User Guide for COFEE v1.1.2

Release Date: September 2009

Microsoft®

NW3C
NATIONAL WHITE COLLAR CRIME CENTER
INTEGRITY QUALITY SERVICE

BJA Bureau of Justice Assistance

Table of Contents

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.

Introduction

What is COFEE?

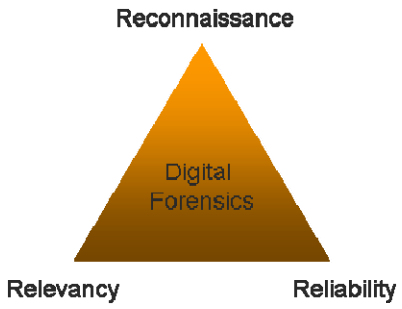
COFEE consists of three major components: the GUI interface for the investigator, the command-line application to be executed on the target machine, and the individual tools which are managed by COFEE and the command-line application.

There are two major types of live forensics investigation tools – Live Information Acquisition tools and Remote Online Acquisition tools. Computer Online Forensic Evidence Extractor (COFEE) is a live information and volatile data forensics acquisition system.

The GUI interface was developed for managing the tool selection, generating scripts, loading programs onto a USB device, and creating a report from the collected data. The command-line application was developed for controlling and executing a set of selected tools on the target machine.

Digital Forensics Attributes and Principles

In any digital forensics investigation, digital forensics specialists and legal advisors should ensure the balance between the three main attributes: Reconnaissance, Relevancy and Reliability of the digital evidence. In any digital forensics investigation, the investigator should always attempt to achieve the maximum amount of data acquisition while having a minimal effect on the integrity or accuracy of the data.



When applying Reconnaissance, Relevancy and Reliability to the live forensics investigation environment, it is paramount that any investigative tool used should operate in the least intrusive way. It is also vital that all operations conducted on a target machine be documented to the best extent possible. This aids in the reliability of the collected data, as well as the integrity of the target machine. Great effort was taken to ensure that the COFEE execution process leaves the smallest footprint possible on the target machine.

Volatile Information Collected

The specific information collected by COFEE varies depending upon which profile is selected, however the type of volatile information collected includes:

- Date and Time
- Open network connections and additional network related information
- User account information (including the currently logged-on user)
- Current processes and services
- Open files and registry information

Why Use COFEE?

In COFEE, the GUI interface is used for the preparation of the forensics tools and the assigning of the digital forensics execution order. According to live forensics guidelines, investigators should take into account the order of evidence volatility, while having minimal interaction with the target machine.

COFEE has been designed to provide the investigator the ability to collect evidence from a target system with the minimum of user interaction. After the GUI interface generates a COFEE USB device (copies all scripts and programs), the investigator can take the device and easily insert it onto a target machine, and begin the collection process by executing a single program.

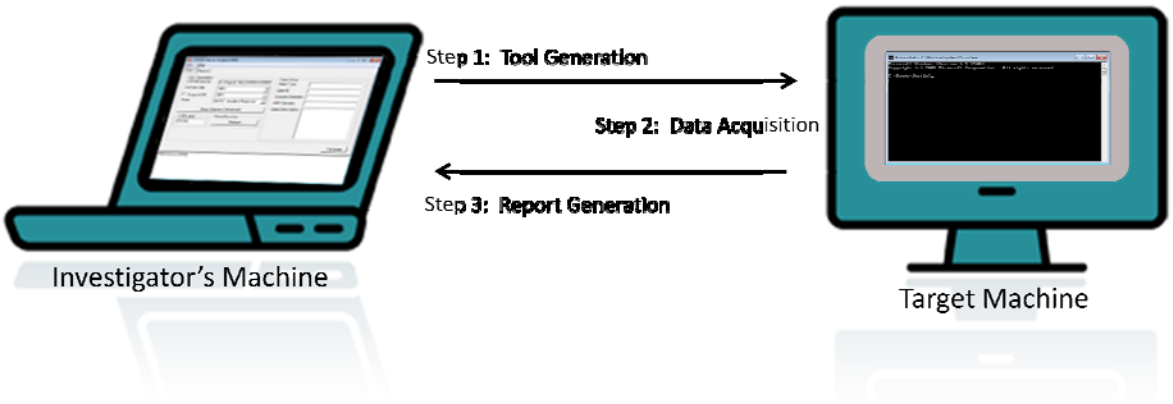
While specific programs have been selected as part of the included profiles, COFEE allows a seasoned investigator to add or remove any program they desire, as well as create any profile to meet their specific investigative needs.

Who Should Use COFEE?

COFEE was designed to meet the needs of two distinct classes of users: the forensic examiner and the front-line investigator. The GUI console, which allows the user to create profiles and generate COFEE USB devices, was designed to be operated by a computer forensic examiner. The creation of profiles requires that the user have a firm understanding of the tools to be executed and the reason behind their inclusion within the profile. The command-line application, however, requires minimal training because the scripting process has already been designed by a forensic examiner. This allows any front-line investigator to use this tool and collect data. Once the data is collected, the USB device should be returned to the forensic examiner for analysis.

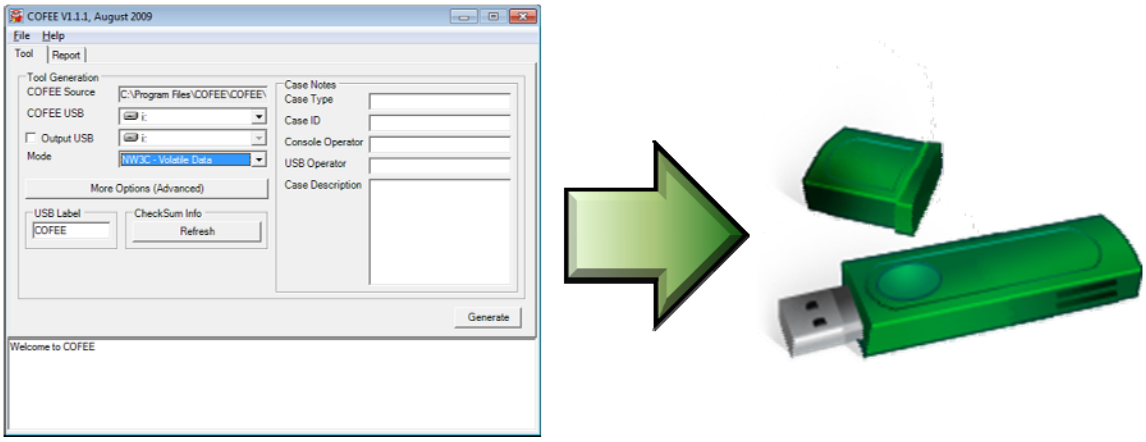
How to Use COFEE

The COFEE execution process is divided into three phases: Tool Generation, Data Acquisition, and Report Generation.



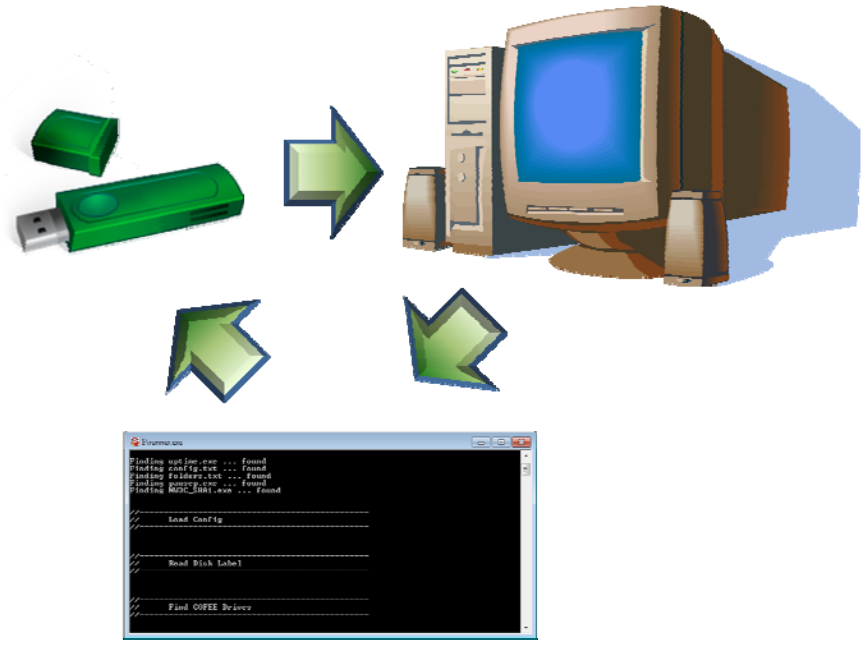
Tool Generation Phase

Digital Forensics Specialists have the ability to select desired tools to run against a target machine based on the individual case requirements. This can be done by either selecting a pre-defined profile, or by manually creating a profile and selecting which tools (including switches) are to be run against the target machine.



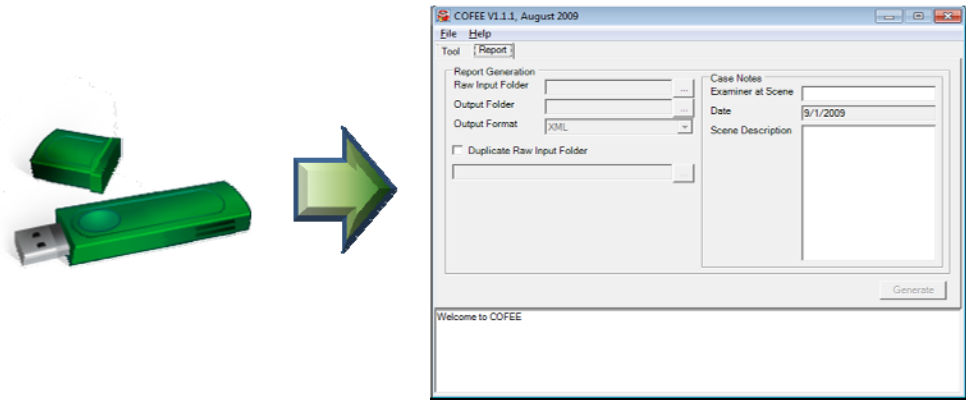
Data Acquisition Phase

After generation of the COFEE device, investigators can take the USB device and insert it into the target machine. Execution of COFEE on the suspect machine will then complete and all collected data will be stored on the USB device.



Report Generation Phase

After the collection of the volatile information from the target machine, investigators can load that information back into the GUI console on the investigator's machine and generate a report based upon the data.



Installation

Prerequisites

Before installing COFEE v1.1.2, please refer to the following hardware and software requirements for the Investigator Machine, USB Removable Device, and the Target Machine.

