Holodeck Enterprise Edition v. 2.5

Help Documentation

Last updated: 5/27/04

Table of Contents

Holodeck Windows and Panes 158

Automated Testing with Holodeck 173

Getting Started

Getting started guide

The best place to start if you are a new user is with the Holodeck Tutorials. The tutorials have been set up so you can start with the first tutorial Setting up your first project and work through to the last while learning all the basics of Holodeck. Holodeck includes an application with easily discoverable bugs written into it, many of the tutorials have been created using this app.

Each of the tutorials should take approximately half an hour to complete, and will teach you not only the basics of Holodeck, but also how to track down the bugs once you've found them, and what many bugs look like when they are discovered in an app.

To learn more about the Holodeck workspace please see the Windows and panes overview.

Holodeck Tutorials

The Holodeck tutorials will help you to discover the power of Holodeck in an easy to learn step by step method. By completing these tutorials you will learn the visual environment of Holodeck as well as methods to more fully test your application.

Each tutorial focuses on a specific task that can help you test your application. We suggest you complete the tutorials in order, however if you already feel comfortable with Holodeck you may choose to review only the sections of interest to you.

Beginner:

Creating your first project – This tutorial will show how to create a project using the BrokenApp that came with Holodeck and save that project to be used in later tutorials.

Takes approximately 10-20 minutes to complete and focuses on the following tasks:

Setting up your first project

The Create a New Project Wizard

Saving the Project

Tracking down and removing a single dll – in this tutorial we will be investigating how the Content Advisor in Internet Explorer works and if there is a way to disable it using Holodeck.

Takes approximately 20-30 minutes to complete and focuses on the following tasks:

Introduction

Before you begin

Load Internet Explorer into Holodeck

Investigating logs

Fail msratings.dll

Restart Internet Explorer

Verify Failure

Dealing with Multiple Processes – This tutorial will help explain how to setup a project with multiple applications under test.

Takes approximately 20 minutes for setup and focuses on the following tasks:

Introduction

Creating a Holodeck project file

Adding a second process to a project

Setting per process items

- **Create a File in Use fault for Notepad.exe**
- **Create a Memory Fault for BrokenApp.exe**
- **Create a memory limit for Notepad.exe**
- **Create a Resource Fault for BrokenApp.exe**
- **Create an API function test for notepad.exe**

Working with Global items

- **Create a report for this project**
- **Creating Corrupted Files**

How to use faults to deprive excel of memory – This tutorial will explain how to deprive an application of physical dependencies such as memory, hard drive space, and network upload and download bandwidth.

Takes approximately 20 minutes for setup and focuses on the following tasks:

Introduction

Set Insufficient Memory

Verify Insufficient Memory

Intermediate:

Learning about API failures during startup and comparing logs – In this tutorial we will learn how to investigate API failures using Holodeck's log and reporting tools.

Takes approximately 20-30 minutes to complete and focuses on the following tasks:

Introduction

Load project

Filtering the log result

Creating a Report for easy viewing

Exporting logs

Comparing logs

Making sense of the difference

Creating Network Corruption Using Regular Expressions– This tutorial covers how to create a network corruption fault, and use regular expressions to find and replace specified strings on the network.

Takes approximately 20 minutes to setup and focuses on the following tasks:

Introduction

Investigate Network Packets

Open Network Corruption Wizard

Select Which Data Should be Corrupted

Select Regular Expressions as the Method of Corruption

Create a Regular Expression and Expansion String

Verify the Fault is set

Using Holodeck to Corrupt files and test file processing – In this tutorial we will corrupt a file using Holodeck's built in file corruption and load it into the application under test.

Takes approximately 20-30 minutes and focuses on the following tasks:

Introduction

Corrupting Files

Using Corrupted Files to test file processing

Viewing the details of the corrupted file

Advanced:

Test Harness and Code Coverage – This tutorial will demonstrate how to use an external test harness and Holodeck's Code Coverage feature to find bugs quickly, easily and efficiently.

Takes approximately 30-40 minutes for setup, and focuses on the following tasks:

Introduction

Create a Holodeck project file

Setup the Test Harness

Begin testing with Code Coverage

How to compare log files

How to deprive your application of its dependencies – This tutorial will explain how to deprive your application of its dependencies such as needed dlls, files, registry keys, and others.

Takes approximately 20 minutes for setup and focuses on the following tasks:

Introduction

Investigate Resources

Set the Resource Fault

Restart BrokenApp with Resource Faults

Investigating the Failure

How to use Holodeck's test automation interfaces – This tutorial will cover how to automatically test your application using Holodeck's built in test harness.

Takes approximately 20 minutes and focusing on the following tasks

Setting up the project for use with the test harness

Setting up the Test Harness

Running Automated tests

Holodeck support center

Questions about Holodeck? Get quality answers and responsive help from the Holodeck **e-mail support team** at:

support@sisecure.com

Feel free to call this support telephone line anytime, a support specialist will return your call promptly.

1-877-SI-HELP-5 (877-744-3575)

Additional Help is available at the **Holodeck Resource Center**.

http://www.sisecure.com/holodeck/learn.shtml

You can find tips to help you use Holodeck more easily in the Tips Section of the Resource Center:

http://www.sisecure.com/holodeck/holodeck_tips.shtml

Be sure to visit the Security Innovation website http://www.securityinnovation.com/ where you will find:

- News
- Technical Papers from our founder James Whittaker and other members of the engineering team at Security Innovation.
- White papers describing some of the foundations behind Holodeck
- Other helpful online resources for securing your application
- Release Notes – known incompatibility and other issues.

Learning Holodeck Basics

How to use this guide

This guide has been separated into several sections. You can explore each section individually to best suit your interests and experience; however the help documentation has been written in such a way that exploring each section in order will be most beneficial. If you are new to Holodeck please read through the Windows and panes overview to familiarize yourself with the layout of the Holodeck workspace; read through the Holodeck Tutorials to learn the features of Holodeck through easy to follow step by step examples.

Note: Many aspects of Holodeck have changed since the previous version; you may want to read each chapter to learn about each new part of Holodeck version 2.5.

For more information on what has change since the last version of Holodeck, please see the What's new in v. 2.5 section.

Other resources

Online Help – Search our website for new help.

Tutorials – Use the tutorials to learn, step by step, new functionality of Holodeck.

Animated Demos – Online Animated Demos show you how to get started with Holodeck as well as advanced topics.

PDF version of the help – Included in the install of Holodeck is a PDF version of these help files, feel free to print this out for offline help.

How to Break Software – Learn how to more fully test your software with this book written by our founder, James Whittaker.

How to Break Software Security – Learn more in depth software security testing with this book, by the same author.

About Fault Injection – Learn more about how Holodeck works with fault injection.

Typographical conventions

Menu items are show in this format: menu name > **menu item name.**

Items in submenus are shown in this format: menu name > submenu name > **menu item name.**

Source code is shown as: `Courier New Fixed Width Font.`

Input typed in verbatim is shown as: **Times New Roman Bold**

Installing and running Holodeck

System Requirements

The following hardware and software is required to run Holodeck version 2.5.

Minimum System requirements for Microsoft Windows:

An Intel Pentium 4 Processor or equivalent, 1.5 GHz or faster

Windows 2000, Windows NT (with Service Pack 3 or later), Windows XP, Windows 2003 Server, Windows Longhorn

Version 4.0 or later of Microsoft Internet Explorer

256 MB of physical random-access memory (RAM)

200 MB of available disk space (80 MB for install, 120 MB for virtual memory if needed)

A 256-color monitor capable of 800 x 600 pixel resolution (millions of colors and 1024 x 768 pixel resolution recommended)

Recommended System requirements for Microsoft Windows:

An Intel Pentium 4 Processor or equivalent, 2.0 GHz or faster

Windows 2000, Windows NT (with Service Pack 3 or later), Windows XP, Windows 2003 Server, Windows Longhorn

Version 4.0 or later of Microsoft Internet Explorer

512 MB of physical random-access memory (RAM)

200 MB of available disk space (80 MB for install, 120 MB for virtual memory if needed)

A 256-color monitor capable of 800 x 600 pixel resolution (millions of colors and 1024 x 768 pixel resolution recommended)

Installing Holodeck

Follow these steps to install Holodeck on a Windows computer.

Note: In certain operating systems, you can install or uninstall Holodeck only if you have Administrative privileges on your computer.

To install Holodeck:

1. Insert the Holodeck CD, or run the installer downloaded from the Security Innovation website
2. Follow the onscreen instructions
3. If prompted, restart your computer.

To register Holodeck:

1. Obtain a Serial Number and Registration Key by purchasing a license either over the phone or online.
2. Choose Help > Register Holodeck …
3. Click Edit…
4. Enter the Serial Number and Registration Key into the text fields.
5. Click Register.
6. Verify License Details to see that registration completed successfully.

Running Holodeck as a Restricted User

To run Holodeck as a restricted user you must give the users group read/write access to both the HolodeckEE registry keys and the Holodeck install directory. To accomplish this follow these directions while logged on as an Administrator:

Note: Simple file sharing must be turned off to give the users group read/write permission to the Holodeck install directory. Follow these directions to turn off simple file sharing:

1) Open any folder
2) Select Tools > Folder Options
3) Select the View tab
4) Uncheck "Use simple file sharing (Recommended)"
5) Click OK

1) Grant the users group read/write access to the HolodeckEE registry keys
   a) Run regedit.exe
      i) Start > Run…
      ii) Type **regedit.exe**
   b) Right click the folder HolodeckEE found at HKEY_LOCAL_MACHINE\SOFTWARE\HolodeckEE and select Permissions
   c) Select the Users group
   d) Grant the Users group full control by selecting the checkbox next to Full Control
   e) Click OK to save the change
2) Grant the Users group read/write access to the install directory of Holodeck
   a) If Holodeck was installed using the default directory it will be located at C:\Program Files\Security Innovation.
   b) Browse to the install directory
   c) Right click the folder Holodeck Enterprise Edition and select Sharing and Security…
   d) Select the Security tab
   e) Select the Users group
   f) Grant the Users group full control by selecting the checkbox next to Full Control
   g) Click OK to save the changes

Holodeck will now work as expected when launched from a restricted user account.

EULA

SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE USING THE HOLODECK^{TM} SOFTWARE ("SOFTWARE"). BY CLICKING "I ACCEPT" AND DOWNLOADING THE SOFTWARE, YOU ARE ACKNOWLEDGING THAT YOU HAVE READ AND UNDERSTAND THIS SOFTWARE LICENSE AGREEMENT AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT, CLICK "I DO NOT ACCEPT" AND DELETE THE SOFTWARE FROM YOUR COMPUTER WITHOUT USING IT.

1. **License Grant.** Subject to the terms of this Software License Agreement ("License"), Security Innovation, L.L.C. ("Licensor") grants you a nontransferable, nonexclusive, limited license to use the Software and any associated documentation files (collectively, the "Products") with which this License is distributed. You may only use the Products for your internal business purposes or for your own personal use. You may not:

- Copy, translate, port, modify, or make derivative works of the Products;

- Assign this License without Licensor’s prior written approval;

- Rent, disclose, publish, sell, assign, lease, sublicense, market, or transfer the Products or use them in any manner not expressly authorized by this Agreement; or

- Derive or attempt to derive the source code, source files, or structure of all or any portion of the Products by reverse engineering, disassembly, decompilation, or any other means.

2. **Ownership.** You have no ownership rights in the Products. Rather, you have a license to use the Products as long as this License remains in effect. Ownership of the Products and all intellectual property rights in them shall remain at all times with Licensor.

3. **Copyright.** The Products contain material that is protected by United States copyright law and trade secret law, and by international treaty provisions. All rights not granted to you by

this License are expressly reserved by Licensor. You may not remove any proprietary notice of Licensor from any copy of the Products.

4. **Confidentiality.** You acknowledge that the Products contain proprietary trade secrets of Licensor and you hereby agree to maintain the confidentiality of the Products using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information, but in no event less than a reasonable degree of care. You agree to reasonably communicate the terms and conditions of this License to those persons employed by you who come into contact with the Products, and to use your best efforts to ensure their compliance with those terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Products for the purpose of deriving the source code for the Products.

5. **Disclaimer of Warranties.** YOU EXPRESSLY AGREE AND ACKNOWLEDGE THAT USE OF THE PRODUCTS IS AT YOUR SOLE RISK. THE PRODUCTS ARE PROVIDED "AS IS," WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND. LICENSOR EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND TITLE/NON-INFRINGEMENT. LICENSOR DOES NOT WARRANT THAT THE PRODUCTS WILL MEET YOUR REQUIREMENTS, THAT THE PRODUCTS ARE COMPATIBLE WITH ANY PARTICULAR HARDWARE OR SOFTWARE PLATFORM, OR THAT THE OPERATION OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE PRODUCTS WILL BE CORRECTED. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCTS IS ASSUMED BY YOU. FURTHERMORE, LICENSOR DOES NOT WARRANT OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE PRODUCTS OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, QUALITY, RELIABILITY, APPROPRIATENESS FOR A PARTICULAR TASK OR APPLICATION, CURRENTNESS, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY LICENSOR OR LICENSOR’S AUTHORIZED REPRESENTATIVES SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF LICENSOR’S OBLIGATIONS HEREUNDER.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. IN THAT EVENT, ANY SUCH IMPLIED WARRANTIES RELATING TO THE PRODUCTS ARE LIMITED IN DURATION TO THIRTY (30) DAYS FROM THE DATE OF FIRST USE OF THE PRODUCTS. THIS WARRANTY GIVES YOU SPECIFIC RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

6. **Limitation Of Liability.** IN NO EVENT SHALL LICENSOR BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR CONNECTED IN ANY WAY WITH USE OF OR INABILITY TO USE THE PRODUCTS, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. LICENSOR’S TOTAL LIABILITY TO YOU FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION

(WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE) SHALL NOT EXCEED THE AMOUNT OF THE LICENSE FEES PAID BY YOU FOR THE PRODUCTS AND DOCUMENTATION.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

7. **Term and Termination.** Upon payment by you of the first year's license fee, the License shall be in effect for an initial term of one (1) year, unless sooner terminated in accordance with this Section. If you are in compliance with the terms and conditions of this License, and provided that you pay the annual renewal license fee each year in the manner prescribed by Licensor, you will have the right to renew the License for successive renewal terms of one (1) year each. You may terminate this License at any time by destroying or returning to Licensor all known copies of the Products in your possession or under your control. This License shall terminate automatically in the event you breach any of the terms and conditions herein. Upon notification of termination, you agree to destroy or return to Licensor all copies of the Products and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and nondisclosure shall survive termination of this License.

8. **License Fees.** License fees are due and payable in advance on an annual basis. The license fee applicable for any renewal year shall be Licensor's then- current license fee for the Products.

9. **Equitable Relief.** You acknowledge and agree that Licensor will be irreparably injured if the provisions of Sections 1 (License Grant) and 4 (Confidentiality) were not capable of being specifically enforced, and agree that Licensor shall be entitled to equitable remedies for any breach of Sections 1 and 4, in addition to, and cumulative with, any legal rights or remedies, including the right to damages.

10. **Severability.** If any provision of this License is found to be invalid or unenforceable by any court, such provision shall be ineffective only to the extent that it is in contravention of applicable laws without invalidating the remaining provisions of the License.

11. **Choice Of Law.** This License shall be construed in accordance with the laws of the State of Florida without reference to the conflicts of law principles thereof.

12. **Venue.** You agree that all actions or proceedings arising in connection with the License shall be tried and litigated exclusively in the state courts located in or for Melbourne, Florida. This choice of venue is intended by the parties to be mandatory and not permissive in nature, and to preclude the possibility of litigation between the parties with respect to, or arising out of, this License in any jurisdiction other than that specified in this Section. Each party waives

any right it may have to assert the doctrine of *forum non conveniens* or similar doctrine or to object to venue with respect to any proceeding brought in accordance with this Section.

13. **Entire Agreement.** This License constitutes the entire agreement between the parties with respect to the subject matter of this License, and supersedes all other prior and contemporary agreements, understandings, and commitments between the parties regarding the subject matter of this License. This License may not be modified or amended except by a written instrument executed by the parties.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS SOFTWARE LICENSE AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

What's new in v. 2.5

What's new in v. 2.5

Enable customers to add new intercepts

Customers can point Holodeck at any win32 DLL or .net assembly and Holodeck will intercept any public methods just as it currently does for system API calls. This allows monitoring and testing of any public interface installed on a tester’s computer

Improve scheduled tests

Add the following constructs to scheduled api tests:

- Fire xx% of time
- Fire based on call stack matching
- Fire on nth instance
- Pause application when test fires (breakpoints)

Improve control of application under test

- Allow the user to remove, stop, or restart any application in the project

Improve file corruption

- Integrate file corruption fully into Holodeck so that files are corrupted at time of use and HD re-directs application to the new corrupted file. Allows a file to be corrupted differently every time it is accessed

Add to default intercept list

- Add the set of ‘dangerous’ APIs from Writing Secure Code, native COM methods, crypt32 functions, and wintrust functions

Improve .NET interception support

- Support reference parameters, private methods, and system.reflection. Merge metadata to remove as many clr version dependencies as possible.

Improve fault scenarios

- Make faults more realistic, ensuring they match real world conditions. Allow users to easily modify faults or add their own custom faults

Add resource based faults

- Create a new test entity that enables faults to easily target a specific file, registry, or process resource rather than always being global to the application

Improve API logging

- Log any intercepted API call regardless of whether it was called directly by the application or not. Show API calls in a tree view with depth according to who made the call.

Fully support Windows services

- Add the ability to launch or attach to any service regardless of whether it is standalone or part of a svchost process. Show available services to launch or attach to similarly to how processes are currently shown.

Improve error-code/return-value mapping

- Use MSDN docs and windows source code scanning to ensure our database of valid return values and error codes is correct for every default intercepted api. This ensures our UI gives the user the correct information when they are creating a test and also makes sure our automatic test generation is generating accurate scenarios

Add .Net to custom intercepts generator

- All users to generate test code for .Net as well as win32 APIs and also for any added intercepts for non-default DLLs and assemblies.

Add network packet logging

- Users can see all network packet traffic from the application under test and then dig into the bits in each packet at will. This will highlight corrupt bytes from network corruption tests so that the user can easily tell how packets have been changed in order to later repro a bug caused by net corruption

Improve code coverage test generation

- Target more than just startup code by varying when the test will be applied.

Integrated Debugger

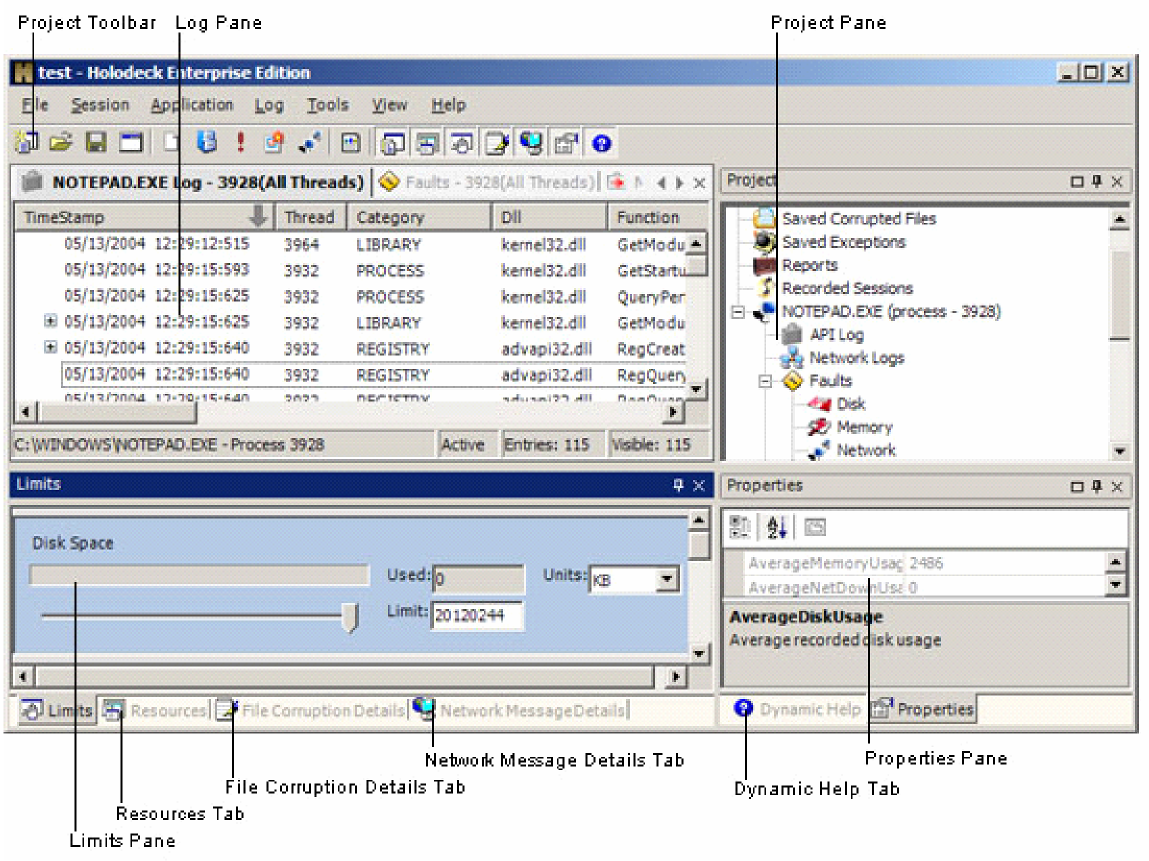
- Add a debugger to Holodeck that catches all app crashes and exceptions creates a minidump that can later be loaded into Visual Studio for debugging.

New help docs

- Revise help docs so that they are task based rather than feature based, add more tutorials, create a start page that always shows on HD launch, create videos that walk the user through the most important tutorials, ship a broken application with Holodeck that is used in tutorials and with which the user can experiment.

Exploring the Holodeck workspace

Windows and panes overview



TimeStamp	Thread	Category	Dll	Function
05/13/2004 12:29:12:515	3964	LIBRARY	kernel32.dll	GetModu
05/13/2004 12:29:15:593	3932	PROCESS	kernel32.dll	GetStartu
05/13/2004 12:29:15:625	3932	PROCESS	kernel32.dll	QueryPer
05/13/2004 12:29:15:625	3932	LIBRARY	kernel32.dll	GetModu
05/13/2004 12:29:15:640	3932	REGISTRY	advapi32.dll	RegCreat
05/13/2004 12:29:15:640	3932	REGISTRY	advapi32.dll	RegQuery

C:\WINDOWS\NOTEPAD.EXE - Process 3928 | Active | Entries: 115 | Visible: 115

Used: 0
Units: KB
Limit: 20120244

AverageMemoryUsag 2486
AverageNetDownUs 0

AverageDiskUsage
Average recorded disk usage

Project toolbar – This toolbar contains items pertaining to your current project, creating a new project, and showing and hiding panes. Follow this link to find out what each does.

Log Pane – The log pane displays all the APIs Holodeck is currently intercepting.

Project Pane – The Project Pane will help you to display and organize your project entries into a tree view. The majority of the information about your project will be accessible from this pane.

Properties Tab – Clicking this tab will show the properties pane will provide you with information regarding selected UI objects. Look here for additional information about the UI you are currently working with

Limits Pane – The limits pane makes it easy to limit the amount of disk, memory, or networking resources your application has available to it.

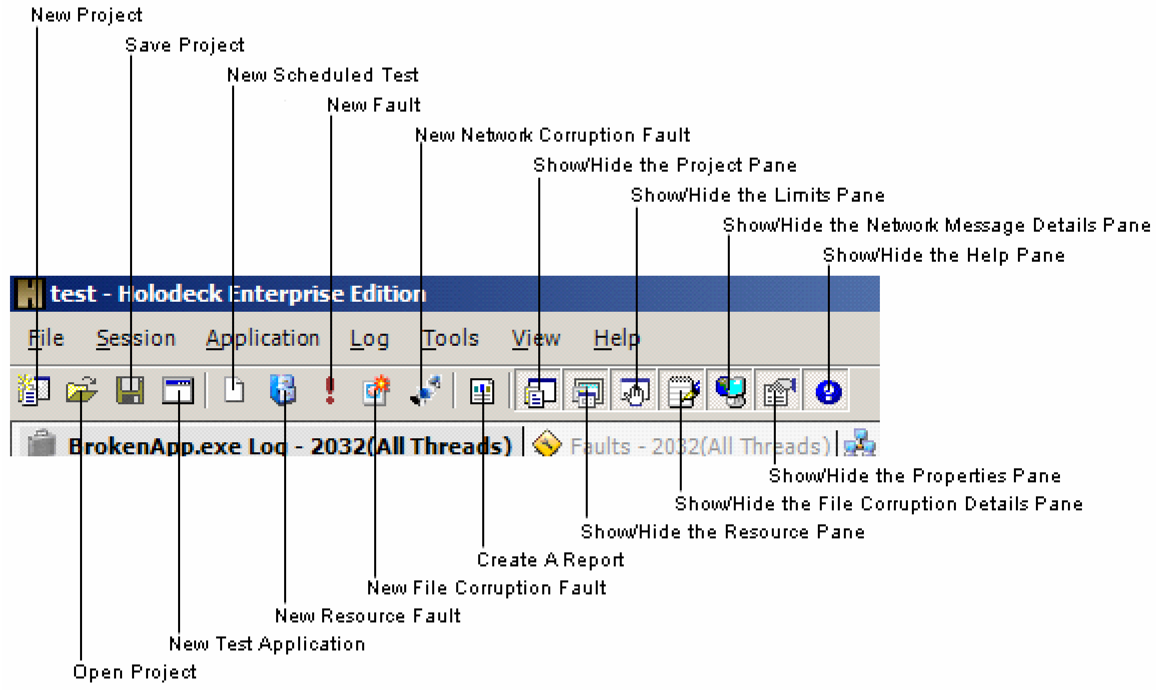
Resource Tab – Clicking this tab will show the Resource Pane which shows the file, folder, process, library, registry resources your application is currently using.

File Corruption Details Tab – Clicking this pane will the File Corruption

Dynamic Help Pane – Watch the Dynamic Help Pane for information on the task you are currently doing. This pane will change and show information and tips to help you complete your task.

Project toolbar

The project toolbar gives you easy access to some of the more common tasks that Holodeck provides; it also gives you an easy way to hide and show the different panes.


New Project
Save Project
New Scheduled Test
New Fault
New Network Corruption Fault
Show/Hide the Project Pane
Show/Hide the Limits Pane
Show/Hide the Network Message Details Pane
Show/Hide the Help Pane
test - Holodeck Enterprise Edition
File
Session
Application
Log
Tools
View
Help
BrokenApp.exe Log - 2032(All Threads)
Faults - 2032(All Threads)
Show/Hide the Properties Pane
Show/Hide the File Corruption Details Pane
Show/Hide the Resource Pane
Create A Report
New File Corruption Fault
New Resource Fault
New Test Application
Open Project

New Project – Opens the new project wizard, to begin testing your application.

Open Project – Opens an open file dialog box so you can select a previously saved project.

Save Project – Saves the current project for later use

New Test Application – allows you to add another test application to the already running project

New Scheduled Test – Opens the new scheduled test wizard so you can create a scheduled test

New Resource Fault – Opens the new resource test wizard so you can create a resource test

New Fault – Opens the faults pane so you can set new faults for your application.

New File Corruption Fault – Opens the new file corruption fault wizard.

New Network Corruption Fault – Opens the new network corruption fault wizard.

Create a Report – Generates a Holodeck report for easy viewing of errors, API calls, and other information regarding your application.

Show/Hide the Project Pane – Shows or hides the project pane

Show/Hide the Resource Pane – Shows or hides the resource pane

Show/Hide the Limits Pane – Shows or hides the Limits pane

Show/Hide the File Corruption Pane – Shows or hides the File Corruption Details pane

Show/Hide the Network Message Details Pane – Shows or hides the network message details pane

Show/Hide the Properties Pane – Shows or hides the properties pane

Show/Hide the Help Pane – Shows or hides the dynamic help pane

Moving, detaching and hiding panels

Holodeck has been created to use a familiar layout design so things are placed in a easy to find and use location. For this reason you can detach, move, or hide any pane. This is especially useful for a multi-monitor environment; you can detach each of the panes and place them on the secondary monitor while having the main window of Holodeck and the Application Under Test in the main window.

To detach a complete pane click the title bar of the pane and drag to the location you desire. Valid docking locations are anywhere along the outer edge of the window. You may also "float" a window anywhere, including separate monitors.

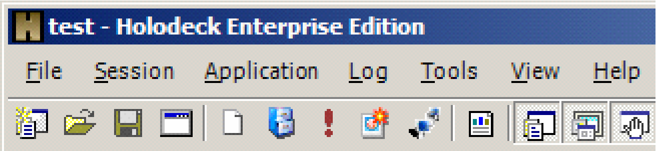
To detach a single pane click the tab, located at the bottom of the pane, and drag to the location you desire. You can dock or float this pane the same way you can a complete pane.

To hide a pane you can "unpin" the pane so it automatically hides itself while not in use. To pin or unpin a pane click the pin icon on the title bar.

To close the pane use the "X" on the title bar of the pane. Once a pane has been closed you can use the button bar at the top of the window, or the view menu open the pane again.

The pane layout is saved each time you close Holodeck

Menus overview



The File menu contains menu items that relate directly to your project file such as: New Project, New Test Application, Open, Close, and Save.

The Session menu contains menu items that relate to all the applications in the session you are currently working with. This includes Test Generation, Recording and Replaying sessions and turning on Per Thread functionality.

The Application menu contains items that apply to the application that currently has focus in Holodeck.

The Log menu contains items to find keywords in the log files and filter the log results.

The Tools menu gives you access to other tools useful for testing your application such as the Custom Intercept Generator and a method to add Holodeck Intercepts.

Use the View menu to show or hide the workspace panes.

The Help menu includes menu items pertaining to the help topics, how to report a bug in Holodeck, register Holodeck, and information about Holodeck.

Menus in Depth

File Menu

The file menu contains items standard to this menu, including items to create a new project, open an existing project, save the current project, close and exit this session.

New Project … - More information on creating a new Holodeck Project.

New Test Application … - Add another test application to the currently running project.

Open Project... – Open a previously saved project.

Close – Close this project, Holodeck will remain active.

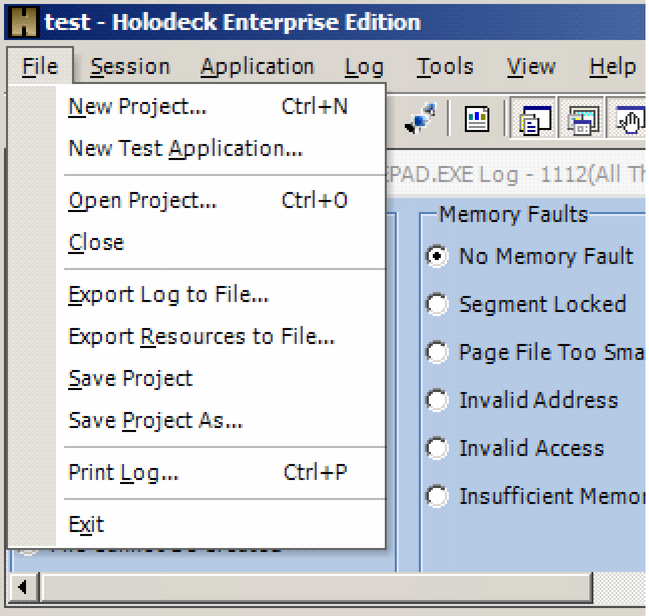
Export Log to File … - Export the currently selected API logs to a file to an easy to read csv spreadsheet file.

