COFEE version 1.1 Runner and NW3C Profiles

Validation Study

9/02/2009

Written and Tested By:

Charles Matt Weir, CISSP
SriHarsha Angara
Graduate Research Students
Florida State University

E-Crime Investigative Technologies Laboratory Background

ECIT

The E-Crime Investigative Technologies Laboratory (ECIT) is a part of Florida State University's computer science department. Its focus is to conduct research in support of digital forensics investigations by developing new technologies and forensic tools to address real-world problems related to electronic and/or digital crime. ECIT often works closely with the Florida Department of Law Enforcement and with the National White Collar Crime Center.

What ECIT Does

ECIT collaborates closely with the Florida Department of Law Enforcement and the National White Collar Crime Center and partners such as the AccessData Corporation. The goal is to build novel systems for E-crime investigations. The mechanism of developing projects is: (1) brainstorming with law enforcement agents and others to determine law enforcement investigative needs; (2) exploring novel technologies to be used in support of the resulting requirements; and (3) developing prototype systems and tools that can be used in investigations.

This has resulted in the development of several computer forensics applications such as the DNA project, dedicated to the cryptanalysis of passwords; the UnMask project, which addresses the issue of automated support for investigation of phishing attacks; and the PAPA project, which was designed to capture interactions with cyber stalkers and perform sting operations.

Research by the ECIT Laboratory has been presented at numerous peer reviewed conferences such as the 2009 IEEE Security and Privacy Conference, the 23rd Computer Security Applications Conference, the 2009 DoD Cybercrime Conference, and more.

Table of Contents

E-Crime Investigative Technologies Laboratory Background 2

Table of Contents 3

Introduction 4

Purpose and Scope 4

Test Result Summary 4

Test Assertions 5

Testing Environment 5

Test Computer 5

Support Software Used 6

Additional Information 6

Test Results 7

Test Results Report Key 7

Report Notes 40

Additional References 40

Glossary 40

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

Run Environments: Windows XP Service Pack 2 and Windows XP Service Pack 3

Supplier: Microsoft & NW3C

Purpose and Scope

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 attempted to make five writes to the target computer's file system. Three of the 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 unlikely to be of any evidentiary interest. The other two attempted writes were made to network shares on the target computer, and were also unlikely to be of any 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."

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. ASUS P5LD2 ("ECIT-01")
    a. Serial Number: 492000411072
    b. Processor: Intel® Pentium® D CPU 3.01 GHZ, 3.00GHZ
    c. Ram: 1 GB RAM
    d. Hard Drive: 80GB

2. ASUS P5LD2 ("ECIT-02")
    a. Serial Number: 492000411074
    b. Processor: Intel® Pentium® D CPU 3.01 GHZ, 3.00GHZ
    c. Ram: 1 GB RAM
    d. Hard Drive: 80GB

3. Dell Optiplex 745 ("ECIT-03")
    a. Serial Number: 492000408775
    b. Processor: Inter® Core™ CPU 6400 @ 2.13 Ghz, 2.13 Ghz
    c. Ram: 2 GB RAM
    d. Hard Drive: 250 GB

Support Software Used

1. Process Monitor was used to record all processes and writes made during the testing of the generated thumb drives. Process Monitor is a free Windows Sysinternals tool written by Mark Russinovich and Bryce Cogswell. This software was downloaded from:

   http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

Additional Information

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

Test Results

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

Test Results Report Key

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

Test Results Report Key			
Test Name:	RunnerTest-NW3C-VolatileDataFormat-0001	**Date**:	29 August 2009
Description:	Running a COFEEE generated thumb drive with the NW3C Volatile Data Profile (SP2)		
Tester Name:	CWeir, SAngara	**Test Machine**:	ECIT-02
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (file system). 4. Executing runner.exe did not cause any direct writes to the suspect drive (registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	The System was loaded with Microsoft Windows XP Service Pack 2 4GB Thumbdrive with the "NW3C – Volatile Data" profile loaded.		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (file system). 4. Executing runner.exe did not cause any direct writes to the suspect drive (registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.	As Expected As Expected As Expected Anomaly Detected As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-02), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran "runner.exe." Start Time: 16:17 (EST) End Time: 16:18 (EST) 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 the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. Each program had been given a unique four digit file name, such as "2134.exe". Each program was verified by either the "INTERNAL FILE NAME", or execution of it on the COFEE GUI		

machine which created the thumb drives, (ECIT-03).

