

FriendlyRoboCopy: A User's Guide

Table of contents

1. General information	
a. About RoboCopy	2
b. About FriendlyRoboCopy.....	2
2. Parameters	
a. Available options	2
b. Defaults	2
c. Portable defaults.....	3
3. Tabs	
a. Case Information tab.....	3
b. Switches tab	3-5
c. Collections tab	
i. Single Collection option	5
j. Batch Collection option	6
4. Messages	
a. Immediately at run time	5
b. General Alerts	6
c. Case Information tab.....	7
d. Switches tab	8
e. Collections tab	8
i. Single Collection.....	8
j. Batch Collection.....	9
5. Log Files Analysis.....	9
6. Comprehensive Log File	10

1. General information

a. About RoboCopy

RoboCopy is a free utility developed and distributed by Microsoft for maintaining and synchronizing data locally or across a network. RoboCopy is targeted to system administrators and information technology professionals.

You can download RoboCopy for free at:

<http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>

For more information about RoboCopy:

- <http://www.ss64.com/nt/robocopy.html>
- <http://people.mills.edu/clavelle/thesis.html>

b. About FriendlyRoboCopy

FriendlyRoboCopy is a free graphical user interface for RoboCopy adapted to the needs of computer forensics examiners. In this regard, it only contains the switches applicable to the industry. You can download FriendlyRoboCopy at <http://people.mills.edu/clavelle/thesis.html>. To run this application, you will need:

- Perl version 5.8.3 or higher installed on your computer. You can download Perl for free from <http://www.activestate.com/Products/ActivePerl/?mp=1>.
- The Win32::DirSize module installed on your computer. To install modules, please refer to: http://www.perlmonks.org/?node_id=434813#installing

FriendlyRoboCopy does not let RoboCopy create folders. If users want to preserve the extracted data in specific folders, they will have to create those folders before running FriendlyRoboCopy.

Some processes will take some time -- like calculating directory sizes and running RoboCopy -- so users are urged to be patient even if the application looks like it froze.

The total size of the source --indicated below the Source Path text field-- is an approximation since users might exclude files or directories from the duplication and the directory calculation method does not take those exclusions into account. The text fields for the name of the comprehensive log file (first tab) and the name of the log file generated by RoboCopy (third tab), which is only available under the Single Collection, can only use alphanumerical character along with spaces and underscore.

2. Parameters

a. Available options

The *Information* menu option along with the *QUIT*, *SAVE DEFAULTS* and *LOAD DEFAULTS* buttons are available through out FriendlyRoboCopy. The *CLEAR* and the *CONTINUE* buttons act on the active tab.

b. Defaults

1) *Case Information tab*

The date is a default that cannot be modified. When the *LOAD DEFAULTS* button is pressed it populates all the fields labeled with **. To save defaults,

first type what you want to save in the text fields that are labeled with ** and then press the *SAVE DEFAULTS* button.

2) *Switches tab*

The */W* and */R* check boxes are checked by default and the number 3 is specified. The */TS* and */FP* check boxes are also checked as defaults. The defaults are reset when the *CLEAR* button is pressed.

None of the check boxes are required to be checked for the application to work, however if a check box is checked and its corresponding text field is not filled, then the application will not let users go on. All switches as well as their corresponding text fields, if it has one, can be saved as defaults. Note that the */NP* switch is hard coded in the application.

3) *Collection tab*

The only default is the *.* from the “Name of files to act upon” text field, which is the RoboCopy default. If the *CLEAR* button is pressed, the default in the text field will be reset.

c. Portable defaults

All fields from the *Case Information* tab marked with a **, any of the check boxes and text fields from the *Switches* tab and the “Names of files to act upon” text field from the *Collection* tab can be saved as defaults. Pressing the *SAVE DEFAULTS* button generates a file called **default.txt**. This file can then be saved on a removable disk and placed where FreindlyRoboCopy runs on another machine. With this feature, examiners only need to type their personal information and switch preferences once. The defaults can be overwritten. The defaults are saved all at once. This means that if the *SAVE DEFAULTS* button is pressed on the second tab, the default.txt file will be created with all of the data that are in the text fields, text areas and check boxes from all three tabs

3. Tabs

a. Case Information

All information on the *Case Information* tab is printed to the comprehensive log file, but it might not all be available to examiners at the time of extraction. As a result, only text fields with * or ** need to be filled out for the program to allow examiners to go on. The *Case Information* tab also allows users to choose the name of the comprehensive log file and to browse for its location.

b. Switches

All information on this tab is printed to the comprehensive log file. This tab allows users to choose the switches that will modify what they are going to copy, what information will go in the log files, and set some network parameters. RoboCopy has more than 50 different switches, but this application only supports those necessary to computer forensics examiners. Below is additional information for each switch that this application supports. For general information, please consult RoboCopy documentation (see section one of this guide).

