Forensic Scenario Bot

User Manual

Contents

Requirements

Operating System: Windows 7, Windows 8, Windows 8.1, Windows 10

Processor: 1GHz x86 or x64 processor.

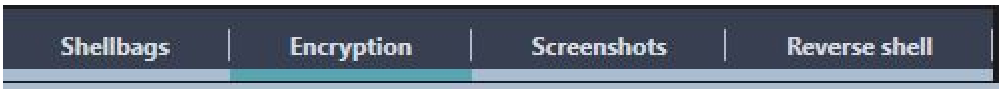
RAM: 2GB RAM.

Additional Software: TrueCrypt and Nmap are required for some scenarios.

Permissions: User must have permission to create files\folders and browse the internet for some functions to run.

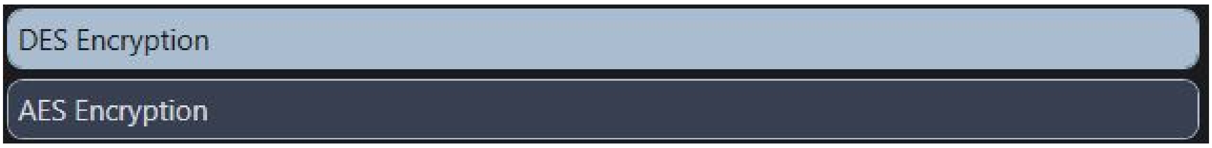
User Interface

Category Tabs



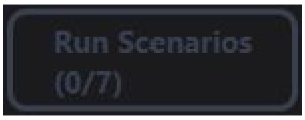
The tabs represent the different scenario categories. Clicking on a tab reveals the actual scenarios which can be selected and information about them. Only one tab can be selected at a time, however multiple scenarios across different tabs can be selected.

Scenario Buttons

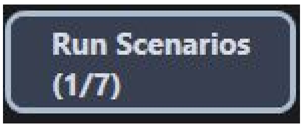


Hovering over a scenario highlights it and displays information about it in the box below. If a scenario is clicked on, then it is selected and remains highlighted. If more than one scenario is selected, the “Run Scenarios” button will become active.