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 File system information, (excluding the "E:" drive which contained the COFEE USB drive), and searching for any "WriteFile" operation.

Assertion 4:
A total of 117 writes/updates/deletions were made to the registry by Runner and its processes (to include all the programs within the selected profile). These results will also include attempts to change the registry that were not allowed (i.e. an attempt was made to delete a key that did not 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.

There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key are as follows: Runner.exe (8), Ipconfig (8), Net (8), Pslist (2), Quser (1), Netstat (16), Sclist (1), Showgrps (1), Systeminfo (8), Cmd (52).

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

In addition to any writes listed above, Ipconfig made writes to the following 5 registry keys:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\3116\DEBUG\Trace Level

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

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

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

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\TypesSupported
```

One delete was attempted by Ipconfig to the following registry key

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\3116\DEBUG\Trace Level
```

Pslist.exe attempted to delete the following 4 registry keys

	HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfOS\Performance\Error Count HKLM\System\CurrentControlSet\Services\PerfProc\Performance\Error Count Netstat attempted to make 2 writes to the following registry key HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs 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. This was done using the filters "Operation is LoadImage", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were unlikely to be of any evidentiary concern. In addition, the modifications were a result of running these tools on a live machine, and could not be avoided. 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 Results Report Key			
Test Name:	RunnerTest-NW3C-IncidentResponseFormat-0002	**Date**:	31 August 2009
Description:	Running a COFEEE generated thumb drive with the NW3C Incident Response Profile (SP2)		
Tester Name:	CWeir, SAngara	**Test Machine**:	ECIT-02
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (file system). 4. Executing runner.exe did not cause any direct writes to the suspect drive (registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	The System was loaded with Microsoft Windows XP Service Pack 2 4GB Thumbdrive with the "NW3C – Incident Response" profile loaded.		
Results By Assertion:	1. All programs identified in the profile were executed.	As Expected	
	2. Results of the tools were properly stored on the investigator's thumb drive.	As Expected	
	3. Executing runner.exe did not cause any direct writes to the suspect drive (file system).	Anomaly Detected	
	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 drive, not from the suspect's machine.	As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-02), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran "runner.exe." Start Time: 10:51 (EST) End Time: 10:53 (EST) 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 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. Each program had been given a unique four digit file name, such as "2134.exe". Each program was verified by either the "INTERNAL FILE NAME", or execution of it on the COFEE GUI machine which created the thumb drives, (ECIT-03).		

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 5 attempted writes to the suspect's machine. This test was performed by filtering the Process Monitor log results to show only File system information, (excluding the "E:" drive which contained the COFEE USB drive), and searching for any "WriteFile" operation.

Handle.exe made three writes to the following file

```
C:\WINDOWS\system32\drivers\PROCEXP100.sys
```

Srvcheck.exe made one write to the following file

```
\\127.0.0.1\PIPE\winreg
```

Showgrps.exe attempted to make the following write, but it failed due to "BAD NETWORK PATH"

```
\\ECIT-02**\MAILSLOT\NET\NETLOGON
```

These file writes are coded into the tools, and are unlikely to be of evidentiary interest.

Assertion 4:
A total of 262 writes/updates/deletions were made to the registry by Runner and its processes (to include all the programs within the selected profile). These results will also include attempts to change the registry that were not allowed (i.e. an attempt was made to delete a key that did not 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.

There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key are as follows: Runner.exe (8), Sclist.exe (1), Showgrps.exe (1), Netstat.exe (16), Autorunsc.exe (8), Getmac.exe (8), Net.exe (9), Psservice.exe (1), Openfiles.exe (1), Ipconfig.exe (8), Tasklist.exe (8), Pslist.exe (2), Hostname.exe (8), Quser.exe (1), Arp.exe (8), Sc.exe (2), cmd (133).