Export Resources to a File – Holodeck can export the current list of resources your application is using to an easy to read csv spreadsheet file.

Save Project – Save the current project for later use.

Save Project As… - Save the current project with a new name.

Print Log … - Print the currently selected API logs.



Memory Faults
● No Memory Fault
○ Segment Locked
○ Page File Too Sma
○ Invalid Address
○ Invalid Access
○ Insufficient Memor

Session Menu

The session menu contains items that apply to all applications and thread in the session.

Code Coverage Test Generator … - Holodeck can help you test your applications more thoroughly by setting faults, limits, and tests while your application is running.

Stress Test Generator … - Holodeck can help stress test your application by creating specific scheduled tests while your application is running.

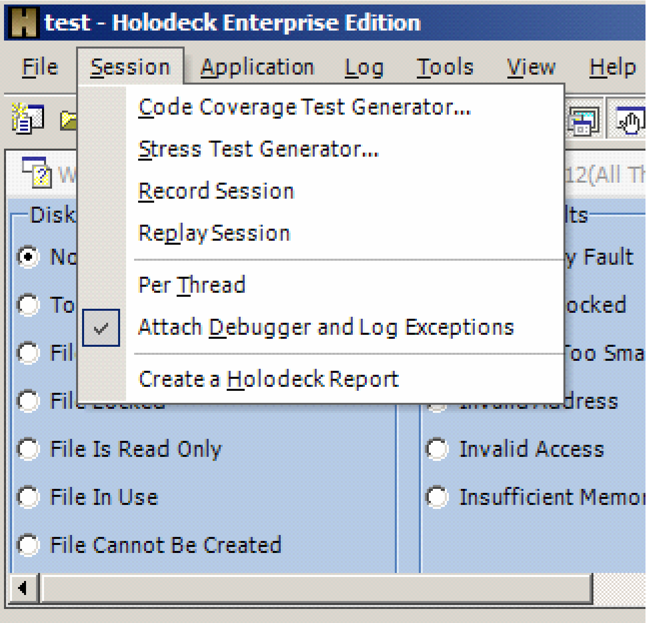
Record Session – Record the tests, limits, faults etc your application undergoes by using this functionality.

Replay Session – Replay a recorded session to reproduce the test environment your application has underwent.

Per Thread – Holodeck automatically logs which APIs are called from which threads, create tests and faults specific to each thread by turning on Per Thread functionality.

Attach Debugger and Log Exceptions – Holodeck defaults to log all exceptions your application creates, you can attach a debugger by double clicking on an exception from the exceptions pane. Toggle this functionality here.

Create a Holodeck Report – Holodeck reports help organize a Holodeck session into a single easy to read file.



Application Menu

The application menu contains items that are specific to each individual application. From this menu you can pause, stop, remove or restart an application in the current project without affecting the other applications in your project.

Child Process Inherits Settings – If your applications spawns a child process you can apply any faults or test to that process automatically.

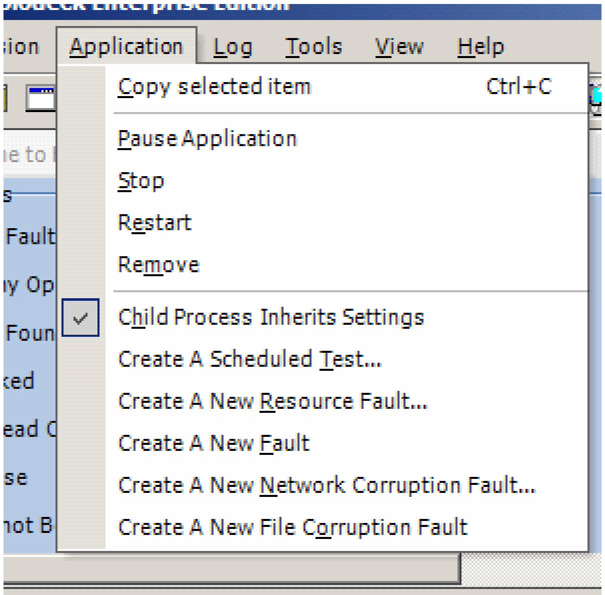
Create a new Schedule Test – Scheduled tests are specific to an individual API function.

Create a new Resource Fault – Resource faults are specific to an individual resource such as a library, process, registry key, or file.

Create a new Fault – Faults are an out of the box testing solutions to help simulate faults common to software and hardware.

Create a new Network Corruption Fault – Holodeck can corrupt network packets being sent or received, through the use of random, find and replace, or regular expression corruption.

Create a new File Corruption Fault – Holodeck can help test file parsing by corrupting individual files.

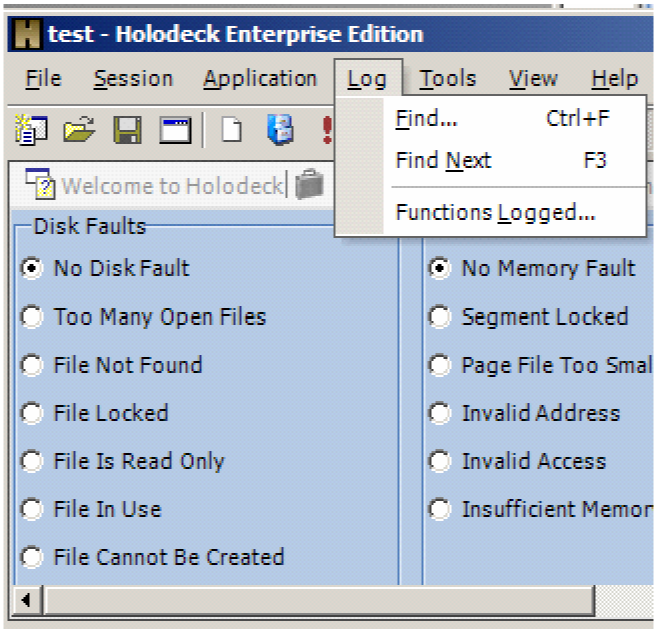

Application
Log
Tools
View
Help
Copy selected item Ctrl+C
Pause Application
Stop
Restart
Remove
✓ Child Process Inherits Settings
Create A Scheduled Test...
Create A New Resource Fault...
Create A New Fault
Create A New Network Corruption Fault...
Create A New File Corruption Fault

Log Menu

The log menu allows you to find specific logged functions in the logs pane, or change which APIs functions are logged.

Find – Quickly search for text within the API logs

Functions Logged – Change which functions are intercepted and logged.



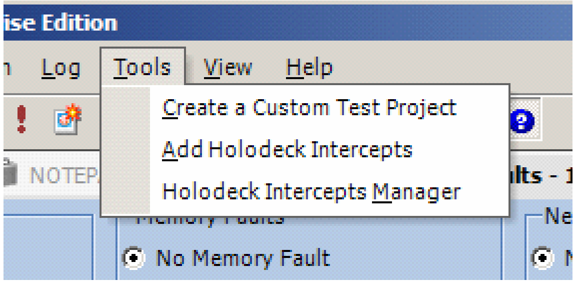
Tools Menu

Holodeck comes with a number of other useful tools.

Create a Custom Test Project – you can create a Visual Studio project to streamline your interception process.

Add Holodeck Intercepts – You can add custom intercepts to Holodeck's list of APIs by running this wizard.

Holodeck Intercepts Manager – Add new or remove intercepts specified by the user in the Holodeck Intercepts Manager.



View Menu

The view menu allows you to toggle which panes are visible, and choose which fields are viewable in the current window.

Project Pane – This pane contains all the information directly related to the current project.

Resource Pane – This pane shows the file, process/library, registry and COM resources your application has touched.

Limits Pane – This pane allows you to set limits on hardware resources such as Memory, Hard Drive Space, and Network upload/download bandwidth.

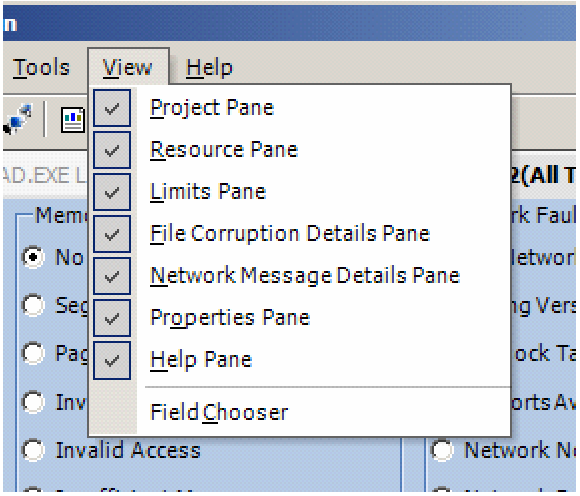
File Corruption Details Pane – This pane shows the details of how Holodeck has corrupted the file.

Network Message Details Pane – This pane shows the detailed data of each network packet.

Properties Pane – This pane shows detailed information about the currently selected item.

Help Pane – This pane changes to show you help related to the current task.

Filed Chooser – The Filed Chooser allows you to change which fields are shown in panes with selectable columns.



Help Menu

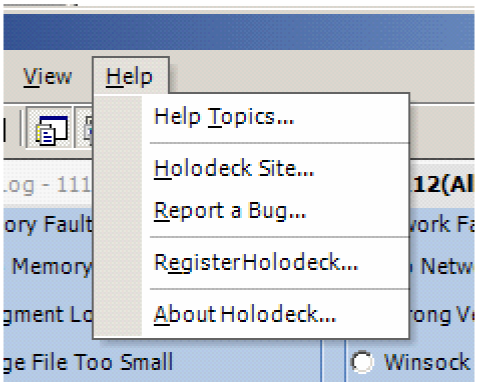
The Help menu includes menu items pertaining to the help topics, how to report a bug in Holodeck, register Holodeck, and information about Holodeck.

Help Topics… - This will display the complete list of Help documentation in the main window.

Holodeck Site… - This will take you to the Holodeck site within Security Innovation

Report a bug… - If you think you’ve found a bug in Holodeck, please let us know so we can make the next version better.

Register Holodeck … - Register Holodeck or get information to register Holodeck here.



Tutorials

Beginner

Creating your first project

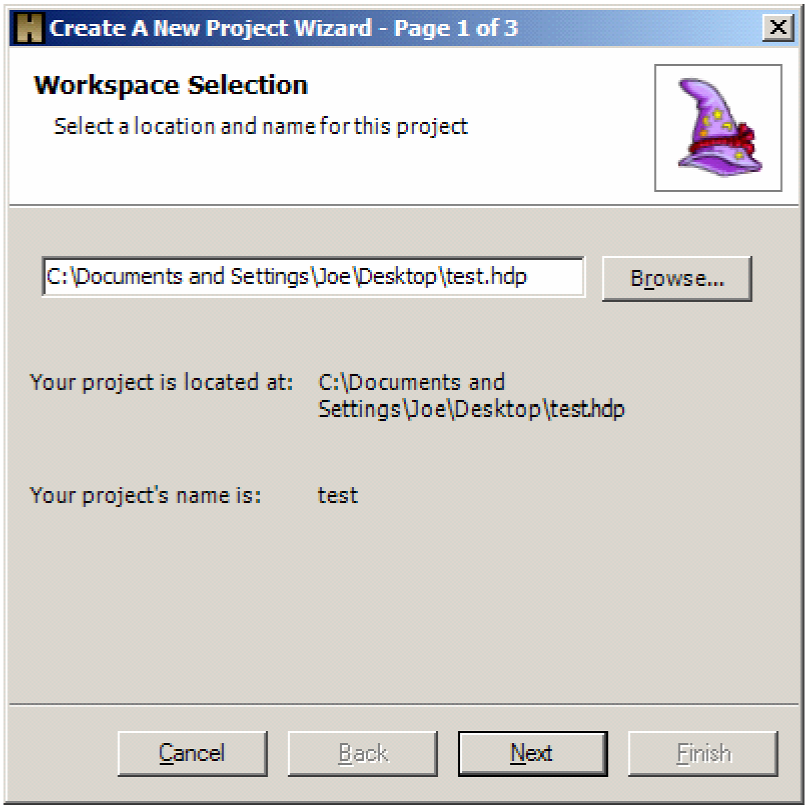
Setting up your first project

In this tutorial we will cover how to create your first project and save it to the hard drive for later use. We will be using the BrokenApp that came with Holodeck to create this project so that in later Tutorials you can simply load this project without having to run though the entire Create a New Project Wizard.

The Create a New Project Wizard

The first page of the Create a New Project Wizard asks for a location to store your project or workspace. This can be anywhere on your harddrive or a network share. You must have complete read/write access to this location.

In this case I have chosen to save the project on the Desktop, and name it test.hdp.



Workspace Selection

Select a location and name for this project

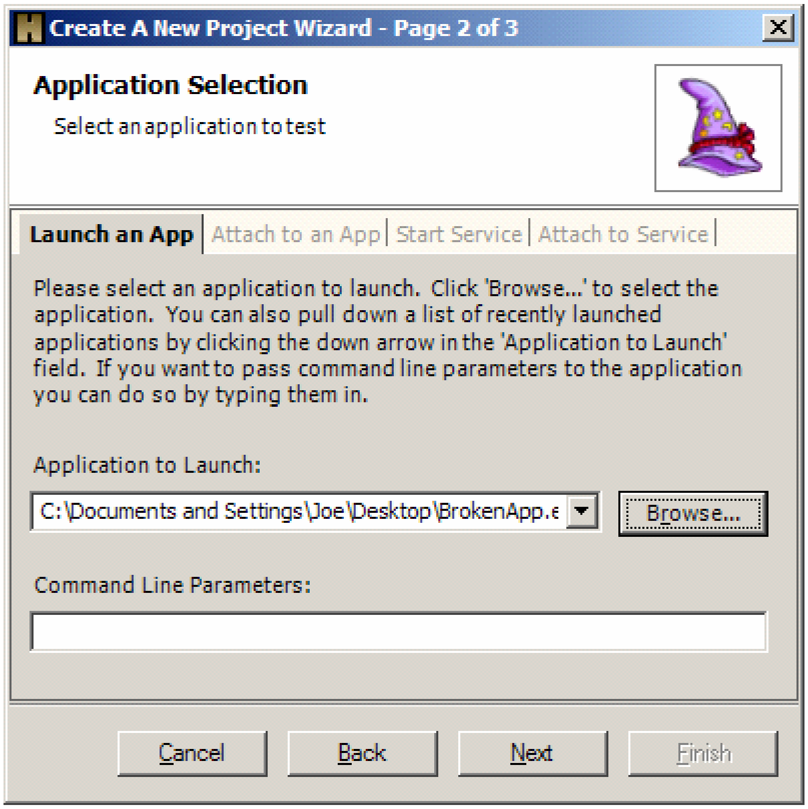
C:\Documents and Settings\Joe\Desktop\test.hdp

Your project is located at: C:\Documents and Settings\Joe\Desktop\test.hdp

Your project's name is: test

The second page of the Create a New Project Wizard is asking which application or service you would like to create this project with. Holodeck supports Launching a new application, attaching to an already running application, Starting a Service, or attaching to an already running service. For this project we want to launch the BrokenApp.

I have placed BrokenApp.exe on my desktop for easy access. It does not require any command line parameters or



Application Selection

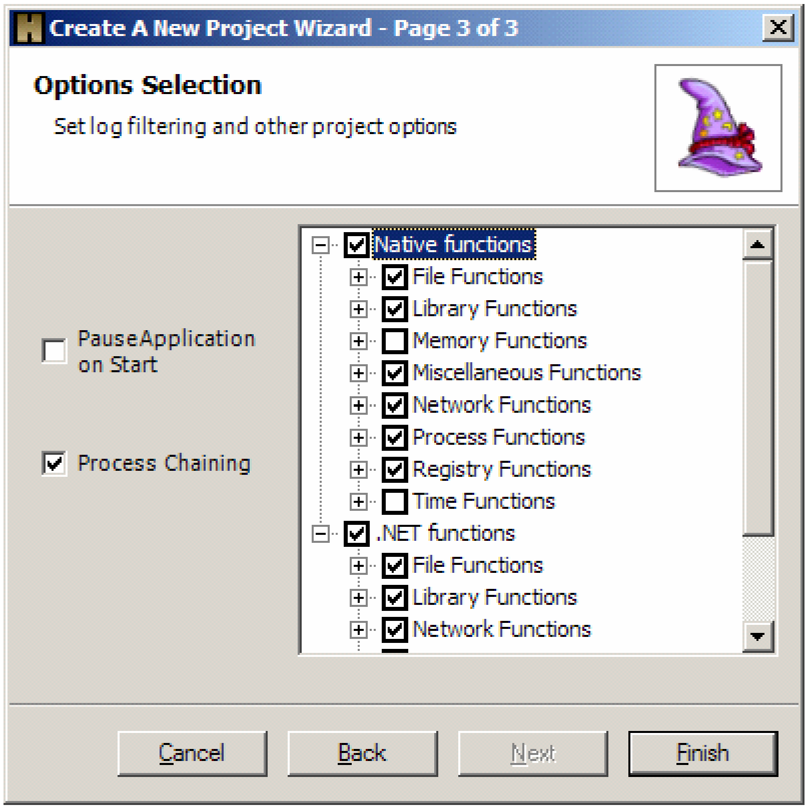
Select an application to test

Please select an application to launch. Click 'Browse...' to select the application. You can also pull down a list of recently launched applications by clicking the down arrow in the 'Application to Launch' field. If you want to pass command line parameters to the application you can do so by typing them in.

Application to Launch: C:\Documents and Settings\Joe\Desktop\BrokenApp.e

Command Line Parameters:

This application was written in Managed C++ code, which means there are both native win32 components and .net functions. We want to intercept all of these API; however, Time and Memory functions are called so often that just logging those functions will give a slight performance degradation. We can perform all the tests in the following tutorials without these functions select.



Create A New Project Wizard - Page 3 of 3

Options Selection

Set log filtering and other project options

□ PauseApplication on Start

☑ Process Chaining

- ☑ Native functions
  - ☑ File Functions
  - ☑ Library Functions
  - □ Memory Functions
  - ☑ Miscellaneous Functions
  - ☑ Network Functions
  - ☑ Process Functions
  - ☑ Registry Functions
  - □ Time Functions
- ☑ .NET functions
  - ☑ File Functions
  - ☑ Library Functions
  - ☑ Network Functions

Saving the Project

Since this project will be used for the later tutorials we would like to save it so we don't have to setup the project each time. Instead we can load a project with all the right logging and pointed to the correct application. This can help save time if you are testing the same application daily. This is also necessary if you are running Holodeck from the command-line.

Since you specified a place for Holodeck to save all related project files, clicking File > Save Project will simply save the latest version of the project to that location.

If you would like to save the project to another location click File > Save Project As… This will bring up a save file dialog for you to specify a new location to save the project.

Tracking down and removing a single dll

Introduction

In this tutorial we would like to investigate how the Content Advisor works and if there is a way to disable it using Holodeck. We will cover the investigation of API calls to find bugs and the creation of a test to disable certain API calls that Internet Explorer uses to enable the Content Advisor.

By watching which API calls are made we can more precisely target certain APIs to find bugs that would otherwise go unnoticed. We can use Holodeck's log features to follow the API call path and watch for abnormal or dangerous API calls. Using the Tests feature of Holodeck we can fail or change the return value of a single API call in order to create abnormal application states.

Before you begin

Set the Content Advisor setting in Internet Explorer: This will set Internet Explorer to begin checking every web page you visit for a Content Rating Certificate.

1) Open MSIE
2) Click Tools -> Internet Options
3) Click on the Content tab
4) Click Enable
5) Leave all the settings at their defaults and click OK

Load Internet Explorer into Holodeck

Load MSIE into Holodeck: In this step we will load MSIE into Holodeck and investigate each API call to see what DLLs requires for start up and also which ones it loads to check the Content Advisor ratings.

1) Start Holodeck and create a new project
   a) File > New Project
   b) Walk through the New Project Wizard
   c) Select Internet Explorer to test (usually located at "C:\Program Files\Internet Explorer\iexplore.exe")
2) MSIE will be automatically started when you click Finish on the final page of the Create new Project Wizard

Investigating logs

By filtering, sorting, and using Holodeck's find feature for the log pane we can locate a specific API call. Internet Explorer loads a library called MSRATING.dll while starting up, and each time it attempts to verify a page's content. This is where Internet Explorer keeps all the information about permissions on each page.

You can sort, filter and add or remove columns in the log pane to make your investigation easier. You can also change the order of the columns by clicking and dragging the columns where you want them to go. In this example we can filter the Category Column in the log pane to show only the LIBRARY Categories. To set this filter click the header of the Category Column and click Custom Filter remove all Categories except Library from the right column, and Click OK. This will filter all categories except LIBRARY out so we can more easily find a specific DLL.

To filter the column to show only API calls that include the string dll in the parameter column you need two lines in the Parameter filter. To open the Parameter Filter window click any parameter header and set these two filters:

The first filter will match and show all log entries that end in **.dll** in the parameter 1 column.

The second filter will match and hide everything else.

Now you can use **Log -> Find** to find the first occurrence of MSRATING.dll as well as looking at the other dlls IE loads. Click in the header of any column to sort the column ascending, or descending, or to filter that column. Filtering the column here will only change the log entries you are currently viewing, Holodeck will continue to intercept and log all API calls. To change which API calls Holodeck will intercept and log click **Log -> Filter**. Click the Function header in the log pane, and click sort. This will sort this column by API name so you can more quickly find the LoadLibrary API calls.

To add or remove a column click **View -> Field Chooser** this will allow you to choose which fields show up in the log pane. If you choose to export the log to a text file this will not change what information is saved; all fields will be exported.

Fail msratings.dll

Create a test to fail lookup on the MSRATING.dll: By creating a test that fails any LoadLibrary call to the MSRATING.dll, Holodeck can simulate a problem with loading MSRATING.dll which will allow us to circumvent all of the IE content ratings.

1) First we want to see if anything interesting happens when we fail this dll. To create a test to fail the lookup on MSRATING.dll simply find an occurrence of the method call (LoadLibraryA), using the **Log -> Find** as described above, in the log window and double click it. This will bring up the Create a Scheduled Test Wizard with the correct API selected automatically.

    a) You can use the default values for the In-Parameters and Out-Parameters, they have been automatically selected by Holodeck when you created the test by double clicking on the log entry.

    b) Change the Return value to 0, the signifies a failed API call

    c) Choose ERROR_FILE_NOT_FOUND as the Error code to return.

2) Make sure you create two separate tests for both the LoadLibraryA and LoadLibraryW API calls by repeating the above steps with LoadLibraryW selected.

3) If we check the Content advisor now, notice the buttons have been disabled. This is odd behavior but if we try to browse anywhere on the web we quickly notice the Content Advisor is still working. Perhaps if we restart IE with the test in place, IE will never get access to MSRATING.dll

Restart Internet Explorer

1) Save your project

    a) File -> Save Project

2) Reload your project with the tests already in place.

    a) File -> Open Project

    b) Holodeck will automatically start IE with all tests, limits, corruption, and faults that were previously set.

Verify Failure

As IE starts up it will try to Load the MSRATING.dll; Holodeck will catch the API call and fail it for IE. When IE can not find the MSRATING.dll it defaults to not allowing the user to browse to any site without a content advisor username and password. This is the desired effect; there was no way to tell which sites were safe and which weren't so IE failed to the safest possible configuration. IE will also disable the Content Advisor Buttons in the Internet Options.

Using the find command in the Holodeck logs we can verify that Holodeck has successfully failed the API calls exactly the way we set in the tests.

Dealing with Multiple Processes

Introduction

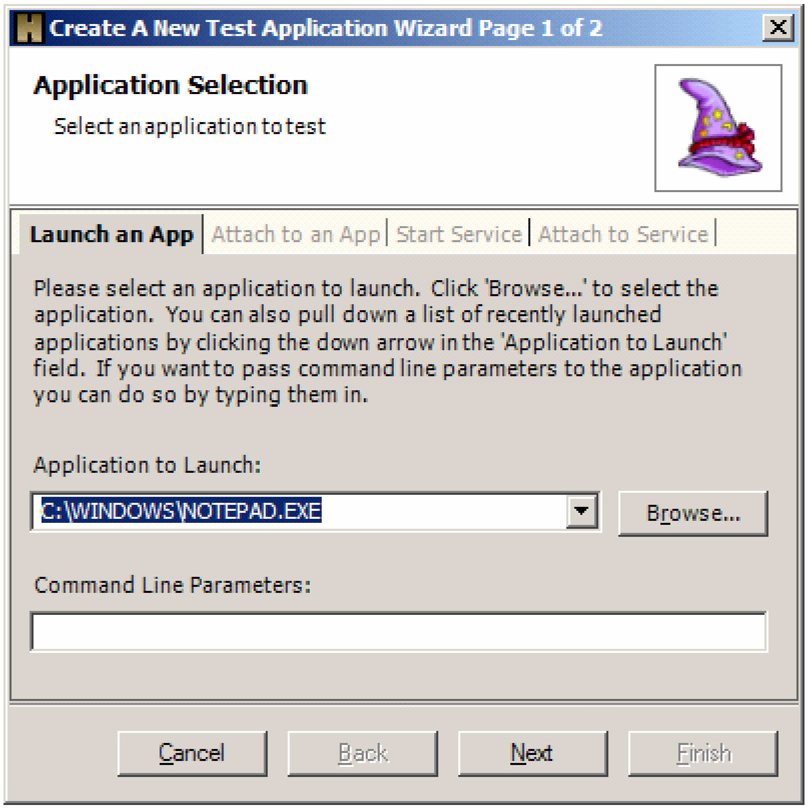
In this tutorial we will explore how to create a Holodeck project that will test multiple applications simultaneously. Doing so will allow you to set faults, tests, and limits on a per application basis. You will also be able to create reports and logs based on the entire project; gathering data from both applications.

To create a project that will eventually be used for multiple test applications simply choose one application first and we will add the second one later, using the New Test Application… functionality. In this example we will use notepad.exe and BrokenApp.exe as the two applications we will test.

Create a new project using BrokenApp.exe with full logging turned on, or load the project you saved using BrokenApp.exe from the first tutorial.

Adding a second process to a project

To add a second application to your project click File > New Test Application…



Please select an application to launch. Click 'Browse...' to select the application. You can also pull down a list of recently launched applications by clicking the down arrow in the 'Application to Launch' field. If you want to pass command line parameters to the application you can do so by typing them in.

Application to Launch: C:\WINDOWS\NOTEPAD.EXE

Command Line Parameters:

This will open a new window that resembles the second and third pages of the new project wizard. In this tutorial we will be adding notepad.exe, which is supplied with Microsoft Windows.

1) Add an application to your project.
   a) Select File > New Test Application…
2) Browse to the BrokenApp.exe in the New Test Application Wizard
   a) Click Browse…
   b) Browse to the location of the notepad.exe, in this example it is located at "C:\WINDOWS"
   c) Select Notepad.exe
   d) Click Open
3) Leave logging settings at their defaults

This will create a new application parent node titled "Notepad.exe" in the Project pane. From here you can create Faults, Limits Corruption, and tests just for that application. In the next topic we will cover how to create these items at a per process level.

Setting Per Process Items

Setting per process items

In this topic we will create a Fault, Limit, Network corruption, and a test at a per process level.

Create a File in Use fault for Notepad.exe

Create a new Memory Fault for BrokenApp.exe

Create a memory limit for Notepad.exe

Create a Resource Fault for BrokenApp.exe

Create an API function test for notepad.exe

Create a File in Use fault for Notepad.exe

1) Select Notepad.exe > Faults > Disk in the project pane
2) Select File in Use in the faults pane
3) Verify failure
    a) Select File > Open…
    b) Notepad will go into a "Not Responding" state because in order to open the Open File Dialog it must load images from the file system, however Holodeck is returning a File in Use fault for every one of those files. This doesn’t allow notepad to open the dialog.
4) Delete the fault
    a) Without closing Notepad return to Holodeck
    b) Delete the fault
    c) Right click the fault and select Delete Fault
5) Notepad will eventually return, but with a few errors. Often the first image on the open file dialog will be missing.
6) Note: cmd.exe will continue to function normally, no fault has been set for this application.

Create a Memory Fault for BrokenApp.exe

1) Right click BrokenApp.exe > Memory Fault and select Create a Fault
2) In the faults pane select Invalid Access.
3) Verify Failure:

    a) Return to Broken.exe
    b) Type a few letters
    c) Attempt to apply bold to the text
    d) The application crashes without throwing an error

Create a memory limit for Notepad.exe

1) Double click Notepad.exe > Limits
2) Slide the memory space slider bar to the left
3) Verify failure
    a) Switch focus to Notepad.exe
    b) Immediately we can see notepad is having problems without memory, the title bar no longer displays the name of the file in stead it is blank.
4) Verify failure further
    a) Begin typing in the main window of notepad
    b) Notice notepad cannot allocate any more memory so after few key presses notepad stops allowing input.
5) Delete the limit
    a) Right click the limit
    b) Select delete
6) Return to notepad, notice the title bar has returned, and you can continue to type in the main window.

Create a Resource Fault for BrokenApp.exe

This doesn’t seem to be working yet, Once I get a fault that shows an error this will be filled in.

TODO

Create an API function test for notepad.exe

1) Select the notepad.exe log by clicking the notepad.exe tab at the top of the logs pane

2) Notepad calls the function "GetVersionExW" every time there is a key pressed so we will set a test on that function.

3) Find an entry in the notepad log that calls the "GetVersionExW" function

   a) Select Log > Find…

   b) Type **GetVersionExW** into the find text box

   c) Click Find

4) Double click the entry in the notepad log that calls the "getVersionExW" function

5) Create a test

   a) Since you opened the Create a Scheduled Test dialog by double clicking a specific log entry the function has already been selected on the first page.

   b) Click Next

   c) We don't want to change any of the in-parameter values so this page stays the same.

   d) Click Next

   e) We don't want to change any of the out-parameter values so this page stays the same.

   f) Click Next

   g) On page 4 of the wizard we want to specify a return value for the function type 1 in the text box

   h) Click Next

   i) Select ERROR_FILE_NOT_FOUND

Working With Global Items

Working with Global items

Some parts of the project are global to the entire project. Reports, and corrupted files are examples of these.

Create a report for this project

Creating Corrupted Files

Create a report for this project

To create a report on all processes and threads in the current project right click the node in the project pane named Reports and select Create a Report. This will create a report under the reports global node named Holodeck Report

Manipulating generated reports

To save a report Right-Click the report and click Save Report, this will allow you to save the report to a remote location to manipulate and compare different reports.

Note: If you create a report and want to share it with someone else you will need to send the html file plus its support files folder "reportname_files"

Renaming Reports do either:

1) To rename a report Right-Click the report and click Rename Report

2) Single click the name of the report you would like to rename.