/L: This switch is used if examiners only want to review the data and not duplicate it. Examiners might need a broad picture of the extraction job before starting.

/E: This switch is used to allow RoboCopy to traverse the file system tree and copy all the requested information through the system.

/S: This switch does the same thing as /E, but does not bother with the empty folders. In general, examiners like to gather as much information as possible and then filter the data later, but this switch is still a valid option.

/COPYALL: This switch allows RoboCopy to capture all copyflags (DATSOU). This program forces users to choose between /COPYALL, /SEC and /COPY.

/COPY: This switch allows RoboCopy to copy only files based on their copyflags. To capture the A, S, and O copyflags, both the source and destination drive need to be formatted with NTFS. This program forces users to choose between /COPYALL, /SEC and /COPY.

/SEC: This switch allows RoboCopy to copy the files with the security attributes (SADT). It requires both the destination and the source drives to be formatted with NTFS. This program forces users to choose between /COPYALL, /SEC and /COPY.

/XF: This switch allows RoboCopy to exclude files from the copying process based on their paths or names specify in the text field. For example with this switch examiners can have RoboCopy exclude *.doc*, *some** and *program.pl* files. This example will not copy any word document, any file that starts with the word “some” or any file that is called “program.pl.” This exclusion applies to the all job.

/XD: This switch allows RoboCopy to exclude directories from the copying process based on their paths or names specified in the text field. For example with this switch examiners can have RoboCopy write *c:\my documents\my name\my directory* and *some** in the text field. This example will not copy the directory called “my directory” in the path “c:\my documents\my name” nor any files from it and will not copy any directory starting with the word “some.” This exclusion applies to the all job.

/W: This switch allows RoboCopy to wait and retry without failing in the event that the network connection is not functioning properly. The default for this application is set to 3 seconds (RoboCopy default is 30). The goals for examiners in using RoboCopy are different than those of system administrators. While the system administrators can afford to have RoboCopy

wait for a better connection—the process is in-house—, computer forensic examiners has only so much time to perform the duplication. This switch tightly relates to the */R*.

/R: This switch determines how many times RoboCopy will retry copying a file, folder or directory once the process failed. The retry process is mostly related to a malfunctioning network connection. The default for this application is set to 3 times (RoboCopy default is 1 million). The goals for examiners in using RoboCopy are different than those of system administrators. While the system administrators want to make sure all data is copied, computer forensic examiners have only so much time to perform the duplication. This switch tightly relates to the */W*.

/TS: This switch is important to examiners because it gathers metadata (in this case the timestamps).

/FP: This switch is important to examiners because it gathers metadata (in this case the full pathnames).

/NP: Even though this switch does not appear on the interface, it is hard coded in the command to RoboCopy and suppresses the display of the progress that RoboCopy is accomplishing in duplicating the data.

c. Collection

In general, this tab's goal is to eliminate unnecessary typing which is known to generate errors.

i. Single Collection

This is to be used when examiners want to image one directory at a time. The *Single Collection* radio button allows examiners to specify the “Name of the files to act upon.” This feature allows the user to determine what RoboCopy will be copying (see */XF* and */XD*). The *Single Collection* radio button also allows users to type the name of the RoboCopy generated log file and to browse for its location. It also lets users browse to chose a source and destination paths.

While the *Single Collection* radio button is selected, the text area reserved for batching is disabled.

Below is a list of what the *CONTINUE* button checks for:

- If all fields are filled.
 - If the available space on the destination is larger than the size of the source. If the amount of data to be copied from the source path is larger than the space available on the destination, the program returns to the *Collection* tab and users are given a chance to fix the problem.
- If there is no error (that this program can detect) in the information given by users, then the application displays a dialogue box summarizing the users choices (Source path, Destination Path, Switches and Log file name and path).

At this point, users can *CANCEL* and the *Collection* tab is cleared of all information and put back to the default (*Batch Collection*) or *CONTINUE* which calls RoboCopy.

After RoboCopy is done with the duplication, the program displays another dialogue box asking users if they want to have FriendlyRoboCopy analyze the log file that was just generated by RoboCopy.