Investigator Machine

Hardware: Pentium 4 or Above
512 MB RAM
USB 1.1 or higher
50MB free hard drive space

Software: Windows XP or Above
.NET Framework 3.5 or higher

USB Removable Device

Hardware: Minimum 1GB Device
Recommended 2GB or larger

File System: FAT32 File System is recommended

Target Machine

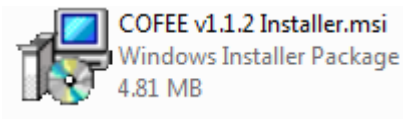
Hardware: USB Port Enabled

Software: Windows XP*

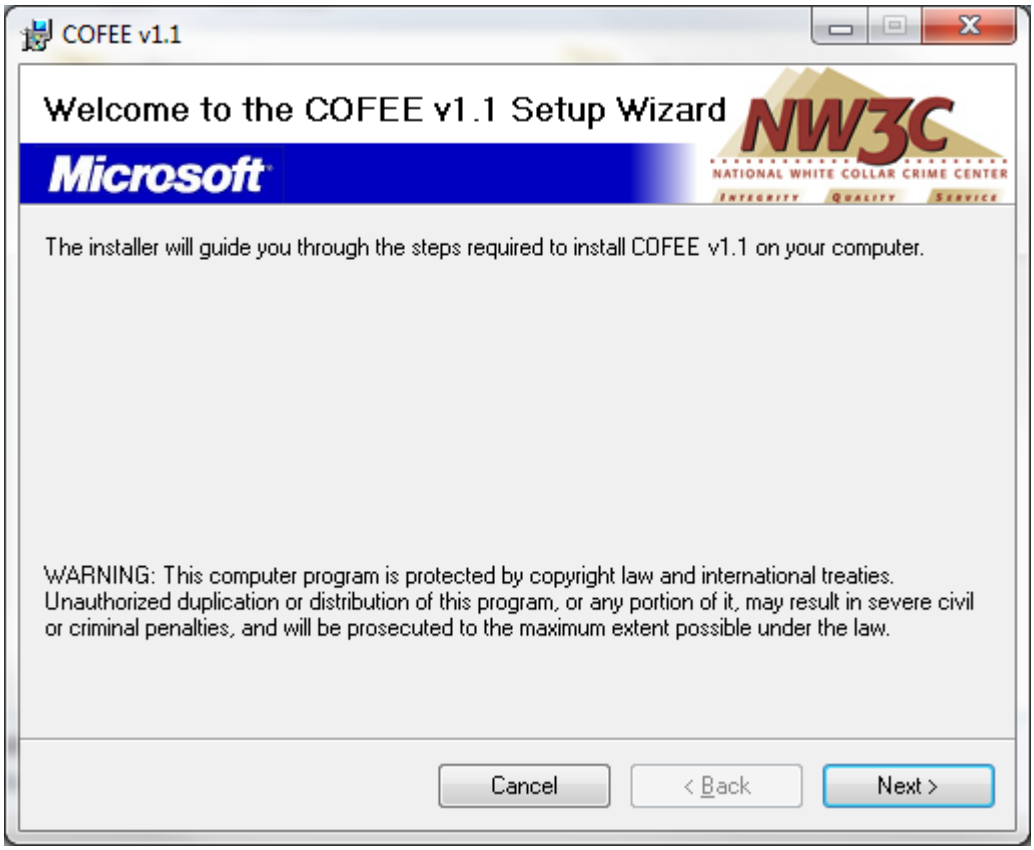
*Windows XP is currently the only supported operating system. It is possible that COFEE will work on additional operating systems, but these operating systems have not been tested, and are not supported.

Installation Steps

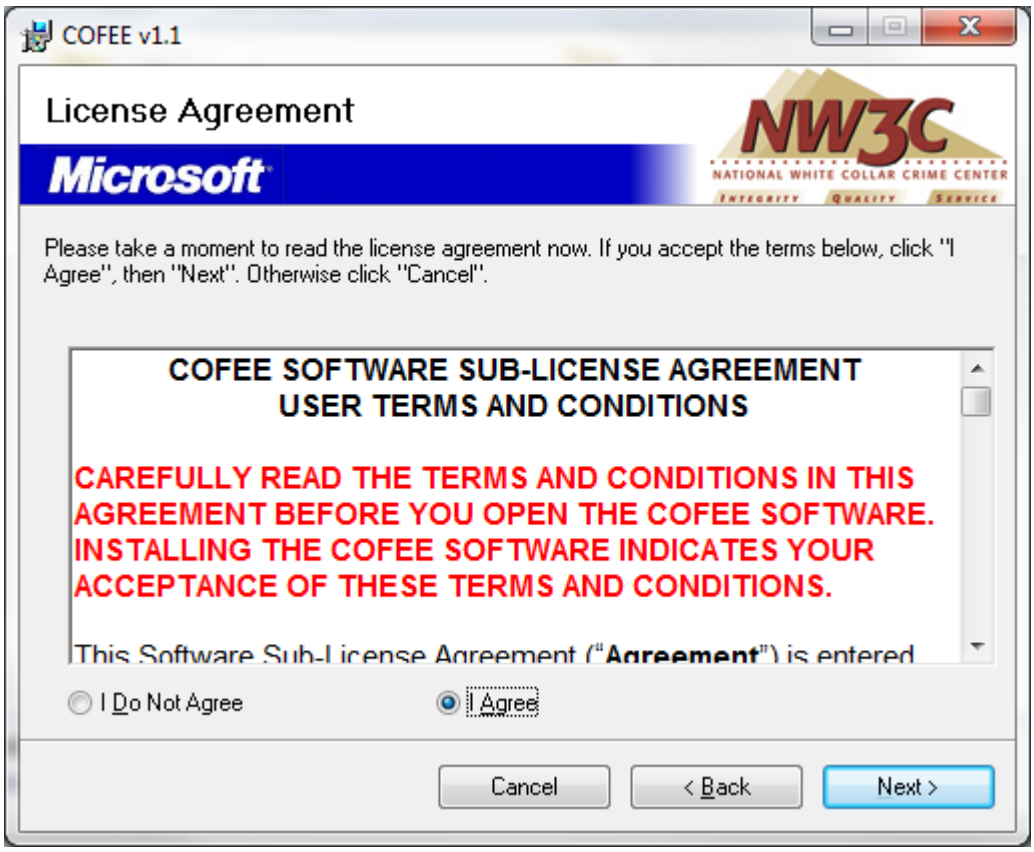
Step 1 – Execute the Installation Program "COFEE v1.1.2 Installer.msi."



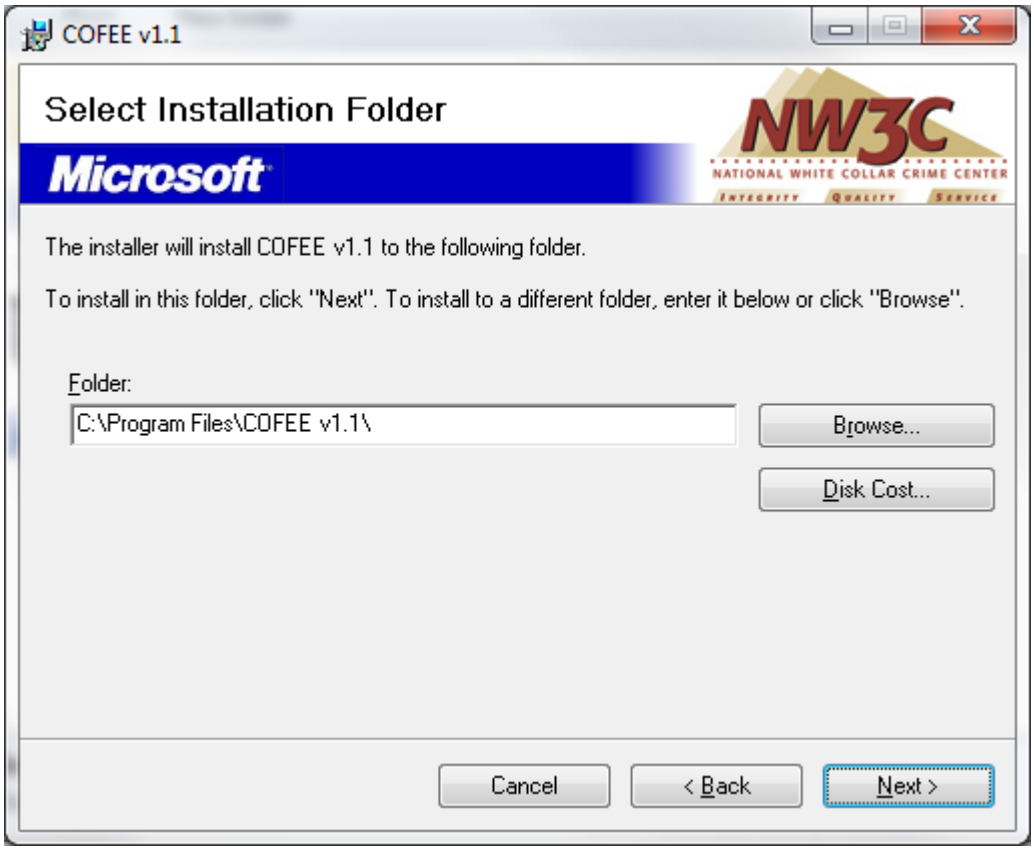
Step 2 – A setup wizard is displayed. Click "Next" to continue.



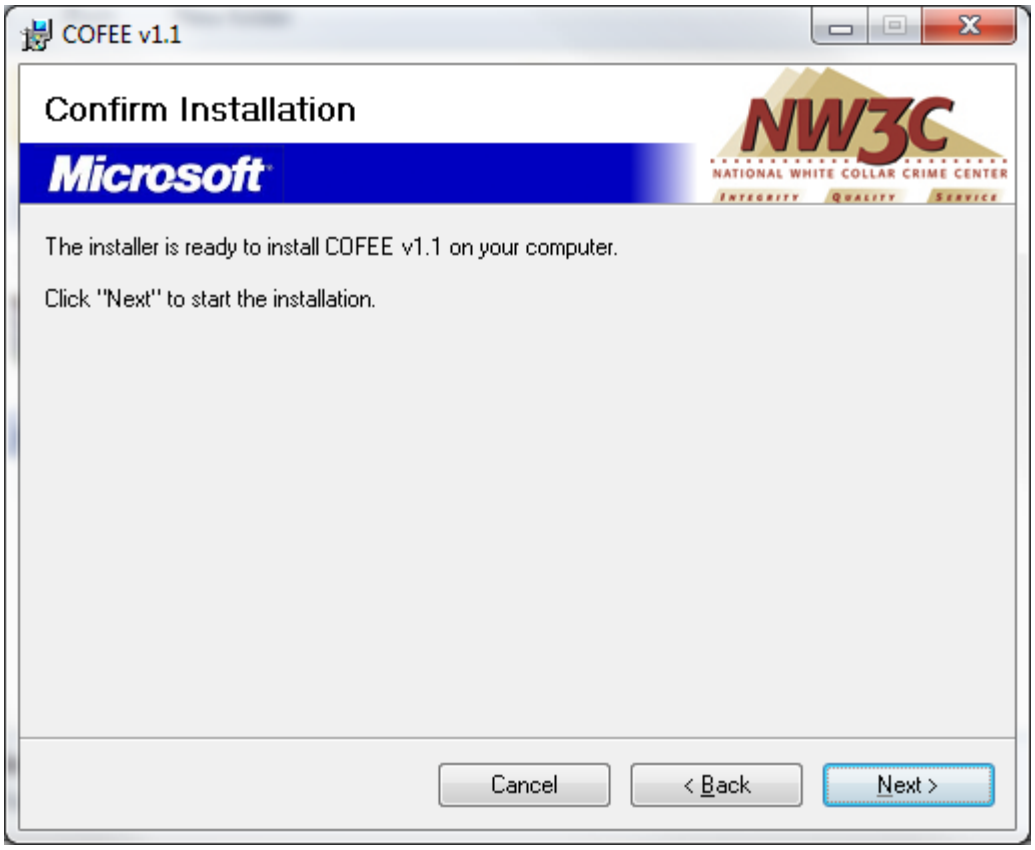
Step 3 – The COFEE License Agreement is displayed. Read the agreement carefully, select "I Agree," and click "Next" to continue.