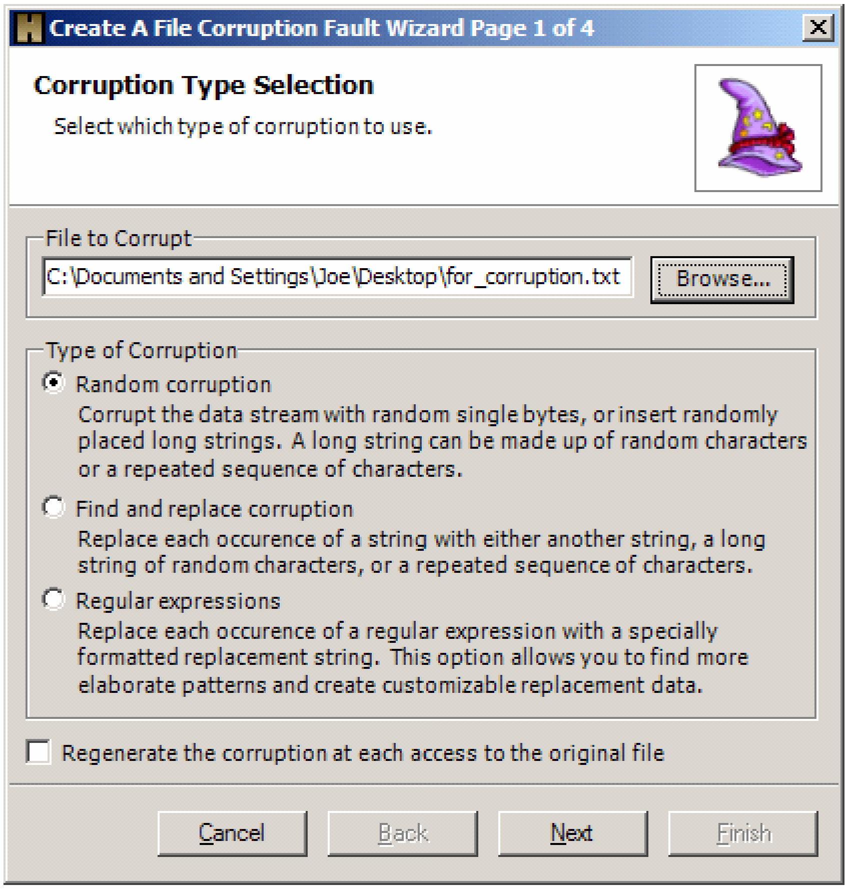
Note: Rename a report before generating a new one to avoid overwriting the old report.

Creating Corrupted Files

The BrokenApp has been created to not do any error checking, so whatever corruption is in the file BrokenApp will display without and change.

To create a corrupted file using Holodeck's built in file corruption click Application > Create a File Corruption Fault

Holodeck automatically creates separate corrupted files so you don't run the risk of corrupting the original source file. In this example I have created a file which is exactly 73 characters by 13 lines long.



Create A File Corruption Fault Wizard Page 1 of 4

Corruption Type Selection

Select which type of corruption to use.

File to Corrupt

C:\Documents and Settings\Joe\Desktop\for_corruption.txt

Type of Corruption

● Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

○ Find and replace corruption

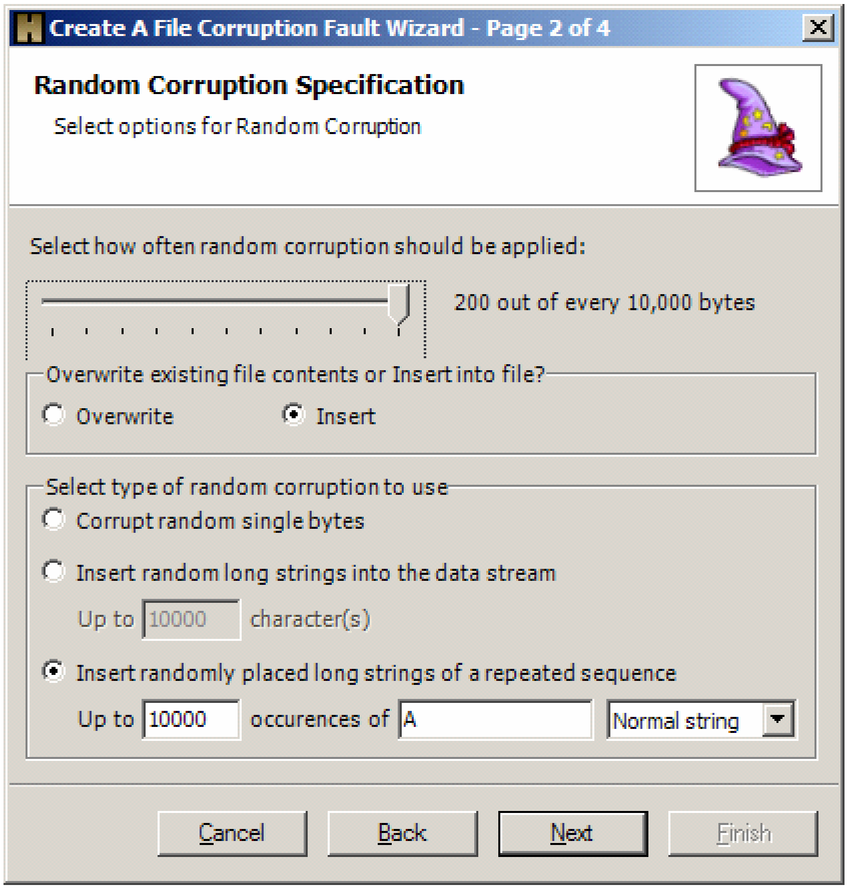
Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

○ Regular expressions

Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

□ Regenerate the corruption at each access to the original file

In this example a randomly placed long string of ‘A’s’ will be inserted into the file, which is easily discoverable.



Create A File Corruption Fault Wizard - Page 2 of 4

Random Corruption Specification

Select options for Random Corruption

Select how often random corruption should be applied:

200 out of every 10,000 bytes

Overwrite existing file contents or Insert into file?

○ Overwrite ● Insert

Select type of random corruption to use

○ Corrupt random single bytes

○ Insert random long strings into the data stream

Up to 10000 character(s)

● Insert randomly placed long strings of a repeated sequence

Up to 10000 occurences of A Normal string

Now whenever the application attempts to access that file Holodeck will use the corrupted file instead.

Load the corrupted file into BrokenApp:

1) Click File > Open… in BrokenApp

2) Select for_corruption.txt

3) Click OK

The corrupted file is now displayed in the main window of BrokenApp.

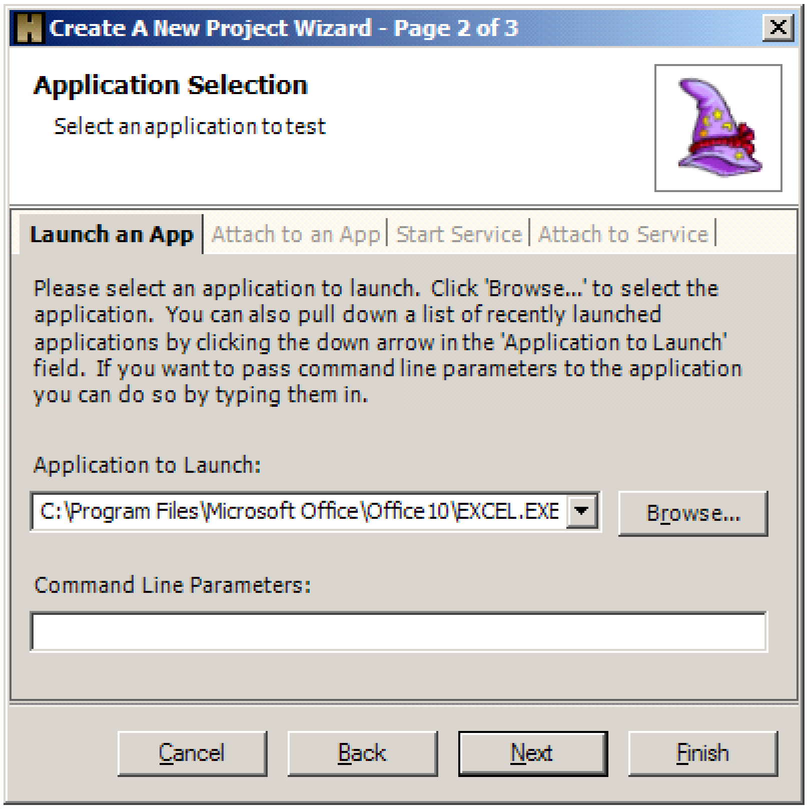
note: a buffer overflow error has been written into the open file function, so BrokenApp may not perform as well as you may expect.

How to use faults to deprive excel of memory

Introduction

This tutorial will cover how to deprive an application of memory by setting the Insufficient Memory fault. The Insufficient Memory fault fails any calls to API functions that try to allocate additional physical memory or virtual memory. Holodeck will not fail functions the de-allocate memory or re-allocate the same amount of memory.

To start this project create a new project using Microsoft Excel and default logging. For more information on how to create a project please see the Setting up your first project tutorial.



Create A New Project Wizard - Page 2 of 3

Application Selection

Select an application to test

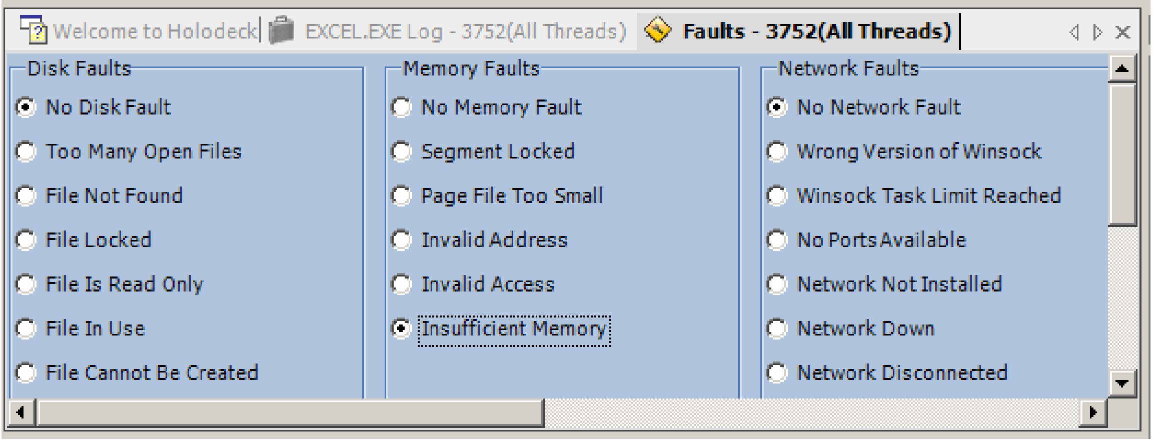
Please select an application to launch. Click 'Browse...' to select the application. You can also pull down a list of recently launched applications by clicking the down arrow in the 'Application to Launch' field. If you want to pass command line parameters to the application you can do so by typing them in.

Application to Launch: C:\Program Files\Microsoft Office\Office10\EXCEL.EXE

Command Line Parameters:

Set Insufficient Memory

Once Excel has finished loading, navigate back to Holodeck. The faults pane should be visible from the default workspace of Holodeck. If the faults pane is not visible double click the faults node in the Project Pane. In the Faults Pane select "Insufficient Memory" under the memory faults heading.



Disk Faults

● No Disk Fault
○ Too Many Open Files
○ File Not Found
○ File Locked
○ File Is Read Only
○ File In Use
○ File Cannot Be Created

Memory Faults

○ No Memory Fault
○ Segment Locked
○ Page File Too Small
○ Invalid Address
○ Invalid Access
● Insufficient Memory

Network Faults

● No Network Fault
○ Wrong Version of Winsock
○ Winsock Task Limit Reached
○ No Ports Available
○ Network Not Installed
○ Network Down
○ Network Disconnected

Verify Insufficient Memory

The Insufficient Memory fault is set as soon as the radio box is checked. To see how Excel does when it runs out of memory, navigate back to Excel and try to complete any task. Excel has completely frozen up, in fact Excel can't even allocate the memory necessary to redraw the window. This is what we expect from an application that runs out of memory space. As soon as the memory fault is lifted, Excel returns to completely normal execution.

Further Exploration:

Try this tutorial using BrokenApp that has shipped with Holodeck. When the Insufficient Memory fault is set BrokenApp quickly fails. You can investigate the failure through the first chance exception it produces. For more information on first chance exceptions and debugging using this information see the Exceptions and Mini-dump section or the resource faults tutorial.

Intermediate

Learning about API failures during startup and comparing logs

Introduction

In this tutorial we will learn how to investigate API failures using Holodeck's logs and reporting tools. Using these features of Holodeck, you can investigate bugs more precisely and in ways never before possible.

The Reports feature allows you to drill down into a compiled version of the data accumulated during a test run. This data includes every log entry, fault, limit, resource dependency, and test that has been created for the current project. Each table in the report can be filtered, modified or manipulated however you see fit, providing a detailed yet precise view of the data.

Comparing logs is a good way to filter out unimportant data on similar runs of an application. Holodeck can export an easy to manipulate, tab delimited, text file containing all of the logs for the current session.

Load project

Load Excel into Holodeck

1) Start Holodeck and create a new project

   a) File > New Project

   b) Walk through the New Project Wizard

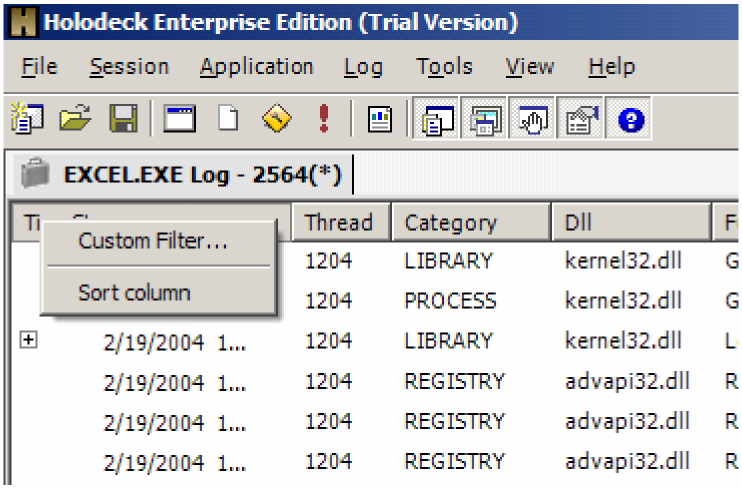
   c) Select Excel to test (usually located at: "C:\Program Files\Microsoft Office\Office10\excel.exe")

   d) Leave all other settings at their default values

2) Excel will automatically be started when you click finish on the New Project Wizard.

Filtering the log result

You can sort, filter, add or remove columns in the log window to make your investigation easier. You can change the order of the columns by clicking and dragging the columns where you want them to go.



Ti	Thread	Category	Dll	F
	1204	LIBRARY	kernel32.dll	G
	1204	PROCESS	kernel32.dll	G
⊞ 2/19/2004 1...	1204	LIBRARY	kernel32.dll	L
2/19/2004 1...	1204	REGISTRY	advapi32.dll	R
2/19/2004 1...	1204	REGISTRY	advapi32.dll	R
2/19/2004 1...	1204	REGISTRY	advapi32.dll	R

Filter the Error Code Column to show only non-success error codes by clicking on the header of the Error Code Column and clicking Custom Filter… In the filter window, add all error codes, then select ERROR_SUCCESS and click the << Remove button. This will show all the failed API calls in the log pane. While this allows you to view all the API failures you'll see that the Reports feature creates a more organized view based on error type, pass/fail, and will allow you to easily drill down on each API Failure.

Click on the header of any column to sort the column or to add a filter. Filtering the column here will only change the log entries you are currently viewing, Holodeck will continue to intercept and log all API calls. To change which API calls Holodeck will intercept and log click Log > Filter on the menu bar.

To add or remove a column click View > Field Chooser this will allow you to choose which fields show up in the log pane. This will not change what information is exported to the log. All fields will be exported.

Creating a Report for easy viewing

We can investigate any failures by wading through some 4000 log entries, but Holodeck includes reporting functionality that can make the process of investigating a run of any application under test very easy.

To create a report right click the Reports node in the Project Pane, and click Create a Report**.** Holodeck will now begin to compile the logs, resources, faults, limits and tests for this project into one easy to read report. Once the report has been created Holodeck will automatically display it in the main window. There is a plethora of information available here, but what we are interested in is the Error Codes Table.

From the Error Codes Table we can drill down to investigate each of the failures Excel encountered while running. Many of these errors are .dll failures which are the standard way of looking for DLLs within a search path, but others can be more serious functionality failures.

By clicking on the plus symbol to the left of Fail you can see a detailed version of the Error Code, and Error Code Type. This will also expand the Count of Occurrence columns to reflect the count of the failures of each Error Code.

By clicking on the plus symbol to the right of Fail you can see detailed information about each API call, this can be filtered by the different error codes. Any column can be sorted ascending or descending by right clicking the column and clicking Sort. Columns can be reordered by dragging them to a different location, or to easily remove a column simply drag it off the table. To add a column you have removed, right click the table and click Field List, this will bring up another window, where you can drag columns around to make data viewing easier. It is interested to note here that during a regular startup, Excel encounters nearly 600 errors, which we can see by repeating the test. This would be a good place to look for exploitable bugs; if Excel failed to load a certain library, or failed a function call it might put the application in a useable but unstable state, which could be a spring board for finding more bugs.

Exporting logs

Holodeck also gives you the ability to export the logs generated when running the Application Under Test in Holodeck. This is useful if you would like to compare the logs in an external editor, such as Excel or Windiff.

Exporting log files

At any time during the execution of the Application Under Test you can export the current log to a text file. Export a log by click File > Export Log to File…

You may want to export the log files of two similar runs of an application to investigate differences between API calls, or the function calls leading up to a crash or bug.

For more information on exporting logs see the Exporting Logs page in the Holodeck in Depth section.

Comparing logs

You can quickly and easily compare the differences between two log files using Windiff, a utility for comparing two similar files which is bundled with Visual Studio.

Example Comparison

Let’s compare the differences in API calls when Excel opens a document by double clicking on it, versus using the quick launch pane. We can do this with one instance of Holodeck by using the multiple test application feature.

To do this first create a new project, and set Excel to be the application under test. Once Excel has started, browse to a simple Excel document and open it by double clicking it. Once the document has finished loading, export the log file to a text document and save for later use.

Once the log has been exported you can close Excel, and open a new instance by clicking File > New Test Application, this will open the New Test Application Wizard which will allow you to select Excel to start again, and create a new API log.

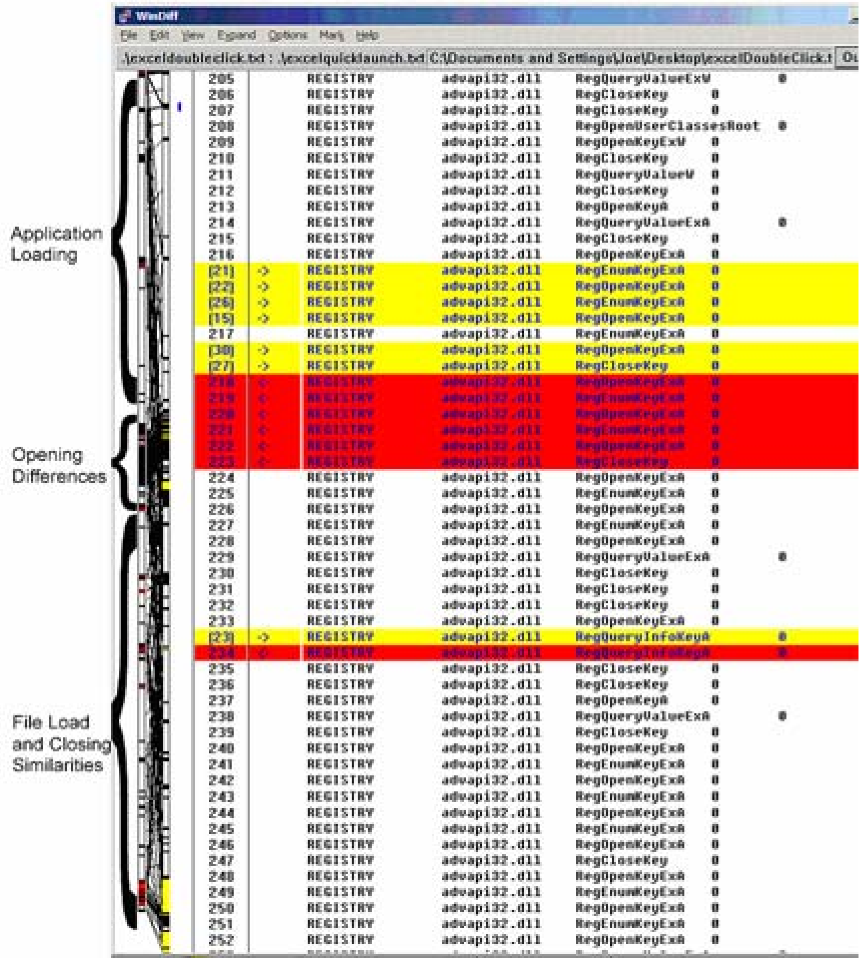
Since you closed the first instance of Excel, the same document should show up in the quick launch bar on the right side of the window. This time, click the link on the sidebar to open the Excel document. Once the document has finished loading, export the log to a file under a different name.

These two logs were created at different times; therefore we have to remove the first two columns, TimeStamp and Thread. API calls often use memory addresses as parameter and return values, each time the application is run the OS may allocate a different memory location we have to remove the Return Value and the Parameter columns as well to ensure we are only comparing the order of API calls.

To open the log files in Excel right click the log file Open With… > Microsoft Excel. Excel will automatically put the data into each column. Click the column header of the TimeStamp column, right click the selected row, and click Delete. This will remove the column, and shift the rest of the data over. Repeat this for the Thread, Return Value and each of the Parameter Columns. Once these columns have been removed you can resave the log as a tab delimited text file. File > Save As…

Making sense of the difference

Now we can load the two files into Windiff, and see the difference in the way Excel loads a file by double clicking on it, or by loading it from the QuickLaunch Bar. We notice that the first 2000 lines of the logs are very similar; this is the startup of the application. The next 1000 lines are where we loaded the files. you may notice that, with the exception of a few operating system dependant calls, the two load methods take a very similar API path.


WinDiff
File Edit View Expand Options Mark Help
Application Loading
Opening Differences
File Load and Closing Similarities

```
.\exceldoubleclick.txt : .\excelquicklaunch.txt C:\Documents and Settings\Joel\Desktop\excelDoubleClick.t
205         REGISTRY     advapi32.dll    RegQueryValueExW         0
206         REGISTRY     advapi32.dll    RegCloseKey      0
207         REGISTRY     advapi32.dll    RegCloseKey      0
208         REGISTRY     advapi32.dll    RegOpenUserClassesRoot   0
209         REGISTRY     advapi32.dll    RegOpenKeyExW    0
210         REGISTRY     advapi32.dll    RegCloseKey      0
211         REGISTRY     advapi32.dll    RegQueryValueW   0
212         REGISTRY     advapi32.dll    RegCloseKey      0
213         REGISTRY     advapi32.dll    RegOpenKeyA      0
214         REGISTRY     advapi32.dll    RegQueryValueExA         0
215         REGISTRY     advapi32.dll    RegCloseKey      0
216         REGISTRY     advapi32.dll    RegOpenKeyExA    0
[21]  ->    REGISTRY     advapi32.dll    RegEnumKeyExA    0
[22]  ->    REGISTRY     advapi32.dll    RegOpenKeyExA    0
[26]  ->    REGISTRY     advapi32.dll    RegEnumKeyExA    0
[15]  ->    REGISTRY     advapi32.dll    RegOpenKeyExA    0
217         REGISTRY     advapi32.dll    RegEnumKeyExA    0
[30]  ->    REGISTRY     advapi32.dll    RegOpenKeyExA    0
[27]  ->    REGISTRY     advapi32.dll    RegCloseKey      0
218   <-    REGISTRY     advapi32.dll    RegOpenKeyExA    0
219   <-    REGISTRY     advapi32.dll    RegEnumKeyExA    0
220   <-    REGISTRY     advapi32.dll    RegOpenKeyExA    0
221   <-    REGISTRY     advapi32.dll    RegEnumKeyExA    0
222   <-    REGISTRY     advapi32.dll    RegOpenKeyExA    0
223   <-    REGISTRY     advapi32.dll    RegCloseKey      0
224         REGISTRY     advapi32.dll    RegOpenKeyExA    0
225         REGISTRY     advapi32.dll    RegEnumKeyExA    0
226         REGISTRY     advapi32.dll    RegOpenKeyExA    0
227         REGISTRY     advapi32.dll    RegEnumKeyExA    0
228         REGISTRY     advapi32.dll    RegOpenKeyExA    0
229         REGISTRY     advapi32.dll    RegQueryValueExA         0
230         REGISTRY     advapi32.dll    RegCloseKey      0
231         REGISTRY     advapi32.dll    RegCloseKey      0
232         REGISTRY     advapi32.dll    RegCloseKey      0
233         REGISTRY     advapi32.dll    RegOpenKeyExA    0
[23]  ->    REGISTRY     advapi32.dll    RegQueryInfoKeyA         0
234   <-    REGISTRY     advapi32.dll    RegQueryInfoKeyA         0
235         REGISTRY     advapi32.dll    RegCloseKey      0
236         REGISTRY     advapi32.dll    RegCloseKey      0
237         REGISTRY     advapi32.dll    RegOpenKeyA      0
238         REGISTRY     advapi32.dll    RegQueryValueExA         0
239         REGISTRY     advapi32.dll    RegCloseKey      0
240         REGISTRY     advapi32.dll    RegOpenKeyExA    0
241         REGISTRY     advapi32.dll    RegEnumKeyExA    0
242         REGISTRY     advapi32.dll    RegOpenKeyExA    0
243         REGISTRY     advapi32.dll    RegEnumKeyExA    0
244         REGISTRY     advapi32.dll    RegOpenKeyExA    0
245         REGISTRY     advapi32.dll    RegEnumKeyExA    0
246         REGISTRY     advapi32.dll    RegOpenKeyExA    0
247         REGISTRY     advapi32.dll    RegCloseKey      0
248         REGISTRY     advapi32.dll    RegOpenKeyExA    0
249         REGISTRY     advapi32.dll    RegEnumKeyExA    0
250         REGISTRY     advapi32.dll    RegOpenKeyExA    0
251         REGISTRY     advapi32.dll    RegEnumKeyExA    0
252         REGISTRY     advapi32.dll    RegOpenKeyExA    0
```

Using Windiff we can see the differences in each file, the first column shows which line corresponds to each file. Red lines come from the first file, Yellow lines from the second file. On the far left a graphical representation of each file is shown where Windiff tries to match each line to the other file, if it can. Here we can see similarities to the way Excel starts up, and the similarities in the way Excel shuts itself down. The middle of the log file we see the drastic difference of how Excel loads by double clicking or by loading from Quick Launch pane.

Creating Network Corruption Using Regular Expressions

Introduction

In this Tutorial we will discover how to find and replace network data using Regular Expressions and Replacement strings. This can be very useful when trying to match a certain string and test client or server parsing. In this tutorial we will search for any base URL and replace it with a long string of the letter ‘A’

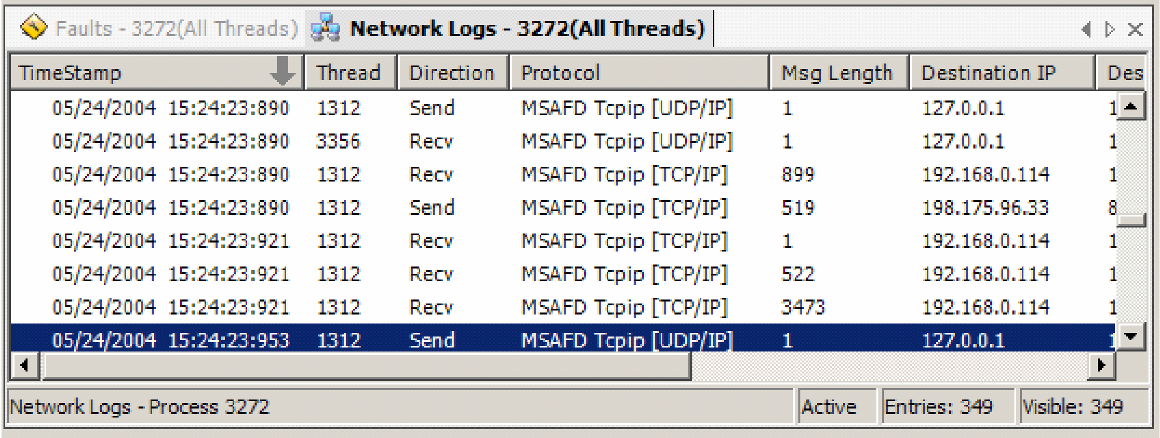
Setup a new project using Internet Explorer as the application under test, with default logging turned on. For more information on how to setup a project see the Setting up your first project Tutorial in the Beginning Tutorials section.

Note: Regular expressions only work with uncompressed data, some web pages may be compressed for better data transfer; Regular Expressions will not match on these pages.

Investigate Network Packets

Once Internet Explorer has loaded, navigate back to Holodeck. From the Project Pane you can investigate network logs, API logs, and exceptions the application has generated.

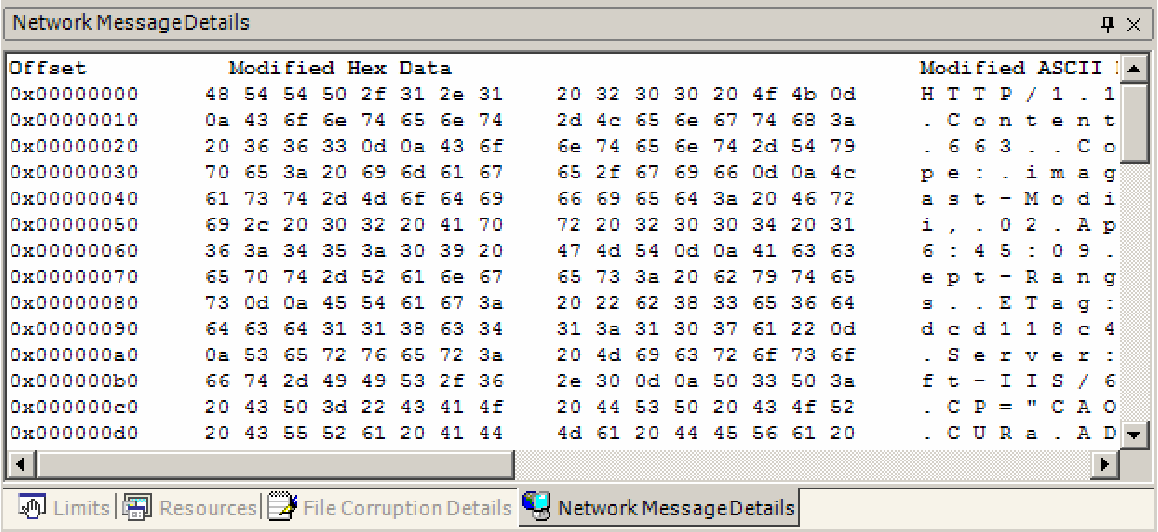
Navigate to the Intel website (www.intel.com); this website is large, unencrypted, and uncompressed which makes investigating network packets easy. Once the Intel page has loaded return to Holodeck and open the Network logs pane by double clicking on the Network Logs node in the Project pane.



TimeStamp	Thread	Direction	Protocol	Msg Length	Destination IP	Des
05/24/2004 15:24:23:890	1312	Send	MSAFD Tcpip [UDP/IP]	1	127.0.0.1	1
05/24/2004 15:24:23:890	3356	Recv	MSAFD Tcpip [UDP/IP]	1	127.0.0.1	1
05/24/2004 15:24:23:890	1312	Recv	MSAFD Tcpip [TCP/IP]	899	192.168.0.114	1
05/24/2004 15:24:23:890	1312	Send	MSAFD Tcpip [TCP/IP]	519	198.175.96.33	8
05/24/2004 15:24:23:921	1312	Recv	MSAFD Tcpip [TCP/IP]	1	192.168.0.114	1
05/24/2004 15:24:23:921	1312	Recv	MSAFD Tcpip [TCP/IP]	522	192.168.0.114	1
05/24/2004 15:24:23:921	1312	Recv	MSAFD Tcpip [TCP/IP]	3473	192.168.0.114	1
05/24/2004 15:24:23:953	1312	Send	MSAFD Tcpip [UDP/IP]	1	127.0.0.1	1

Network Logs - Process 3272 | Active | Entries: 349 | Visible: 349

See the rest of the packet message by selecting the Network Message Details Pane which should be located at the bottom of the window. The Network Message Details Pane shows the entire Network Packet in its Hex and ASCII representation. Any Network corruption will also show up here.



