NW3C
NATIONAL WHITE COLLAR CRIME CENTER
INTEGRITY QUALITY SERVICE

COFEE v1.1.2 GUI CONSOLE

Validation Study

9/29/2009

Written and Tested By:

Mark Bowser, CFCE
Computer Crime Specialist, NW3C

Justin Wykes, 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.

BJA
Bureau of Justice Assistance
U.S. Department of Justice

Table of Contents

Introduction

The purpose of this report is to document the validation of Computer Online Forensic Evidence Extractor's (COFEE) ability to properly format, wipe, and generate a profile to a thumb drive. This report includes the validation of COFEE's ability to generate a report from collected data.

COFEE is a live information and volatile data acquisition suite. It is a GUI console based digital forensics tool developed for live (volatile) forensics evidence acquisition and analysis.

Tool Tested:	Computer Online Forensic Evidence Extractor (COFEE)
Version:	1.1.2
Run Environments:	Microsoft Windows XP with Service Pack 3
Supplier:	Microsoft and NW3C

Purpose and Scope

This validation study was conducted to verify COFEE properly formats, wipes, and generates profile(s) to a thumb drive, including its ability to generate a report from collected data.

This validation study was conducted to ensure that COFEE consistently completed all of its required actions.

Test Result Summary

All test assertions conducted on COFEE were successful.

COFEE successfully generated a listed profile, a user created profile, formatted an attached device as FAT 32 and overwrote or wiped data existing in unallocated space on the device.

COFEE successfully generated a detailed report of the results of the collected data from a specified profile.

There were no unexpected anomalies found during testing.

Test Assertions

The following test assertions were designed based upon the listed features of the COFEE tool

1. COFEE will not format a drive smaller than 1 GiB in size.
2. COFEE will only format drives 1 GiB in size or larger.
3. COFEE will format drives 2 GiB or larger.
4. COFEE will display a warning when formatting a drive between 1 GiB and 2 GiB.
5. COFEE will format a selected drive as FAT 32.
6. COFEE will format and wipe drives 1 GiB in size or larger.

7. COFEE will display a warning when formatting and wiping a drive between 1 GiB and 2 GiB in size.
8. An investigator can create their own application profile.
9. An investigator can save their own application profile for future use.
10. An investigator created profile can be used after COFEE is closed and restarted.
11. COFEE will not generate a profile on a device smaller than 1 GiB in size.
12. COFEE will generate a profile on a 1 GiB device along with its required files.
13. COFEE will generate a 2 GiB or larger drive with a profile.
14. All data generated by the programs in the specified profile were successfully created in the report.
15. COFEE successfully verified the HASH values of the files generated in the specified profile to ensure that no changes have been made since their creation.

Testing Environment

Test Computer

1. Dell Latitude D-820 Laptop ("CHAD")
    a. T2500 CPU 2.00GHz
    b. 2 GB RAM
    c. Serial-ATA 2.5" Hard Drive
        i. Hitachi 60 GiB, 7200 RPM, Model HTS721060G9A00
        ii. Serial Number: MPCCN8Y3HULBGL
        iii. The drive contained one Primary Partition which was reported as 55.88 GB
2. Gateway 600YG2 Laptop ("Abe")
    a. Serial Number: 0029567634
    b. Intel Pentium 4 – Mobile 2.00GHz
    c. 512 MB RAM
    d. PATA 2.5" Hard Drive
        i. IBM IC25N030ATCS04-0 30GB Hard Drive
        ii. Serial Number: DAH4W0AB
        iii. The drive contained one Primary Partition which was reported as 27.94 GB
3. Thumb Drives formatted as FAT 32.
    a. 512 MB Hitachi S/N-HTS721060G9SA00
    b. 1 GiB Lexar Jump Drive S/N-106A20320411403085
    c. 2 GiB Rally S/N-AA04012700061222
    d. Serial-ATA 2.5" Hard Drive
        1. 80 GiB Seagate 5400 RPM
        2. Serial Number: 5ly3lpna
        3. Connected by a Serial ATA to USB convertor
        4. S/N 6&a48b458

Support Software Used

1. Microsoft Windows XP Pro with SP 3 was used to create known data on the tested thumb drives. This software is licensed to NW3C.
2. AccessData FTK imager v. 2.5.5 was used to verify that deleted data was wiped.