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

In addition to any writes listed above, autorunsc made writes to the following 4 registry keys:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
{f8da80be-94b8-11de-83d9-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
{b50bbec3-94b9-11de-b2a5-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
{b50bbec2-94b9-11de-b2a5-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
E\BaseClass
```

In addition to the above, Arp.exe made 1 write to the following registry key

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

In addition to any writes listed above, Ipconfig.exe made writes to the following 5 registry keys:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\7000\DEBUG\Trace Level

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Eve
ntMessageFile

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Cat
egoryMessageFile

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Cat
egoryCount

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Typ
esSupported
```

In addition to the above, Ipconfig.exe attempted to delete the following registry key

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\7000\DEBUG\Trace Level
```

In addition to the above, Pslist.exe attempted to delete the following 4 registry keys

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

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

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

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

In addition to the above, Handle made writes to the following 4 registry keys

```
HKLM\System\CurrentControlSet\Services\PROCEXP100\Type

HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl

HKLM\System\CurrentControlSet\Services\PROCEXP100\Start

HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath
```

	In addition to the above, Handle made 2 deletes to the following registry keys
	`HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum`
	`HKLM\System\CurrentControlSet\Services\PROCEXP100`
	In addition to the above, Netstat made writes to the following 2 registry keys
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	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. This was done using the filters "Operation is Load Image", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe.
	Additional Tester Notes:
	While there were several writes to the system's registry, the registry keys modified were unlikely to be 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, five additional writes were attempted to the target computer, with only 4 of the writes being successful. Just as with the above registry modifications, these writes were unlikely to modify any files of evidentiary concern, and could not be avoided short of not running the programs in question.
	While there were slight changes to the registry, and several writes to the target machine, 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 Results Report Key			
Test Name:	RunnerTest-NW3C-VolatileDataFormat-0003	**Date**:	31 August 2009
Description:	Running a COFEEE generated thumb drive with the NW3C Volatile Data Profile (SP2)		
Tester Name:	CWeir, SAngara	**Test Machine**:	ECIT-01
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (file system). 4. Executing runner.exe did not cause any direct writes to the suspect drive (registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	The System was loaded with Microsoft Windows XP Service Pack 2 4GB Thumbdrive with the "NW3C – Volatile Data" profile loaded.		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (file system). 4. Executing runner.exe did not cause any direct writes to the suspect drive (registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.	As Expected As Expected As Expected Anomaly Detected As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-01), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran "runner.exe." Start Time: 13:41 (EST) End Time: 13:42 (EST) 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 the assertions listed above. The results of the analysis are detailed below: Assertion 1: An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. Each		

program had been given a unique four digit file name, such as “2134.exe”. Each program was verified by either the “INTERNAL FILE NAME”, or execution of it on the COFEE GUI machine which created the thumb drives, (ECIT-03).

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 File system information, (excluding the “E:” drive which contained the COFEE USB drive), and searching for any “WriteFile” operation.

Assertion 4:
A total of 117 writes/updates/deletions were made to the registry by Runner and its processes (to include all the programs within the selected profile). These results will also include attempts to change the registry that were not allowed (i.e. an attempt was made to delete a key that did not 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.

There were 105 writes made to the registry key below. The breakdown of the programs that updated this registry key are as follows: Runner.exe (8), Ipconfig (8), Net (8), Pslist (2), Quser (1), Netstat (16), Sclist (1), Showgrps (1), Systeminfo (8), Cmd (52).

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

In addition to any writes listed above, Ipconfig made writes to the following 5 registry keys:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\3074\DEBUG\Trace Level

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\Ev
entMessageFile

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\Ca
tegoryMessageFile

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\Ca
tegoryCount

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\Ty
pesSupported
```

One delete was attempted by Ipconfig to the following registry key

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\3074\DEBUG\Trace Level
```

Pslist.exe attempted to delete the following 4 registry keys

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

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

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

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

Netstat attempted to make the following two writes