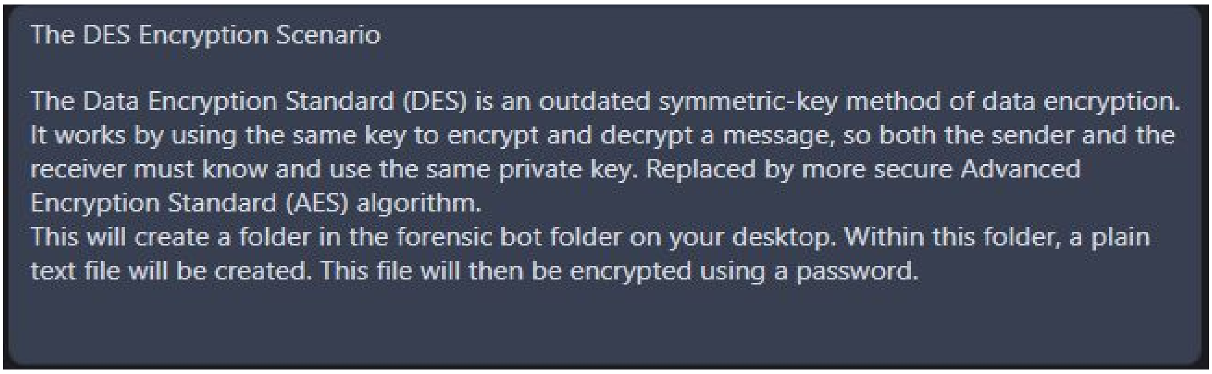
Inactive



Active



Description Box

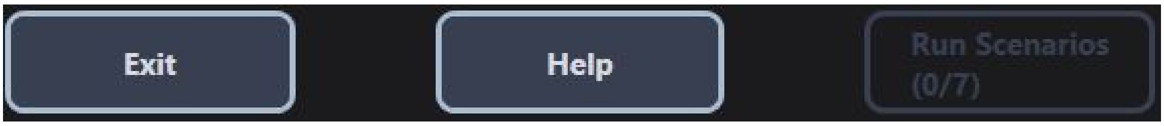


The DES Encryption Scenario

The Data Encryption Standard (DES) is an outdated symmetric-key method of data encryption. It works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. Replaced by more secure Advanced Encryption Standard (AES) algorithm.
This will create a folder in the forensic bot folder on your desktop. Within this folder, a plain text file will be created. This file will then be encrypted using a password.

Information about a scenario will appear in the box when a scenario item is hovered on.

Function Buttons



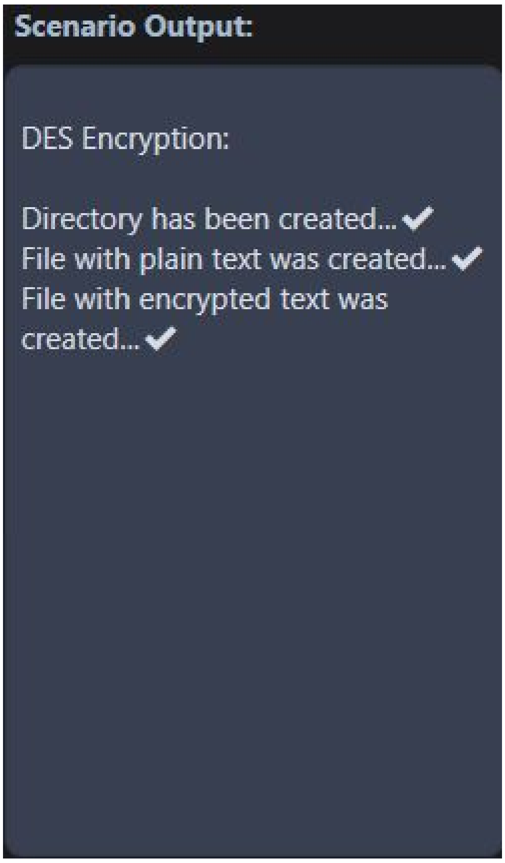
The exit button terminates the program. If there are running scenarios, the user will be asked to confirm that they want to exit.

The help button displays the user manual.

The run scenarios button executes the selected scenarios.

Exports the output from the last session into a text file.

Output Window



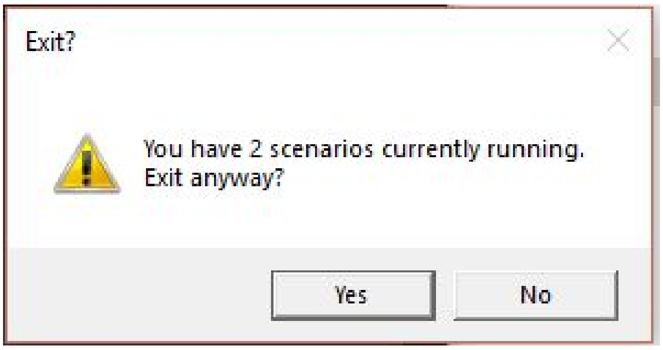
```
DES Encryption:

Directory has been created... ✓
File with plain text was created... ✓
File with encrypted text was
created... ✓
```

The Output Window gives the scenario descriptions, important information and, while the program is running, will show a live log of the programs activities.

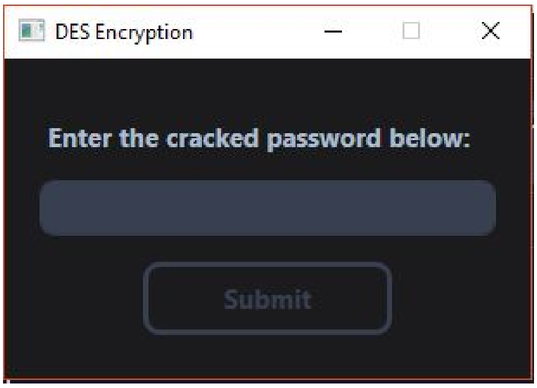
This window also shows the full log after it has executed.