If *YES* is pressed, the results are printed to the comprehensive log file. If *NO* is pressed, the program write to the comprehensive log file that users did not request FriendlyRoboCopy to analyze the log file.

j. Batch Collection

This is to be used when examiners want to image more than one directory at a time. The *Batch Collection* radio button allows the examiners to browse for the location of the RoboCopy generated log files—the full name required in the text area is used to name the log files generated by RocoCopy. This radio button also lets users browse to chose a source and destination paths.

The text area to the right of the screen entitled “Enter user name, full name....” allows users to enter all of the directories that need to be copied. At this time, there is no limit to the number of lines that can be specified, but it is not recommended to batch more than 999 directories at a time.

The format in this text area is strictly enforced: name of the directory comma full name. Do not use tab and respect the rule of one directory per line. Once the *CONTINUE* button is pressed, the application does the following:

- Checks if all the fields are appropriately filled. If not, the program displays a dialogue box pointing to all the information users are expected to fill.
- Generates a table in the place of the text area with the name of the directory in one column and the size of that directory in the other. If the size is “0”, it means that either the directory does not exist or it actually has nothing in it. This might take a while to generate especially if there are lots of directories with lots of data in them. Also, this program does not check for duplicates.
- Displays the total of the source directories under the source path.
- Displays the available space under the destination path.
- Generates two new buttons—the *MAKE CHANGES* button and the *OK* button.
 - The *MAKE CHANGES* button allows users to return to the previous screen to edit any of the fields.
 - The *OK* button does the following:
 - Checks if the destination drive has enough space to receive the data from the source. If there is not enough space on the destination drive, the program generates an alert. The program then goes back to the entry text area where all fields can be modified.

- If the *OK* button is pressed and there is enough space on the destination to save all the source data, the application displays a dialogue box summarizing users' choices (Source path, Destination Path, Switches and Log file name and path).

At this point, the user can *CANCEL* and the *Collection* tab is cleared of all information and put back to the default (*Batch Collection*) or *CONTINUE* which calls RoboCopy.

During the duplication, a text area displays which file RoboCopy is processing. After RoboCopy is done with the duplication, the program displays another dialogue box asking users if they want to have FriendlyRoboCopy analyze the log files that were just generated by RoboCopy.

If *YES* is pressed, the results of the analysis are printed to the comprehensive log file. If *NO* is pressed, the program writes that the analysis was not required to the comprehensive log file.

4. Messages

Below is a list of all "Alert" dialogue boxes through out the application:

- a. Immediately at run time:
 - "*You need Active Perl version 5.8.3 or higher*" is displayed as the program is launched if the user does not have the right Perl version. Since the program will not run properly if this version is not installed, the application closes immediately after users press the *OK* button.
 - "*You need to install the Win32::DirSize module. Please refer to the user guide (under the Information menu.)*" is displayed if the module called Win32::DirSize is not properly installed. Since the program will not run properly if this module is not installed, the application closes immediately after users press the *OK* button.
 - "*robocopy.exe not found. Please refer to the user guide (under the Information menu.)*" is displayed if RoboCopy is not installed in the same directory as FriendlyRoboCopy. Since the program will not run properly if this program is not installed, the application closes immediately after users press the *OK* button. Refers to section one of this guide for instruction on where to find and how to install RoboCopy.
 - "*The Information tab will not work properly. Make sure RoboCopy.pdf and Guide.pdf are in the folder where this application runs.*" is displayed when FriendlyRoboCopy is not able to find at least one of the two mentioned files in the location where the FriendlyRoboCopy runs. This will not stop the program from running properly, users will not be able to refer to the documentation.
- b. General Alerts
 - "*Are you sure you want to quit the program?*" is displayed to give users a chance to change their mind or to catch them pressing this button in error. Since the *QUIT* button is very close to the *CLEAR* or the *SAVE DEFAULTS*

button and that the information required by the application can be long to re-type, this alert is a safety net.

c. Case Information tab

- "*Complete ALL Required Fields*" is displayed if at least one required text area or entry field is left empty. The only way to get ride of this alert is to fill out all required fields.

d. Switches

- "*Please enter a value in the field as well as check the box for the XF switch*" is displayed when the check box of the switch /XF is checked but the corresponding text field is empty or when the text field has information in it and the check box is not checked. The way to get ride of this alert is to either uncheck /XF and leave the text field empty or fill the text field with the appropriate information.