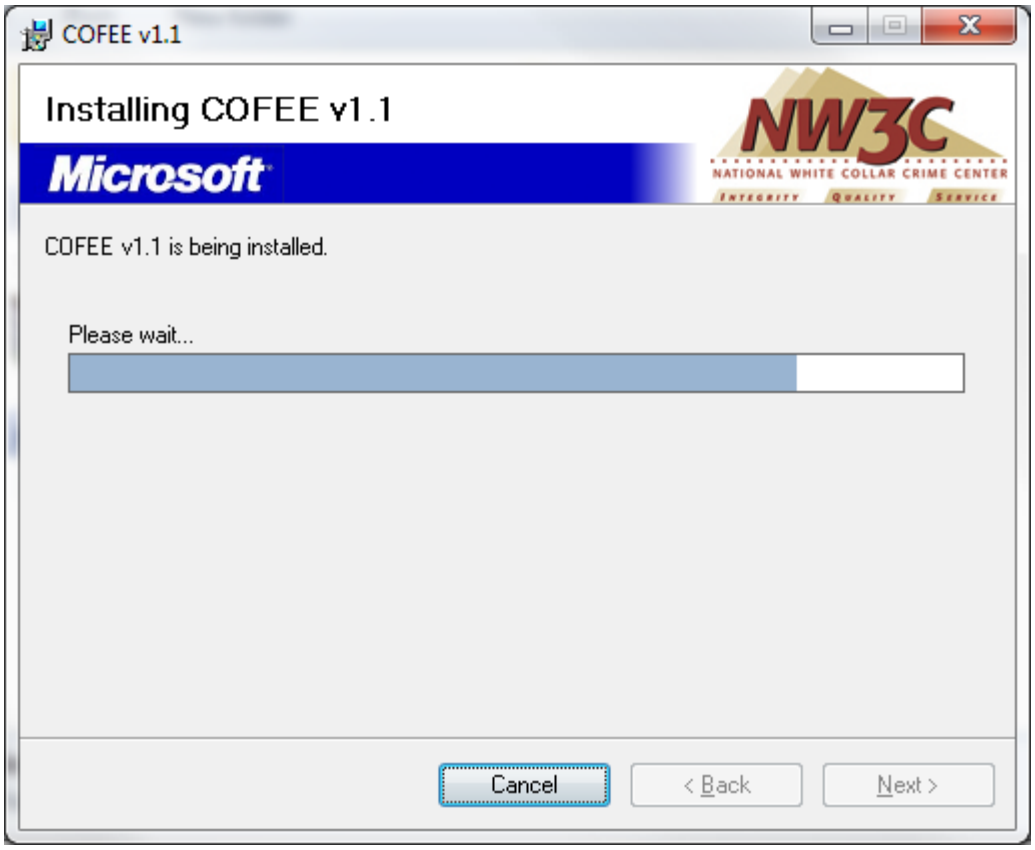
Step 4 – Select the folder in which to install COFEE. By default, the programs will be installed to "C:\Program Files\COFEE v1.1\." The "Disk Cost" button will display the amount of space the COFEE installation will take up on the investigator's computer based upon the installation folder selected. After selecting the installation folder, click "Next" to continue.



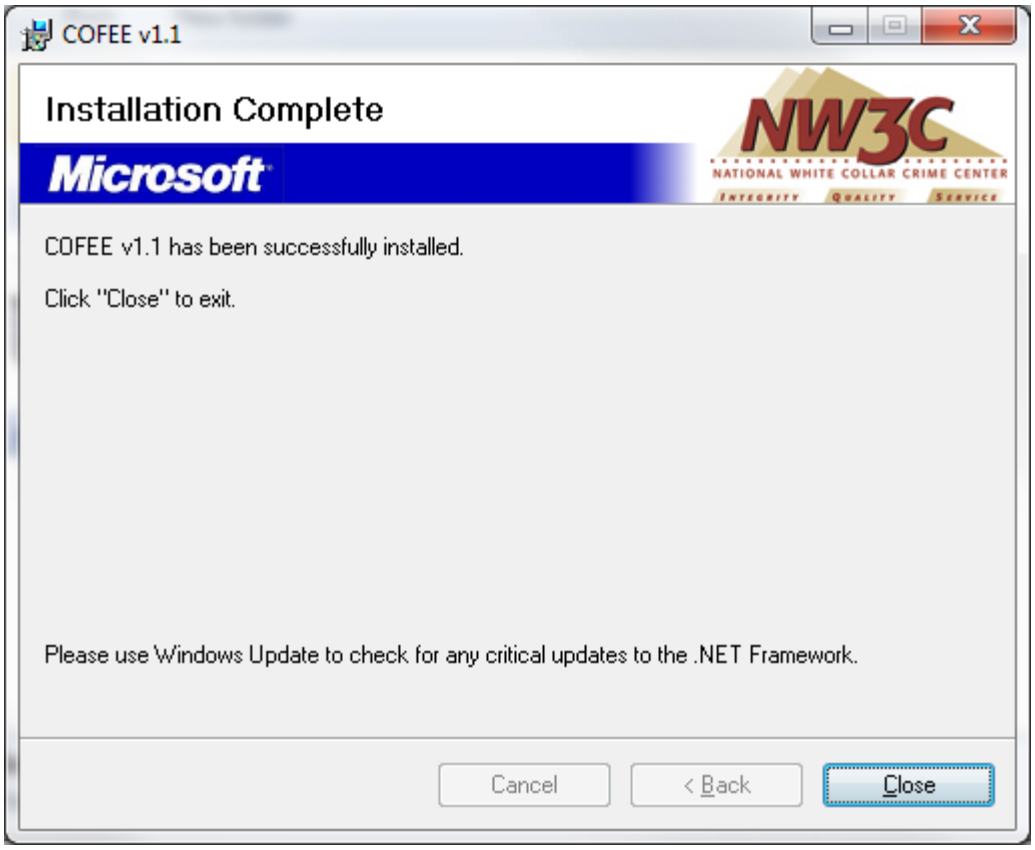
Step 5 – Click “Next” to continue.



Step 6 – Wait for the installation to finish.



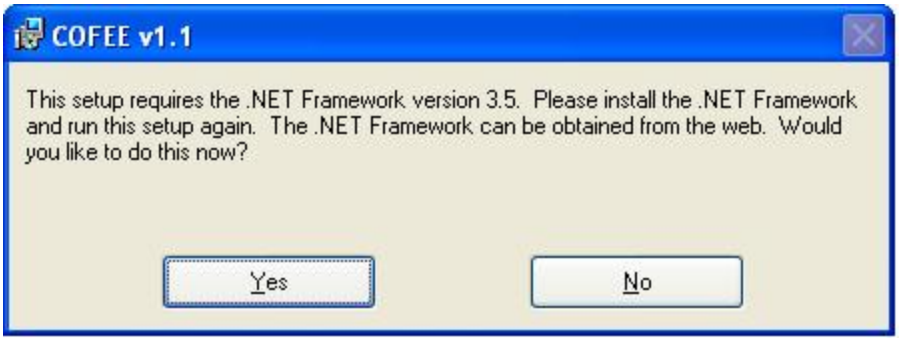
Step 7 – Installation Complete. Click “Close” to exit.



COFEE will install a shortcut on the investigator’s desktop, as well as create a program group under the start menu. Either can be used to start COFEE.

Installation Troubleshooting

If during the installation process, the following screen appears, the system does not currently have the required version of the .NET framework. COFEE v1.1.2 requires .NET 3.5 which can be downloaded from Microsoft.



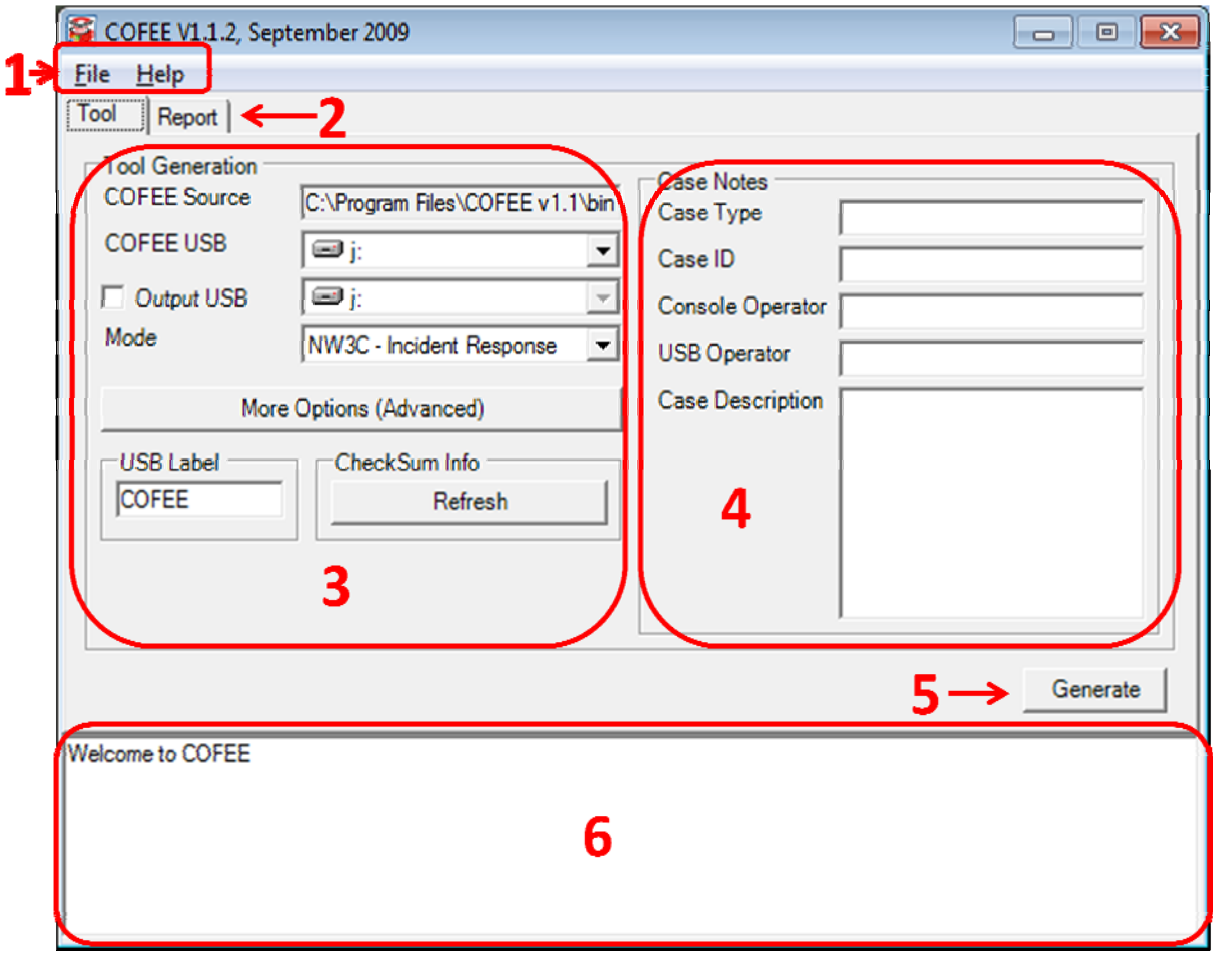
To upgrade, click “Yes.” This will require a working Internet connection. Clicking “Yes” will open a web browser and navigate to a Microsoft webpage which contains the installation for the most recent version of the .NET framework. Click the Install button, and follow the installation instructions. Once the .NET framework is installed, try the COFEE installation again.

Operation Instructions for Device Generation

Program Startup

The first step to running COFEE is to connect the USB device into the investigator's machine, and ensure that Windows has properly recognized the drive prior to launching COFEE. After the drive has been recognized, launch COFEE.