```
HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPo
llTimeMilliSecs

HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPo
llTimeMilliSecs
```

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. This was done using the filters "Operation is LoadImage", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe.

Additional Tester Notes:
While there were several writes to the system's registry, the registry keys modified were unlikely to be of any evidentiary concern. In addition, the modifications were a result of running these tools on a live machine, and could not be avoided. 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 Results Report Key			
Test Name:	RunnerTest-NW3C-IncidentResponseFormat-0004	**Date**:	31 August 2009
Description:	Running a COFEEE generated thumb drive with the NW3C Incident Response Profile (SP2)		
Tester Name:	CWeir, SAngara	**Test Machine**:	ECIT-01
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (file system). 4. Executing runner.exe did not cause any direct writes to the suspect drive (registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	The System was loaded with Microsoft Windows XP Service Pack 2 4GB Thumbdrive with the "NW3C – Incident Response" profile loaded.		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (file system). 4. Executing runner.exe did not cause any direct writes to the suspect drive (registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.	As Expected As Expected Anomaly Detected Anomaly Detected As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-01), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran "runner.exe." Start Time: 15:22 (EST) End Time: 15:24 (EST) 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 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. Each program had been given a unique four digit file name, such as "2134.exe". Each program was verified by either the "INTERNAL FILE NAME", or execution of it on the COFEE GUI machine which created the thumb drives, (ECIT-03).		

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 5 attempted writes to the suspect's machine. This test was performed by filtering the Process Monitor log results to show only File system information, (excluding the "E:" drive which contained the COFEE USB drive), and searching for any "WriteFile" operation.

Handle.exe made three writes to the following file

```
        C:\WINDOWS\system32\drivers\PROCEXP100.sys
```

Srvcheck.exe made one write to the following file

```
        \\127.0.0.1\PIPE\winreg
```

Showgrps.exe attempted to make the following write, but it failed due to "BAD NETWORK PATH"

```
        \\ECIT-01**\MAILSLOT\NET\NETLOGON
```

These file writes are coded into the tools, and are unlikely to be of evidentiary interest.

Assertion 4:
A total of 262 writes/updates/deletions were made to the registry by Runner and its processes (to include all the programs within the selected profile). These results will also include attempts to change the registry that were not allowed (i.e. an attempt was made to delete a key that did not 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.

There were 239 writes made to the registry key below. The breakdown of the programs that updated this registry key are as follows: Runner.exe (8), Sclist.exe (1), Showgrps.exe (1), Netstat.exe (16), Autorunsc.exe (8), Getmac.exe (8), Net.exe (9), Psservice.exe (1), Openfiles.exe (1), Ipconfig.exe (8), Tasklist.exe (8), Pslist.exe (2), Hostname.exe (8), Quser.exe (1), Arp.exe (8), Sc.exe (2), Cmd (133).

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

In addition to any writes listed above, autorunsc made writes to the following 4 registry keys:

```
        HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
        {5878707d-94b8-11de-8dc5-806d6172696f}\BaseClass

        HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
        {883190a4-9654-11de-9b57-00173115d87b}\BaseClass

        HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
        {429adec3-94b9-11de-9b4e-806d6172696f}\BaseClass

        HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
        {429adec2-94b9-11de-9b4e-806d6172696f}\BaseClass
```

In addition to the above, Arp.exe made 1 write to the following registry key

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

In addition to any writes listed above, Ipconfig.exe made writes to the following 5 registry keys:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\8109\DEBUG\Trace Level

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Eve
ntMessageFile

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Cat
egoryMessageFile

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Cat
egoryCount

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\Typ
esSupported
```

In addition to the above, Ipconfig.exe attempted to delete the following registry key

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\8109\DEBUG\Trace Level
```

In addition to the above, Pslist.exe attempted to delete the following 4 registry keys

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

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

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

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

In addition to the above, Handle made writes to the following 4 registry keys