- "*Please enter a value in the field as well as check the box for the XD switch*" is displayed when the check box of the switch /XD is checked but the corresponding text field is empty or when the text field has information in it and the check box is not checked. The way to get ride of this alert is to either uncheck /XD and leave the text field empty or fill the text field with the appropriate information.

- "*Please enter a value in the field as well as check the box for the W switch*" is displayed when the check box of the switch /W is checked but the corresponding text field is empty or when the text field has information in it and the check box is not checked. The way to get ride of this alert is to either uncheck /W and leave the text field empty or fill the text field with a number.

- "*Please enter a value in the field as well as check the box for the R switch*" is displayed when the check box of the switch /R is checked but the corresponding text field is empty or when the text field has information in it and the check box is not checked. The way to get ride of this alert is to either uncheck /R and leave the text field empty or fill the text field with a number.

- "*Please chose between COPY, SEC or COPYALL switches*" is displayed when more than one of the specified switches is checked. The way to get ride of this alert is to only select one of the three switches.

- "*Please enter a value in the field as well as check the box for the COPY switch*" is displayed when the check box of the switch /COPY is checked but the corresponding text field is empty or when the text field has information in it and the check box is not checked. The way to get ride of this alert is to either uncheck /COPY and leave the text field empty or fill the text field with one or a combination of the letter *datsou*.

e. Collections

i. Single Collection:

- "*Identify which files you want. Enter a Destination, Source path and the log file name* " is displayed when one or more of the required field is not filled. The only way to get ride of this alert is to fill out all required fields. The

first sentence refers to the first text field (“*Names of files to act Upon*”) and the second part refers to the name of the log file and its path, and the path of the source and destination drives.

- “*Destination is too small to get all the data from the source path.*” is displayed when the source is larger than the space available on the destination. The only way to get ride of this alert is to change either the source or destination folders.

j. Batch Collection:

- “*Identify which files you want. Enter the destination, source and log paths. Fill out the textarea in this format: bbotta, Brent Botta.*” is displayed when the one or more of the fields are either empty or in the case of the text area not properly filled out. The first sentence refers to the first text field (“*Names of files to act Upon*”), the second sentence refers to the path of the log file, the path of the source and destination drives and the third sentence refers to the text area meant to capture the different folders/user directories and the name for the log files. The only way to get ride of this alert is to fill out all required fields in the expected way.

- “*Destination is too small to get all the data from the source path*” is displayed when the source (total) is larger than the space available on the destination. The only way to get ride of this alert is to change either the source or destination folders.

5. Log File Analysis

RoboCopy generates a log file for each directory processed.

FriendlyRoboCopy has the capabilities of opening each log file and reporting the following errors in the comprehensive log file:

- Error 16. This error means that a serious error happened. RoboCopy did not copy any files. This is either a usage error or an error due to insufficient access privileges on the source or destination directories. This might be generated because examiners requested the /S switch and did not have the required permission to copy those files. The comprehensive log file reports the path of the RoboCopy generated log file where this problem occurred.

- Error 8. This error means that some files or directories could not be copied. Some error occurred during copying and the retry limit was exceeded. This error should be investigated further since there should not be a problem in copying them at least as far as permission is concerned.

- Error 4. This error means that there are some mismatched files or directories in what tried to copy. This error should not be encounter by examiners if this is the first time that they try to collect data with RoboCopy to this destination. However, if this error is reported, examiners want to investigate the problem that occurred.

FriendlyRoboCopy also reports the following in the comprehensive file:

- The number of directories skipped by RoboCopy. This will happen if examiners have already copied some data. This is worth investigating if no prior extraction was done.
- The number of files skipped by RoboCopy. This will happen if examiners have already copied some data. This is worth investigating if no prior extraction was done.
- The number of directories that RoboCopy failed to copy. Usually the FAILED field refers to network problems.
- The number of files that RoboCopy failed to copy. Usually the FAILED field refers to network problems.

For more information on the meaning for the errors, refer to RoboCopy documentation (see section one of this guide).

6. Comprehensive Log File

The goal of the comprehensive log file is to gather important information about the examination that RoboCopy is not programmed to do. This text file includes:

- The date along with all data typed in the fields from the *Case Information* tab,
- All chosen RoboCopy switches from the *Switches* tab,
- The name and path of the log files generated by RoboCopy,
- The path and size of the source directory(ies),
- The path and available space of the destination directory,
- The name of each users in the source directory in the case of a batch process,
- Result of the log file(s) analysis.