GUI Interface



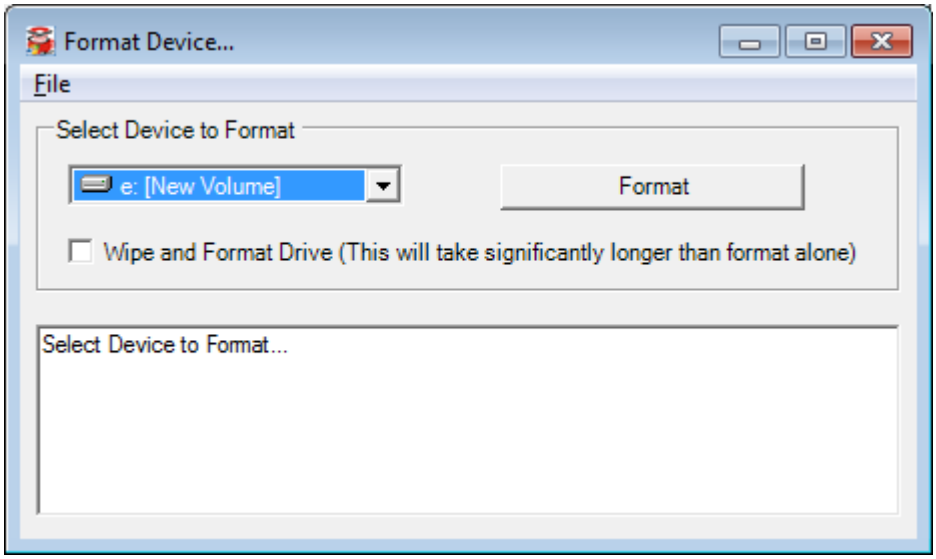
Tool Generation GUI

1. Menu System
    a. File Menu
        i. Format Device – Allows the user to format (and wipe) a USB device as FAT32
        ii. Exit – Closes COFEE
    b. Help Menu
        i. Log – Will display the COFEE log file
        ii. About – Displays the "About" screen
2. Tab Selection
        i. "Tool" tab – Used to generate a COFEE thumb drive
        ii. "Report" tab – Used to create a report from collected data (will be discussed in a different section)

3. Tool Generation – Set the options for device generation
4. Case Notes – Allows the investigator to enter information about the case that will appear in the final report
5. Generate – This button will generate the thumb drive based upon the options selected
6. Message box – This section displays information about current COFEE processes

Format Device

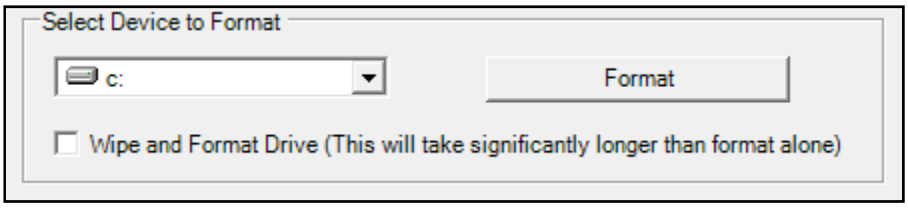
The menu option "Format Device" will open a new window which will allow the user to format and wipe any attached device. COFEE will format the selected device as FAT32, and will only allow devices 1GB or larger to be formatted or wiped. If the device is between 1GB – 2GB, COFEE will display a message reminding the user that the recommended device size for COFEE is 2GB or larger.



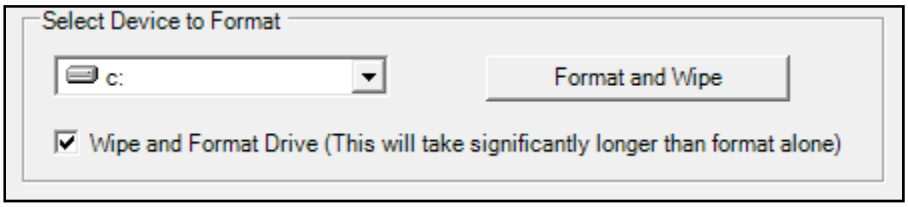
Step 1 – Select the device to format from the drop down box.

Step 2 – Check the box "Wipe and Format Drive" to wipe the device as well as format. Skip this step if only a format is desired.

Step 3 – Click the button to proceed (the button text will vary depending on whether the user is only formatting or conducting a wipe as well).



Click Format if only a format is required



Click Format and Wipe to format and wipe the device

Generating a COFEE Thumb Drive

The primary purpose of COFEE is to generate a thumb drive which runs a pre-determined set of programs that collects valuable data from a suspect's machine.

Tool Generation

Below is a listing of the fields in the Tool Generation Section of COFEE (see Section 3 of the "Tool Generation GUI" screenshot):

1. COFEE Source – This section is automatically filled-in during the installation process.
2. COFEE USB – This section allows the user to select which device becomes the COFEE device (i.e., select the device to send the COFEE USB files to).
3. Output USB – This is an advanced option which allows the user to select a second device for the storage of the saved data.
    a. This option is not recommended
4. Mode – The profile used to generate the USB device.
    a. A profile contains a listing of programs and switches that will be copied to the thumb drive, which will then be run against the suspect's machine.
5. More Options (Advanced) – An advanced option which allows users to modify or create their own profile(s).

a. This section requires the user to have a thorough knowledge of the programs and their switches. If any switch or program is added incorrectly, it can severely damage the suspect's machine, as well as the integrity of any evidence collected.

6. USB Label – Allows the user to select the volume label of the generated thumb drive. The default label is "COFEE."

7. Checksum Info/Refresh – Whenever a new tool is added to a profile, this button needs to be clicked so that COFEE can obtain a checksum value of that file.

    a. During the generation process, COFEE automatically uses the checksum values to ensure the proper files are copied to the USB device.

Case Notes

This section contains five fields which can be filled in by the investigator (see Section 4 of the "Tool Generation GUI" screenshot). None of these items are mandatory, however the contents of these fields (whether filled in or not) will appear in the final report. The user has the option of entering:

1. Case Type
2. Case ID
3. Console Operator
4. USB Operator
5. Case Description

USB Generation Steps

The following are the recommended steps necessary to create a COFEE USB Device, assuming that the user has already connected the desired USB device (and that Windows has finished recognizing it), and has already launched COFEE.

Step 1 – (If necessary) Format/Wipe the USB Device

Step 2 – Select the USB Device under the COFEE USB drop down box

Step 3 – Leave the Output box unchecked

Step 4 – Select the desired profile from the Mode drop down box

Step 5 – Enter any relevant case note information

Step 6 – Click Generate

After all items have been transferred to the USB device a message which says "Done" will appear. The generation process is then complete.

Advanced Operations

Output USB

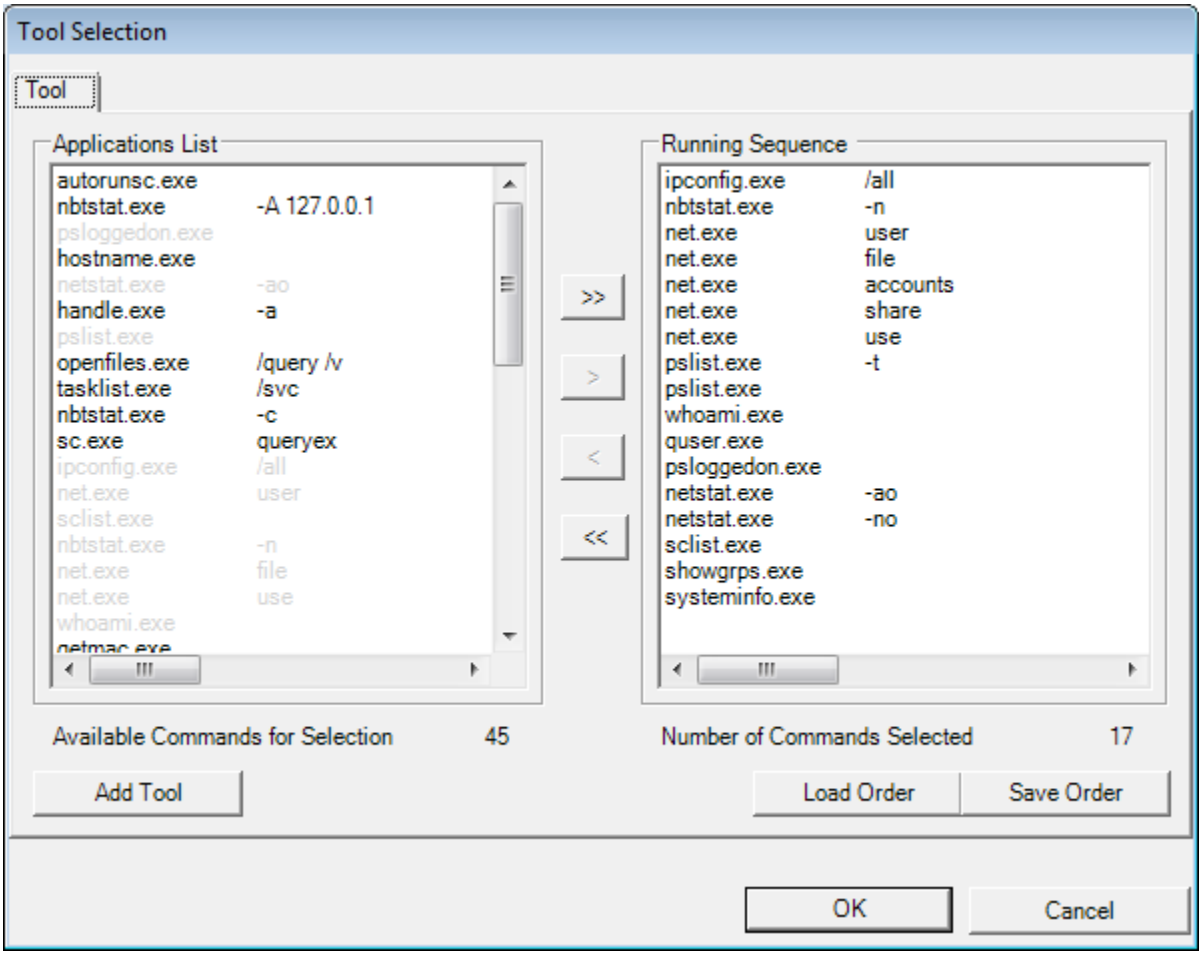
The Output USB option allows a user to decouple the location to which the COFEE programs (the programs that are copied when a USB device is generated) and the acquired data are stored. To separate the locations, check the "Output USB" option and select a different device for the storage of the acquired data. However, it is HIGHLY recommended that the same device be used for both the storage of the COFEE programs, as well as the acquired data.

More Options (Advanced)

The "More Options (Advanced)" button allows a user to create and/or modify non-default profiles. COFEE comes with two default profiles: NW3C – Incident Response and NW3C – Volatile Data. To create or modify a profile, follow these steps:

Step 1 – Select a profile to use as a base template in the Mode dropdown list (see Section 3 of the "Tool Generation GUI" screenshot)

Step 2 – Click the "More Options (Advanced)" button, and the following screen will appear

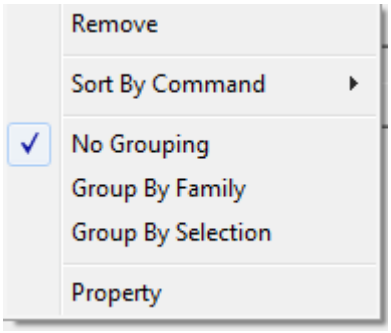


The Tool Selection Screen

The tool selection screen consists of two primary lists of files: Applications List and Running Sequence. The Running Sequence is the "profile." The applications (with switches) listed here are the programs that will run as part of the profile, and will run in that particular order. The Applications List consists of all applications and switches which have been entered into COFEE (typically as part of a previous profile creation). Each item in the list consists of a combination of one application and its switch(es). A program may also be entered without a switch. A single application may be listed multiple times if each instance uses a different switch (or combination of switches). For example, in the screenshot above, "net.exe" is listed in the profile five times, but each time with a different switch. Any one item from the Application List can only be added once to the running sequence. If that item already exists in the running sequence, it will be grayed out in the Application List and will not allow it to be copied again.

Applications List Menu

If the user right-clicks on an item within the Applications List, the following menu appears:



1. Remove: This will remove the selected item from the Application List
2. Sort By Command: Sorts the items in the Application List
3. No Grouping: Items are displayed by application name
4. Group By Family: Organizes programs by family
5. Group By Selection: Groups by Available or Already Selected (for the current profile)
6. Property: Displays the property screen for that entry

Adding Pre-Defined Program(s) to Running Sequence

Adding a pre-defined program (including pre-defined switches) to the Running Sequence is a simple process.

Step 1 – Select the desired tool in the Application List

Step 2 – Click the single right arrow – This adds the selected item to the Running Sequence

The user can also choose to add all of the available programs into the Running Sequence by clicking on the double right arrow.

Removing Program(s) from Running Sequence

Removing a pre-defined program from the running sequence is done in the opposite way that a pre-defined application is added.

