drive drivers finish drive and started Process Monitorion loaded, and had begun capturing d ran "runner.exe."	hed load or.	ling, the tester
		Start Time: 8:31 am	End Time: 8:33 am		
		Monitor capture and s	completion of runner, the tester saved the log file to the thumb driving of the assertions listed above below:	ve. The l	og file was
			e thumb drive's file system indicato W3C-Volatile Data profile were su		
		An examination of the	Process Monitor logs indicates th	at 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).

 ${\tt HKLM} \\ {\tt SOFTWARE} \\ {\tt Microsoft} \\ {\tt Cryptography} \\ {\tt RNG} \\ {\tt Seed} \\$ 

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

 $\label{thm:local} \begin{tabular}{l} HKLM\software\mbox{\tt Microsoft\scalebase} \end{tabular} $$ TrapPollTimeMilliSecs $$ $$$ 

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\ControlFlags

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
  Tracing\Microsoft\eappcfq\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\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\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\EventMessageFile

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

	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:	Runr	nerTest008 Date: 26 August 2009					
Description:	Runr	ning a COFEE generated thumb drive with the NW3C Incident Response Profile (SP3)					
Tester Name:		JWykes		Test Machine:	Jim		
Assertions Tes	sted:	<ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's thumb drive.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive's File System.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive's Registry.</li> <li>The tools executed were run from the thumb drive, not from the suspect's machine.</li> </ol>					
Unique Setup							
Information:		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				l in the profile were	As Exp	ected	
Assertion:		the inv	of the tools we estigator's thun			ected	
			-	did not cause any di Irive (File System).	rect Anoma	aly Detected	
			ng runner.exe of the the suspect of	did not cause any di Irive (Registry).	rect Anoma	aly Detected	
				re run from the thu spect's machine.	mb As Exp	ected	
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\
            {\tt Tracing \backslash Microsoft \backslash eappcfg \backslash traceIdentifier \backslash 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\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

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:

 ${\tt HKLM} \\ {\tt System} \\ {\tt CurrentControlSet} \\ {\tt Services} \\ {\tt PerfProc} \\ {\tt Performance} \\ {\tt Error} \\ {\tt Count} \\$ 

### 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:	Runne	erTest009	Date:	26 August 2009
Description:	Runni	ng a COFEE generated thumb drive with the NW3C Volatil	e Data P	Profile (SP2)
Tester Name:		MBowser Test Machine: Pa	at	
Assertions Tes	sted:	<ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's thumb drive.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive (File System).</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive (Registry).</li> <li>The tools executed were run from the thumb drive, not from the suspect's machine.</li> </ol>		
Unique Setup		System was loaded with Microsoft Windows XP Service F	Pack 2.	
Information:		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		All programs identified in the profile were	As Exp	pected
Assertion:		executed.  2. Results of the tools were properly stored on the investigator's thumb drive.		pected
		<ol><li>Executing runner.exe did not cause any direct writes to the suspect drive (File System).</li></ol>		pected
		<ol> <li>Executing runner.exe did not cause any direct writes to the suspect drive (Registry).</li> </ol>		aly Detected
		<ol><li>The tools executed were run from the thumb drive, not from the suspect's machine.</li></ol>	As Exp	pected
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 s Monitor capture and saved the log file to the thumb driv examined later for testing of the assertions listed above. analysis are detailed below:	e. The l	og file was
		Assertion 1: An examination of the thumb drive's file system indicate associated with the NW3C-Volatile Data profile were sucdisk.		
		An examination of the Process Monitor logs indicates the	at all of t	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).

 ${\tt HKLM} \\ {\tt SOFTWARE} \\ {\tt Microsoft} \\ {\tt Cryptography} \\ {\tt RNG} \\ {\tt Seed} \\$ 

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\CategoryMessageFile

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

<pre>HKLM\System\CurrentControlSet\Services\Eventlog\</pre>	ί.
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\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:	Runn	erTest010	[	Date:	26 August 2009
Description:	Runn	ing a COFEE generated thumb	drive with the NW3C Incid	ent Respo	onse Profile (SP2)
Tester Name:		MBowser Test Machine: Pat			
Assertions Tes	sted:	<ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's thumb drive.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive's File System.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive's Registry.</li> <li>The tools executed were run from the thumb drive, not from the suspect's machine.</li> </ol>			
<b>Unique Setup</b>		System was loaded with Micr	osoft Windows XP Service	Pack 2.	
Information:		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		1. All programs identifie	ed in the profile were	As Expe	ected
Assertion:		executed.  2. Results of the tools w the investigator's thu		As Expe	ected
		writes to the suspect			ly Detected
		writes to the suspect			ly Detected
			rere run from the thumb uspect's machine.	As Expe	ected
Tester Notes:		drive, not from the suspect's machine.  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			
		An examination of the Proces	ss Monitor logs indicates th	at all of tl	he 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:

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

```
\label{thm:cosoftware} HKCU\Software\Microsoft\Windows\Current\Version\Explorer\Mount\Points2 \\ \left\{ab7c3e54-924c-11de-83b1-00e0b8534ba4\right\}\BaseClass \\ HKCU\Software\Microsoft\Windows\Current\Version\Explorer\Mount\Points2 \\ \left\{e727fc90-921e-11de-b2a5-806d6172696f\right\}\BaseClass \\ HKCU\Software\Microsoft\Windows\Current\Version\Explorer\Mount\Points2 \\ \left\{e727fc91-921e-11de-b2a5-806d6172696f\right\}\BaseClass \\ HKCU\Software\Microsoft\Windows\Current\Version\Explorer\Mount\Points2 \\ \left\{e727fc92-921e-11de-b2a5-806d6172696f\right\}\BaseClass \\ \\ \left\{e727fc92-921e-11de-b2a5-806d6172696f\right\}
```

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
```

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

 $\label{thm} \begin{tabular}{l} HKLM\softWare\mbox{\tt Microsoft\RFC1156Agent\CurrentVersion\Name} \\ Parameters\mbox{\tt TrapPollTimeMilliSecs} \\ \end{tabular}$ 

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: Runn	nerTest011 Date: 26 August 2009		
<b>Description</b> : Runr	ning a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP2)		
Tester Name:	MBowser Test Machine: Paul		
Assertions Tested:	<ol> <li>All programs identified in the profile were executed.</li> <li>Results of the tools were properly stored on the investigator's thumb drive.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive (File System).</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive (Registry).</li> <li>The tools executed were run from the thumb drive, not from the suspect's</li> </ol>		
Unique Setup	machine.  System was loaded with Microsoft Windows XP Service Pack 2.		
Information:	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:	All programs identified in the profile were executed.  As Expected		
Assertion.	<ul><li>2. Results of the tools were properly stored on the investigator's thumb drive.</li></ul>		
	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).  Anomaly Detected		
	5. The tools executed were run from the thumb  As Expected		
Tester Notes:	drive, not from the suspect's machine.  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		

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).

 ${\tt HKLM} \\ {\tt SOFTWARE} \\ {\tt Microsoft} \\ {\tt Cryptography} \\ {\tt RNG} \\ {\tt Seed} \\$ 

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\CategoryMessageFile
HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\EventMessageFile
HKLM\System\CurrentControlSet\Services\Eventlog\ Application\ESENT\TypesSupported
In addition to any writes listed above, <i>pslist.exe</i> 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."

As Expected

**Overall Success:** 

Test Name:	RunnerTest012	<b>Date</b> : 26 August 2009		
Description:	Running a COFEE generated thumb drive with the N			
Tester Name:				
Assertions Tested:	<ol> <li>Results of the tools were properly store</li> <li>Executing runner exe did not cause any</li> </ol>	<ol> <li>Results of the tools were properly stored on the investigator's thumb drive.</li> <li>Executing runner.exe did not cause any direct writes to the suspect drive's</li> </ol>		
	Registry.	<ul><li>4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry.</li><li>5. The tools executed were run from the thumb drive, not from the suspect's</li></ul>		
Unique Setup		P Service Pack 2.		
Information:	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
	1GB PNY Attaché Thumb Drive with the "NW3C as well as Process Monitor. Internal ID#: IR1 Drive SN#FAV3RW6Q0			
Results By	All programs identified in the profile we			
Assertion:	executed.  2. Results of the tools were properly store investigator's thumb drive.	ed on the As Expected		
	Executing runner.exe did not cause any writes to the suspect drive (File System)	•		
	4. Executing runner.exe did not cause any writes to the suspect drive (Registry).	· ·		
	<ol><li>The tools executed were run from the t drive, not from the suspect's machine.</li></ol>	·		
Tester Notes:	The thumb drive was first connected to the mabooting to Windows. After the thumb drive dri navigated to the thumb drive and started Proces	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 of the thumb drive and ran "runner.exe."	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	6 am		
	Immediately after the completion of runner, th capture and saved the log file to the thumb driv testing of the assertions listed above. The resu	ve. The log file was examined later for		
	Assertion 1: An examination of the thumb drive's file system associated with the NW3C-Incident Response p disk.			
	An examination of the Process Monitor logs ind associated with the NW3C-Incident Response p 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:

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

 $\label{local-bound} HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\\ \left\{02bb35eb-1621-11da-840f-806d6172696f\right\}\BaseClass$ 

 $\label{local-bound} HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\\ \left\{02bb35ec-1621-11da-840f-806d6172696f\right\}\BaseClass$ 

 $\label{lem:hcu} HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\\ c583de36-925c-11de-b154-000d6119d38a\BaseClass$ 

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

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

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

### 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)