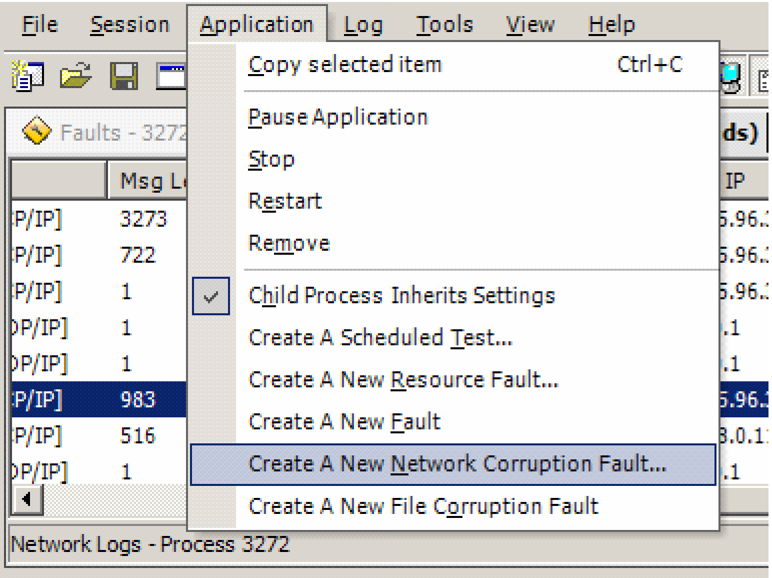
```
Offset             Modified Hex Data                                          Modified ASCII
0x00000000       48 54 54 50 2f 31 2e 31    20 32 30 30 20 4f 4b 0d    H T T P / 1 . 1
0x00000010       0a 43 6f 6e 74 65 6e 74    2d 4c 65 6e 67 74 68 3a    . C o n t e n t
0x00000020       20 36 36 33 0d 0a 43 6f    6e 74 65 6e 74 2d 54 79    . 6 6 3 . . C o
0x00000030       70 65 3a 20 69 6d 61 67    65 2f 67 69 66 0d 0a 4c    p e : . i m a g
0x00000040       61 73 74 2d 4d 6f 64 69    66 69 65 64 3a 20 46 72    a s t - M o d i
0x00000050       69 2c 20 30 32 20 41 70    72 20 32 30 30 34 20 31    i , . 0 2 . A p
0x00000060       36 3a 34 35 3a 30 39 20    47 4d 54 0d 0a 41 63 63    6 : 4 5 : 0 9 .
0x00000070       65 70 74 2d 52 61 6e 67    65 73 3a 20 62 79 74 65    e p t - R a n g
0x00000080       73 0d 0a 45 54 61 67 3a    20 22 62 38 33 65 36 64    s . . E T a g :
0x00000090       64 63 64 31 31 38 63 34    31 3a 31 30 37 61 22 0d    d c d 1 1 8 c 4
0x000000a0       0a 53 65 72 76 65 72 3a    20 4d 69 63 72 6f 73 6f    . S e r v e r :
0x000000b0       66 74 2d 49 49 53 2f 36    2e 30 0d 0a 50 33 50 3a    f t - I I S / 6
0x000000c0       20 43 50 3d 22 43 41 4f    20 44 53 50 20 43 4f 52    . C P = " C A O
0x000000d0       20 43 55 52 61 20 41 44    4d 61 20 44 45 56 61 20    . C U R a . A D
```

You can use these logs to investigate exactly how to corrupt the message for maximum application penetration, which will help find bugs deeper within your codebase.

Open Network Corruption Wizard

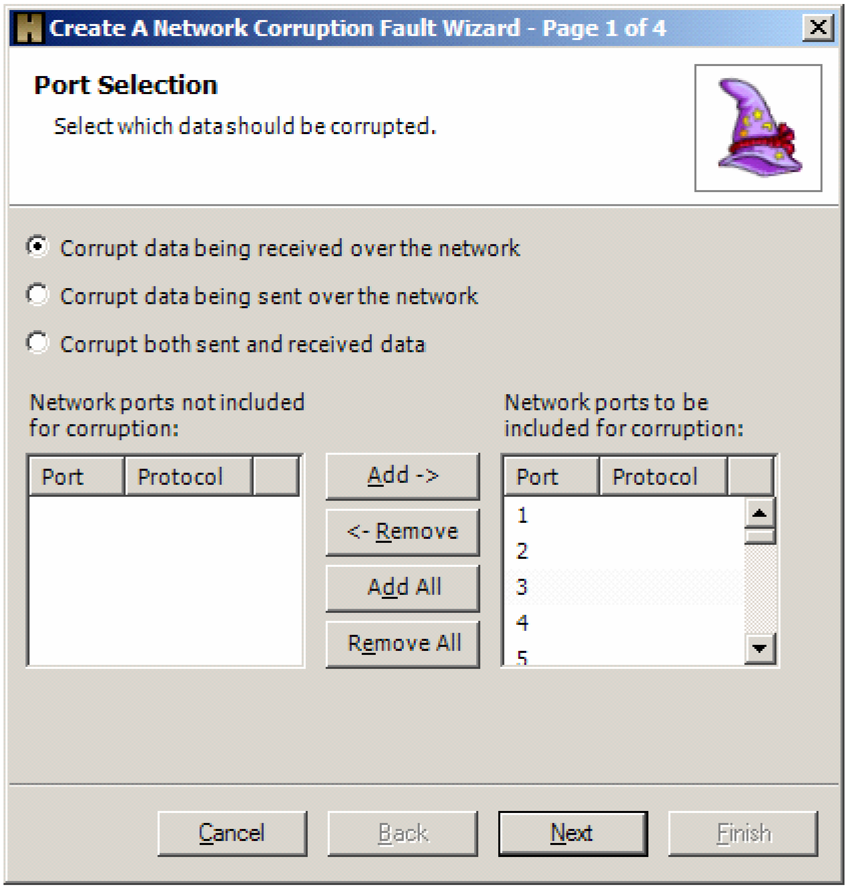
We want to corrupt any occurrence of a base URL, and replace it with a long string of the letter ‘A’. This will help test packet parsing, and will make any errors we find very easy to discover in the web browser or the Network Message Details Pane.

Open the Network Corruption Wizard by selecting Application > "Create A New Network Corruption Fault…"


File
Session
Application
Log
Tools
View
Help
Copy selected item Ctrl+C
Pause Application
Stop
Restart
Remove
✓ Child Process Inherits Settings
Create A Scheduled Test...
Create A New Resource Fault...
Create A New Fault
Create A New Network Corruption Fault...
Create A New File Corruption Fault
Faults - 3272
Msg L
IP
Network Logs - Process 3272

Select Which Data Should be Corrupted

Select all ports and protocols and only data being received over the network since we only want to test the client.



Create A Network Corruption Fault Wizard - Page 1 of 4

Port Selection

Select which data should be corrupted.

● Corrupt data being received over the network

○ Corrupt data being sent over the network

○ Corrupt both sent and received data

Network ports not included for corruption:

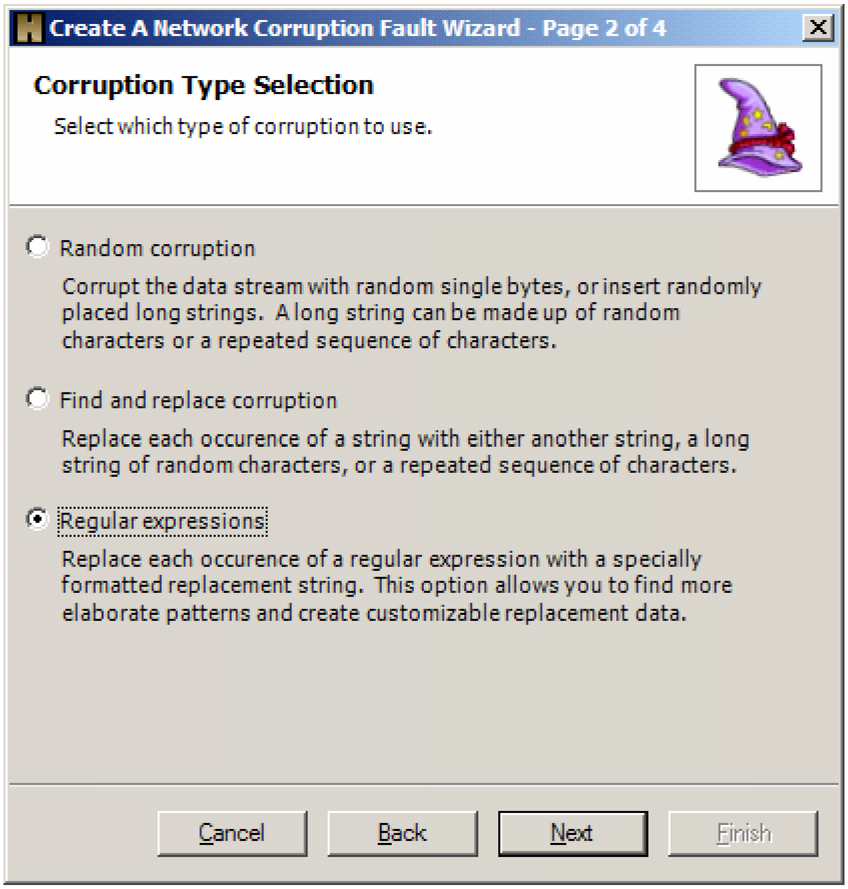
Port	Protocol

Network ports to be included for corruption:

Port	Protocol
1	
2	
3	
4	
5	

Select Regular Expressions as the Method of Corruption

This will open the regular expression page of the network corruption wizard.



Create A Network Corruption Fault Wizard - Page 2 of 4

Corruption Type Selection

Select which type of corruption to use.

○ Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

○ Find and replace corruption

Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

● Regular expressions

Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

Create a Regular Expression and Expansion String

Create a regular expression to match on the domain of any URL (iegwww.google.com, or slashdot.org) and replace it with 1000 to 5000 of the letter ‘A’.

The regular expression to match any domain is as follows:

`([wW]{3,}\.)?([abcefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]+)\.(com|net|org)`

`([wW]{3,}\.)?` - this part matches an optional capital or lowercase "www."

`([abcefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]+)` – this part matches any length string consisting of upper or lowercase alphabet letters, greater than 1 (eg. "abc", "aRdfpQ", etc.)

`\.(com|net|org)` – this part matches a period followed by any one of the following, "com", "net", or "org"

The expansion string to expand between 1000 and 5000 'A's is as follows:

`$S1000,5000,A$`

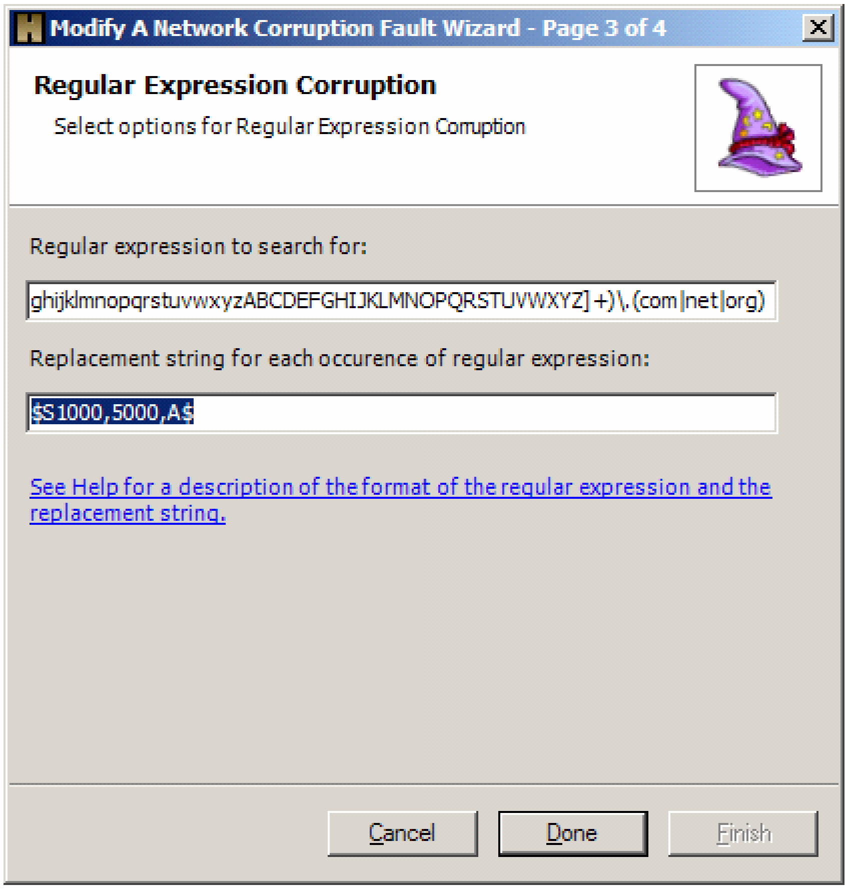
`S` – shows this will expand to a string

`1000` – the minimum number of repetitions

`5000` – the maximum number of repetitions

`A` – the string to expand

By enclosing this string in '`$`' Holodeck knows this is a string to expand.



Modify A Network Corruption Fault Wizard - Page 3 of 4

Regular Expression Corruption

Select options for Regular Expression Corruption

Regular expression to search for:

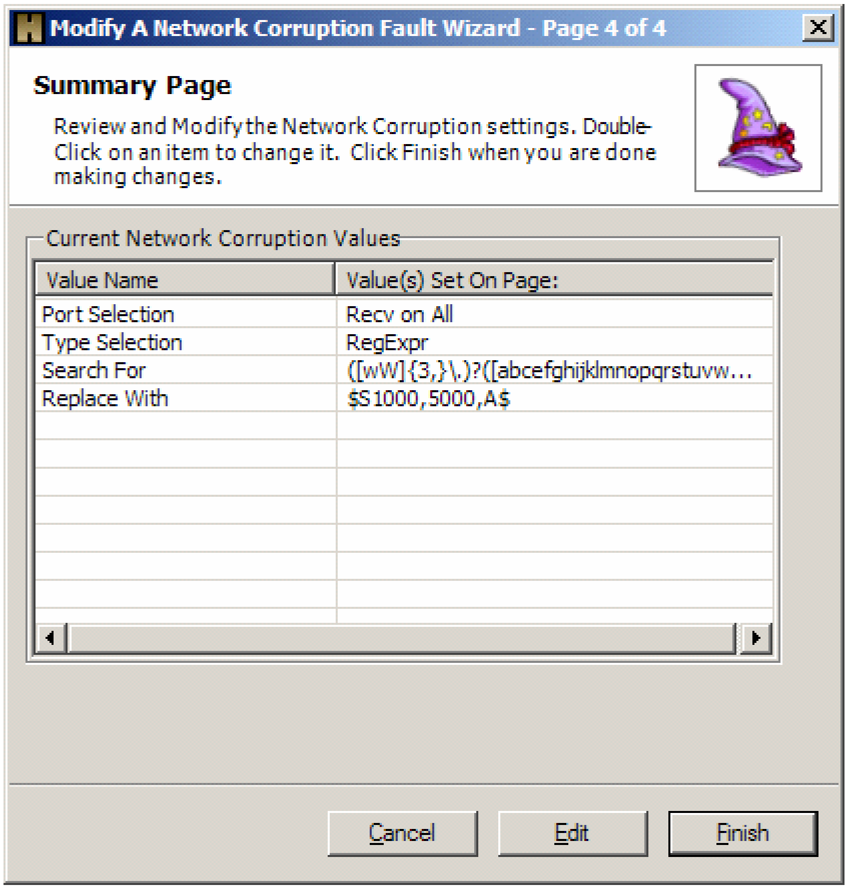
`ghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]+)\.(com|net|org)`

Replacement string for each occurence of regular expression:

`$S1000,5000,A$`

See Help for a description of the format of the regular expression and the replacement string.

The final page of the wizard shows a summary of the corruption fault you have just created. You can go back and change any one of the settings for the fault from this page, simply select the value name you wish to change and click Edit.



Modify A Network Corruption Fault Wizard - Page 4 of 4

Summary Page

Review and Modify the Network Corruption settings. Double-Click on an item to change it. Click Finish when you are done making changes.

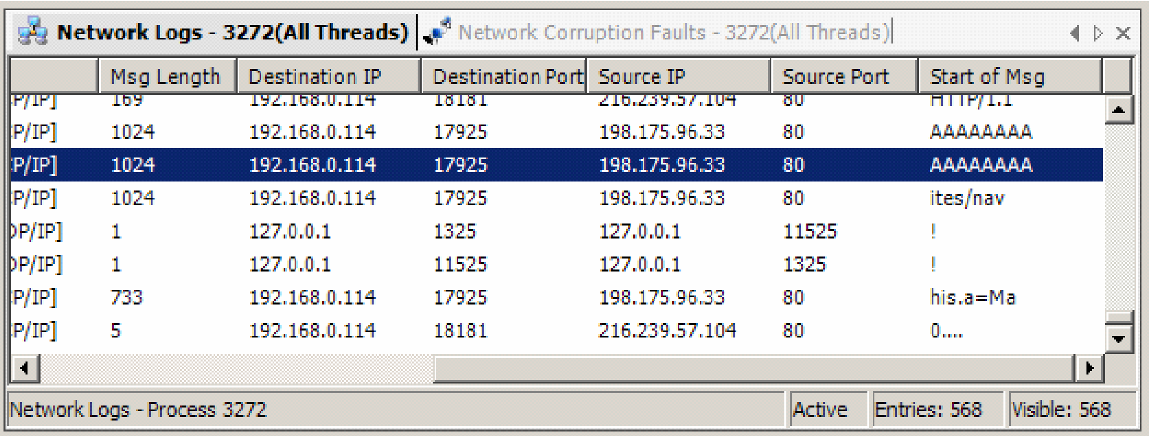
Current Network Corruption Values

Value Name	Value(s) Set On Page:
Port Selection	Recv on All
Type Selection	RegExpr
Search For	([wW]{3,}\.)?([abcefghijklmnopqrstuvw...
Replace With	$S1000,5000,A$

Verify the Fault is set

When we click on any link on the Intel web page Holodeck immediately starts replacing all base URLs with long strings of the letter 'A'. On this machine it makes Internet Explorer unusable, but you can make sure the fault has set by checking the Network Logs in the Network Logs Pane, and the Network Message Details Pane.

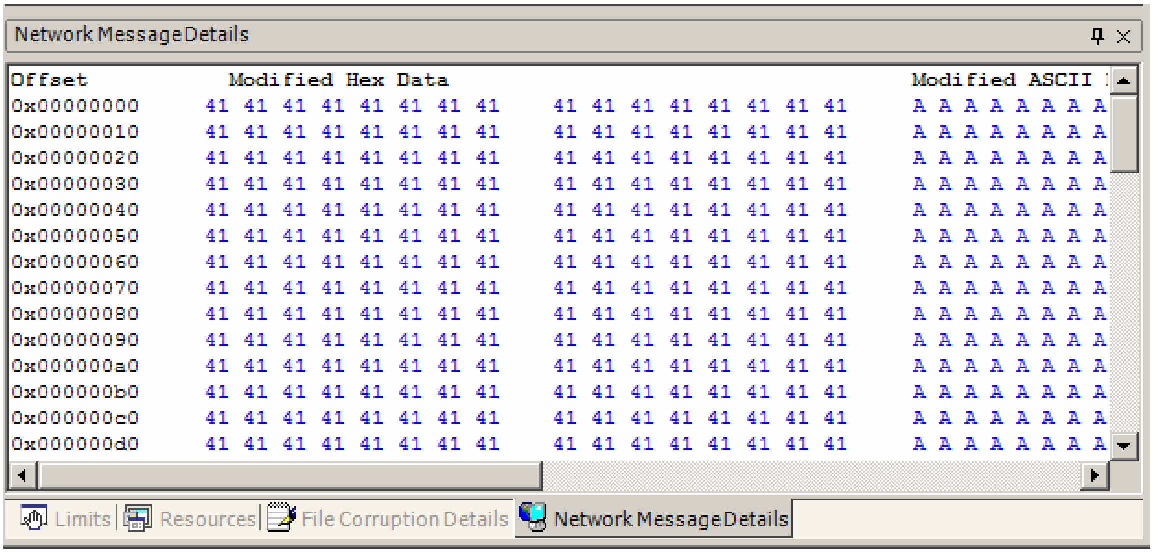
To check the Network Logs navigate back to the Network Logs Pane by double-clicking on the Network Logs node in the Project Pane. In the screenshot below you can see two network messages that have been corrupted.


Network Logs - 3272(All Threads)
Network Corruption Faults - 3272(All Threads)

	Msg Length	Destination IP	Destination Port	Source IP	Source Port	Start of Msg
P/IP]	169	192.168.0.114	18181	216.239.57.104	80	HTTP/1.1
P/IP]	1024	192.168.0.114	17925	198.175.96.33	80	AAAAAAAA
P/IP]	1024	192.168.0.114	17925	198.175.96.33	80	AAAAAAAA
P/IP]	1024	192.168.0.114	17925	198.175.96.33	80	ites/nav
P/IP]	1	127.0.0.1	1325	127.0.0.1	11525	!
P/IP]	1	127.0.0.1	11525	127.0.0.1	1325	!
P/IP]	733	192.168.0.114	17925	198.175.96.33	80	his.a=Ma
P/IP]	5	192.168.0.114	18181	216.239.57.104	80	0....

Network Logs - Process 3272 | Active | Entries: 568 | Visible: 568

The following is the Network Message Details for this Network Packet, all changes Holodeck makes show up in blue in the Modified columns, to the right of the Modified Columns are the Original Data columns, overwritten or changed data will show up in red here.



```
Offset          Modified Hex Data                                                   Modified ASCII
0x00000000     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000010     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000020     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000030     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000040     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000050     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000060     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000070     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000080     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x00000090     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x000000a0     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x000000b0     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x000000c0     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
0x000000d0     41 41 41 41 41 41 41 41    41 41 41 41 41 41 41 41    A A A A A A A A
```

Using Holodeck to corrupt files and test file processing

Introduction

This tutorial will cover how to corrupt a text file and test file processing using BrokenApp that was supplied with your Holodeck package. Holodeck’s file corruption faults can be a very powerful tool to test file processing because it corrupts the file on a bitwise level. This simulates actual corruption that may occur because of corrupted RAM, Hard Drive sectors, or a bad network transfer.

The sections of this tutorial include:

Corrupting Files

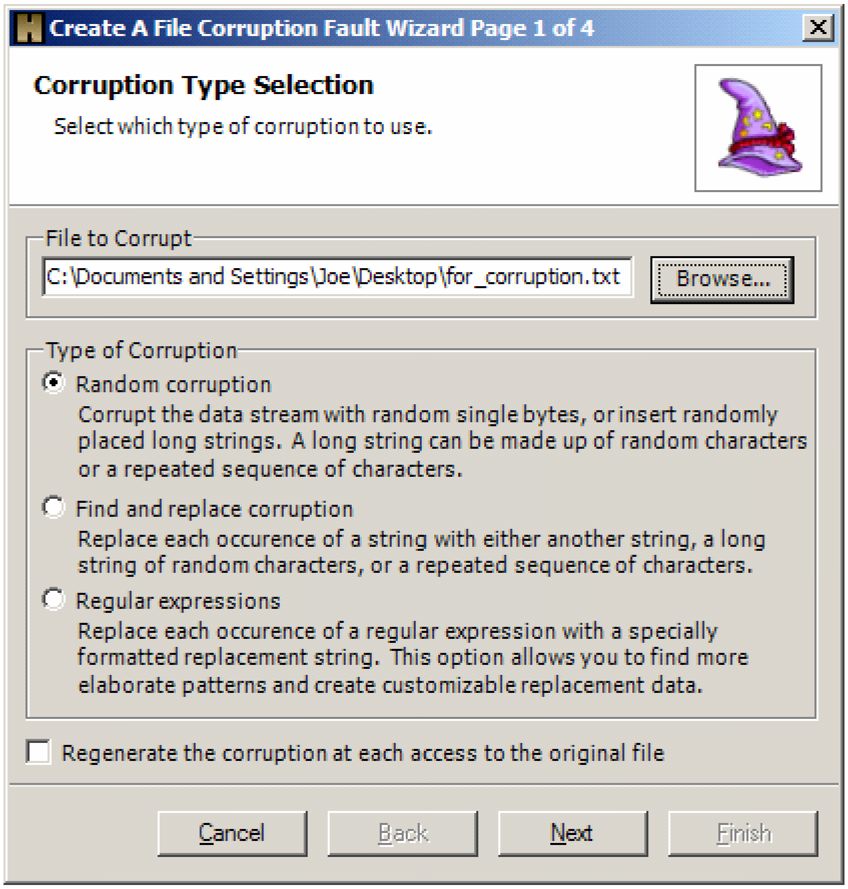
When you create a File corruption fault Holodeck does not corrupt the original file, but rather when the Application Under Test attempts to access that file it redirects the Application Under Test to a corrupted version of the file. This is useful because it allows you to corrupt a single file many different ways to test all aspects of file processing.

To create a file corruption fault click Application -> Create a New File Corruption Fault… This will bring up the file corruption wizard.

The first page asks for which file to corrupt, and how you would like to corrupt it. Create a text file with the following text, save it as for_corruption.txt to your desktop.

```
This file has been created to show off the file corruption of
Holodeck.
It should be exactly 73 characters long and 13 lines
down.xxxxxxxxxxxxx
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
This file has been created to show off the file corruption of
Holodeck.
```

In this tutorial we want to create random corruption throughout this file. Holodeck's File corruption will select random bits to corrupt in random lengths throughout the file. This can generate anywhere from only slightly corrupted data, to extremely corrupted data.



Create A File Corruption Fault Wizard Page 1 of 4

Corruption Type Selection

Select which type of corruption to use.

File to Corrupt

C:\Documents and Settings\Joe\Desktop\for_corruption.txt

Type of Corruption

● Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

○ Find and replace corruption

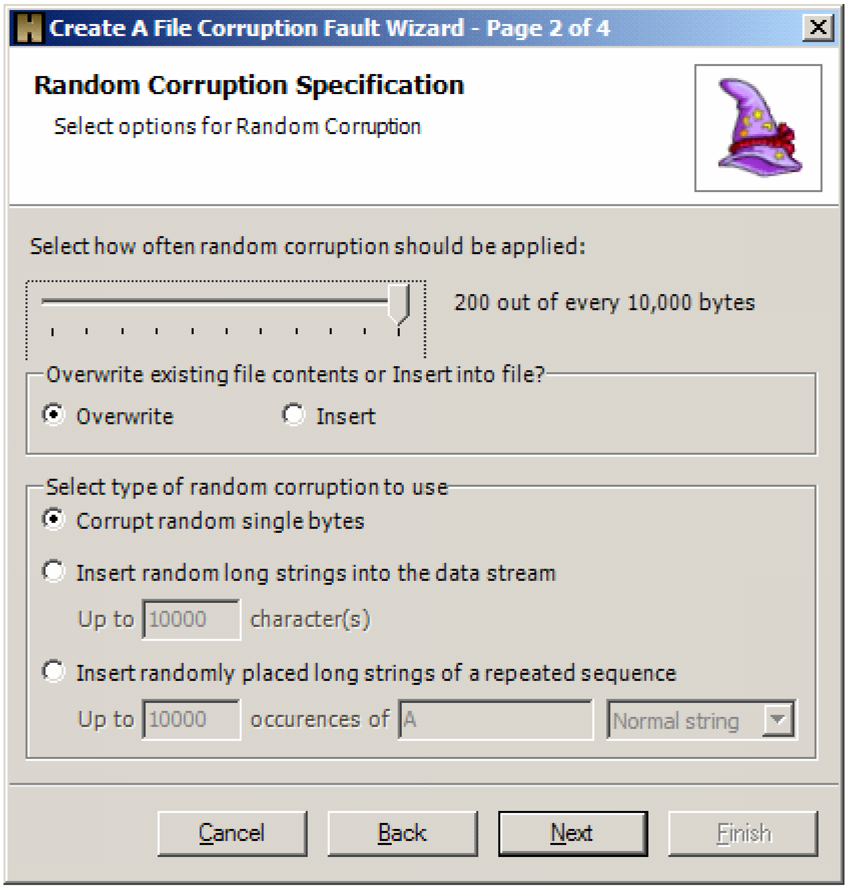
Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

○ Regular expressions

Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

□ Regenerate the corruption at each access to the original file

For our purposes we want the file to be as corrupted as possible so the corruption will find any easy to find file reading bugs. Slide the corruption amount slider all the way to the right until it displays 200 out of every 10,000 bytes to be corrupted. Leave Overwrite and Corrupt random single bytes at their default values.



Create A File Corruption Fault Wizard - Page 2 of 4

Random Corruption Specification

Select options for Random Corruption

Select how often random corruption should be applied:

200 out of every 10,000 bytes

Overwrite existing file contents or Insert into file?

● Overwrite ○ Insert

Select type of random corruption to use

● Corrupt random single bytes

○ Insert random long strings into the data stream

Up to 10000 character(s)

○ Insert randomly placed long strings of a repeated sequence

Up to 10000 occurences of A Normal string

The final page shows a summary of the file corruption that you have selected. To return to any page, simply highlight the information you would like to change, and click edit; doing this will return you to the page of the wizard which contains that information.

Using Corrupted Files to test file processing

BrokenApp has been written to display any file corruption exactly as it exists in the file. This allows us to see exactly how Holodeck corrupted the file, however the application you are testing may try to do some amount of file recovery, if this is the case we can use the File Corruption Details pane to see exactly what the

Viewing the details of the corrupted file

To view the details of a corrupted file, see the File Corruption details pane. This pane shows a hexadecimal view as well as the standard ASCII view of the data. The hexadecimal view can be very useful for finding out exactly how the Holodeck file corruptor has changed your file.

All changes made to the file are highlighted in red.

Advanced

Test Harness and Code Coverage

Introduction

This tutorial will demonstrate how to use an external test harness and Holodeck's Code Coverage feature to find bugs quickly, easily and efficiently. The Code Coverage feature runs tests based on the resources and API calls used by the program. For example: if the Application Under Test uses LoadLibraryA, an API used to load DLLs, the Code Coverage feature will fail that call on one of its runs. More information about the Code Coverage feature can be found in the Holodeck help documents.

By using an external test harness we can automate the use of Code Coverage test generation. The test harness will launch Holodeck; Holodeck in turn will launch the application under test and start testing. By using Holodeck's Recorded Session feature we can track which faults were set and when they were executed. Our test harness will catch exceptions thrown by the application under test and log them to a time stamped file. By comparing the two we will have a direct cause and effect relationship.