Message Boxes



You have 2 scenarios currently running.
Exit anyway?

Standard message boxes are used for user prompts or to relay information.



Blue message boxes are used in the Encryption Scenarios to check passwords.

Encryption Scenarios

AES Encryption

The AES Encryption Scenario initially creates a plain text file. This is then encrypted.

The files created during the AES Encryption scenario can be found in the **\ForensicBot\AES-String\** directory on your desktop. Here the program will deposit an encrypted text file.

By finding the password used and entering this into the AES Decrypt Scenario, you can create the plain text version of this file.

-HINT-

The RAM will have a record of the password used. It is unlikely that this will be in a readable format. Perhaps it is a hash value?

DES Encryption

The DES Encryption Scenario initially creates a plain text file. This is then encrypted.

The files created during the DES Encryption scenario can be found in the **\ForensicBot\DESEncryption\** directory on your desktop. Here the program will deposit an encrypted text file.

By finding the password used and entering this into the DES Decrypt Scenario, you can create the plain text version of this file.

-HINT-

The RAM will have a record of the password used. It is unlikely that this will be in a readable format. Perhaps it is a hash value?

TrueCrypt

The Truecrypt Scenario will mount an encrypted M: drive on your PC. Within this drive will be a text file. The drive will then be dismounted.

On the desktop, the **\ForensicBot\True Crypt** folder will contain a copy of this encrypted drive. Should you find the password in the RAM, You can attempt to mount the drive yourself.

By finding the password used and entering this into the TrueCrypt Decrypt Scenario, you can validate that the password found is correct.

-HINT-

The RAM will have a record of the password used. It SHOULD be relatively easy to locate if you can find references to the mounted drive.

Browse Scenario

The Browse Scenario will browse to several websites one by one attempting to navigate to a link on each website it visits in incognito mode (or private browsing).

-HINT-

While a browser is using private browsing, they try not to write information to the hard drive. RAM still keeps a record of the websites visited.

Search Scenario

The Search Scenario will search for a keyword pair in a search engine in incognito mode (or private browsing) and attempt to navigate to a link found on the search page.

-HINT-

While a browser is using private browsing, they try not to write information to the hard drive. RAM still keeps a record of the websites visited.

Screenshot Scenarios

The Screenshot Scenarios will take several snapshots of your windows. Each time the resulting JPG will be moved and renamed.

-HINT-

Look in the RAM for files being moved and renamed. These files may appear out of place in your "special" directories such as Documents\ and Videos\.

ShellBags Scenario

The ShellBags Scenario creates several randomly named files and folders. It then copies, moves and deletes files within the folders. The ShellBags in the Windows Registry will have a record of these activities and the RAM will have a record of changes made to the registry.

-HINT-

A good knowledge of the registry is needed here. There isn't much more help to be given…

Troubleshooting F.A.Q

Q. I’m running a scenario and it repeatedly fails at the same stage.

A. Check that you have the required permissions for that PC.

Q. I cannot select a scenario because the button is gone!

A. You may not have the required software installed.

Q. I think I’ve found the password but the program tells me it is incorrect.

A. Passwords are case sensitive. Also, ensure that the password you’ve found is for the correct scenario.

Q. The program run for a while then crashed near the end of its operations.

A. Perhaps you are running too many scenarios. Everything is designed to run through RAM. The more scenarios that are run at a time, the more RAM is used.

Q. The Browser Scenarios don’t always visit new links.

A. This is normal. If a website is running primarily Flash, it can be problematic for the program to use. Try the scenario again, it may work a second time.