```
HKLM\System\CurrentControlSet\Services\PROCEXP100\Type

HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl

HKLM\System\CurrentControlSet\Services\PROCEXP100\Start

HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath
```

	In addition to the above, Handle made 2 deletes to the following registry keys
	`HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum`
	`HKLM\System\CurrentControlSet\Services\PROCEXP100`
	In addition to the above, Netstat made writes to the following 2 registry keys
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	`HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters\TrapPollTimeMilliSecs`
	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. This was done using the filters "Operation is Load Image", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe.
	Additional Tester Notes:
	While there were several writes to the system's registry, the registry keys modified were unlikely to be 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, five additional writes were attempted to the target computer, with only 4 of the writes being successful. Just as with the above registry modifications, these writes were unlikely to modify any files of evidentiary concern, and could not be avoided short of not running the programs in question.
	While there were slight changes to the registry, and several writes to the target machine, 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 Results Report Key			
Test Name:	RunnerTest-NW3C-IncidentResponseFormat-0005	**Date**:	1st September, 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP3)		
Tester Name:	SAngara, CWeir	**Test Machine**:	ECIT-02
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. Used 2G PNY Attache' Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor		
Results By Assertion:	1. All programs identified in the profile were executed.	As Expected	
	2. Results of the tools were properly stored on the investigator's thumb drive.	As Expected	
	3. Executing runner.exe did not cause any direct writes to the suspect drive (File System).	Anomaly Detected	
	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 drive, not from the suspect's machine.	As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-02), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran "runner.exe." Start Time: 10:32 (EST) End Time: 10:34 (EST) 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 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. Each program had been given a unique four digit file name, such as “2134.exe”. Each program was verified either by the “INTERNAL FILE NAME”, or execution of it on the COFEE GUI machine which created the thumb drives, (ECIT-03).

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 5 attempted writes to the suspect’s machine. This test was performed by filtering the Process Monitor log results to show only File system information, (excluding the “E:” drive which contained the COFEE USB drive), 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
```

One of which failed due to FAST I/O DISALLOWED.

In addition to the above writes, one write was made by srvcheck.exe to

```
        \\127.0.0.1\PIPE\winreg
```

In addition to the above write, one write was attempted (but failed, due to BAD NETWORK PATH) by showgrps.exe to

```
        \\ECIT-02**\MAILSLOT\NET\NETLOGON
```

These file writes are coded into the tools, and are unlikely to 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\MountPoints
2\{f8da80be-94b8-11de-83d9-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints
2\{be33e6dc-963d-11de-b2b0-00173115d853}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints
2\{b50bbec3-94b9-11de-b2a5-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints
2\{b50bbec2-94b9-11de-b2a5-806d6172696f}\BaseClass
```

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

```
HKLM\System\CurrentControlSet\Services\PROCEXP100\Type
HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl
HKLM\System\CurrentControlSet\Services\PROCEXP100\Start
HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath
```

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

```
HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum
HKLM\System\CurrentControlSet\Services\PROCEXP100
```

In addition to any writes/deletes listed above, ipconfig.exe also made a one delete to the following registry key:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\6407\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\RFC1156Agent\CurrentVersion\Parameters\TrapPollMillSecs

HKLM\SOFTWARE\Microsoft\ESENT\Process\6407\DEBUG\Trace Level

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

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

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

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

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

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

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

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

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

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

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

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

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


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

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

HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\CategoryMessageFile
```

	`HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\CategoryCount`
	`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 attempted to make two deletes on each 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. This was done using the filters "Operation is LoadImage", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe.
	Additional Tester Notes:
	While there were several writes to the system's registry, the registry keys modified were unlikely to be of any evidentiary concern. In addition, the modifications were a result of running these tools on a live machine, and could not be avoided. 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."
	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 Results Report Key			
Test Name:	RunnerTest-NW3C-VolatileDataFormat-0006	**Date**:	1st September, 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP3)		
Tester Name:	SAngara, CWeir	**Test Machine**:	ECIT-02
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. Used 2G PNY Attache' Thumb Drive with the "NW3C – Incident Response" profile loaded.		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect's machine.	As Expected As Expected Anomaly Detected Anomaly Detected As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-02), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran "runner.exe." Start Time: 11:53 (EST) End Time: 11:53 (EST) 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 the assertions listed above. The results of the analysis are detailed below:		

Assertion 1:
An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. Each program had been given a unique four-digit file name, such as "2134.exe". Each program was verified either by the "INTERNAL FILE NAME", or execution of it on the COFEE GUI machine which created the thumb drives, (ECIT-03).

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 File system information, (excluding the "E:" drive which contained the COFEE USB drive), and searching for any "WriteFile" operation.