Create a Holodeck project file

1) Open Holodeck
2) Create a new project
3) Store your project in a logical location (for this test we'll store our project at C:\test\notepadCodeCoverage.hdp)
    a) Select the program you wish to test (for this test we'll use C:\windows\notepad.exe)
    b) Check the APIs you wish to log (for this test we'll use the default logging)
    c) Perform the action in the application under test that you would like to test (for example: opening a file)
4) Save your project and close Holodeck

Setup the Test Harness

The test harness is a piece of software that is responsible for launching Holodeck with command line options, this software is not part of Holodeck and must be supplied by the user. The Test Harness is also responsible for terminating the test at appropriate times and monitoring the application under test for exceptions. When launching Holodeck the following command line options are available:

/record – turns on session recording

/silent – runs Holodeck minimized and with no popup UI

/codecoverage:[high|medium|low] – turns on code coverage with either high, medium or low settings

/randomstress:[high|medium|low] – turns on random stress testing with either high, medium or low settings

/intelligentstress:[high|medium|low] – turns on intelligent stress testing with either high, medium or low settings

The test harness must terminate the test process after Holodeck has finished running each test so that Holodeck can restart the Application Under Test with new faults set. The test harness is also responsible for monitoring and recording errors thrown by the Application Under Test, it is highly recommended that these are time stamped so that they may be easily compared to Holodeck's recorded session xml files.

Begin testing with Code Coverage

As Holodeck finds errors in the application under test unexpected error dialogues may appear, or for more serious errors, a debugger may be instantiated. Your test harness should be written in such a way that it can handle these problems and either continue on or terminate so the next test can run. Throughout the entire testing process, Holodeck is recording the faults and tests that are set, while the test harness is recording the errors. When you have collected all of the information needed or when test generation is complete, close the test harness.

Command to run Holodeck with code coverage silently and recording the session:

```
HolodeckGUI.exe /record /silent /codecoverage:high
```

How to compare log files

The two files we will compare are Holodeck's Recorded Session log (Recorded Sessions\Recorded Session #1.xml) and the log from our test harness. By matching the timestamps, or the order of execution, we can tell which faults caused which errors, making for easy reproduction. To match the timestamps, open the Recorded Sesson.xml file and look for the TimeStamp attribute of the <Log> tag, then look at your own timestamp from your test harness. When two match, you have found the cause of the fault (the <Inject> tag from Recorded Session.xml) and what happened (the log file from the test harness). The two log files are included in the resources section of this document.

How to Compare Log Files:

Using the Recorded Session #1.xml file and a test harness that logs each crash with a timestamp you can match which fault caused which timestamp. Notice the timestamp is set as soon as that fault was set, which may or may not cause an immediate failure in the Application Under Test.

Match timestamps by working backward in time from the Exception, you can see which faults, tests, and limits were set before the exception happened. The Test Harness Log timestamps are often a few seconds after the Recorded Sessions #1.xml timestamps, because the Application Under Test often does not fail immediately after a fault is set. Multiple Faults, Tests, or Limits might be set for any given Exception, so when working backwards you will have to keep track of how each Fault, Test, or Limit was set, deleted or modified. It is also important to make sure you consider Session numbers, each session is a new instance of the Application Under Test, which means all Faults, Tests, and Limits have been reset, be sure not to traverse Sessions or you will not be matching the proper Exceptions with the proper Recorded Session.

The following logs match up as follows:

Fault 1 (File not found) caused the first Exception

Fault 2 (Can't access file) caused the third Exception

Fault 3 (Access denied to file) caused the second Exception

Fault 4 (File is write protected) caused the fourth Exception

1. Recorded Session #1.xml

```
<Recorded_Session>

<Record>

<Log  Index="1"

    TimeStamp="7/21/2003 17:8:12.906"

    Session="1"

    AppName="notepad.exe" />

<Inject Type="21" Name="File not found" Enabled="2" />
```

```
</Record>

<Record>

<Log Index="1"

  TimeStamp="7/21/2003 17:8:20.109"

  Session="2"

  AppName="notepad.exe" />

<Inject Type="21" Name="Can't access file" Enabled="2" />

</Record>

<Record>

<Log Index="1"

  TimeStamp="7/21/2003 17:8:26.718"

  Session="3"

  AppName="notepad.exe" />

<Inject Type="21" Name="Access denied to file" Enabled="2" />

</Record>

<Record>

<Log Index="1"

  TimeStamp="7/21/2003 17:9:13.625"

  Session="4"

  AppName="notepad.exe" />

<Inject Type="21" Name="File is write protected" Enabled="2" />

</Record>

</Recorded_Session>
```

2. TestHarnessLog.txt

```
-------- First chance exception, VERY LOW chance of exploitation --------

Exception #1 in test case #2

Process HolodeckGui.exe caused access violation:

Read of 0x00000000 at instruction 0x040f5314

Test case started at 7/21/2003 17:8:14.76
```

```
-------- First chance exception, LOW chance of exploitation -----
---

Exception #2 in test case #2

Process HolodeckGui.exe caused access violation:

Read of 0x0000004c at instruction 0x040f19c6

Test case started at 7/21/2003 17:8:28.40



-------- First chance exception, LOW chance of exploitation -----
---

Exception #3 in test case #2

Process HolodeckGui.exe caused access violation:

Read of 0x0000004c at instruction 0x77e73887

Test case started at 7/21/2003 17:8:22.9



-------- First chance exception, VERY LOW chance of exploitation
--------

Exception #4 in test case #2

Process HolodeckGui.exe caused access violation:

Read of 0x00000000 at instruction 0x0390e241

Test case started at 7/21/2003 17:9:16.10
```

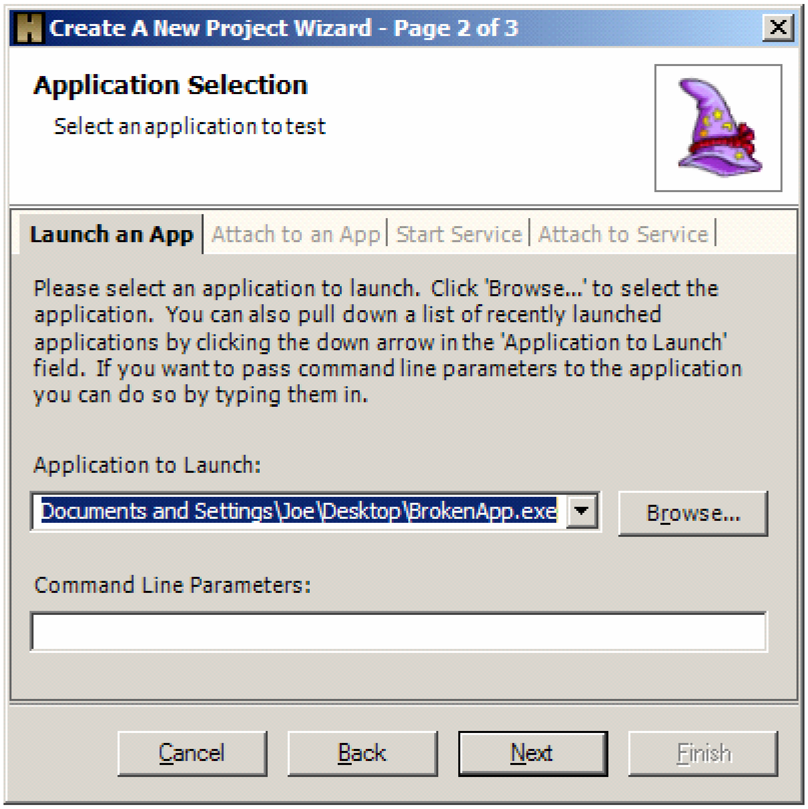
How to deprive your application of its dependencies

Introduction

In this Tutorial we will be exploring a method to discover which resources your application uses, and how to deny access to those resources to find new bugs. During this process we will uncover the resources that the BrokenApp uses while it loads, then set a resource fault so that it can no longer access it, then restart the app to find out what happens.

Create a new Project

To set up this Tutorial create a new project using BrokenApp as the Application Under Test, with default logging plus all the native API functions turned on. For more information on how to do this please see the Setting up a New Holodeck Project Tutorial.



Please select an application to launch. Click 'Browse...' to select the application. You can also pull down a list of recently launched applications by clicking the down arrow in the 'Application to Launch' field. If you want to pass command line parameters to the application you can do so by typing them in.

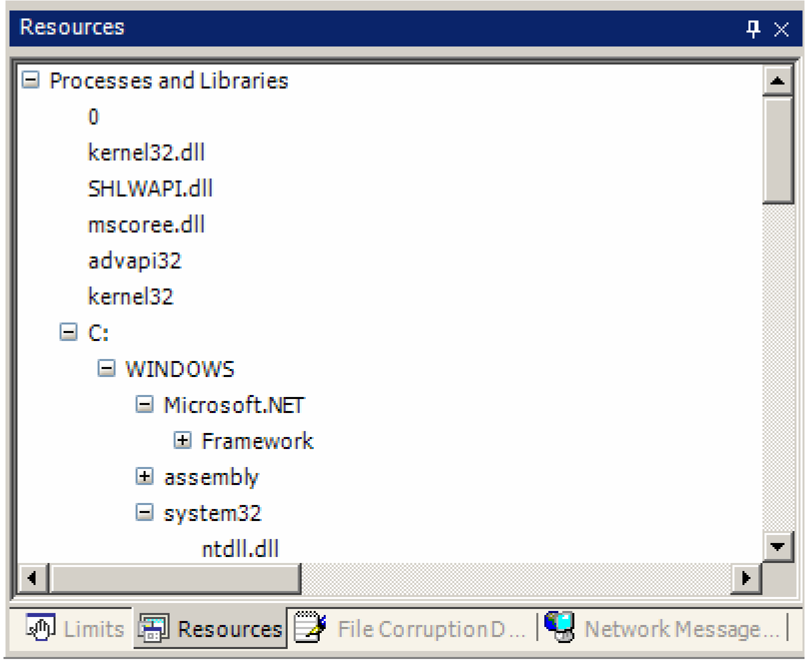
Application to Launch: Documents and Settings\Joe\Desktop\BrokenApp.exe

Command Line Parameters:

Investigate Resources

Once the application has started up, navigate to the resource pane by clicking the tab in the lower pane that says "Resources." Holodeck will show all the resources that BrokenApp has touched on startup. More resources might show up here as the application is used, but we can find a pretty nice bug without having to do that.

If you drill down into the processes and libraries resource node you will find a dll called RichEd20.dll. This dll is responsible for all the rich text editing that BrokenApp is able to do. We want to see what happens when BrokenApp is unable to load this dll when it is starting up.

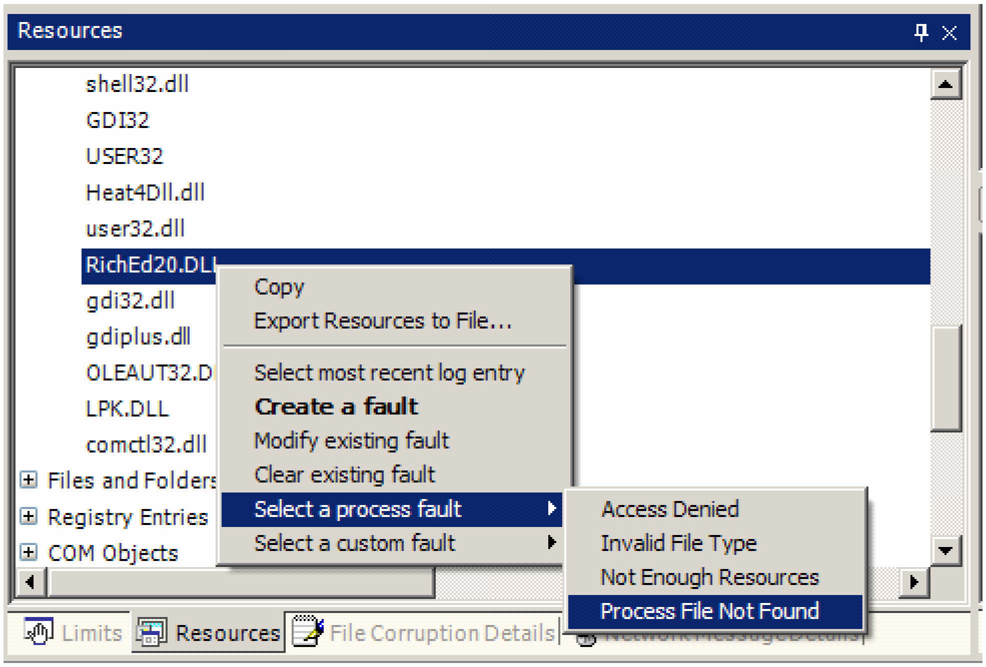


```
⊟ Processes and Libraries
      0
      kernel32.dll
      SHLWAPI.dll
      mscoree.dll
      advapi32
      kernel32
   ⊟ C:
      ⊟ WINDOWS
         ⊟ Microsoft.NET
            ⊞ Framework
         ⊞ assembly
         ⊟ system32
               ntdll.dll
```

Set the Resource Fault

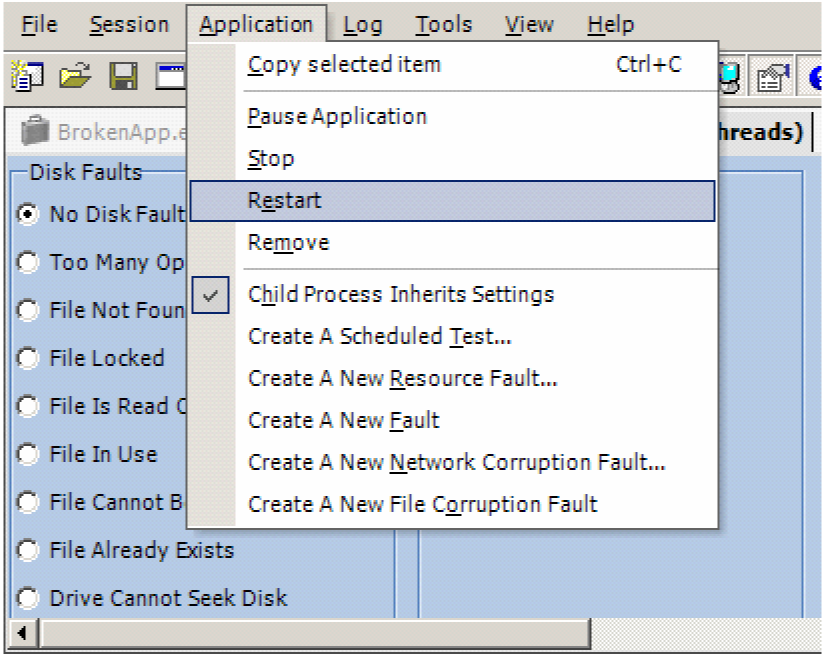
Now that we have done the research we need to do, the next step is to set a resource fault and restart the application. Often the application loads the entire library into memory, and doesn’t access it after that; this is why we need to restart the application.

To set a resource fault, find the resource in the resource pane and right click it. If you select "Create a fault" Holodeck will launch the "Create a Fault Wizard" with the correct resource automatically checked. However Holodeck allows you to set a fault quickly by using the "Set a Process Fault" menu. After you select one of the faults in this menu that fault is set immediately. Set the "Process file not found" fault on RichEd20.dll. This fault will fail any attempts to load a library or create a process which is what happens when the BrokenApp tries to load this dll.

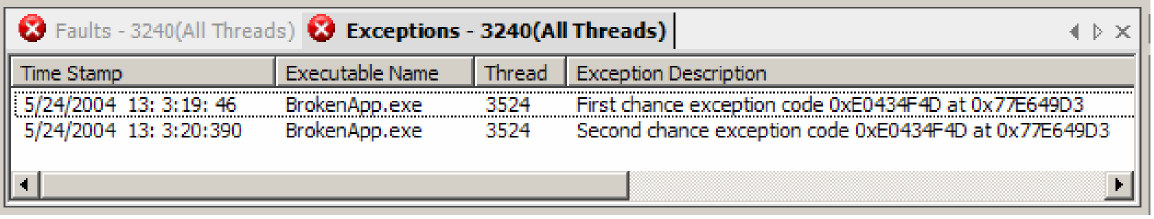


Restart BrokenApp with Resource Faults

Since this dll is loaded into memory when BrokenApp starts up we have to restart the application to see any changes. Restart BrokenApp by selecting Application > Restart. When you restart the BrokenApp Holodeck will remember any Resource Faults you have previously set and apply them to the application as it starts up.



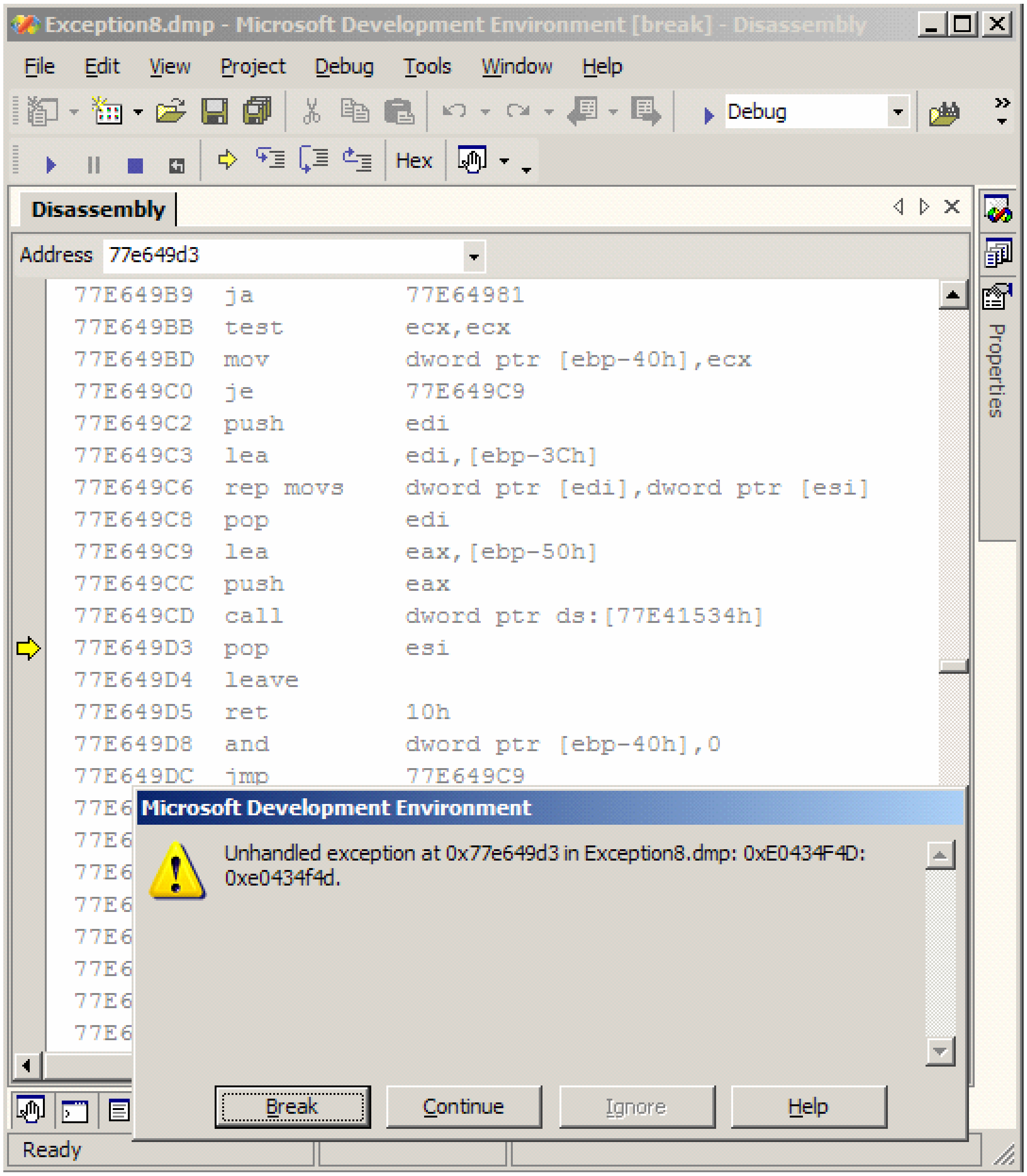
As BrokenApp starts up it will fail as soon as it tries to load the RichEd20.dll library. Two exceptions will be thrown, the first chance exception is caught by Holodeck before the application has a chance to deal with it, first chance exceptions will be caught in any application every time there is an exception thrown. Holodeck immediately gives the exception back to the application so it can handle it. If the application does not handle it, which broken app does not, a second chance exception is thrown. At this point since BrokenApp does not handle the exception it crashes.



Time Stamp	Executable Name	Thread	Exception Description
5/24/2004 13: 3:19: 46	BrokenApp.exe	3524	First chance exception code 0xE0434F4D at 0x77E649D3
5/24/2004 13: 3:20:390	BrokenApp.exe	3524	Second chance exception code 0xE0434F4D at 0x77E649D3

Investigating the Failure

We can load the debugging information into Visual Studio.net and reproduce the crash. To load the debugging information into Visual Studio double-click one of the exception nodes in the Project pane. This will show the Exception pane in the main window. The Exception pane shows every exception your application has thrown, whether it handled it or not. Double-click the exception you want to debug in this pane and Holodeck will launch Visual Studio and load the exception debugging information. You can reproduce the crash or exception by pressing f5. If source code is available for the crash Visual Studio will load it and highlight the offending line. If no source code is available Visual Studio will ask to show the assembly code, and highlight the last instruction to be called.



Address 77e649d3

```
77E649B9  ja        77E64981
77E649BB  test      ecx,ecx
77E649BD  mov       dword ptr [ebp-40h],ecx
77E649C0  je        77E649C9
77E649C2  push      edi
77E649C3  lea       edi,[ebp-3Ch]
77E649C6  rep movs  dword ptr [edi],dword ptr [esi]
77E649C8  pop       edi
77E649C9  lea       eax,[ebp-50h]
77E649CC  push      eax
77E649CD  call      dword ptr ds:[77E41534h]
77E649D3  pop       esi
77E649D4  leave
77E649D5  ret       10h
77E649D8  and       dword ptr [ebp-40h],0
77E649DC  jmp       77E649C9
77E6
77E6
77E6
77E6
77E6
77E6
77E6
77E6
```

Microsoft Development Environment

Unhandled exception at 0x77e649d3 in Exception8.dmp: 0xE0434F4D: 0xe0434f4d.

How to use Holodeck's test automation interfaces

Introduction

Holodeck in depth

Introduction to Holodeck in depth

This section covers each feature in Holodeck in detail. Research how to test your application more fully by understanding how to use the features of Holodeck completely.

Each of the following chapters contain all the advanced features of Holodeck.

New Project Wizard – Holodeck can be attached to or launch applications or services.

Creating Tests – Scheduled tests allow you to fail a single API call based on that function’s input and output parameters.

Creating Limits – Holodeck can limit physical resources such as memory, hard drive space, and network bandwidth your application has available to it; use this to simulate different hardware configurations.

Creating Faults – Faults are common failures a system might have, such as an invalid address for memory, or a network disabled error for the network.

Resource Faults – Resource faults are faults that simulate problems accessing or loading a resource such as a process, library, file, folder, registry key, registry value or COM Object.

Working with Logs – Holodeck logs all the API’s you select, you can filter, sort, change which functions are logged, export and more.

Working with Reports – Holodeck can generate an easy to read report on your current project. This report contains information for every process in the project including logs, faults, limits, etc..

Using Automatic Test Generation – Holodeck can automatically generate tests, limits, and faults for you through the use of code coverage or stress test generation.

Generating Network Corruption Faults – The Network Corruption Fault Wizard will help you create corruption within network packets.

Generating File Corruption – Holodeck helps test File parsing by corrupting files.

Using regular expressions and Replacement strings – Regular Expressions and Replacement strings can be used in conjunction with Network and File Corruption Faults.

Multiple Threads and Processes – Holodeck can be focused on a single thread or follow multiple process.

Exceptions and Mini-dumps – See how Holodeck catches Exceptions and creates mini-dumps to aid in debugging crashes in the application under test.

Recording and Replaying Sessions – Holodeck allows you to record the tests Holodeck makes to help you reproduce bugs and verify failures.

Add New Holodeck Intercepts – You can add new intercepts to Holodeck easily to help you intercept custom libraries.

New Project Wizard

New Project Wizard

The new test project walks you through the steps to create a new project. Holodeck allows you to Launch an application to test, attach to an already running application, launch a service, or attach to an already running service.

Launch an Application – Launch an application to test an application. This option gives you control to test startup functions.

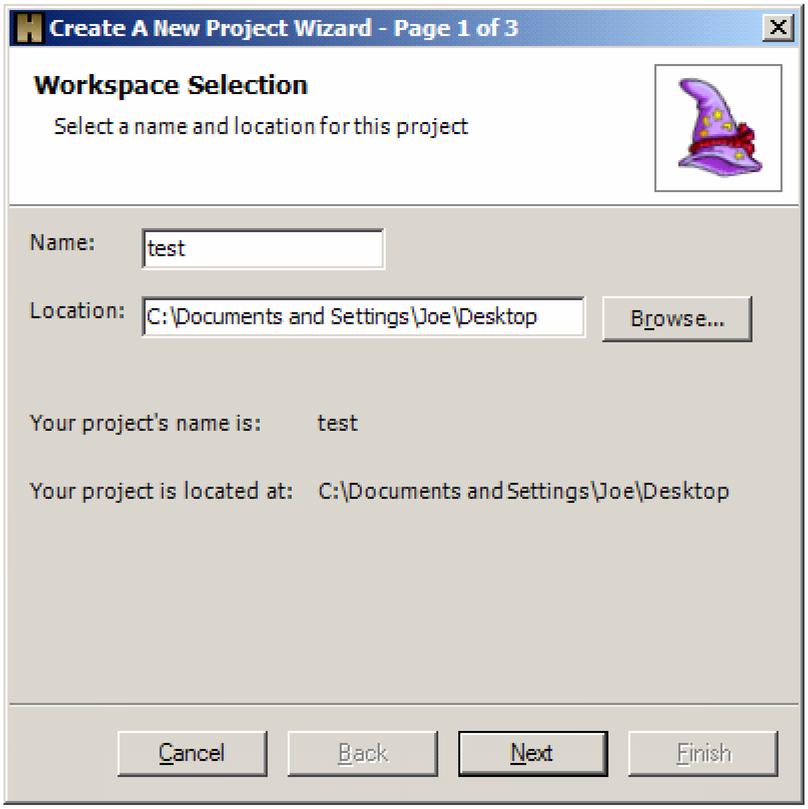
Attach to an Application – This option gives you the ability to attach Holodeck to an already running process.

Start a Service – Launch a service, all services which are enabled and not currently running are available for launch.

Attach to a Service – All services that are currently running are available to be launched.

New Project Options – The final page of the Wizard allows you to select how Holodeck monitors your application or service.

Choose one of the above links for more information on that creating a project of that type.



Create A New Project Wizard - Page 1 of 3

Workspace Selection

Select a name and location for this project

Name: test

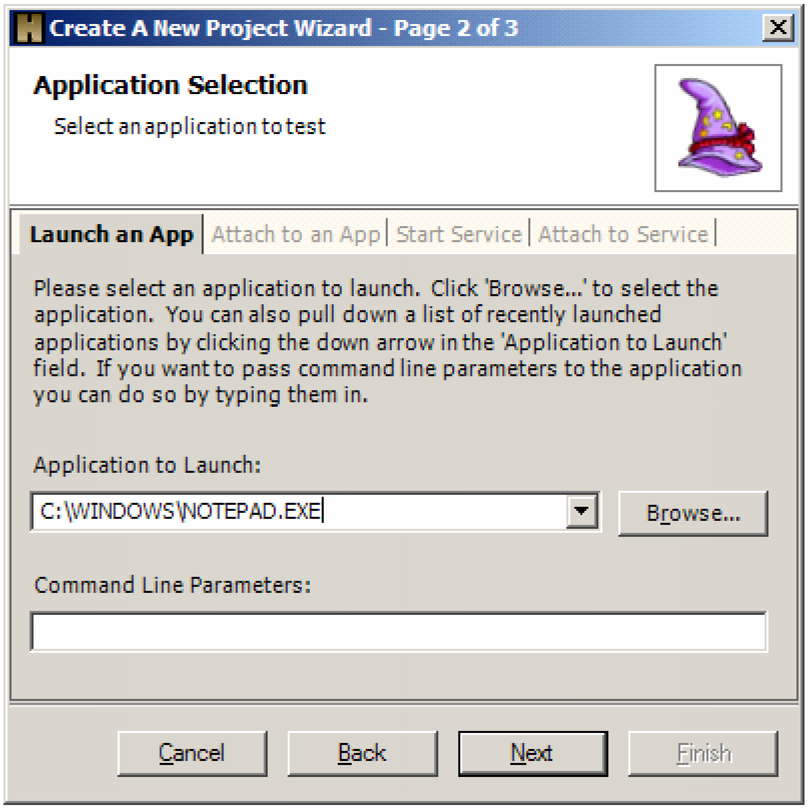
Location: C:\Documents and Settings\Joe\Desktop

Your project's name is: test

Your project is located at: C:\Documents and Settings\Joe\Desktop

Launch an Application

Use this option to test an application that is not currently running. This is good because you can pause the application on start to set test, limits, etc before the application loads, which enables you to test the startup of the application. If your application requires command line parameters you can specify them in the Command Line Parameters text box.



Application Selection

Select an application to test

Please select an application to launch. Click 'Browse...' to select the application. You can also pull down a list of recently launched applications by clicking the down arrow in the 'Application to Launch' field. If you want to pass command line parameters to the application you can do so by typing them in.

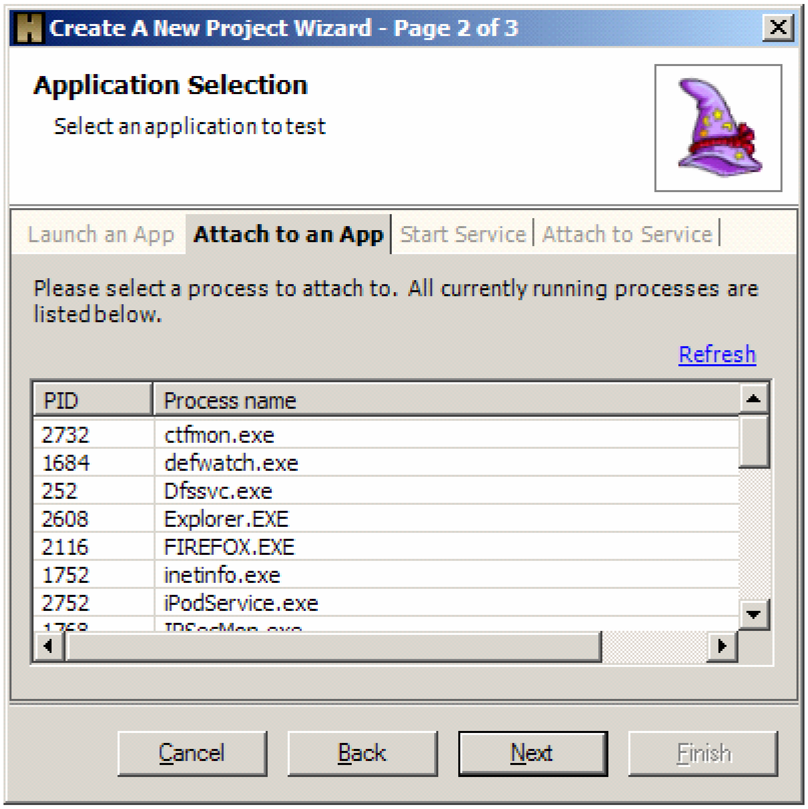
Application to Launch: C:\WINDOWS\NOTEPAD.EXE

Command Line Parameters:

Continue to the New Project Options to complete the wizard.

Attach to an Application

Use this option to attach Holodeck to a currently running application. This is useful for testing applications that start up with the operating system, run in the background, or are required to run for normal operation of the computer.