Step 1 – Select the desired tool in the Running Sequence

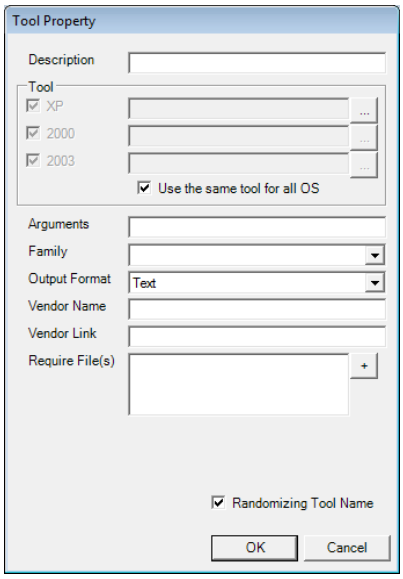
Step 2 – Click the single left arrow – This removes the selected item from the Running Sequence

The user can also choose to remove all of the programs from the Running Sequence by clicking on the double left arrow.

Adding a New Tool or New Switch to the Application List

Instances will arise when an investigator will wish to use either a tool which was not included with COFEE, or use a switch which did not come pre-defined by COFEE. The process for either of these options is the same:

Step 1 – Click "Add Tool" (see the "Tool Selection Screen" screenshot) – the following screen appears



Step 2 – Enter a description for the tool. This description will show up in the final report and is designed to state the purpose of the application.

Step 3 – Select the tool.

> **Step 3a** – If the tool is OS independent, ensure that the "Use the same tool for all OS" option is checked, and then click on the top browse button ("…" – in line with XP). A standard file location dialog box will open. Find and select the tool, then click OK. This will populate all three boxes of the tool section.
>
> **Step 3b** – If the tool isn't OS independent, yet there is a version of the software available for each OS (e.g., netstat.exe), the user has the option of using a separate program for Windows XP, 2000, and 2003. When the programs are run as part of the COFEE process, the program will determine what OS is currently running, and use the appropriate file. To do this, ensure that the "Use the same tool for all OS" option is unchecked, and then load the file for each OS by clicking on its corresponding browse button ("…"). If the application is unavailable for any of the listed OS's, uncheck that particular box (XP, 2000, 2003).

Step 4 – Enter all of the desired switches for the program. The user can leave this box empty if no arguments are used.

Step 5 – Select the family for which this program will belong. The family represents the "purpose" of the tool, and is used by COFEE to organize the acquired data. For example, the program "netstat.exe" belongs to the family "network," while the program "quser.exe" belongs to the family "users." The family options are: network, process, services, users, password, policy, registry, log, file, memory, opt_tool, and misc.

Step 6 – Select the output format extension of the tool. This affects the output format of the tool. For example, the option "Text" expects the output of the program to be text. The complete list of available output formats are: Text, Image, Directory, and Memory Dump.

Step 7 –The information entered in the Vendor Name and Vendor Link fields will be listed in the final report.

Step 8 – Enter any additional required files. For example, some programs require specific Dynamic Linked Library (DLL) files to be included for the program to run properly. This section tells COFEE what other programs to put on the USB device other than the selected program.

Step 9 – Ensure that "Randomizing Tool Name" is checked. This ensures that the programs copied to the USB device have a unique file name, minimizing any possibility of running a program from the suspect's machine.

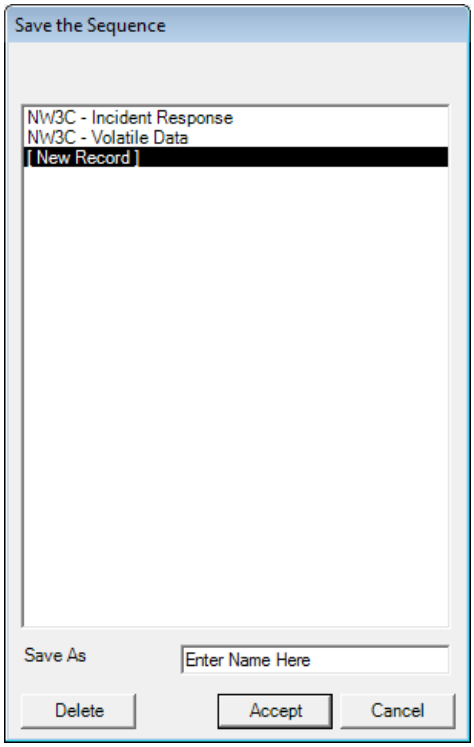
Step 10 – Click OK

If any new programs are added, ensure that the CheckSumInfo "Refresh" button is clicked when returning to the main COFEE GUI screen. If a new CheckSum isn't created, the process will create an error when trying to generate a USB device.

Saving a Modified Profile

An investigator may want different sets of profiles for different scenarios. After the configuration of a new running sequence, COFEE provides the ability for a user to save the new profile.

Step 1 – Click "Save Order" button on the main Tool Selection screen (see "Tool Selection Screen" screenshot) and the following screen appears



Step 2 – In the "Save As" section, type the name of the new profile

Step 3 – Click "Accept"

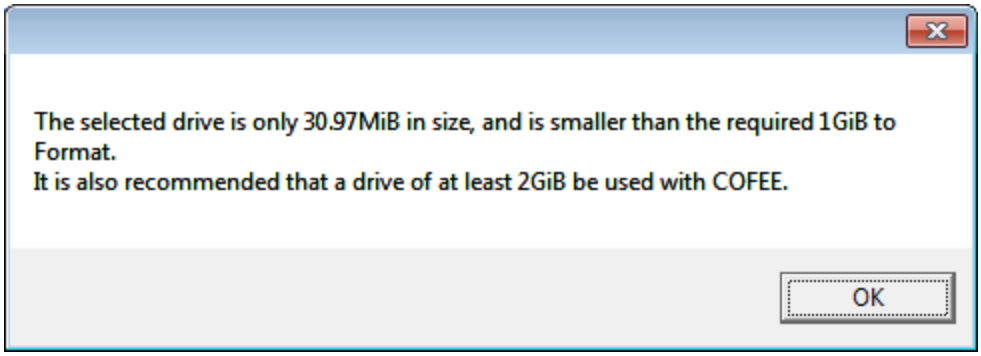
Loading a Profile to Modify

By default, the More Options window will load whichever profile is selected on the main window. However, the user has the option to load a different profile to work on by clicking the "Load Order" button and selecting which profile they wish to modify (or view).

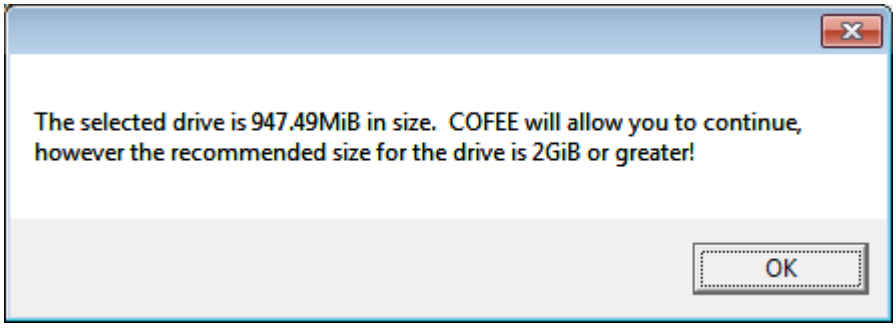
USB Generation Troubleshooting

Format Troubleshooting

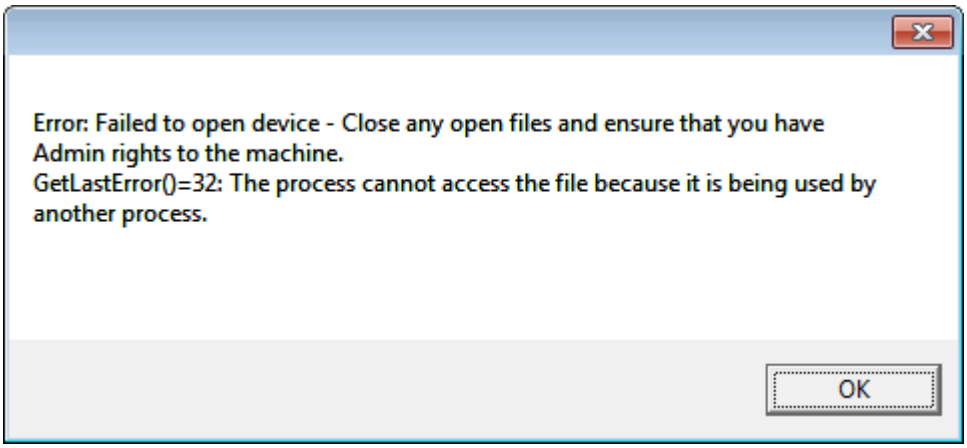
1. If the following screen appears, this indicates that the drive is under the required size, and will not let the user continue. To correct this problem, use a larger USB device.



2. If the following screen appears, this indicates that the drive is between 1GB and 2GB. This warning indicates that the drive is below the recommended size; however, COFEE will allow the user to continue.



3. This following error most often occurs if the user has the device open (e.g., open in Windows Explorer). The drive to be formatted cannot be open, nor can any file on the device be open for format to properly occur; ensure that they are all closed, and try again.



4. An error similar to that displayed in item 3 above will occur if the user attempts to format the device prior to Windows completing the driver installation for that device.

Generation Troubleshooting

A message box stating “Interrupted” appears. This indicates that some process, during the generation of the USB device, failed and needs to be remedied. To determine the exact error look at the text in the white message box (see Section 6 of the “Tool Generation GUI” screenshot) on the COFEE main screen.

Checksum Mismatch – This most commonly occurs when a new, or updated, program file is added by a user. This problem is easily remedied by clicking on the ‘Checksum Info – Refresh’ button. After this process completes, the user can go through the generation process again. The following example indicates that there was a checksum error with the file ipconfig.exe:

```
The checksum of following file(s) do(es) not match
C:\Program Files\COFEE v1.1\bin\Win2k\ipconfig.exe
Generation is stopped due to hash mismatch
Please verify or remove above problem file(s)
If validated, click [Refresh Checksum]
```

Operation Instructions for the COFEE USB Device

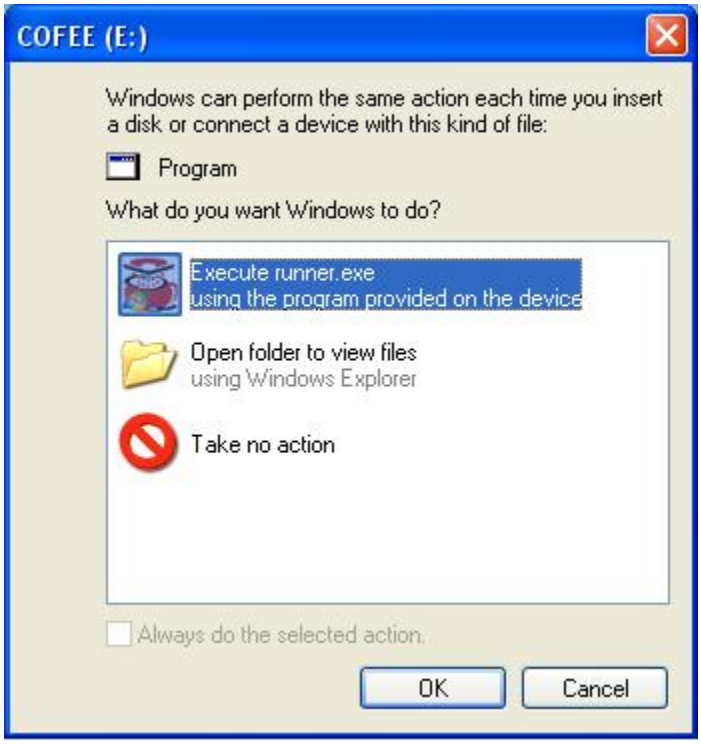
Beginning the COFEE Process

Similar to running on the investigator's machine, the first step to running the COFEE USB Device is to connect the USB device into the suspect's machine, and ensure that Windows has properly recognized the drive.