Test Results

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

Test Results Report Key

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

Test Results

Test Name:	**COFEE Format 001**	**Date:**	**Sept 09,2009**
Description:	Using COFEE to format 512 MB thumb drive in FAT 32 FS		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	COFEE will not Format a drive smaller than 1GiB		
Unique Setup Information:	512MB Hitachi thumb drive. (S/N-HTS721060G9SA00)		
Results By Assertion:	COFEE will not format a 512 MB thumb drive.	As Expected	
Tester Notes:	**512 MB Thumb Drive** 1. Inserted the thumb drive with a small text file on it into USB port and allowed for the OS to install drivers. 2. Executed COFEE.exe. 3. W/I COFEE I Clicked on File, Format Device. 4. Clicked on the Drop down menu and selected the correct drive letter for the thumb drive. 5. Left Clicked Format button. 6. Message stating "The selected drive is 480.71MB in size, and is smaller than the required 1GiB to Format. It is also recommended that a drive of at least 2GiB be used with COFEE." 7. Clicked OK. 8. In Windows Explorer I verified that text file was still allocated and format type is FAT 32 had not changed on the thumb drive.		

Test Name:	**COFEE Format 002**	**Date**:	**Sept 09,2009**
Description:	Using COFEE to format 1GiB thumb drive in FAT 32 FS		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	1. COFEE will only format drives 1GiB in size or larger. 2. COFEE will display a warning when formatting a drive between 1GiB and 2GiB . 3. COFEE will format the selected drive as FAT 32.		
Unique Setup Information:	1GiB Lexar Jump drive thumb drive (S/N-106A20320411403085)		
Results By Assertion:	1. COFEE will only format drives greater than 1GiB. 2. COFEE will display a warning when formatting a drive between 1GiB and 2GiB . 3. COFEE will format the selected drive as FAT 32.	As Expected As Expected As Expected	
Tester Notes:	**1 GiB Thumb Drive** 1. Inserted the thumb drive with a small text file on it into USB port . 2. Executed COFEE.exe. 3. W/I COFEE I Clicked on File, Format Device. 4. Drop down menu selected the correct drive letter for the thumb drive. 5. Left Clicked Format button. 6. Message stating "The selected drive is 987.58 COFEE will allow you to continue, however the recommended size for the drive is 2GiB or greater" 7. Clicked OK. 8. In Windows Explorer I verified that text file was now unallocated 9. Format type is FAT 32 on the thumb drive.		
Overall Success:	As Expected		

Test Name:	**COFEE Format 003**	**Date:**	**Sept 09,2009**
Description:	Using COFEE to format 2 GiB thumb drive in FAT 32 FS		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	1. COFEE will format drives 2 GiB in size. 2. COFEE will format the selected drive as FAT 32.		
Unique Setup Information:	2GiB Rally thumb drive (S/N-AA04012700061222)		
Results By Assertion:	1. COFEE will format drives greater than 1GiB. 2. COFEE will format the selected drive as FAT 32.	As Expected As Expected	
Tester Notes:	**2 GiB Thumb Drive** 1. Inserted the thumb drive with a small text file on it into USB port 2. Executed COFEE.exe. 3. W/I COFEE I Clicked on File, Format Device. 4. Clicked on the drop down menu and selected the correct drive letter for the thumb drive. 5. Left Clicked Format button. 6. In Windows Explorer I verified that text file was now unallocated and format type is FAT 32 on the thumb drive.		
Overall Success:	As Expected		

Test Name:	**COFEE Format 004**	**Date:**	**Sept 2nd, 2009**
Description:	Using COFEE to format 80 GiB USB drive in FAT 32 FS		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	1. COFEE will format drives 80 GiB in size. 2. COFEE will format the selected drive as FAT 32.		
Unique Setup Information:	Serial-ATA 2.5" Hard Drive 5. 80 GiB Seagate 5400 RPM 6. Serial Number: 5ly3lpna 7. Connected by a Serial ATA to USB convertor 8. S/N 6&a48b458		
Results By Assertion:	1. COFEE will format drives greater than 1GiB. 2. COFEE will format the selected drive as FAT 32.	As Expected As Expected	
Tester Notes:	**80 GiB USB Drive** 1. Inserted the USB drive with a small text file on it into USB port 2. Executed COFEE.exe. 3. W/I COFEE I Clicked on File, Format Device. 4. Clicked on the drop down menu and selected the correct drive letter for the USB drive. 5. Left Clicked Format button. 6. In Windows Explorer I verified that text file was now unallocated and format type is FAT 32 on the thumb drive.		
Overall Success:	As Expected		