Assertion 4:
A total of 132 writes/updates/deletions were made to the registry by Runner and its processes (to include all the programs within the selected profile). These results will also include attempts to change the registry that were not allowed (i.e. an attempt was made to delete a key that did not 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.

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, 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, ipconfig.exe made one delete to the following registry key: HKLM\SOFTWARE\Microsoft\ESENT\Process\1475\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\LogSessionName 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\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\LogSessionName 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\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\QUtil\LogSessionName 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\traceIdentifier\Guid HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\QUtil\traceIdentifier\BitNames HKLM\SOFTWARE\Microsoft\ESENT\Process\1475\DEBUG\Trace Level HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\EventMessageFile

```
HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESEN
T\CategoryMessageFile

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESEN
T\CategoryCount

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESEN
T\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 attempted to make two deletes 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. This was done using the filters "Operation is LoadImage", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe.

Additional Tester Notes:
While there were several writes to the system's registry, the registry keys modified were unlikely to be of any evidentiary concern. In addition, the modifications were a result of running these tools on a live machine, and could not be avoided. 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."

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 Results Report Key			
Test Name:	RunnerTest-NW3C-VolatileDataFormat-0007	**Date**:	1st September, 2009
Description:	Running a COFEE generated thumb drive with the NW3C Volatile Data Profile (SP3)		
Tester Name:	SAngara, CWeir	**Test Machine**:	ECIT-01
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator’s thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive’s File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive’s Registry. 5. The tools executed were run from the thumb drive, not from the suspect’s machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. Used 2G PNY Attache’ Thumb Drive with the “NW3C – Incident Response” profile loaded.		
Results By Assertion:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator’s thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive (File System). 4. Executing runner.exe did not cause any direct writes to the suspect drive (Registry). 5. The tools executed were run from the thumb drive, not from the suspect’s machine.	As Expected As Expected Anomaly Detected Anomaly Detected As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-01), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran “runner.exe.” Start Time: 12:25 (EST) End Time: 12:25 (EST) 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 the assertions listed above. The results of the analysis are detailed below:		

Assertion 1:
An examination of the thumb drive's file system indicated that all of the programs associated with the NW3C-Volatile Data profile were successfully copied to the disk. Each program had been given a unique four-digit file name, such as "2134.exe". Each program was verified either by the "INTERNAL FILE NAME", or execution of it on the COFEE GUI machine which created the thumb drives, (ECIT-03).

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 File system information, (excluding the "E:" drive which contained the COFEE USB drive), and searching for any "WriteFile" operation.

Assertion 4:
A total of 132 writes/updates/deletions were made to the registry by Runner and its processes (to include all the programs within the selected profile). These results will also include attempts to change the registry that were not allowed (i.e. an attempt was made to delete a key that did not 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.

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, 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, ipconfig.exe made one delete to the following registry key:

```
HKLM\SOFTWARE\Microsoft\ESENT\Process\2916\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\LogSessionName

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\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\BitNa
mes

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

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\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Tracing\Microsoft\eappprxy\traceIdentifier\BitN
ames

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

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\traceIdentifier\Guid

HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Tracing\Microsoft\QUtil\traceIdentifier\BitName
s