Once the device is connected, there are two possible methods for executing the COFEE process: If autorun is enabled on the suspect machine, or if it isn't. Both methods are described below:

With Autorun Enabled

If autorun is enabled, the following screen will appear after Windows has finished recognizing the USB device:



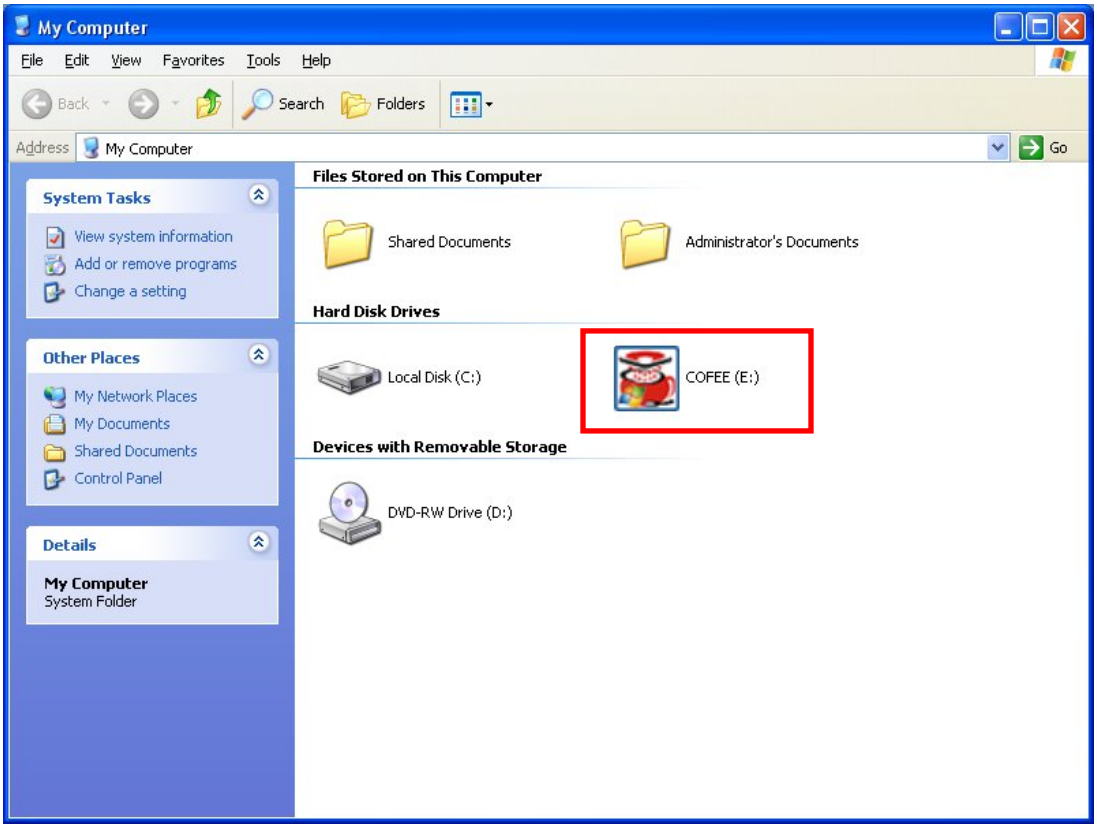
To begin the COFEE process, ensure the option "Execute runner.exe" is selected and click OK.

Without Autorun Enabled

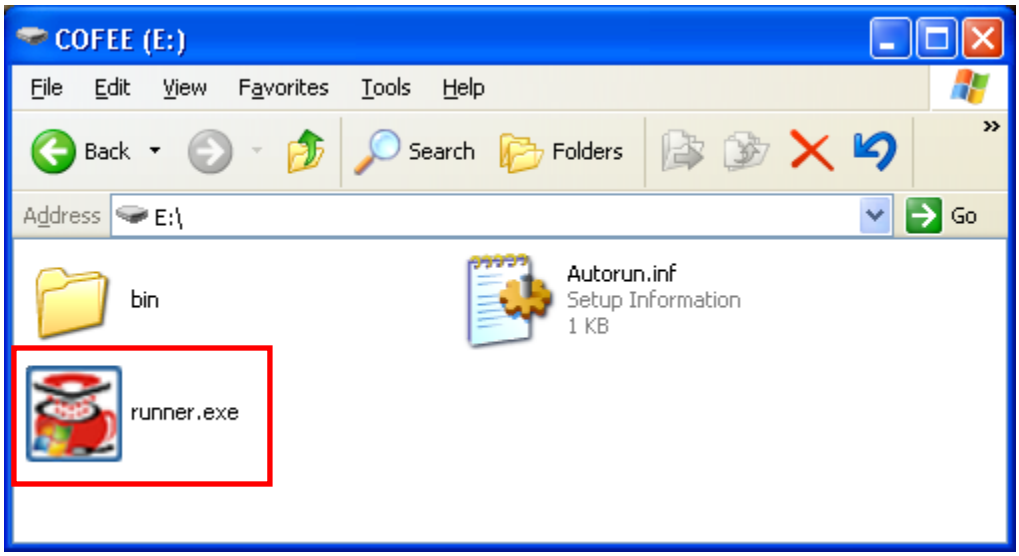
If the above screen does not appear, then it is likely that Autorun is not enabled on the suspect's machine. To begin the COFEE process, follow the steps below:

Step 1 – Open "My Computer." This can be done by either opening the icon on the suspect's desktop, or by selecting "START" and then "My Computer."

Step 2 – Select and Open the COFEE USB Device. The device can easily be identified by both the volume label, as well as the icon associated with the drive. In the following example, the E: drive is the COFEE USB Device.

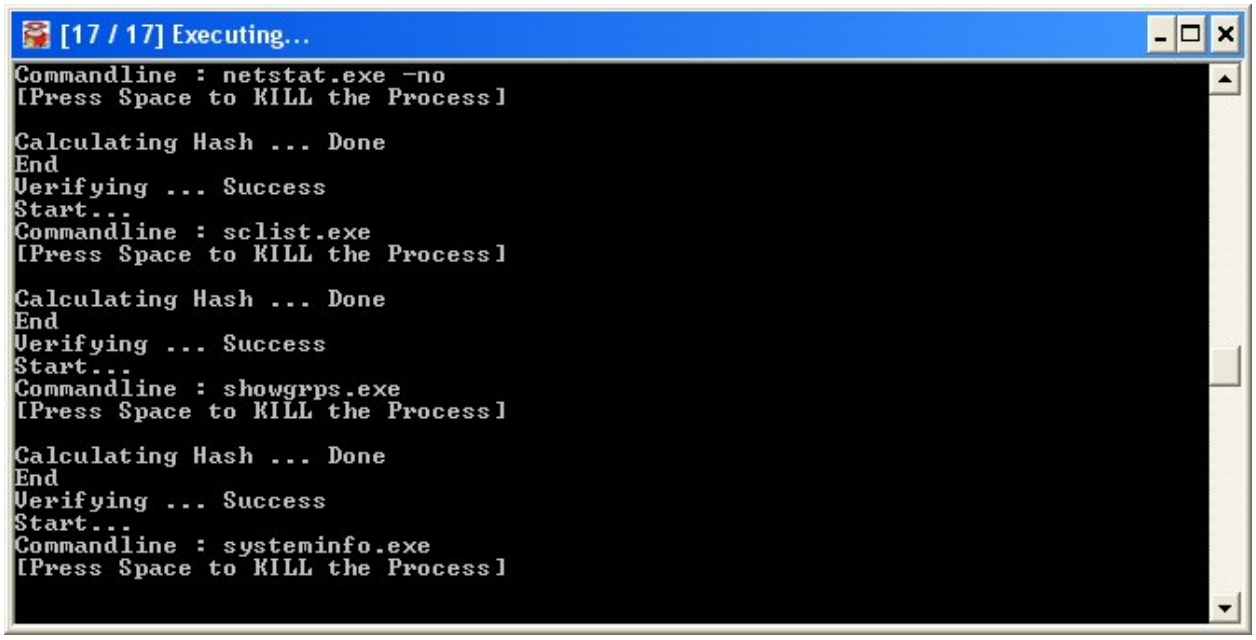


Step 3 – Find and execute the file "runner.exe" - At this point, the COFEE process has begun.



Removing the USB Device

While the COFEE process is running, a window similar to that below will be displayed. When the window closes, the process has completed.



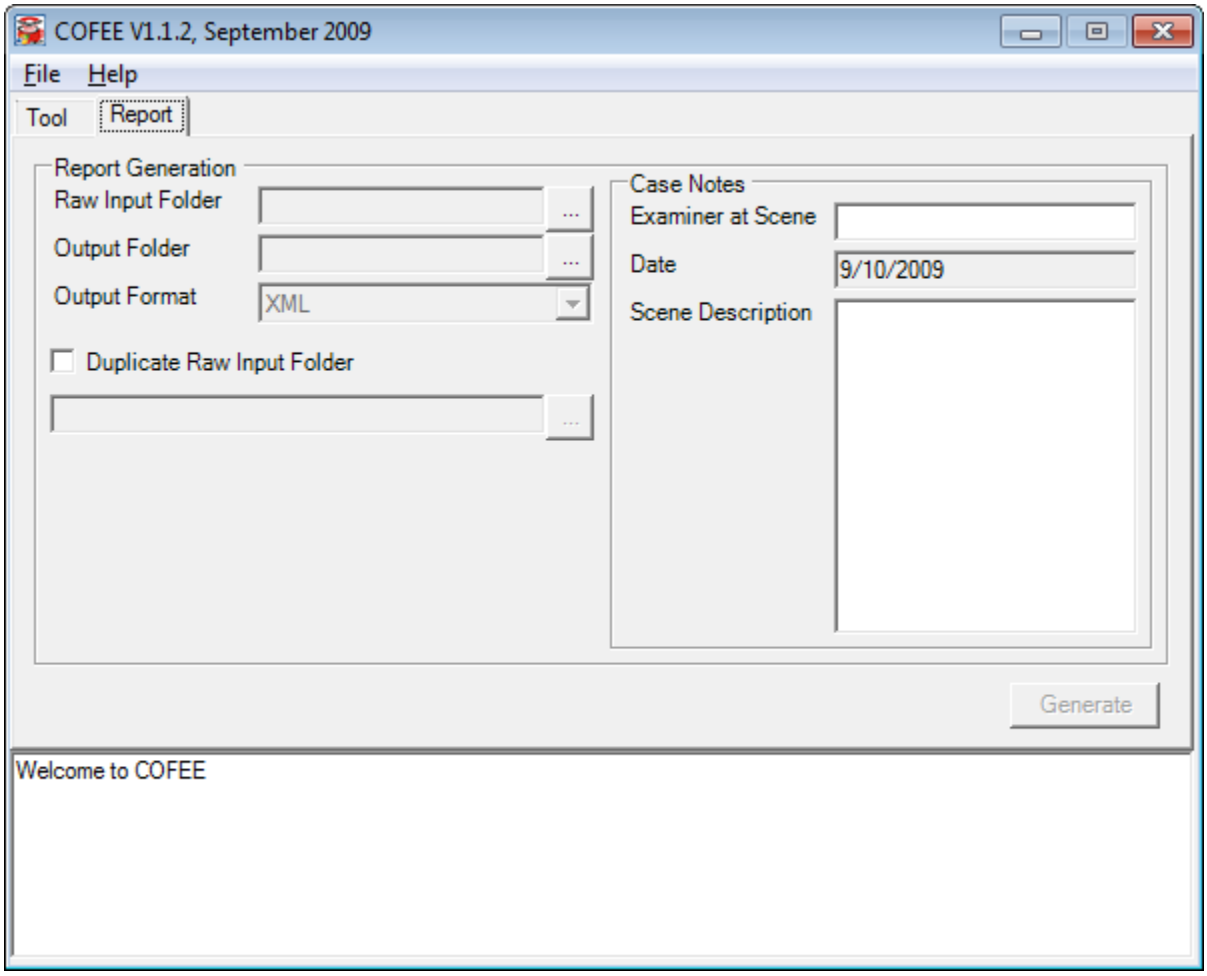
When the process is complete, follow standard procedures to safely remove the device. At this point all information has been captured, and the USB device can be returned for report generation and analysis.