Test Name:	**COFEE Profile Creation 001**	**Date:**	**Sept 09,2009**
Description:	Using COFEE to create and save a user defined profile.		
Tester Name:	Mbowser	**Test Machine**:	Chad
Assertions Tested:	1. A user can create their own application profile. 2. A user can save their own application profile for future use. 3. A user created profile can be used after COFEE is closed and restarted.		
Unique Setup Information:	None		
Results By Assertion:	1. A user can create their own application profile. 2. A user can save their own application profile for future use. 3. A user created profile can be used after COFEE is closed and restarted.	As Expected As Expected As Expected	
Tester Notes:	1. Opened the COFEE program 2. Clicked on the “More Options (Advanced)” button 3. Removed all applications in the right screen by left clicking the double left arrow. 4. Highlighted and added one application from the left screen (net.exe was used for this test) and clicked the right arrow moving the applications to the right side of the screen. 5. Added an application that was not included any of the preexisting profiles by clicking on “Add Tool.” a. reg.exe was used for this test b. reg.exe was obtained from a previous version of the COFEE install. 6. Tool Property box opened, and the following information was entered: a. Description: b. Tool: Entered the location of reg.exe c. Arguments: blank d. Family: Registry e. Output Format: Text f. Vendor Name: blank g. Vendor Link: blank h. Required File(s): blank 7. Clicked “OK” 8. Added the new program to the running sequence by highlighting reg.exe and clicking the right arrow. 9. Clicked “Save Order” and gave the profile a unique name. (Marks) 10. Clicked the OK button. 11. Closed and restarted COFEE. 12. Observed that the Marks profile was listed – and loaded correctly.		
Overall Success:	As Expected		

Test Name:	**COFEE USB Drive Creation 001**	**Date:**	**Sept 09,2009**
Description:	COFEE will generate a 1GiB thumb drive with a profile.		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	COFEE will generate a profile on a 1 GiB device along with its required files.		
Unique Setup Information:	1 GiB Lexar Jump drive thumb drive (S/N- 106A20320411403085)		
Results By Assertion:	COFEE will generate a profile on a 1 GiB device along with its required files.	As Expected	
Tester Notes:	**1GiB thumb drive** 1. Inserted the formatted FAT 32 thumb drive into USB slot on the computer. 2. Opened the COFEE program. 3. Selected the drive letter drop down menu for the Thumb drive. 4. Selected the desired profile which was created during the test "COFEE Profile Creation 001." (Marks) 5. Click Generate button. 6. Opened Windows Explorer and verified the application from the selected profile were included on the thumb drive. (net.exe, reg.exe) 7. 12 Additional files were added to the thumb drive (Runner.exe, Autorun.inf, NW3C_SHA1.exe, Uptime.exe, Pausep.exe, Casenotes.txt, checksum, config.txt, DILABEL, filelist.txt, folders.txt, require.txt), 8. Click OK button. 9. Opened Windows Explorer and verified the applications from the selected profile were included on the thumb drive.		
Overall Success:	As Expected		