Application Selection

Select an application to test

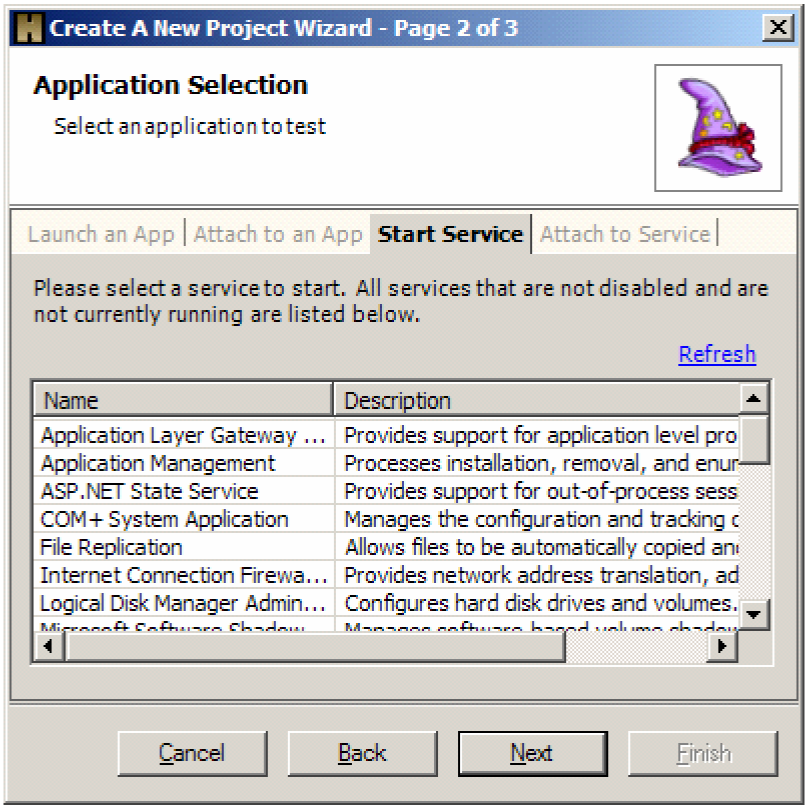
Please select a process to attach to. All currently running processes are listed below.

PID	Process name
2732	ctfmon.exe
1684	defwatch.exe
252	Dfssvc.exe
2608	Explorer.EXE
2116	FIREFOX.EXE
1752	inetinfo.exe
2752	iPodService.exe

Continue to the New Project Options to complete the wizard.

Start a Service

Holodeck can help test services including system services and application services. Holodeck will launch the service and begin logging immediately.



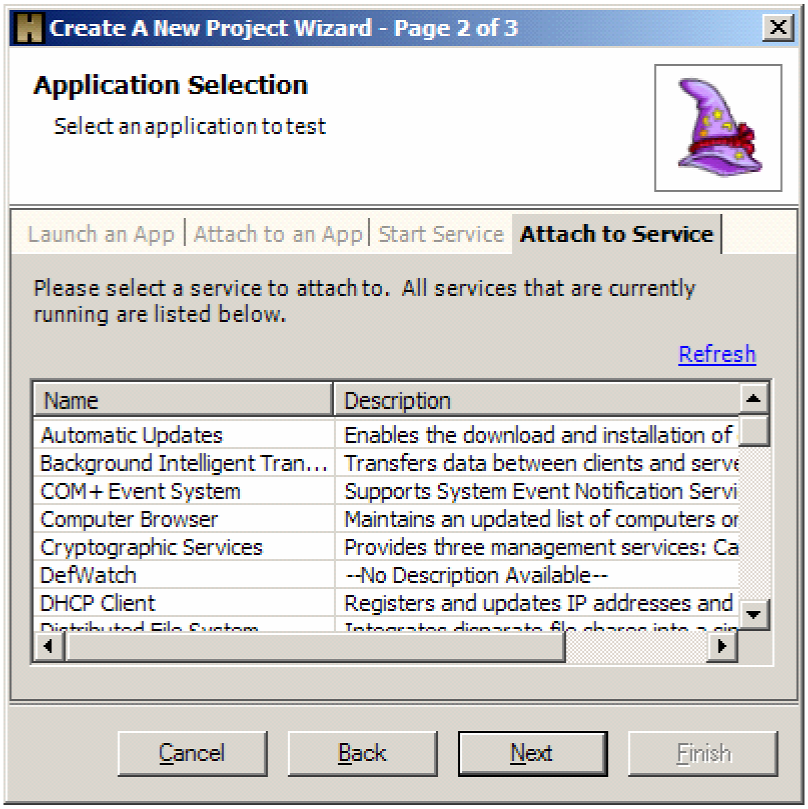
Please select a service to start. All services that are not disabled and are not currently running are listed below.

Name	Description
Application Layer Gateway ...	Provides support for application level pro
Application Management	Processes installation, removal, and enur
ASP.NET State Service	Provides support for out-of-process sess
COM+ System Application	Manages the configuration and tracking c
File Replication	Allows files to be automatically copied an
Internet Connection Firewa...	Provides network address translation, ad
Logical Disk Manager Admin...	Configures hard disk drives and volumes.
Microsoft Software Shadow...	Manages software-based volume shadow

Continue to the New Project Options to complete the wizard.

Attach to a Service

You can attach Holodeck to a Service that is already running. Holodeck will begin logging API function calls as soon as the wizard has completed.



Please select a service to attach to. All services that are currently running are listed below.

Name	Description
Automatic Updates	Enables the download and installation of
Background Intelligent Tran...	Transfers data between clients and serve
COM+ Event System	Supports System Event Notification Servi
Computer Browser	Maintains an updated list of computers or
Cryptographic Services	Provides three management services: Ca
DefWatch	--No Description Available--
DHCP Client	Registers and updates IP addresses and
Distributed File System	Integrates disparate file shares into a sin

Continue to the New Project Options to complete the wizard.

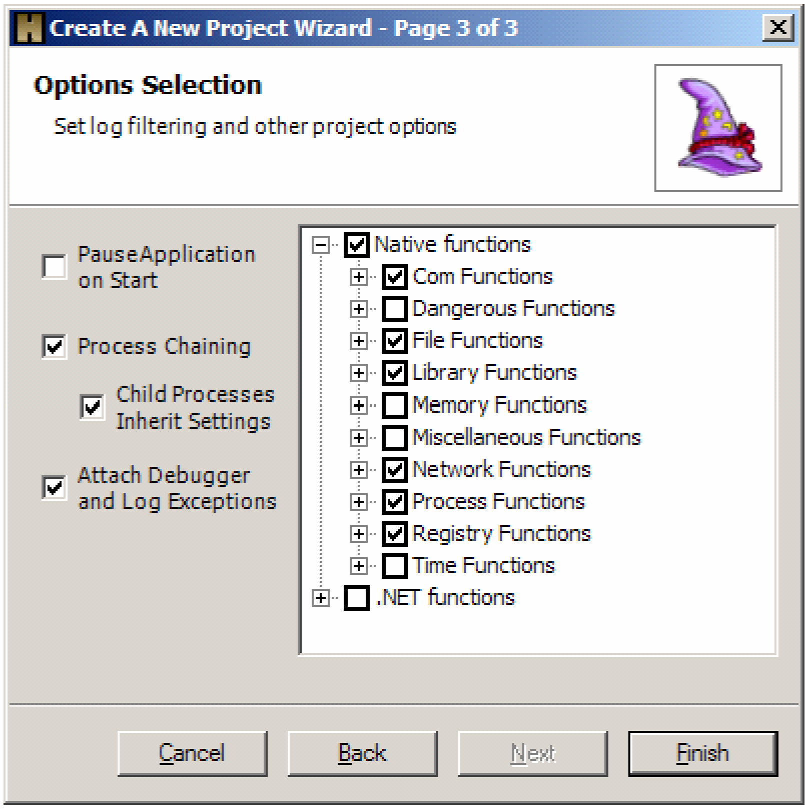
New Project Options

This page allows you to set options on how Holodeck monitors your application. Turning on more function logging will increase the number of tests and faults that are available, however more logging may impair the performance of your application.

You can pause your application on start to set tests, limits, faults etc. before your application starts up. If you are attaching Holodeck to an already running instance of an application or service Holodeck will pause the application or service when the wizard has finished; to resume execution of your application uncheck Application > Pause Application.

If Process Chaining is turned on Holodeck will automatically attach itself to any processes your application launches. If you check Child Process Inherit Settings, any process your application launches will automatically inherit the same tests, limits, faults etc. that were set for the parent application.

Holodeck comes with a built in Debugger which catches exceptions and creates mini-dump files. Check "Attach Debugger and Log Exceptions" to enable this feature.



Create A New Project Wizard - Page 3 of 3

Options Selection

Set log filtering and other project options

☐ PauseApplication on Start

☑ Process Chaining

☑ Child Processes Inherit Settings

☑ Attach Debugger and Log Exceptions

- ☑ Native functions
  - ☑ Com Functions
  - ☐ Dangerous Functions
  - ☑ File Functions
  - ☑ Library Functions
  - ☐ Memory Functions
  - ☐ Miscellaneous Functions
  - ☑ Network Functions
  - ☑ Process Functions
  - ☑ Registry Functions
  - ☐ Time Functions
- ☐ .NET functions

Creating Tests

Tests

Tests are a way to inject targeted failures; a test targets a single API call based on matching the in parameters you specify. If it matches the result, it will output the return value, error codes, and out parameters you specify.

This is a good way to test specific function calls to find out what might happen if external API calls fail.

To Create a test see the Creating a test topic in this section.

The Scheduled Test Wizard will help walk you through the steps to create a scheduled test.

Tests can fire 100% of the time, a lesser percentage or the time or based on the function calls on the stack. For more information on Creating a Test Based on Stack Matching please see the help topic in this section.

How to tell if a test fires:

You can tell if a test has fired by looking in the API logs. If the test has fired you will see the error-code and return values set by the test.

You can see how many times a test has fired by selecting the test in the project pane, and looking to the Properties Pane.

Creating and Deleting a test

You can create a **New Scheduled Test** by any of the following methods

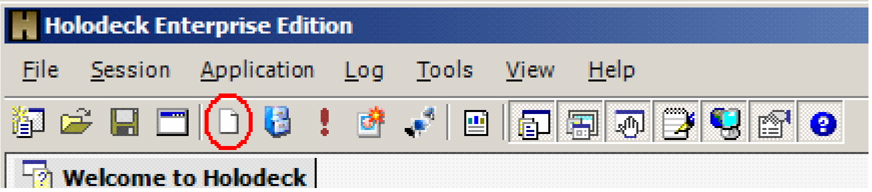
1) From Log entries

   a) Double Click any Log entry to open the Scheduled Test Wizard

   Note: this is a good way to create a scheduled test because it then loads the Wizard with the correct API function selected.

2) From the Context menu.

   a) Click the **New Scheduled Test Button**



3) From the Menu

   a) Click **Application** > **Create a Scheduled Test**

4) From the Project Pane

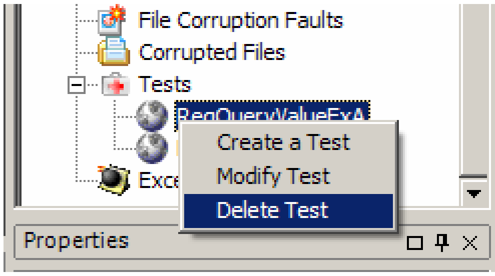
   a) Right click the Tests Node under the Application for which you would like to create a test.

   b) Select Create a new Test.

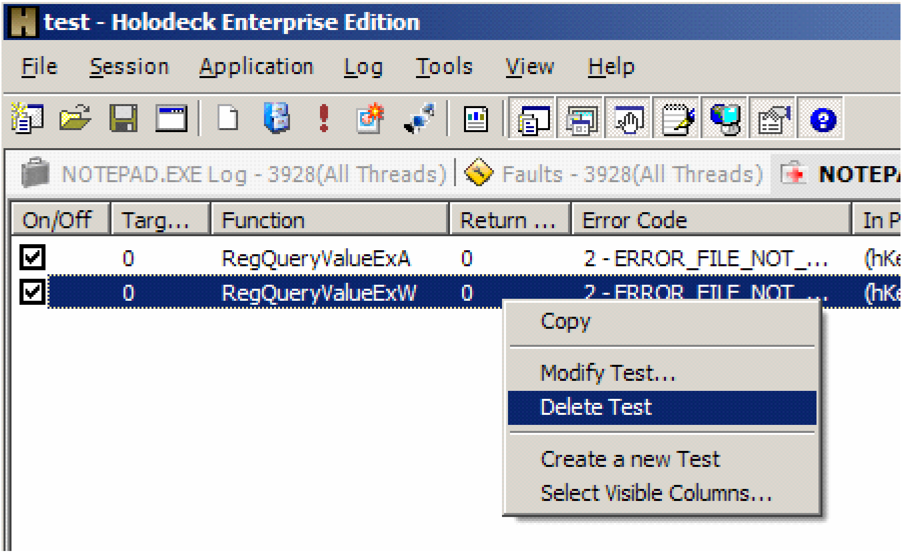
Note: if you create a test in per thread mode you can create a test for a single thread.

Deleting a test

To delete a test, find the test in the project pane, right click and select Delete test.



You can also delete a test by right clicking the test in the tests pane and selecting Delete test.

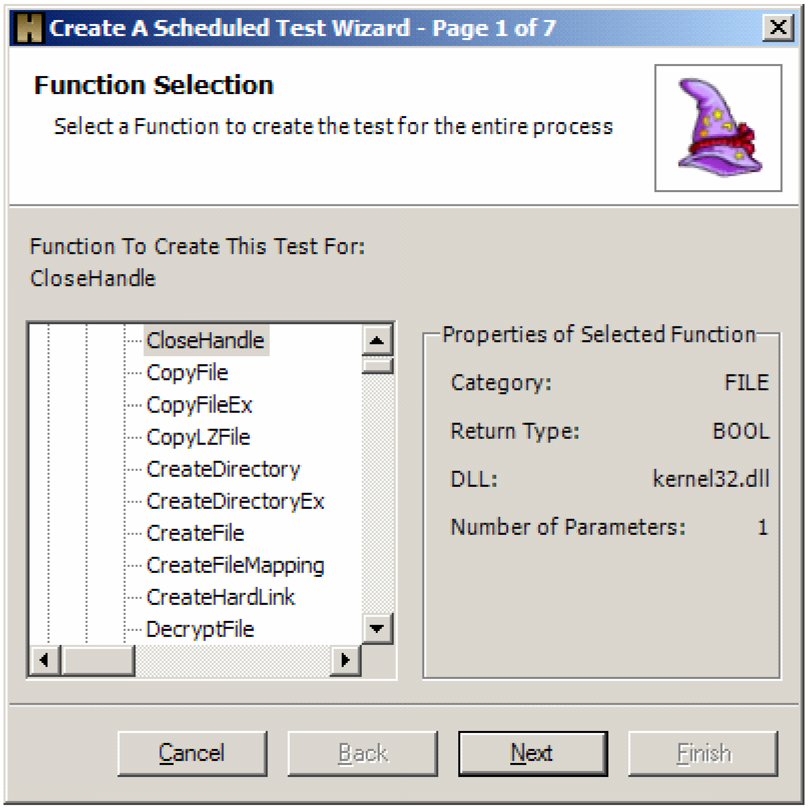

test - Holodeck Enterprise Edition
File Session Application Log Tools View Help
NOTEPAD.EXE Log - 3928(All Threads)
Faults - 3928(All Threads)
NOTEP
Copy
Modify Test...
Delete Test
Create a new Test
Select Visible Columns...

On/Off	Targ...	Function	Return ...	Error Code	In P
☑	0	RegQueryValueExA	0	2 - ERROR_FILE_NOT_...	(hKe
☑	0	RegQueryValueExW	0	2 - ERROR_FILE_NOT_...	(hKe

Scheduled Test Wizard

Create A Scheduled Test Wizard – This wizard will help you fail a certain function call, focus

1) The Function Selection Window allows you to select a function to create the test for the entire process. If you used the log pane to create a new test the correct function will already be



Create A Scheduled Test Wizard - Page 1 of 7

Function Selection

Select a Function to create the test for the entire process

Function To Create This Test For:
CloseHandle

Properties of Selected Function

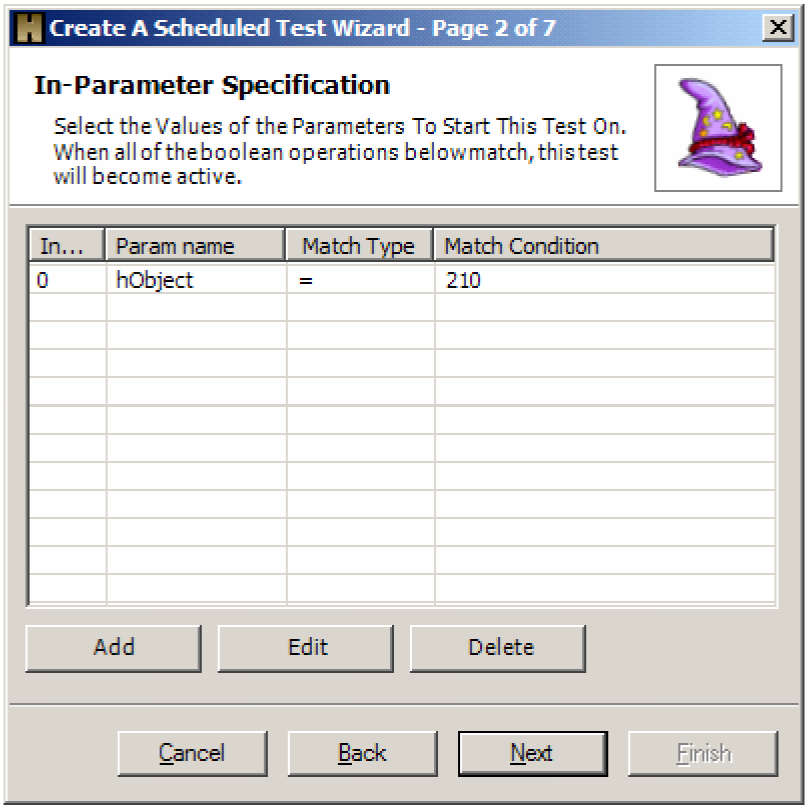
Category: FILE

Return Type: BOOL

DLL: kernel32.dll

Number of Parameters: 1

2) The In-Parameter Specification Window allows you to select the Values of the Parameters to start this test on. When all of the Boolean operations below match, this test will become active. In parameters are most likely sent from the application under test, which make it easy to fire a controlled test this way. In this example this test will be fired every time the application tries to close the handle with ID 210.



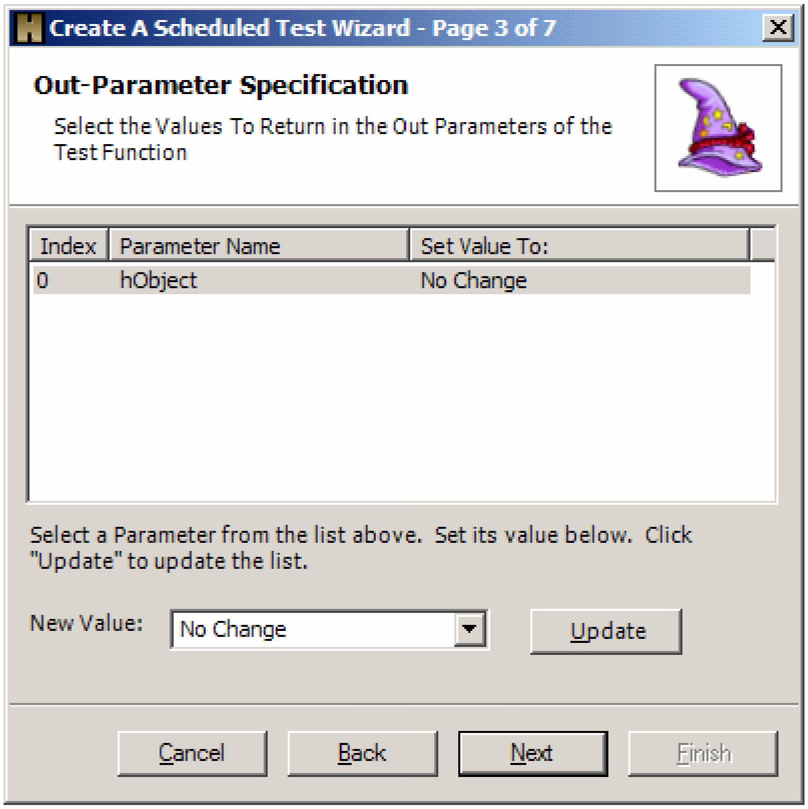
Create A Scheduled Test Wizard - Page 2 of 7

In-Parameter Specification

Select the Values of the Parameters To Start This Test On. When all of the boolean operations below match, this test will become active.

In...	Param name	Match Type	Match Condition
0	hObject	=	210

3) The **Out-Parameter Specification Window** allows you to select or change the values to return in the out parameters of the test function. When the test fires Holodeck will replace whatever the original out-parameter value was with the out-parameter value you specify in this page of the wizard. Often the application under test may assume certain values for each out-parameter, this is a likely place to find bugs. By changing the out-parameters to unexpected values you can ensure your application will fail properly if there is an error in the API call, or the API is called incorrectly.



Create A Scheduled Test Wizard - Page 3 of 7

Out-Parameter Specification

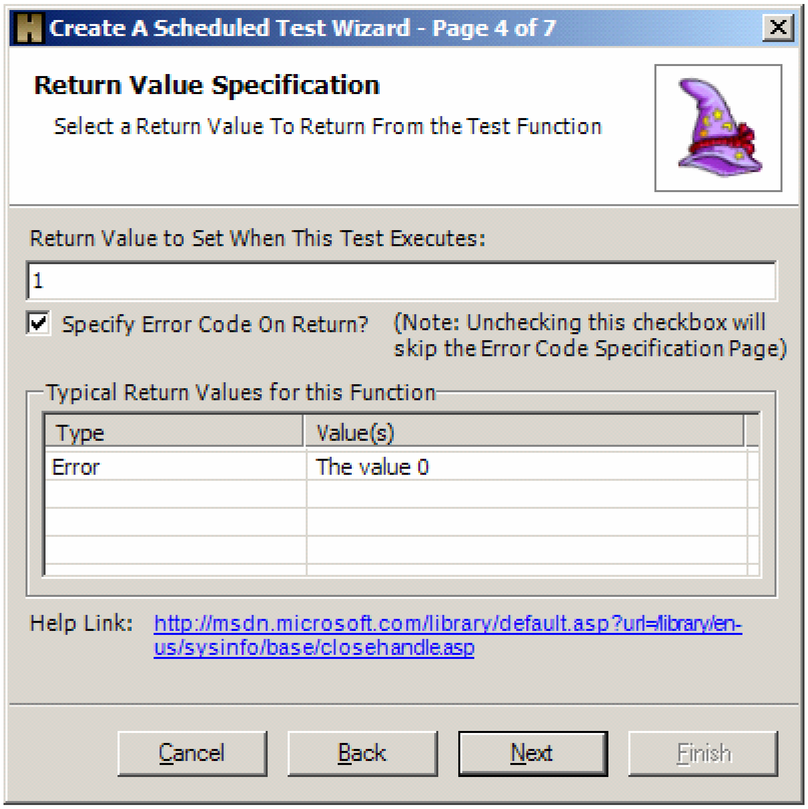
Select the Values To Return in the Out Parameters of the Test Function

Index	Parameter Name	Set Value To:
0	hObject	No Change

Select a Parameter from the list above. Set its value below. Click "Update" to update the list.

New Value: No Change

4) The **Return Value Specification Window** allows you to select a return value to return from the test function. Besides changing out-parameters, Holodeck can also change the return value of the API call.



Create A Scheduled Test Wizard - Page 4 of 7

Return Value Specification

Select a Return Value To Return From the Test Function

Return Value to Set When This Test Executes: 1

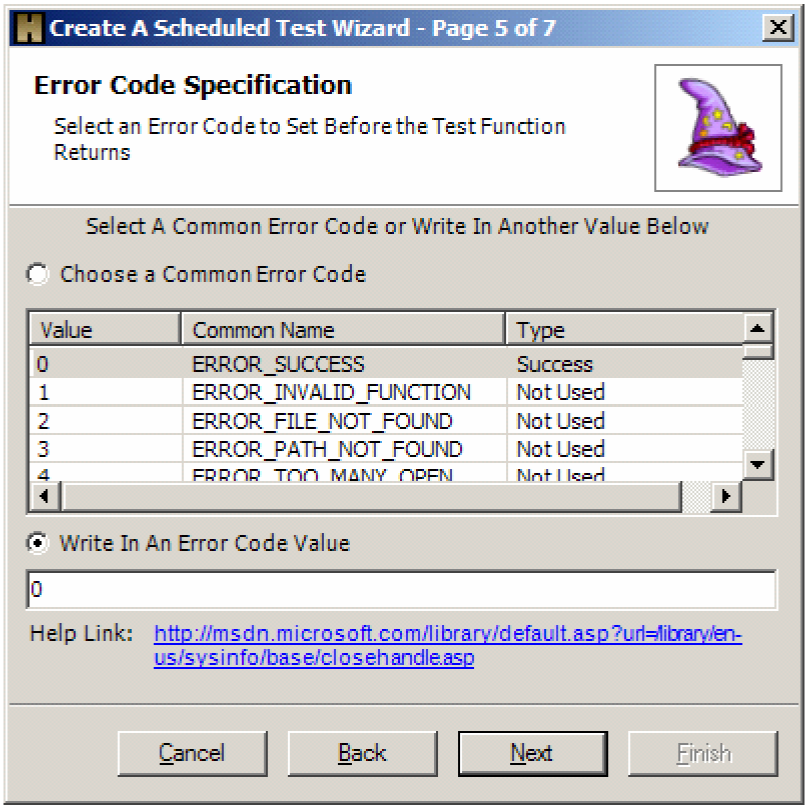
☑ Specify Error Code On Return? (Note: Unchecking this checkbox will skip the Error Code Specification Page)

Typical Return Values for this Function

Type	Value(s)
Error	The value 0

Help Link: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/closehandle.asp

5) The **Error Code Specification Window** allows you to select an Error Code to be Set Before the Test Function Returns. Holodeck will set the specified error code using the setLastError system call. Doing this will make the application under test believe the last API call had some error, which could uncover bugs in the application code.



Error Code Specification

Select an Error Code to Set Before the Test Function Returns

Select A Common Error Code or Write In Another Value Below

○ Choose a Common Error Code

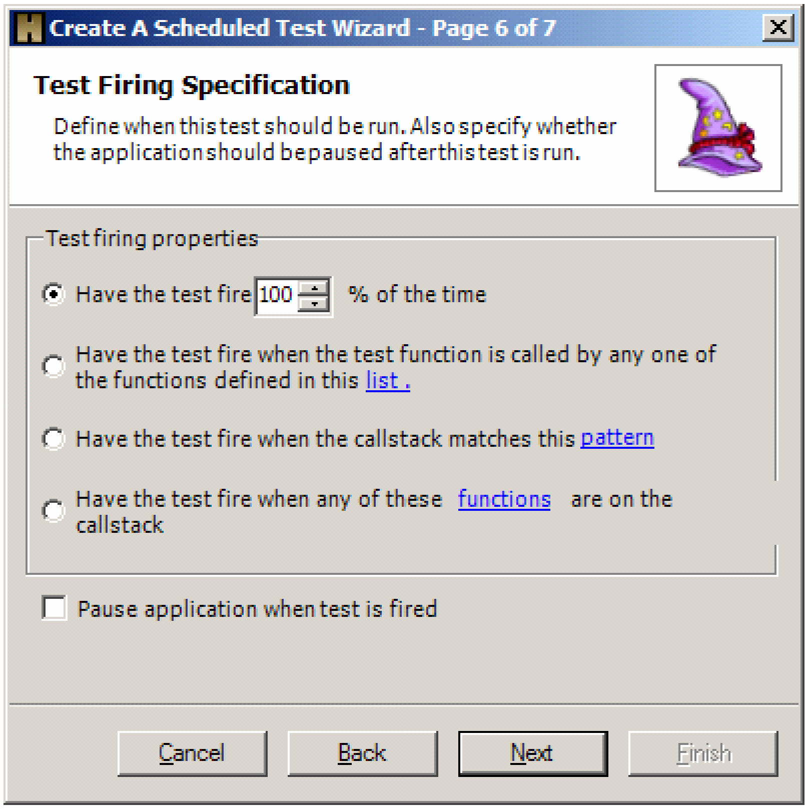
Value	Common Name	Type
0	ERROR_SUCCESS	Success
1	ERROR_INVALID_FUNCTION	Not Used
2	ERROR_FILE_NOT_FOUND	Not Used
3	ERROR_PATH_NOT_FOUND	Not Used
4	ERROR_TOO_MANY_OPEN	Not Used

● Write In An Error Code Value

0

Help Link: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/closehandle.asp

6) The **Test Firing Specification** allows you to change the amount a specific test fires during the run of the Application Under Test. Often an error does not happen every time an API call is made. On this page you can specify how often a test fires. It may be useful to specify a certain application state such as a function on the call stack.



Create A Scheduled Test Wizard - Page 6 of 7

Test Firing Specification

Define when this test should be run. Also specify whether the application should be paused after this test is run.

Test firing properties

● Have the test fire 100 % of the time

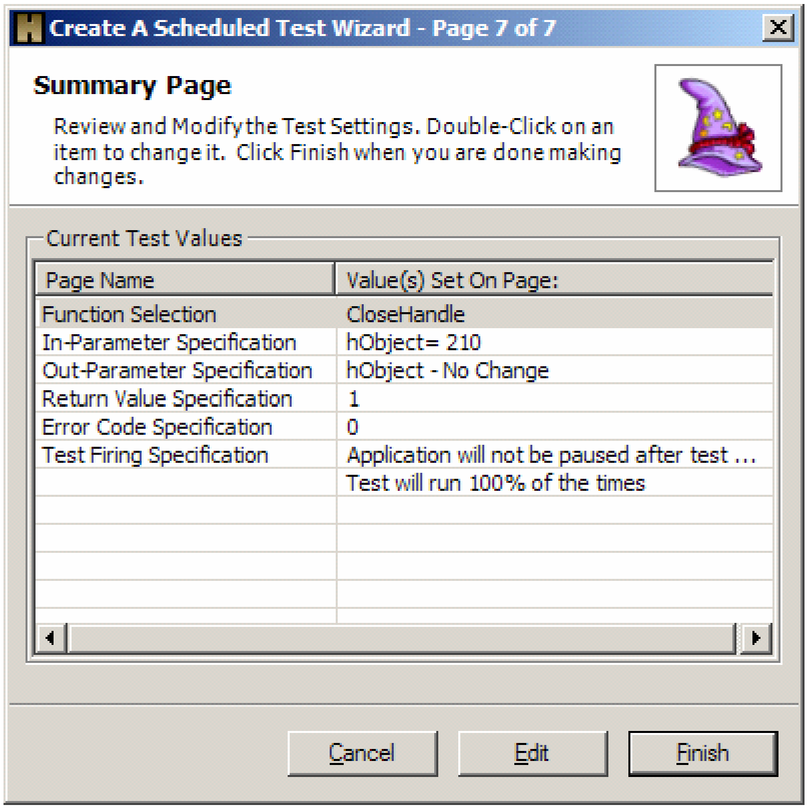
○ Have the test fire when the test function is called by any one of the functions defined in this list .