Note: For individuals who would like further verification that the process has properly completed, the investigator at the scene can view the COFEE.log file which is located in the data storage directory (See "Generating a Report of the Collected Data" for more information concerning the data storage directory). The final item in the log file should be "[End]."

Generating a Report of the Collected Data

Create a Report from the Collected Data

Once the data has been acquired from the suspect's machine, an HTML-based report can be generated of the collected data. To begin the process, click on the Report Tab on COFEE's main screen.



Step 1 – Connect the USB drive to the investigator's computer.

Step 2 – Select an Input Folder - Click the browse button ("…") under Raw Input Folder and select the acquired data's output folder. The standard convention will have the data stored on the USB device under the following folder:

out-[Computer Name]-[YYMMDDHHMMSS]
(e.g., out-administrator-2009092110213)

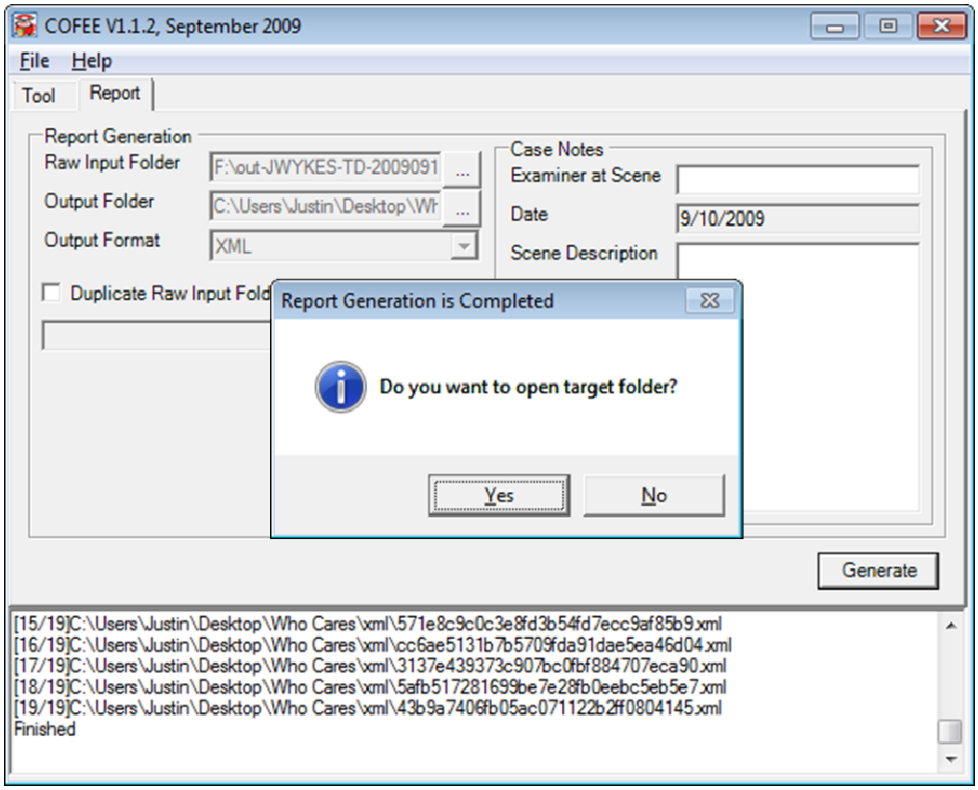
The "Computer Name" will be the Computer Name of the suspect machine, while the date/time will be when the COFEE process started on the suspect machine.

Step 3 – Select an Output Folder – Click the browse button ("…") under Output Folder and select the desired folder in which to generate the report (the user can also create a folder in the browse screen).

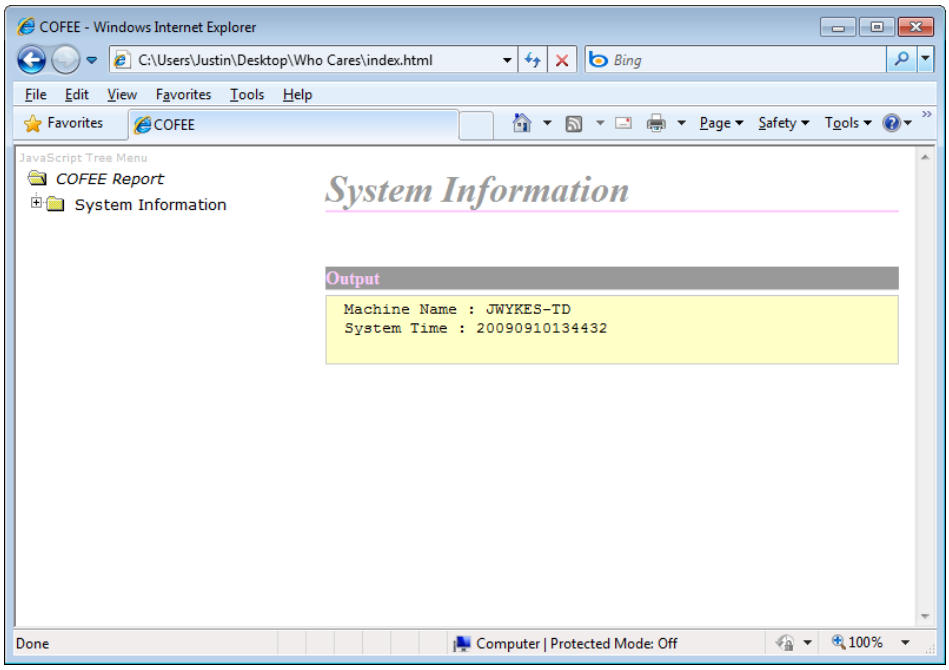
Step 4 – Fill in any Case Notes. These fields are optional and will appear in the final report.

Step 5 – Click "Generate."

Step 6 – When the report is finished generating, COFEE will ask if the user wants to open the target folder. At this point, the report is generated; clicking "Yes" will direct the user to the folder containing the report. If the user clicks "No," the report can still be found in the folder identified in Step 3.

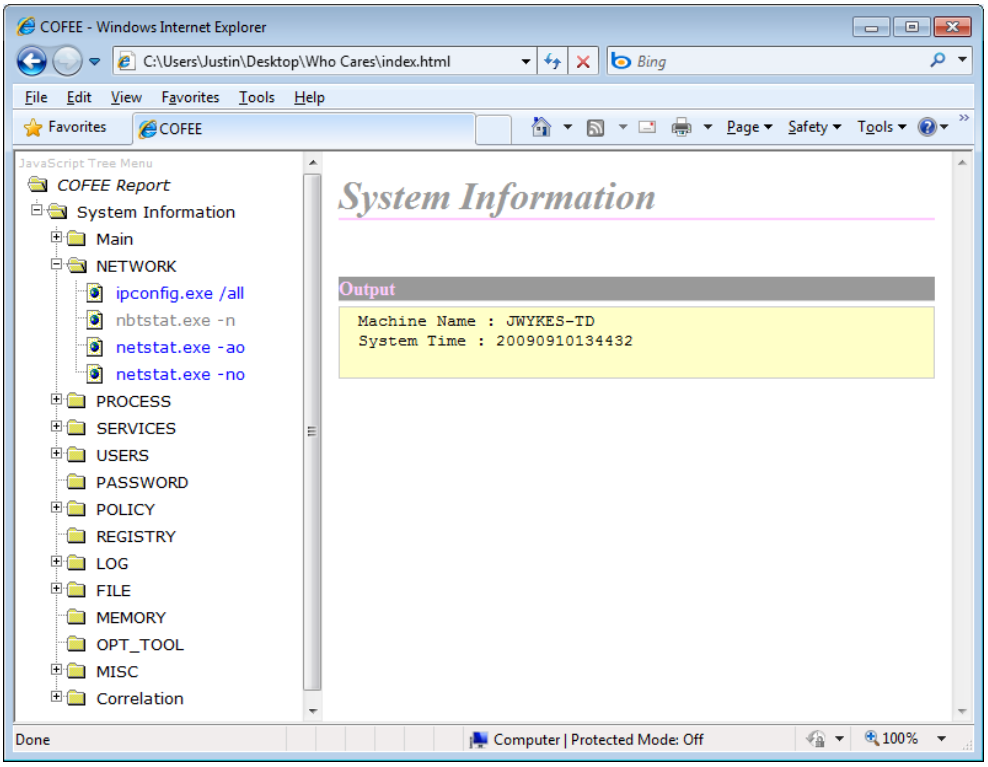


Step 7 – Open the "index.html" file to view the report.



Interpretation of Reports

The COFEE report is generated in an XML format and is displayable in all major web browsers (e.g., Internet Explorer and Firefox). The report is generated in two frames: the left frame contains a navigational menu to view the report, while the right contains the actual report data.



Screenshot of Sample Report

Menu Navigation

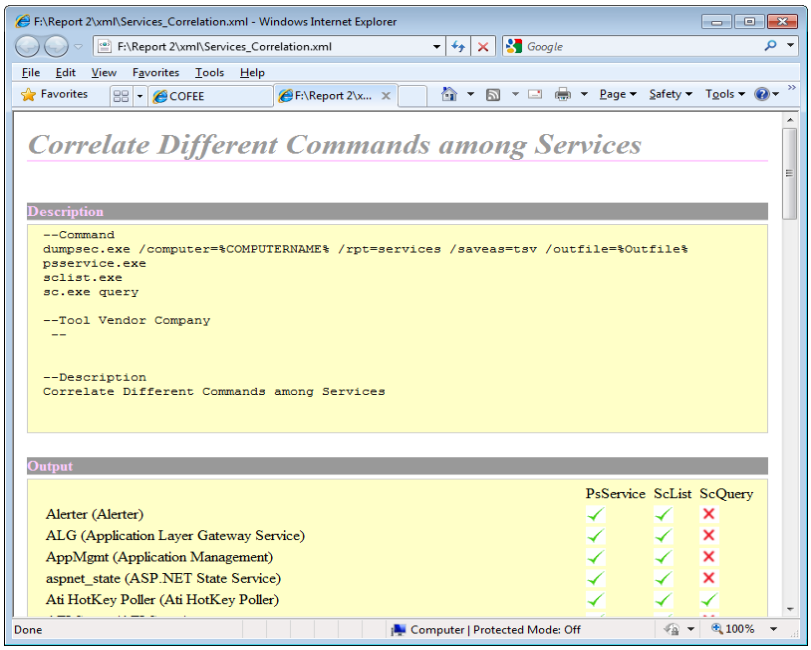
Menu Folders

The COFEE navigation frame (left) is divided into 14 sections. There is one folder for each of the 12 "families": network, process, services, users, password, policy, registry, log, file, memory, opt_tool, and misc. These folders contain the results of any file that was designated as part of that particular family.

The Main folder contains the COFEE log file which is generated when the process is run on the suspect machine and any case notes which were entered (either during the USB device generation or during the report generation).

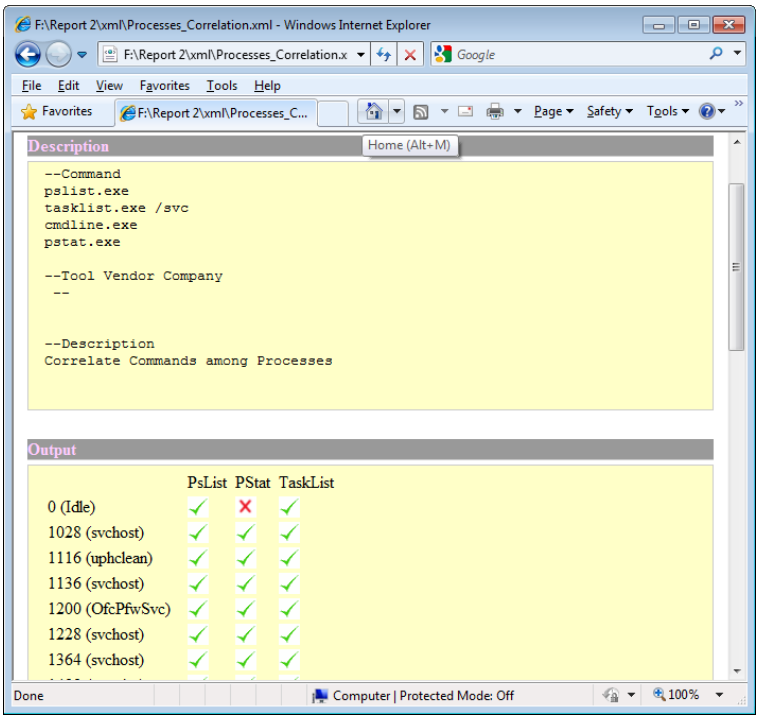
The Correlation folder contains up to three reports that are generated based upon what programs are run: Lsof, Services_Correlation, and Processes_Correlation.