Test Name:	**COFEE USB Drive Creation 002**	**Date**:	**Sept 09,2009**
Description:	COFEE will generate a 2GiB thumb drive with a profile.		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	COFEE will generate a 2 GiB or larger drive with a profile.		
Unique Setup Information:	2 GiB Rally thumb drive (S/N- AA04012700061222)		
Results By Assertion:	COFEE will generate a profile on a 2 GiB device along with its required files.	As Expected	
Tester Notes:	**2GiB thumb drive**: 1. Created a user profile on COFEE using two programs (net.exe, reg.exe) 2. Inserted the formatted FAT 32 thumb drive into USB slot on the computer. 3. Opened the COFEE program. 4. Selected the drive letter drop down menu for the Thumb drive. 5. Selected the profile desired. (Marks) 6. Click Generate button. 7. Opened Windows Explorer and verified the application from the selected profile were included on the thumb drive. (net.exe, reg.exe) 8. 12 Additional files were added to the thumb drive (Runner.exe, Autorun.inf, NW3C_SHA1.exe, Uptime.exe, Pausep.exe, Casenotes.txt, checksum, config.txt, DILABEL, filelist.txt, folders.txt, require.txt), 9. Click OK button. 10. Opened Windows Explorer and verified the applications from the selected profile were included on the thumb drive.		
Overall Success:	As Expected		

Test Name:	**COFEE USB Drive Creation 003**	**Date**:	**Sept 09,2009**
Description:	COFEE will generate a 512 MB thumb drive with a profile.		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	COFEE will not generate a profile on a device smaller than 1GiB		
Unique Setup Information:	512 MB Hitachi thumb drive (S/N-HTS721060G9SA00)		
Results By Assertion:	COFEE will not generate a profile on a device smaller than 1GiB	As Expected	
Tester Notes:	**512 MB Thumb Drive** 1. Inserted the formatted FAT 32 thumb drive into USB slot on the computer. 2. Opened the COFEE program. 3. Selected the drive letter drop down menu for the Thumb drive. 4. Selected the profile desired. (Marks) 5. Click Generate button. 6. Received an error message stating “The selected drive is only 480.71 MB in size, and is too small to use with COFEE.” 7. Opened Windows explorer and verified that no files were placed on the thumb drive.		
Overall Success:	As Expected		

Test Name:	**COFEE USB CREATION 004**	**Date:**	**Sept 2nd, 2009**
Description:	COFEE will generate an 80 GiB USB drive with a profile.		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	COFEE will generate a 2 GiB or larger drive with a profile.		
Unique Setup Information:	Serial-ATA 2.5" Hard Drive 80 GiB Seagate 5400 RPM Serial Number: 5ly3lpna Connected by a Serial ATA to USB convertor S/N 6&a48b458		
Results By Assertion:	COFEE will generate a profile on a device larger than 2 GiB in size along with its required files.	As Expected	
Tester Notes:	**80 GiB USB Drive** 1. Created a user profile on COFEE using two programs (net.exe, reg.exe) 2. Inserted the formatted FAT 32 thumb drive into USB slot on the computer. 3. Opened the COFEE program. 4. Selected the drive letter drop down menu for the Thumb drive. 5. Selected the profile desired. (Marks) 6. Click Generate button. 7. Opened Windows Explorer and verified the application from the selected profile were included on the thumb drive. (net.exe, reg.exe) 8. 12 Additional files were added to the thumb drive (Runner.exe, Autorun.inf, NW3C_SHA1.exe, Uptime.exe, Pausep.exe, Casenotes.txt, checksum, config.txt, DILABEL, filelist.txt, folders.txt, require.txt), 9. Click OK button. 10. Opened Windows Explorer and verified the applications from the selected profile were included on the thumb drive.		
Overall Success:	As Expected		

Test Name:	**COFEE Format/Wipe 001**	**Date**:	**Sept 09,2009**
Description:	Using COFEE to format and wipe a thumb drive 1 GiB in size.		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	1. COFEE will Format and Wipe drives 1GiB or larger in size. 2. COFEE will display a warning when formatting and Wiping a drive between 1GiB and 2GiB . 3. COFEE will format the selected drive as FAT 32.		
Unique Setup Information:	1GiB Lexar Jump drive thumb drive (S\N-106A20320411403085)		
Results By Assertion:	1. COFEE will Format and Wipe drives 1GiB or larger in size.	As Expected	
	2. COFEE will display a warning when formatting and wiping a drive between 1GiB and 2GiB.	As Expected	
	3. COFEE will format the selected drive as FAT 32.	As Expected	
Tester Notes:	**1GiB Thumb Drive** 1. Inserted the thumb drive with a small text file on it into USB port and allowed for the OS to install drivers. 2. Executed COFEE.exe. 3. W/I COFEE I Clicked on File, Format Device. 4. Checked the box in the menu for “wipe and format Drive” 5. Drop down menu selected the correct drive letter for the thumb drive. 6. Left Clicked Format button. 7. Clicked OK. 8. Message stating “The wiping process is about to begin”. 9. Clicked OK. 10. In Windows Explorer I verified that text file was now unallocated and format type is fat 32 on the thumb drive. 11. Viewed the physical device using FTK imager and observed that the data had been deleted, a Fat 32 file system was installed, and the unallocated sectors/clusters had been overwritten with random Hex codes.		
Overall Success:	As Expected		