HKLM\SOFTWARE\Microsoft\ESENT\Process\2916\DEBUG\Trace Level

HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESEN
```

	`T\EventMessageFile`
	`HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\CategoryMessageFile`
	`HKLM\System\CurrentControlSet\Services\Enventlog\Application\ESENT\CategoryCount`
	`HKLM\System\CurrentControlSet\Services\Enventlog\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 attempted to make two deletes 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. This was done using the filters "Operation is LoadImage", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe.
	Additional Tester Notes:
	While there were several writes to the system's registry, the registry keys modified were unlikely to be of any evidentiary concern. In addition, the modifications were a result of running these tools on a live machine, and could not be avoided. 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."
	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 Results Report Key			
Test Name:	RunnerTest-NW3C-IncidentResponseFormat-0008	**Date**:	1st September, 2009
Description:	Running a COFEE generated thumb drive with the NW3C Incident Response Profile (SP3)		
Tester Name:	SAngara, CWeir	**Test Machine**:	ECIT-01
Assertions Tested:	1. All programs identified in the profile were executed. 2. Results of the tools were properly stored on the investigator's thumb drive. 3. Executing runner.exe did not cause any direct writes to the suspect drive's File System. 4. Executing runner.exe did not cause any direct writes to the suspect drive's Registry. 5. The tools executed were run from the thumb drive, not from the suspect's machine.		
Unique Setup Information:	System was loaded with Microsoft Windows XP Service Pack 3. Used 2G PNY Attache' Thumb Drive with the "NW3C – Incident Response" profile loaded, as well as Process Monitor		
Results By Assertion:	1. All programs identified in the profile were executed.	As Expected	
	2. Results of the tools were properly stored on the investigator's thumb drive.	As Expected	
	3. Executing runner.exe did not cause any direct writes to the suspect drive (File System).	Anomaly Detected	
	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 drive, not from the suspect's machine.	As Expected	
Tester Notes:	For this test, the COFEE thumb drive was reformatted, and rebuilt on the COFEE GUI machine, (ECIT-03). The thumb drive was then connected to the target machine, (ECIT-01), after the target system had finished booting to Windows. After the thumb drive was loaded, the tester navigated to the thumb drive and started Process Monitor. One Process Monitor loaded, and had begun capturing data; the tester navigated to the thumb drive and ran "runner.exe." Start Time: 12:45 (EST) End Time: 12:47 (EST) 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 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. Each program had been given a unique four digit file name, such as "2134.exe". Each program was verified by either the "INTERNAL FILE NAME", or execution of it on the COFEE GUI machine which created the thumb drives, (ECIT-03).

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 5 attempted writes to the suspect's machine. This test was performed by filtering the Process Monitor log results to show only File system information, (excluding the "E:" drive which contained the COFEE USB drive), 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
```

one of which failed due to FAST I/O DISALLOWED.

In addition to the above writes, one write was made by srvcheck.exe to

```
        \\127.0.0.1\PIPE\winreg
```

In addition to the above write, one write was attempted (but failed, due to BAD NETWORK PATH) by showgrps.exe to

```
        \\ECIT-01**\MAILSLOT\NET\NETLOGON
```

These file writes are coded into the tools, and are unlikely to 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\MountPoints
2\{5878707d-94b8-11de-8dc5-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints
2\{883190a4-9654-11de-9b57-00173115d87b}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints
2\{429adec3-94b9-11de-9b4e-806d6172696f}\BaseClass

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints
2\{429adec2-94b9-11de-9b4e-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\Type
HKLM\System\CurrentControlSet\Services\PROCEXP100\ErrorControl
HKLM\System\CurrentControlSet\Services\PROCEXP100\Start
HKLM\System\CurrentControlSet\Services\PROCEXP100\ImagePath
```

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

```
HKLM\System\CurrentControlSet\Services\PROCEXP100\Enum
HKLM\System\CurrentControlSet\Services\PROCEXP100
```

In addition to any writes/deletes listed above, ipconfig.exe also made a one delete to the following registry key:

	HKLM\SOFTWARE\Microsoft\ESENT\Process\3230\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\RFC1156Agent\CurrentVersion\Parameters\TrapPollMillSecs
	HKLM\SOFTWARE\Microsoft\ESENT\Process\3230\DEBUG\Trace Level
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\LogSessionName
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\Active
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\ControlFlag
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\Guid
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\BitNames
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\LogSessionName
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\Active
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\ControlFlag
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\traceIdentifier\Guid
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappprxy\traceIdentifier\BitNames
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\QUtil\LogSessionName
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\QUtil\Active
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\QUtil\ControlFlag
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\QUtil\BitNames
	HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\EventMessageFile HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\CategoryMessageFile HKLM\System\CurrentControlSet\Services\EventLog\Application\ESENT\CategoryCount 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 attempted to make two deletes on each 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. This was done using the filters "Operation is LoadImage", and "Path ends with .dll then exclude". Note: .dll files were loaded from the target's computer and used by Runner.exe and programs invoked by Runner.exe. Additional Tester Notes: While there were several writes to the system's registry, the registry keys modified were unlikely to be of any evidentiary concern. In addition, the modifications were a result of running these tools on a live machine, and could not be avoided. 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." 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

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 52 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)