1. Lsof – List Opened Files with Network Connection: Shows the Process, Port Number, and open files correlation. The information collected comes from the following programs: "pslist.exe", "openports.exe –netstat", and "handle.exe –a." If none of these programs are run, this report will not be displayed; if only a portion of the files are run, this report will be based on only the programs that ran.
2. Services_Correlation – Correlate Different Commands among Services: This report displays the services as reported by different programs. The following programs are used by this report: "dumpsec.exe /computer=%COMPUTERNAME% /rpt=services /saveas=tsv /outfile=%Outfile%", "psservice.exe", "sclist.exe", and "sc.exe query." This report will list services which were reported by the programs, with a "check mark" or an "X" indicating whether a particular tool reported a specific service. Like the other correlation reports, only those programs which were actually run will show up in this report (of the programs listed above).



Services_Correlation Screenshot

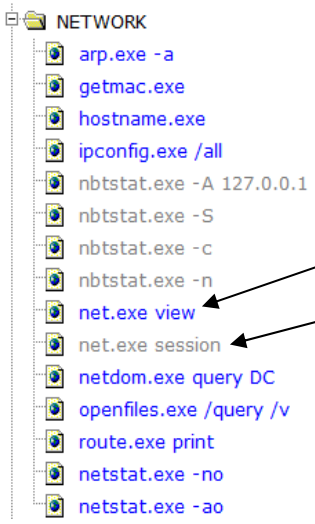
3. Processes_Correlation – Correlate Commands among Processes: Similar to the services correlation report, but correlates running processes versus services. The programs used to generate the report are: “pslist.exe”, “tasklist.exe /svc”, “cmdline.exe”, and “pstat.exe.”



Processes_Correlation Screenshot

Program Reports

Each program run has its own report within the full COFEE report. If the program name is highlighted in blue, then COFEE was able to obtain valid output from that program. If the program name is highlighted in gray, then there was likely an error in collection and there is no collected data for that particular file.



For example, in the listing on the left:

net.exe view – Valid data was collected and is in the report

net.exe session – No data was collected due to an error

Each report has the following sections:

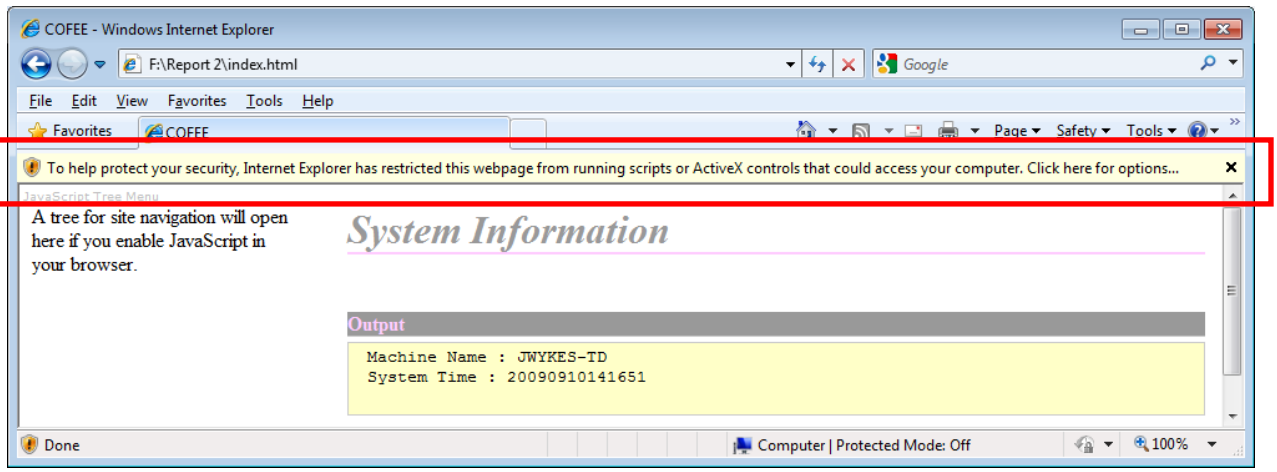
1. **Description:** Displays a listing of the program run, and the description of that particular program.
2. **Hash Matching Result:** A hash of all of the stored data is created and compared to the hash which was created when the data was originally collected. This section displays to the reader whether the two hash values matched. If the values do not match, this could indicate that someone has modified that particular output file.
3. **Start Time:** The time the program started on the suspect machine.
4. **End Time:** The time the program ended on the suspect machine.
5. **Output:** This contains the stored output of that program.

If an error occurred, a sixth section will be displayed:

6. **Error:** Displays what error occurred when the program attempted to run (e.g., "Access Denied").

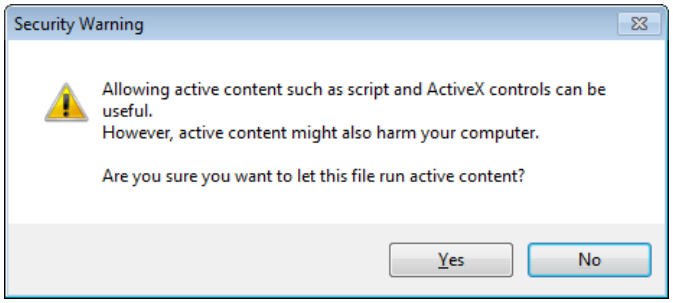
Report Troubleshooting

Often, a JavaScript warning will display when attempting to view the report in Internet Explorer.



To correct this problem:

1. Right-Click on the Warning Bar
2. Select “Allow Blocked Content…”



3. Click “Yes”
4. The report should reload with no problems.

Appendix

NW3C – Volatile Data Profile

The NW3C – Volatile Data Profile was developed to allow an investigator to collect potentially important volatile data prior to seizing a machine for a full forensic examination. This profile was designed so that none of the programs run causes any direct writes to the suspect's file system.

Programs & Arguments

Application	Argument	Description
ipconfig.exe	/all	List Network Configuration
nbtstat.exe	-n	Lists local NetBIOS names
net.exe	user	Displays users on the computer and/or domain
net.exe	file	Display opened shared files on the server
net.exe	accounts	Adjust account settings. Displays info such as Password age, minimum length, Lockout threshold, etc.
net.exe	share	Local Network Shares
net.exe	use	Connects or disconnects your computer from a shared resource or displays information about your connections
pslist.exe	-t	Displays process tree
pslist.exe		Process Information Lister
whoami.exe		Displays the user the system is currently logged in as
quser.exe		Displays information about users logged onto the system
psloggedon.exe		Logon Session Displayer
netstat.exe	-ao	Displays protocol statistics and current TCP/IP network connections. Displays all connections and listening ports, and the owning process ID associated with each connection
netstat.exe	-no	Displays protocol statistics and current TCP/IP network connections. Displays addresses and port numbers in numerical form, and the owning process ID associated with each connection
sclist.exe		Displays service list for local machine
showgrps.exe		Displays groups that users are members of
systeminfo.exe		Displays operating system configuration information for a local or remote machine, including service pack levels

NW3C – Incident Response Profile

The NW3C – Incident Response Profile was designed for Incident Response investigations in which the investigator is not able to perform a forensic analysis on the target machine. This profile was designed to have *minimal* impact on the suspect's file system.

Programs & Arguments

Program	Arguments	Description
arp.exe	-a	Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
at.exe		Lists scheduled events
autorunsc.exe		Displays programs scheduled to autorun during boot
getmac.exe		Displays MAC Address
handle.exe	-a	Ever wondered which program has a particular file or directory open? Handle is targeted at searching for open file references. Dump information about all types of handles, not just those that refer to files. Other types include ports, Registry keys, synchronization primitives, threads, and processes.
hostname.exe		List Host(Computer) Name
ipconfig.exe	/all	Shows detailed IPCONFIG information
msinfo32.exe	/report %OUTFILE%	Will create a report of msinfo32. Essentially system information
nbtstat.exe	-n	Lists Local NETBIOS Names
nbtstat.exe	-A 127.0.0.1	Lists the *remote* machines name table given its IP address (local host) [NETBIOS over TCP/IP]
nbtstat.exe	-S	Lists session table with the destination IP [NETBIOS over TCP/IP]
nbtstat.exe	-c	Lists NBT's cache of remote [machine] names and their IPs [NETBIOS over TCP/IP]
net.exe	share	Local Network Shares
net.exe	use	Connects or disconnects your computer from a shared resource or displays information about your connections.
net.exe	file	Display opened shared files on the server.
net.exe	user	Displays users on the computer and/or domain.
net.exe	accounts	Adjust account settings. Displays info such as Password age, minimum length, Lockout threshold, etc.
net.exe	view	Displays a list of computers in a specified workgroup or the shared resources available on a specified computer.
net.exe	start	Start the specified network service. Will List Started Services

net.exe	Session	Display all sessions connected to the computer and deletes them if specified.
net.exe	localgroup administrators /domain	Lists members of administrators group for the domain. Error printed if no domain exists
net.exe	localgroup	Displays list of Group Aliases for System (e.g., Guests, Administrators, Power Users, etc.)
net.exe	localgroup administrators	Lists members of the administrators group
net.exe	group	Add, delete, view, and otherwise manage network workgroups.
netdom.exe	query DC	Only works with a Domain Controller put in the "DC" spot
netstat.exe	-ao	Displays protocol statistics and current TCP/IP network connections. Displays all connections and listening ports, and the owning process ID associated with each connection
netstat.exe	-no	Displays protocol statistics and current TCP/IP network connections. Displays addresses and port numbers in numerical form, and the owning process ID associated with each connection.
openfiles.exe	/query/v	Lists files and folders that have been remotely opened on the system. Must have admin privileges
psfile.exe		Local and Remote Network File Lister
pslist.exe		Process Information Lister
pslist.exe	-t	Displays process tree
psloggedon.exe		Logon Session Displayer
psservice.exe		Lists services on a local or remote system
pstat.exe		Pstat.exe is a Resource Kit utility that provides information about the processes and drivers that are currently running on your computer. For diagnostic purposes, the most useful information is the list of loaded drivers at the end of the output.
psuptime.exe		Displays the systems current "up time"
quser.exe		Displays information about users logged onto the system
route.exe	print	Displays routing information
sc.exe	query	Queries the status for a service, or enumerates the status for types of service
sc.exe	queryex	Queries the extended status for a service, or enumerates the status for types of service
sclist.exe		Displays service list for local machine
showgrps.exe		Displays groups that users are members of.
srvcheck	\\127.0.0.1	Check Server Information
tasklist.exe	/svc	Displays services hosted on each process
whoami.exe		Displays the user the system is currently logged in as

COFEE Version Change Log

Version 1.1 NW3C Updates to original COFEE (includes removal of FCIV and PIPE, as well as modification of FORMAT/WIPE and the creation of NW3C profiles).
A SHA1 hashing utility created and implemented to replace FCIV.
A Quick FAT32 Format utility created to replace Format/Wipe issues.
Modified COFEE to use Cipher to wipe unallocated area of the thumb drive.

Version 1.1.1 Modified the Wipe portion. Wipe now Formats, then Wipes with SDELETE (with the –c argument), and then Formats again.
Modified source code to remove Cipher and replace with SDelete option to overwrite unallocated area of thumb drive with one pass of zeroes.

Version 1.1.2 Fixed bug which would not allow drives with drive labels to be formatted or wiped.