○ Have the test fire when the callstack matches this pattern

○ Have the test fire when any of these functions are on the callstack

□ Pause application when test is fired

7) The **Summary / Modifications Page** allows you to review and Modify Test Settings. If you wish to change any of the settings on this page, highlight the setting you would like to change and click edit. This will return you to the page of the wizard where that information can be changed.



Summary Page

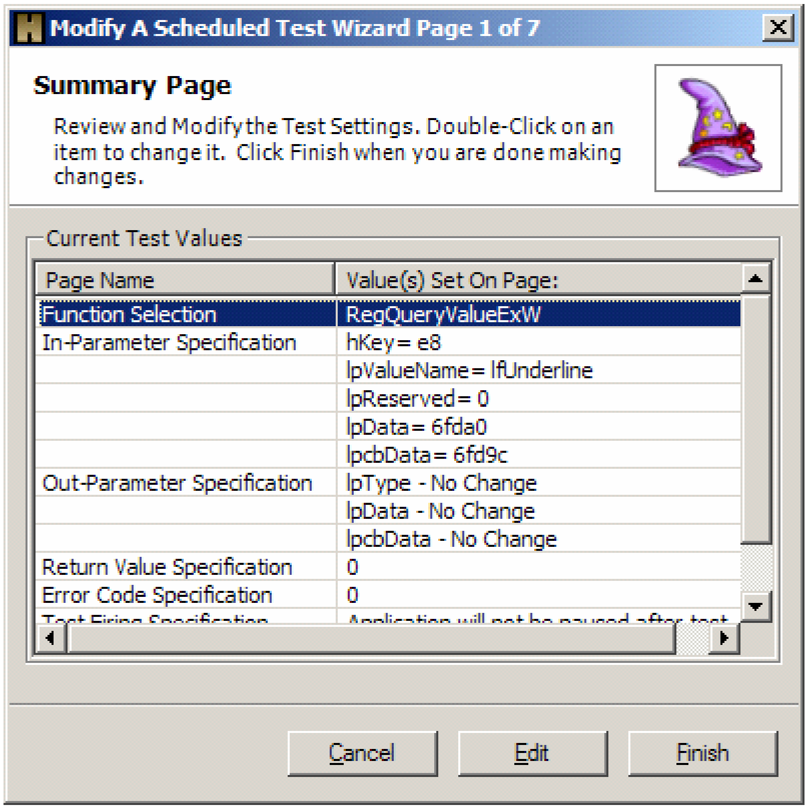
Review and Modify the Test Settings. Double-Click on an item to change it. Click Finish when you are done making changes.

Current Test Values

Page Name	Value(s) Set On Page:
Function Selection	CloseHandle
In-Parameter Specification	hObject= 210
Out-Parameter Specification	hObject - No Change
Return Value Specification	1
Error Code Specification	0
Test Firing Specification	Application will not be paused after test ...
	Test will run 100% of the times

Modifying a test

Modifying Tests - Right click the test you wish to Modify in the Project pane and click Modify Test or Double click the Project you would like to modify. This will bring up the Summary / Modifications page of the New Scheduled Test Wizard



Modify A Scheduled Test Wizard Page 1 of 7

Summary Page

Review and Modify the Test Settings. Double-Click on an item to change it. Click Finish when you are done making changes.

Current Test Values

Page Name	Value(s) Set On Page:
Function Selection	RegQueryValueExW
In-Parameter Specification	hKey= e8
	lpValueName= lfUnderline
	lpReserved= 0
	lpData= 6fda0
	lpcbData= 6fd9c
Out-Parameter Specification	lpType - No Change
	lpData - No Change
	lpcbData - No Change
Return Value Specification	0
Error Code Specification	0
Test Firing Specification	Application will not be paused after test

To modify any part of the test simply select the page name in the table and click edit, this will bring you directly to that page of the wizard.

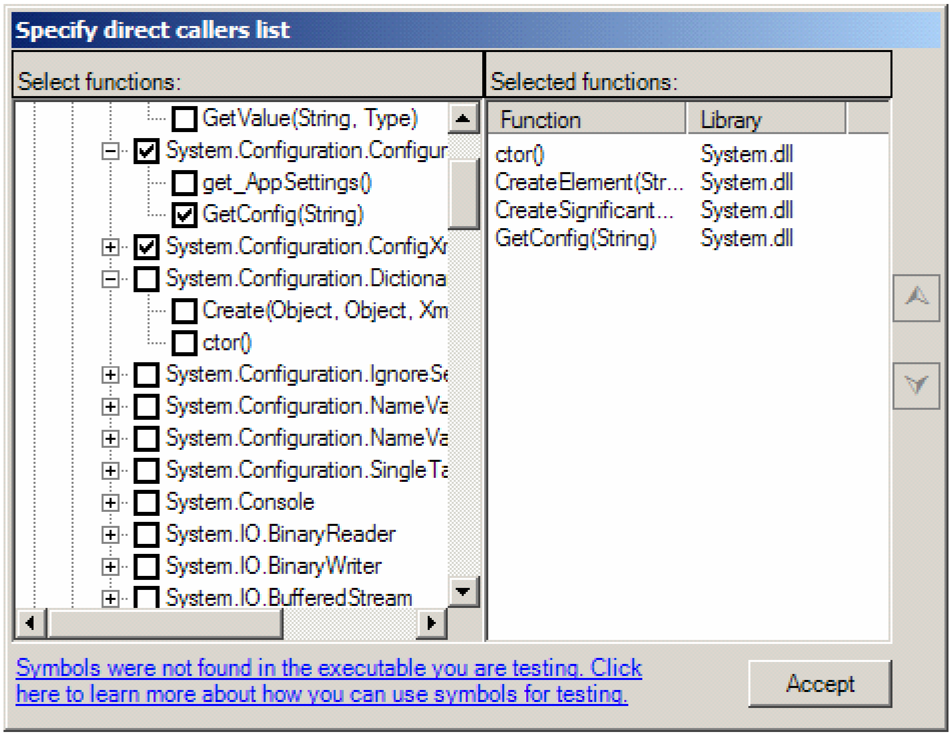
Creating a Test Based on Stack Matching

When testing a debug version of the application Holodeck can read the symbols and give you the ability to fire a test only when certain functions are on the system stack.

For example:

With symbols information, a test could be created which would only fire if the function under test was called from a particular function inside the application.

This can be very useful when trying to focus a test to fire only when a certain system state is present, ie. a certain function has called the function for which the test was set.



- □ GetValue(String, Type)
- ☑ System.Configuration.Configur
  - □ get_AppSettings()
  - ☑ GetConfig(String)
- ☑ System.Configuration.ConfigXr
- □ System.Configuration.Dictiona
  - □ Create(Object, Object, Xm
  - □ ctor()
- □ System.Configuration.IgnoreSe
- □ System.Configuration.NameVa
- □ System.Configuration.NameVa
- □ System.Configuration.SingleTa
- □ System.Console
- □ System.IO.BinaryReader
- □ System.IO.BinaryWriter
- □ System.IO.BufferedStream

Function	Library
ctor()	System.dll
CreateElement(Str...	System.dll
CreateSignificant...	System.dll
GetConfig(String)	System.dll

Symbols were not found in the executable you are testing. Click here to learn more about how you can use symbols for testing.

Creating Limits

Limits overview

In Holodeck it is possible to view how much of the disk or memory resources the Application Under Test is using and to restrict those resources to simulate different test scenarios without having to physically change the memory or disk availability on the test machine. These limits include Disk Limits, Memory Limits, and Network Limits. Use these limits to simulate different hardware configurations without having to change your system hardware. Use the limits pane to set and remove limits from your test application.

Limits:

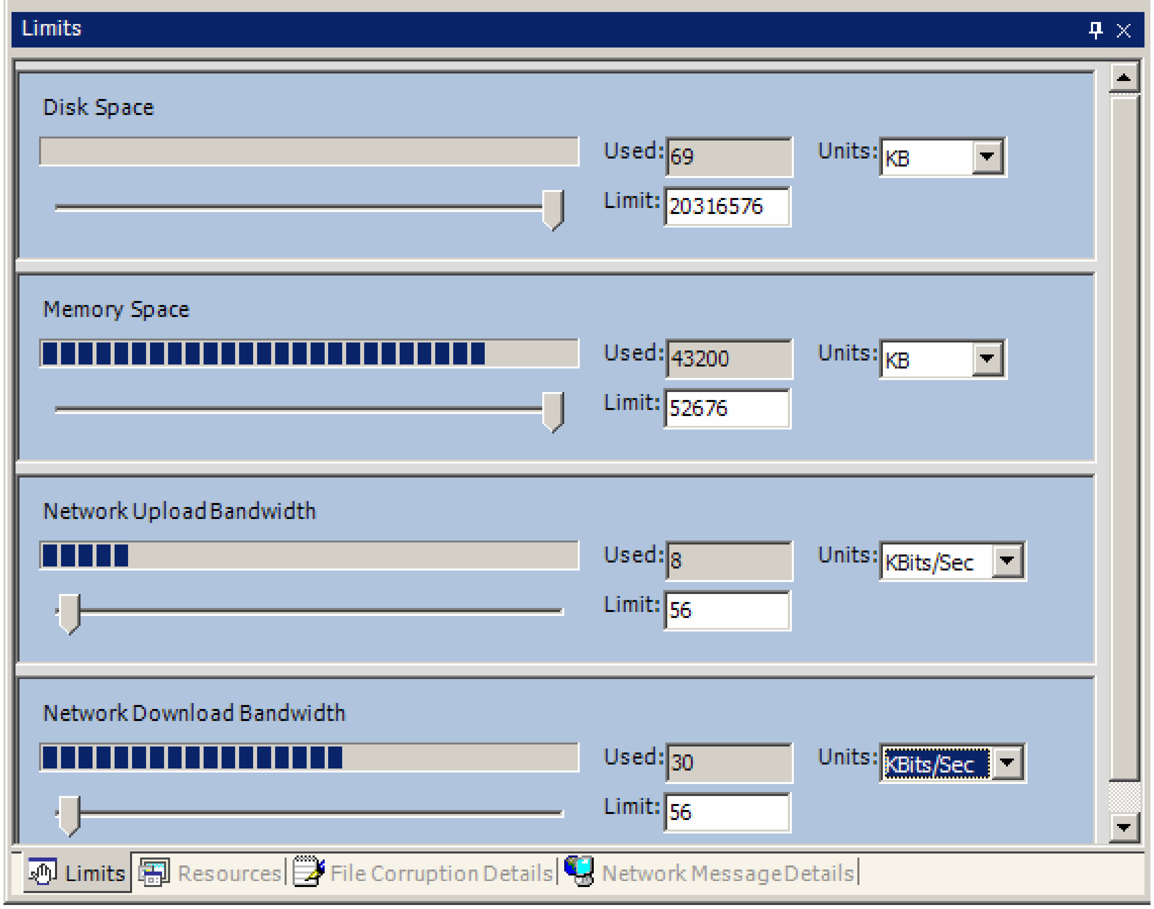
To view the amount of disk or memory resources currently being used by the Application Under Test make sure Holodeck is configured to show the Limits pane by clicking View on the Menubar and making sure Limits Pane has a check beside it.

Once the Limits Pane has been selected under the View menu, click the Limits tab at the bottom of the screen in the Limits Pane. This will bring up the Limits pane which shows the total amount of each resource used. If a limit has been set the limit will be shown on the slider-bar and in the limit text box. Each resource can be limited to see how your program will handle under limited resource conditions.

For example if you wanted to see how your application dealt with a small amount of memory you could slide the slider bar down until Holodeck was limiting the memory resources to extreme levels. This is useful for finding out how your application reacts to low memory conditions.

The Used Text Box contains how much of a resource is in use by the Application Under Test.

Note: Depending on external factors, suck as other applications and services running on the system, Holodeck will automatically adjust the amount of available disk and memory space available to your application.



Limits

Disk Space

Used: 69

Units: KB

Limit: 20316576

Memory Space

Used: 43200

Units: KB

Limit: 52676

Network Upload Bandwidth

Used: 8

Units: KBits/Sec

Limit: 56

Network Download Bandwidth

Used: 30

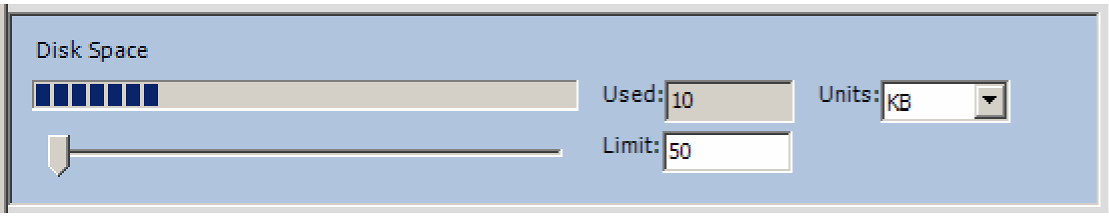
Units: KBits/Sec

Limit: 56

Creating a Disk Space limit

This limits the amount of Hard Drive Space available to the Application Under Test. Using this feature you can test the Application Under Test’s ability to handle errors such as Low or Filled Disk Space.

Open the limits pane by clicking **View** and making sure there is a checkmark by the **Limits Pane**.



Disk Space

Used: 10

Units: KB

Limit: 50

Create a limit:

With the Limits Pane visible use the slider bar or the text box labeled **Limit** to set a limit, or type in a specific disk limit to the disk limit text box. You can choose to display the available and limited disk space in Bytes, Kilobytes, or Megabytes.

Note: The minimum limit for Disk Space is the amount the Application Under Test is currently using.

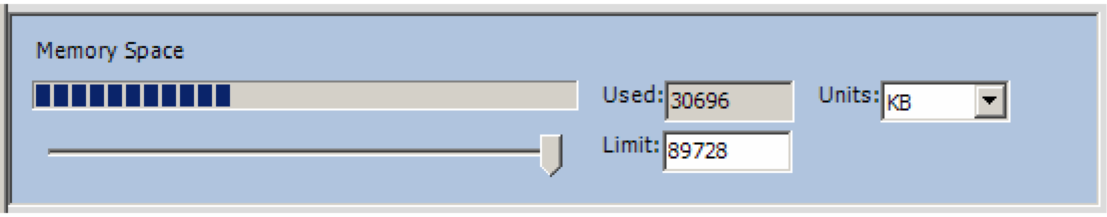
Remove a limit:
To remove a limit, simply slide the slider bar all the way to the right, or delete the node in the project pane.

How Limits and Resources are calculated:
The amount used is updated through the monitor of API calls that allocate disk space. The total disk space amount is then incremented by the allocation request amount in these API calls. Before each request for disk space is permitted, Holodeck checks to ensure the amount being allocated is below the set limit. If the Application Under Test goes above the limit the API call requesting disk space is failed. If a file is moved and the size is smaller than the original file size the amount used is decremented and the limit won't fire. Holodeck uses win32 API's to get the max disk space available. Percent used is calculated using the disk space used through the API calls and the max disk space available. When a limit is set the max disk space available is artificially reduced and the progress bar is recalculated (percentage of limit, instead of percentage of hardware capacity).

Creating a Memory Space limit

This limits the amount of Memory space available to the Application Under Test. Test the Application Under Test's ability to function under low memory conditions using memory limits.

Open the limits pane by clicking **View** and making sure there is a checkmark by the **Limits Pane**.



Memory Space

Used: 30696

Units: KB

Limit: 89728

Create a limit:

With the Limits Pane visible use the slider bar or the text box labeled **Limit** to set a limit, or type in a specific memory amount. You can choose to display the available and limited memory space in Bytes, Kilobytes, or Megabytes.

Note: The minimum limit for Memory Space is the amount the Application Under Test is currently using.

Remove a limit:

To remove a limit, simply slide the slider bar all the way to the right, or delete the node in the project pane.

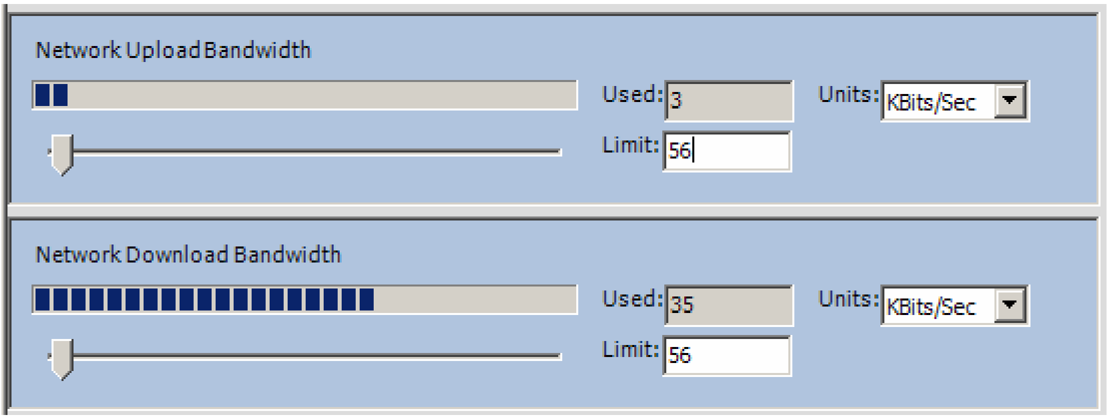
How Limits and Resources are calculated:

The amount used is updated through the monitor of API calls that allocate memory. The total memory amount is then incremented by the allocation request amount in these API calls. Before each request for memory is permitted, Holodeck checks to ensure the amount being allocated is below the set limit. If the Application Under Test goes above the limit the API call requesting memory is failed. Holodeck uses win32 API's to get the max memory available. Percent used is calculated using the memory used through the API calls and the max disk space available. When a limit is set the max memory available is artificially reduced and the progress bar is recalculated (percentage of limit, instead of percentage of hardware capacity).

Creating a Network Bandwidth limit

This feature is useful for network dependent applications; simulate any network connection speed, or completely stop your network connection for a moment to see if the Application Under Test can recover. You can have different upload and download limits in a single project by changing either the Network Upload Bandwidth or the Network Download Bandwidth.

Open the limits pane by clicking **View** and making sure there is a checkmark by the **Limits Pane.**



Network Upload Bandwidth

Used: 3

Units: KBits/Sec

Limit: 56

Network Download Bandwidth

Used: 35

Units: KBits/Sec

Limit: 56

Create a limit:

With the Limits Pane visible use the slider bar or the text box labeled **Limit** to set a limit, or type in a specific network speed. For greater precision you can choose between Bytes, Kilobytes, and Megabytes per second.

Remove a limit:

To remove a limit, slide the slider bar all the way to the right, or delete the limit node from the project pane.

How Network Limits work:

Holodeck intercepts all Winsock APIs, among which are functions which send and receive network data. By buffering the incoming and outgoing data Holodeck is capable of limiting the speed of the network to a user specified value. If this specified value for speed is greater than what a network connection can handle, the network speed will automatically be set to the maximum speed which the connection is capable of handling.

note: upload and download limits work for all stream based sockets.

Creating Faults

Faults Overview

Faults are preset error conditions that will help you test your application easily. There are six categories including one to create your own faults to test your application specifically. Faults set and fail an array of tests that simulate common errors.

For instance, the "File Not Found" fault fails all calls that have to do with copying, deleting, moving, replacing, searching, opening and operations having to do with attributes for files. These faults simulate the same errors the operating system would throw.

Adding and Removing a fault – Learn each of the ways to add and remove faults.

Adding custom faults – Holodeck allows you to create your own faults, learn how to create faults focused to fail a set of API functions you specify.

Types of faults – a list of the types of faults and a description of each category.

Adding and Removing a fault

To add a fault simply select the fault in the faults pane.

1) Click the Create new Fault button on the Project Toolbar or right click one of the fault nodes in the Project pane and select Add New Fault

2) With the Faults pane visible select up to one fault from each category.

You can remove a fault by either:
1) Right clicking the fault in the **Project pane**, under **Faults** and selecting **Delete Fault**
2) Selecting **No Disk Faults, No Memory Faults, or No Network Faults** in the **Faults pane.**

Adding custom faults

You can create your own faults to fail a specific set of API functions simply by editing the faults.xml file located in the function_db folder within the Holodeck install folder (default: C:\Program Files\Security Innovation\Holodeck Enterprise Edition\function_db).

Open faults.xml in a text or XML editor, and within the beginning and ending <Faults> tag insert your custom fault as follows.

Example:

This XML snippet, when added to faults.xml will create a fault named "My Fault"

```
<Fault Name="My_Fault " Type="Disk" ReturnValue="0" ErrorCode="112">
    <Function Name="CopyFileA" Allocation="GT">
     <CheckResource ParamIndex="1" Exists="2"/>
     <MatchParams>
       <MatchParam Name="bFailIfExists" TestOperator="=" TestValue="1"
              CompareAsType="3" ID="2"/>
     </MatchParams>

    </Function>

</Fault>
```

The fault name will show up in the faults pane as "My Fault" under the disk column, Holodeck converts underscores ‘_’ to spaces.
Unless the function tag overrides the setting, all function in this fault will use a returnValue of 0 and an ErrorCode of 112

Each function to be failed has to have it’s own <Function> tag, to have this function fail under every circumstance simply use the closed tag form (<Function Name="CopyFileB" />)
In this case the function to be failed is the "CopyFileA" API function, and will only fire when this function tries to allocate more space than it had originally had.

The CheckResource tag checks to see if the resource with handle 1 does not exist.

The MatchParams tag allows you to only fire when certain parameters are matched. In this case this test will only fire if the parameter named bFailIfExists matches the test value, 1, exactly. Holodeck will compare the actual value and the TestValue as a Boolean. ID is the zero based index of the parameter to match.

<Fault> tag – the main tag for the custom fault

Attribute	Description	Example	Required

Name	The Name of your custom fault	My_Custom_Fault	Required
Type	Which category this will show up. Valid values are: Disk, Memory, Network, Registry, Process, Custom	Custom	Required
ReturnValue	The value to return when the API call is failed	0	Required
ErrorCode	The error code to set using the setlasterror system call	8	Required

<Function> tag – the individual function to fail

Attribute	Description	Example	Required
Name	The Name of the API function to fail	LoadLibraryA	Required
OverrideErrorCode	You can override the error code implied from the parent fault tag by setting the code here	8	Implied
OverrideReturnValue	You can override the return value implied from the parent fault tag by setting the return value here	0	Implied
PassThrough	If PassThrough is set to true the actual API function will be called and Holodeck will use that return value, instead of the error value specified in the fault element. Valid Values are: True, False	True	Implied
Exception	While using .net function calls it might be necessary to specify an exception code to be set	3221225495	Implied
Allocation	The amount of memory or disk use caused by this call. Valid Values are: • GT – only fire if disk or mem usage increases by this call • LT – only fire if disk or mem usage decreases by this call • GTE – only fire if disk or mem usage increases or is unchanged • LTE – only fire if disk or mem usage decreases or is unchanged	GT	Implied

	• E – only fire if disk or mem usage unchanged		

<MatchParams> tag – Fire the test if all the attributes match the api call.

Attribute	Description	Example	Required
Name	The Name of the parameter to match	lpFileName	Required
TestOperator	How the test value will be compared to the incoming parameter value. Valid values are: • = – test value matches param value exactly • != – test value does not match param value • < – test value is less than the param value • > – test value is greater than the param value • <= – test value is less than or equal to the param value • >= - test value is greater than or equal to the param value • starts with – A string parameter starts with the test value • ends with – a string parameter ends with the test value • contains – a string parameter contains the test value (could also start or end with the value) • not contains – a string parameter does not contain the test value • binary contains – a binary flag parameter has OR’d test test value in • binary not contains – a binary flag parameter hasn’t OR’d the test value in • =resource – a path or handle	not contains	Required

	parameter represents the test value resource path • !=resource – a path or handle parameter does not represent the test value resource path • contains resource – a path or handle value contains the test value resource path • not contains resource – a path or handle value does not contain the test value resource path • starts with resource path – a path or handle value represents a resource path that starts with the test value resource path		
TestValue	The value to compare. All characters except ‘(‘, ‘)’, ‘{‘, ‘}’, ‘$’, ‘\’, ‘?’, ‘/’, ‘.’, ‘*’, ‘+’, ‘^’, and ‘|’ can be used normally. To use these characters you must precede that character with the ‘\’ character.	"\\."	Required
CompareAsType	The type of the test value to compare: Valid Values: 0 - NullType 1 - StringType 2 - WideStringType 3 - BooleanType 4 - IntegerType 5 - UnsignedLongType 6 - RealType 7 - PointerType 8 - PointerPointerType 9 - Integer64Type 10 -OutStringType 11 -OutWideStringType	1	Required

	12 -IgnoreType		
ID	The zero based index of the parameter to match.	0	Required

<CheckResource> tag - check for a resource existence or non-existence before firing the test

Attribute	Description	Example	Required
ParamIndex	The index of the parameter that represents the resource to check. Could be a handle or a string resource path.	0	Required
Exists	• 1 – only fire if the resource exists • 2 – only fire if the resource doesn’t exist • 3 – fire if the resource doesn’t exist then create it	1	Required

Types of faults

Types of Faults
1) **Disk Faults** – These faults include faults that have to do with Hard Drive and File I/O corruption Corrupt Structure.
2) **Memory Faults** – These faults are thrown when the operating systems has problems looking up objects in memory Page file too small.
3) **Network Faults** – Network faults can be anything from a wrong version of Winsock, to the Network is completely disconnected.
4) **Registry Faults** – manipulate how your application is able to read and write registry values.
5) **Process/Library Faults** – Process and Library faults can be very helpful while testing process manipulation, you can also remove access to important libraries using these faults.
6) **Custom Faults** – Custom faults, as set in the Faults.xml file will be listed here.

Holodeck sets all the error conditions the operating system would set if the API actually failed.

Fault Categories

Disk Faults

Faults that are common to storage media, such as the Hard Drive, Flash media, Optical etc.

Too Many Open Files – Any attempts to open, create, or find a file will be failed; sets the error code 4, Error too many open files, on return.

File Not Found – Any attempts to copy, create, delete move, replace, find, open or get/change file attributes are failed in this fault; sets the error code 2, Error File Not Found, on return.

File Locked – Any attempt to access the file for any reason is failed; sets the error code 33, Error Lock Violation, on return.

File Is Read Only – Fails copy, create, delete, move, replace, write, or change attributes on the file; sets the error code 6009, Error File Read Only, on return.

File In Use – Functions copy, create, delete, move, replace open and setting file attributes are failed; sets the error code 32, Error Sharing Violation, on return.

File Cannot Be Created – Any attempts to create a file, including copying, moving, and replacing files are failed; sets the error code 82, Error Cannot Make, on return.

File Already Exists – Fails attempts to copy, move, or create a file which manipulates the filename; sets the error code 183, Error Already Exists, on return.

Drive Cannot Seek Disk – Fails any attempts to access or modify any file for any reason; sets the error code 25, Error Seek, on return.

Disk Full – Fails attempts to allocate more space on the disk, this includes copying, creating, replacing, and writing files; sets the error code 112, Error Disk Full, on return.

Data Error – Fails any attempt to access any file for any reason; sets the error code 23, Error CRC, on return.

Corrupt Structure - Any attempt to access any file for any reason is failed; sets the error code 23, Error CRC, on return.

Cannot Remove Directory – Fails calls to RemoveDirectoryA and RemoveDirectoryW; sets the error code 16, Error Current Directory, on return.

Access Denied To File – Any attempt to access any file for any reason is failed; sets the error code 5, Error Access Denied, on return.

Note: some individual functions use override values for error codes and return values, for more information see the faults.xml file located in <Holodeck Enterprise Edition Install Path>\function_db\faults.xml

Memory Faults

Memory Faults are faults focused to simulate failures in system memory, these faults extend to virtual memory.

Segment Locked – Calls to functions freeing, allocating, or discarding are failed; sets the error code 212, Error Locked, on return.

Page File Too Small – Attempts to allocate more memory are failed; sets the error code 1454, Error Pagefile Quota, on return.

Invalid Address – Calls to functions that free or allocate virtual memory or map user pages are failed; sets the error code 487, Error Invalid Address, on return.

Invalid Access – Attempts to access or allocate memory are failed; sets the error code 998, Error No Access, on return.

Insufficient Memory – Calls to functions that allocate more memory are failed, this also includes functions that reallocate a greater amount of memory than was previously specified; sets the error code 8, Error Not Enough Memory, on return.

Note: some individual functions use override values for error codes and return values, for more information see the faults.xml file located in <Holodeck Enterprise Edition Install Path>\function_db\faults.xml

Network Faults

Network faults help simulate failures that are common to network protocols. These include faults that might happen physically, as well as software problems.

Network Disconnected – Fails calls that attempts to connect, send and receive on the network; sets the error code 10050, WSA net Down, on return.

Network Not Installed = Fails all calls to WSAStartup; sets the error code 10091, WSA system not ready, on return.

Wrong Version of Winsock - Fails all calls to WSAStartup; sets the error code 10092, WSA Version not supported, on return.

Winsock Task Limit Reached - Fails all calls to WSAStartup; sets the error code 10067, WSA procedure limit, on return.

No Ports Available – Fails calls to bind, connect, and WSAConnect; sets the error code 10048, WSA address in use, on return.

Network Down – Fails any calls to any API having to do with the network; sets the error code 10050, WSA net down, on return.

Note: some individual functions use override values for error codes and return values, for more information see the faults.xml file located in <Holodeck Enterprise Edition Install Path>\function_db\faults.xml

Registry Faults

Registry Faults simulate failures common to registry values. These faults can be applied without running the risk of corrupting of deleting registry values.

Value Not Found – Attempts to delete or query registry values are failed; sets the error code 0, Error Success, on return and returns 2 as the return value.

Value Cannot Be Written – Any attempt to write (set) a registry value is failed; sets the error code 0, Error Success, on return and returns 1013 as the return value.

Value Cannot Be Read – Any attempt to read a registry value is failed, this includes enumerating and querying registry values; sets the error code 0, Error Success, on return and returns 1012 as the return value.

Registry Is Corrupt – Any attempt to access a registry key for any reason is failed; sets the error code 0, Error Success, on return and returns 1015 as the return value.

Query Buffer Too Small – Attempts to query a registry value are failed; sets the error code 0, Error Success, on return and returns 234 as the return value.

No More Query Items – Functions trying to enumerate registry values are failed; sets the error code 0, Error Success, on return and returns 259 as the return value.

No Log Space – All attempts to access a registry key for any reason are failed; sets the error code 0, Error Success, on return and returns 1019 as the return value.

Key Not Found – Calls to functions that delete, open, replace, restore or unload a registry value are failed; sets the error code 0, Error Success, on return and returns 2 as the return value.

Key Marked For Deletion – Attempts to delete, enumerate, flush, query, save, set or get the registry key's security is failed; sets the error code 0, Error Success, on return and returns 1018 as the return value.

Key Is Corrupt – Any attempt to access a registry key for any reason is failed; sets the error code 0, Error Success, on return and returns 1010 as the return value.

Key Cannot Be Opened – Attempts to create, enumerate, open, query, save or set registry values are failed; sets the error code 0, Error Success, on return and returns 1011 as the return value.

IO Operation Failed – Attempts to load, restore, save and unload registry keys are failed; sets the error code 0, Error Success, on return and returns 1016 as the return value.

Access Denied – Any attempt to access a registry key for any reason is failed; sets the error code 0, Error Success, on return and returns 5 as the return value.

Note: some individual functions use override values for error codes and return values, for more information see the faults.xml file located in <Holodeck Enterprise Edition Install Path>\function_db\faults.xml

Process/Library Faults

Faults of the Process/Library type are failures in loading external processes and libraries.

Process File Not Found – Calls to functions trying to load a library, create a process or load a module are failed; sets the error code 2, Error File Not Found, on return and returns 0 as the return value.