Test Name:	**COFEE Format/Wipe 002**	**Date**:	**Sept 09,2009**
Description:	Using COFEE to format and wipe a thumb drive 2 GiB in size.		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	1. COFEE will Format and Wipe drives greater than 1GiB. 2. COFEE will format the selected drive as FAT 32.		
Unique Setup Information:	2GiB Rally thumb drive (S\N-AA04012700061222)		
Results By Assertion:	1. COFEE will Format and Wipe drives greater than 1GiB. 2. COFEE will format the selected drive as FAT 32.	As Expected As Expected	
Tester Notes:	**2GiB Thumb Drive** 1. Inserted the thumb drive with a small text file on it into USB port and allowed for the OS to install drivers. 2. Executed COFEE.exe. 3. W/I COFEE I Clicked on File, Format Device. 4. Checked the box in the menu for "wipe and format Drive" 5. Drop down menu selected the correct drive letter for the thumb drive. 6. Left Clicked Format button. 7. Clicked OK. 8. Message stating "The wiping process is about to begin". 9. Clicked OK. 10. In Windows Explorer I verified that text file was now unallocated and format type is fat 32 on the thumb drive. 11. Viewed the physical device using FTK imager and observed that the data had been deleted, a Fat 32 file system was installed, and the unallocated sectors/clusters had been overwritten with random Hex codes.		
Overall Success:	As Expected		

Test Name:	**COFEE Format/Wipe 003**	**Date**:	**Sept 2nd,2009**
Description:	Using COFEE to format and wipe a USB drive 80 GiB in size.		
Tester Name:	MBowser	**Test Machine**:	Chad
Assertions Tested:	1. COFEE will Format and Wipe drives greater than 1GiB. 2. COFEE will format the selected drive as FAT 32.		
Unique Setup Information:	Serial-ATA 2.5” Hard Drive 1. 80 GiB Seagate 5400 RPM 2. Serial Number: 5ly3lpna 3. Connected by a Serial ATA to USB convertor 4. S/N 6&a48b458		
Results By Assertion:	1. COFEE will Format and Wipe drives greater than 1GiB. 2. COFEE will format the selected drive as FAT 32.	As Expected As Expected	
Tester Notes:	**80GiB USB Drive** 1. Inserted the USB hard drive with a small text file on it into USB port and allowed for the OS to install drivers. 3. Executed COFEE.exe. 4. W/I COFEE I Clicked on File, Format Device. 5. Checked the box in the menu for “wipe and format Drive” 6. Drop down menu selected the correct drive letter for the thumb drive. 7. Left Clicked Format button. 8. Clicked OK. 9. Text box alerted that wiping was complete. 10. Text box alerted that format was complete. 11. In Windows Explorer I verified that text file was now unallocated and format type is fat 32 on the thumb drive. 12. Viewed the physical device using FTK imager and observed that the data had been deleted, a Fat 32 file system was installed, and the unallocated sectors/clusters had been overwritten with E5 Hex codes.		
Overall Success:	As Expected		

Report Notes

This validation was conducted in conjunction with validations of the COFEE Runner and NW3C profiles. All assertions listed were validated and met expectations.

Additional References

Wykes, J. (2009). *COFEE v1.1 – Runner & NW3C Profiles*. National White Collar Crime Center.

Glossary

Format: Format prepares the logical drives for use by the operating system. Part of this process is creating certain "housekeeping" areas that contain structures for keeping track of file locations, root directory entries, etc.

Wipe: The process of overwriting unallocated data that exist on a digital storage device. COFEE wipes by overwriting the unallocated space with hex 00 characters.