Not Enough Resources – Calls to functions trying to load a library, create a process or load a module are failed; sets the error code 8, Error Not Enough Memory, on return and returns 0 as the return value.

Invalid File Type – Calls to functions trying to load a library are failed and use the error code 126, Error Mod Not Found, and return a value of 1, functions trying to create a process, or load a module are failed and use a return value of 0 and an error code of 193.

Access Denied - Calls to functions trying to load a library, create a process or load a module are failed; sets the error code 5, Error Access Denied, on return and returns 0 as the return value.

Note: some individual functions use override values for error codes and return values, for more information see the faults.xml file located in <Holodeck Enterprise Edition Install Path>\function_db\faults.xml

Custom Faults

Any faults of the type Custom or that are unrecognizable to Holodeck will be listed in this column.

COM Object Does Not Exist – Fails CoCreateInstance and CoCreateInstanceEx with a return value of 2147746132 and error code of 0, Error Success. Fails OleCreate, and OleCreateEx with a return value of 2147942414 and error code 0, Error Success.

Refer to the Adding custom faults section for more information on adding your own faults.

Resource Faults

Resource Fault Overview

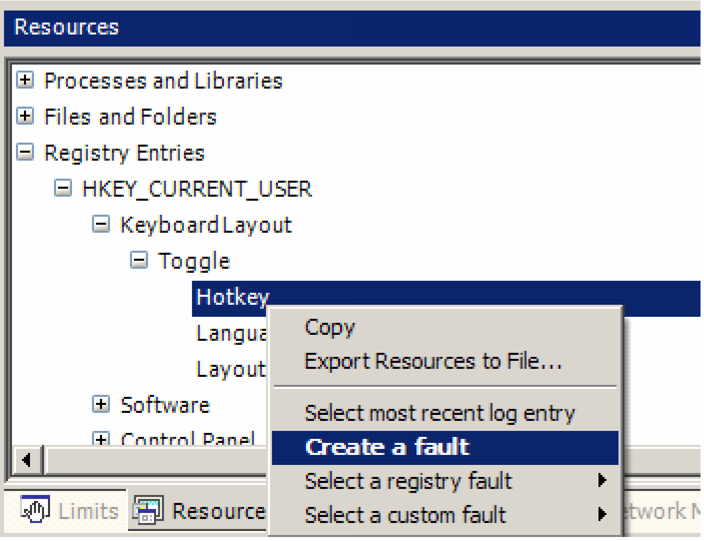
Resource faults are faults that are focused on a single Process, Library, Files, Folders, and Registry Entries. Holodeck allows you to create many different types of faults that are related to errors that commonly happen with each category of resource.

Adding and Removing a Resource Fault – Learn how to add or remove a resource fault.

Create a New Resource Fault Wizard – The resource fault wizard helps you create a Resource Fault.

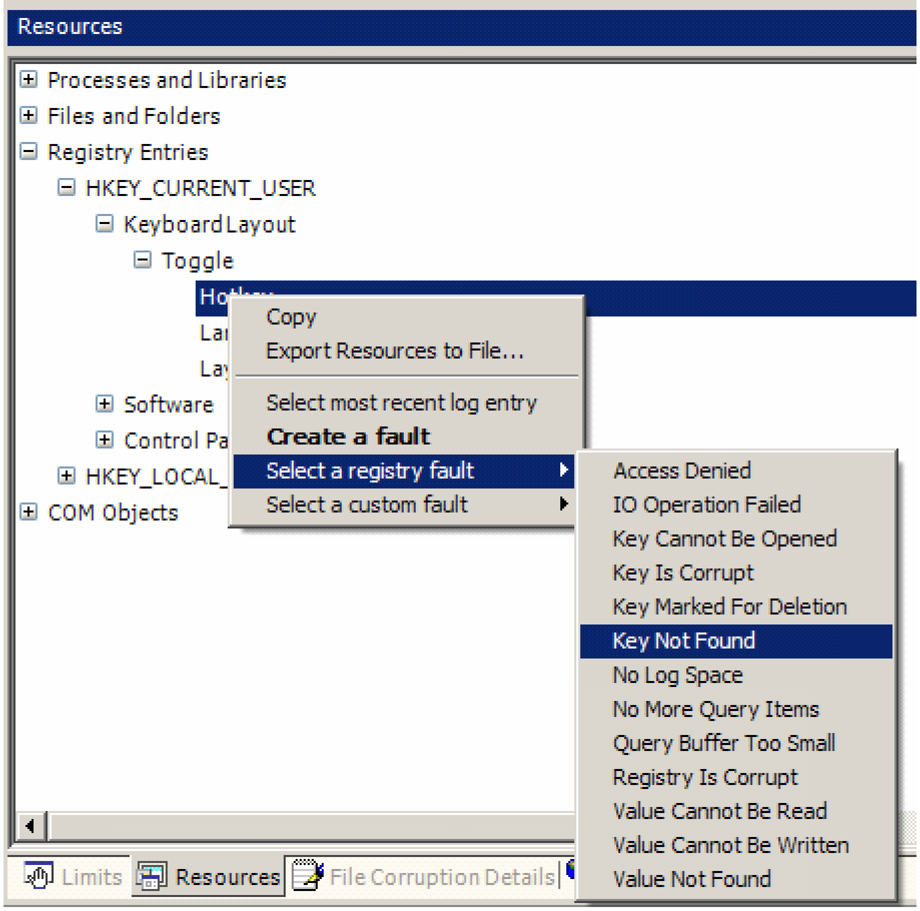
Adding and Removing a Resource Fault

A resource fault can be added by either selecting Application > Create a new Resource Fault… or by finding the resource in the resource pane, right-clicking and selecting "Create a Fault." You can also set a resource fault by right clicking the Resource Fault Node in the Project Pane and selecting "Create a Resource Fault." Once a Resource Fault has been set that resource will be displayed in red text.



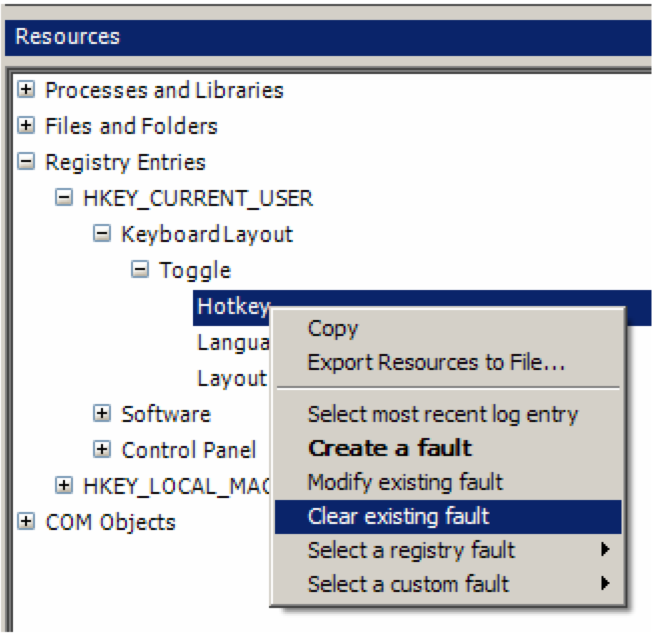
If you create the fault by the later method the Create a New Resource Fault wizard will have the correct resource already selected, otherwise you will have to find the correct resource in the resource tree on the first page of the wizard.

You can quickly set Resource faults without having to go through the Resource Fault Wizard by finding the correct resource, right-clicking and selecting "Select a Fault > Fault Name." This will set the fault immediately.

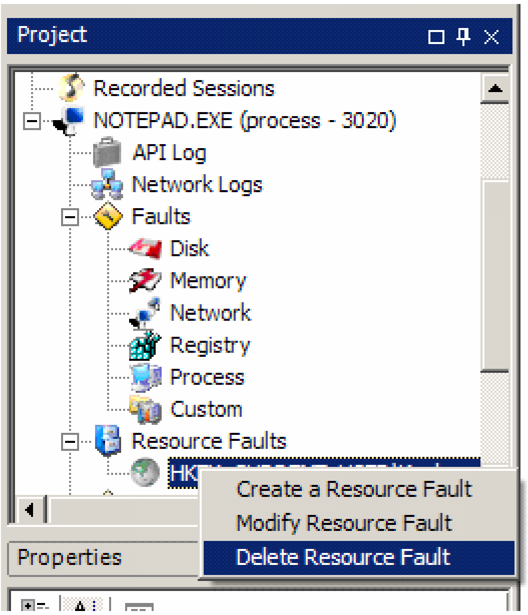


To remove a Resource fault:

Find the resource in the Resource Pane right-click and select "Clear Existing Fault"

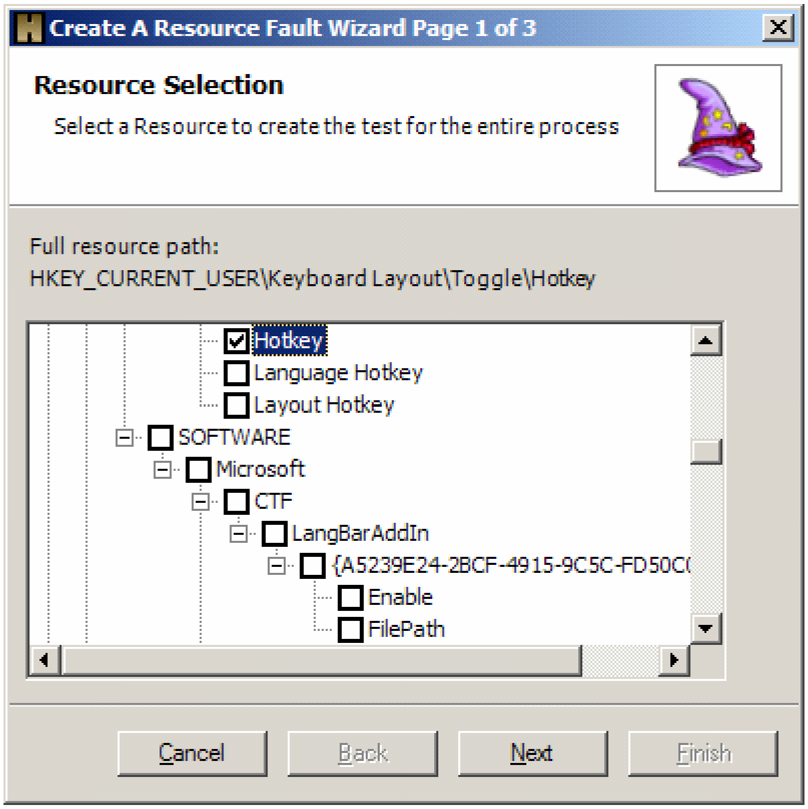


Or right-click the fault in the Project pane under the Resource Faults Node and select "Delete Resource Fault"



Create a New Resource Fault Wizard

The first page of the Create a New Resource Fault Wizard allows you to select which resource you would like to set a fault for. You can select more than one of the same type of Resource; multiple selections between categories (e.g. registry and process) are not allowed.



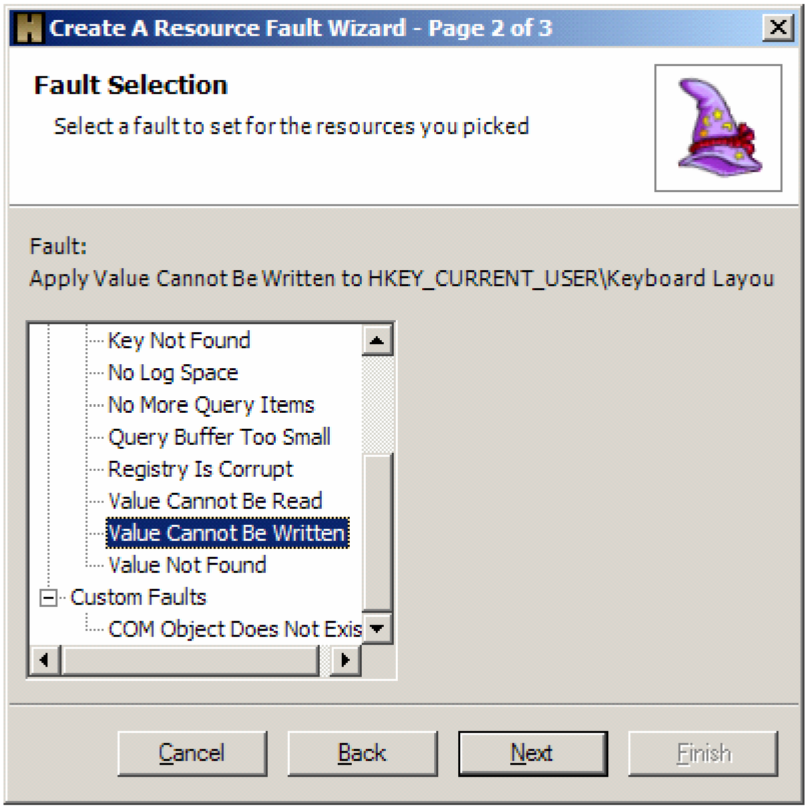
Resource Selection

Select a Resource to create the test for the entire process

Full resource path:
HKEY_CURRENT_USER\Keyboard Layout\Toggle\Hotkey

☑ Hotkey
□ Language Hotkey
□ Layout Hotkey
□ SOFTWARE
□ Microsoft
□ CTF
□ LangBarAddIn
□ {A5239E24-2BCF-4915-9C5C-FD50C(
□ Enable
□ FilePath

The second page shows only the Resource Faults that are allowed for the category of fault you have selected. Custom Resource Faults will also be shown, only one fault may be selected.



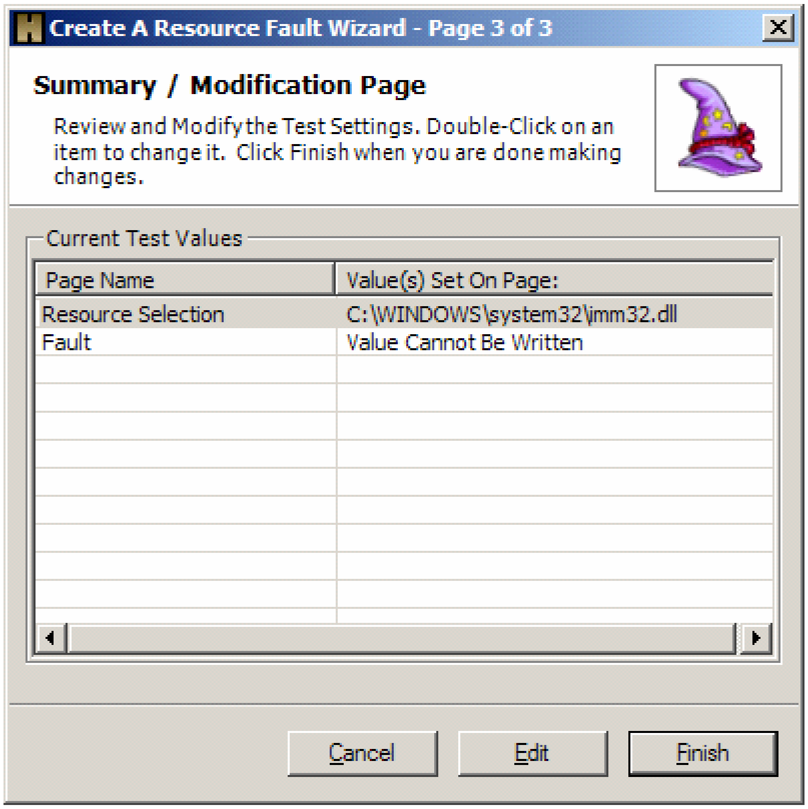
Fault Selection

Select a fault to set for the resources you picked

Fault:
Apply Value Cannot Be Written to HKEY_CURRENT_USER\Keyboard Layou

- Key Not Found
- No Log Space
- No More Query Items
- Query Buffer Too Small
- Registry Is Corrupt
- Value Cannot Be Read
- Value Cannot Be Written
- Value Not Found
- Custom Faults
  - COM Object Does Not Exis

The final page is a summary page, you can return to either page quickly by selecting the Page Name and clicking edit. This will return you to the page that value was set on, so you can edit it.



Summary / Modification Page

Review and Modify the Test Settings. Double-Click on an item to change it. Click Finish when you are done making changes.

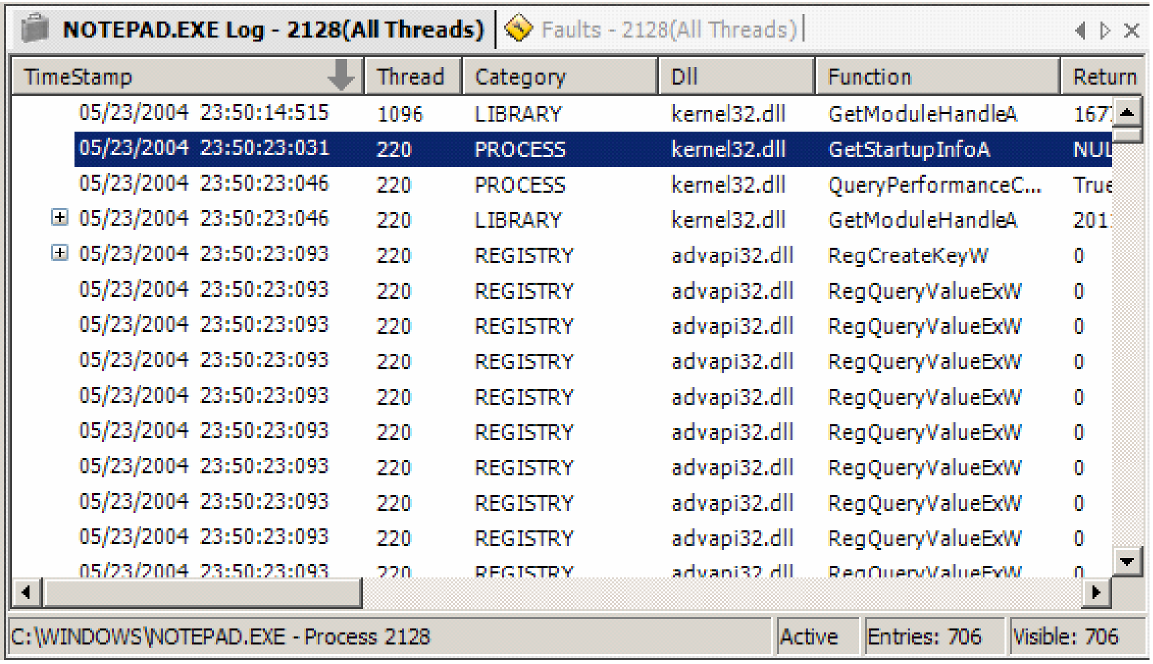
Current Test Values

Page Name	Value(s) Set On Page:
Resource Selection	C:\WINDOWS\system32\imm32.dll
Fault	Value Cannot Be Written

Working with Logs

Logs Overview

As soon as you begin the Application Under Test Holodeck will start to log the API calls you have selected. The log pane will hold any logs you are currently viewing. Logs can be filtered, sorted, or exported to make working with the data Holodeck provides as easy as possible.



NOTEPAD.EXE Log - 2128(All Threads) | Faults - 2128(All Threads)

TimeStamp	Thread	Category	Dll	Function	Return
05/23/2004 23:50:14:515	1096	LIBRARY	kernel32.dll	GetModuleHandleA	167
05/23/2004 23:50:23:031	220	PROCESS	kernel32.dll	GetStartupInfoA	NUL
05/23/2004 23:50:23:046	220	PROCESS	kernel32.dll	QueryPerformanceC...	True
⊞ 05/23/2004 23:50:23:046	220	LIBRARY	kernel32.dll	GetModuleHandleA	201
⊞ 05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegCreateKeyW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0
05/23/2004 23:50:23:093	220	REGISTRY	advapi32.dll	RegQueryValueExW	0

C:\WINDOWS\NOTEPAD.EXE - Process 2128 | Active | Entries: 706 | Visible: 706

For more information on working with the log files Holodeck creates see the following help topics:
Log Categories – a complete list of the Log Categories, and an explanation.

Custom Log Filtering and Sorting – You can sort and filter log files without affecting which functions are intercepted and logged.

To find text in the log files – Find specific text within the API function Logs

Changing which functions are logged – Change which API functions are intercepted and logged.

Exporting logs – Export log files to easy to parse Excel Comma Separated Value File (csv)

Printing Logs – Holodeck can print the API logs for

Exporting Resource Logs – Export a complete list of the resources your application has accessed.

Network Logs – Holodeck intercepts and logs each Network Packet, view the Network Logs for information regarding Network Packets.

Log Categories

TimeStamp – This is the precise time in which Holodeck logged the API call the format of this category is Month/Day/Year Hour:Minute:Second:Milisecond.

Thread – If the Application Under Test has multiple threads they will show up here, by thread number.

Category – This is the main category of the API call, Categories include:
COM – API functions included in the COM (Common Object Model)
FILE – API functions having to do with file manipulation such as: file attributes, disk space, file size, creating and deleting files, etc.
LIBRARY – API functions having to do with library functions such as: loading libraries and getting module handles.
MISCELLANEOUS – API functions that don't fit into any other category.
MEMORY – API functions having to do with Memory calls such as: LocalAlloc, LocalFree, HeapSize etc.
NETWORK –API functions having to do with Network calls including socket manipulation and sending and receiving calls.
PROCESS – Includes thread and process specific function calls including CreateThread, and GetStartupInfoA
REGISTRY – Registry Specific API calls are contained in this category, including Opening, Querying, Closing and others.
DANGEROUS – These are dangerous APIs as listed in the Writing Secure Code Book.

DLL – This column shows which .dll the intercepted API is located in.

Function – This shows which API calls the Application Under Test has called. The next few columns are information about that function call.

Return Value - The value returned from the function called, often these return values will be memory addresses, but more useful information might be looking for 1’s or 0’s (representing the call was made successfully or unsuccessfully) or values smaller than a memory address (actually useful return values)

Error Code – This column shows the error code returned by the API function. This is not set by all functions, some use return values to give staus. Error Code List

Exception – If the function raised an exception it will show up in this column, this only applies while testing .net applications. Exception List

List of Parameters – These columns contains all the out parameter values.

Custom Log Filtering and Sorting

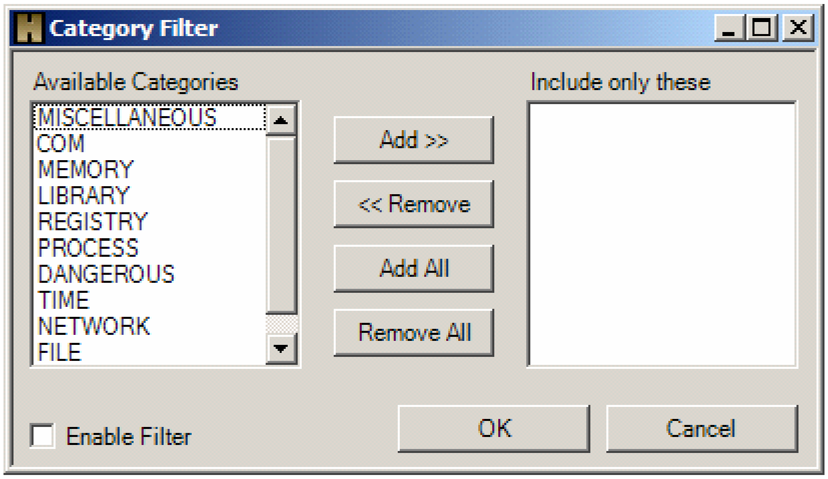
Each log view can be filtered and sorted based on each header column. Filtering a log does not affect which API calls are logged; it simply changes the view in the current log pane. The log pane is, by default, sorted by the timestamp of the API call. This can be changed to sort on any column.

To filter on a column:

1) Right-click the column to filter on.

2) Select Custom Filter…

3) The following shows up for Category filtering



4) Select which categories to include and click OK.

Enable filter will automatically be selected. If a column has a filter set the column text will be shown in blue.

To remove a filter reselect Custom Filter… from the log column and uncheck "Enable Filter"

To sort a column:

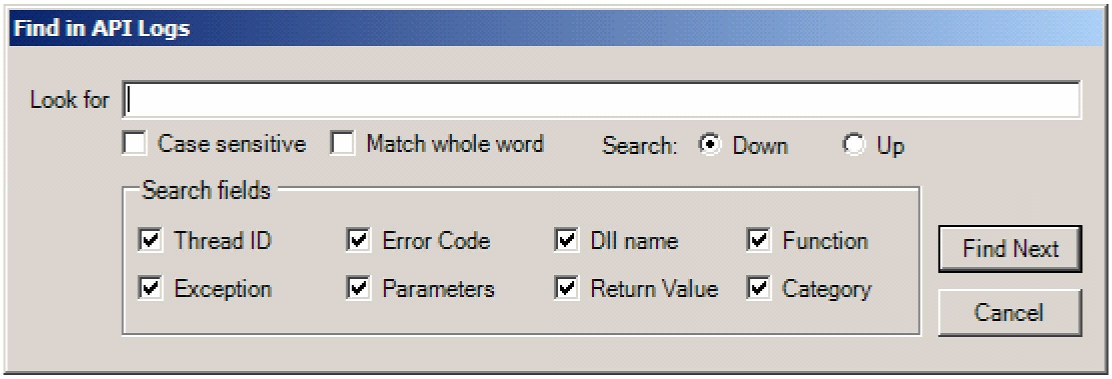
Clicking the column header once sorts the column in ascending order; clicking the column again will sort the column in descending order.

The column the log file is currently is sorted by is represented by a grey arrow to the right of the column header.

Note: Function filters in the log pane only apply to top level nodes. For instance, if you filter out a function, it may still show as a child of some other function. This also means that if you filter a function that has unfiltered children, those children will never show in the log since the parent was filtered out. This does not apply if you change which functions are logged in this case the functions are never intercepted.

To find text in the log files

With the log pane open, either select Log > Find… or press Ctrl-f. This will bring up the "Find in API Logs" dialog box. This find field works similarly to most other find commands. You can select to only search on certain fields, or change case sensitivity. Matching the whole word will only return matches that the word stands alone for instance searching for "free" would match only cases of "free" but not "FreeLibrary"



Find in API Logs

Look for

□ Case sensitive □ Match whole word Search: ● Down ○ Up

Search fields

☑ Thread ID ☑ Error Code ☑ Dll name ☑ Function

☑ Exception ☑ Parameters ☑ Return Value ☑ Category

Changing which functions are logged

Enabling more API functions to be logged increases the number of tests available to you. Decreasing the number of API function logged increases Holodeck’s performance and uses less RAM.

To enable or disable APIs to be logged click Log > Functions Logged… from the menu.

Note: when a function is no longer being logged there is no way to intercept that function.

Exporting Logs

Holodeck can export a log file for external manipulation in an easy to parse Excel Comma Separated Value File. This can be helpful when trying to compare two different runs of the same application.

To export a log click File > Export Log to File…

Once the log file has been exported it can be easily manipulated by any spreadsheet program.

Exporting a log file will ignore any Autofilters and field settings you may have set during testing, the exported log file will contain all available data for the process you save.

Log files contain the following information for each log entry:

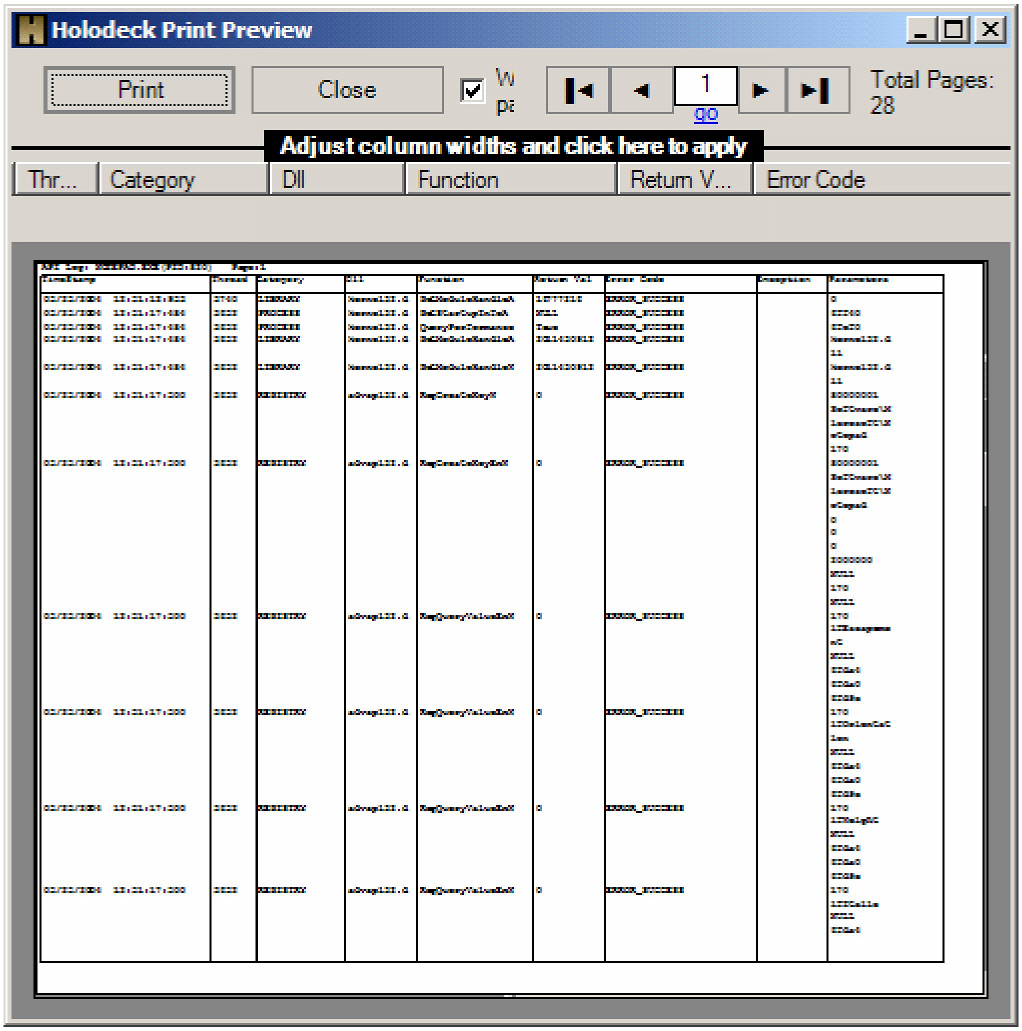
- Category
- DLL Name

- Error Code
- Function
- Parameters
- Return Value
- Time Stamp

For more information on these categories please see the Log Categories section.

Printing Logs

Holodeck allows you to print the complete list of API logs easily through the Print Preview Dialog (below). Preview individual pages using the forward and back buttons located at the top right of the window. Adjust columns widths by dragging the dividers of the column headers, after the column has been resized click the button above to apply the new column size settings.



Exporting Resource Logs

Holodeck can export a log file of all the resources your application uses. This is useful when comparing different builds, or to track resource usage changes.

To export the resource log click File > Export Resources to File…

Each log entry contains the following information:

- Type – The type of the resource, FILE, PROCESS, or REGISTRY
- Resource – The path to the resource.
- TimeStamp – The time when the Resource was last used.
- LastFunction – The last function to use this resource.
- ErrorCode – The Error Code set by the last function.

- ReturnValue – The return value returned by the last function.
- NumHits – The number of times this resource was touched by the application

Network Logs

Network logs are logs specific to data being sent and received over the network. These can be extremely powerful when trying to see exactly what data was sent over the network and how it was sent.

Network logs include information on each network message including:

TimeStamp – The time at which the message was sent or received.

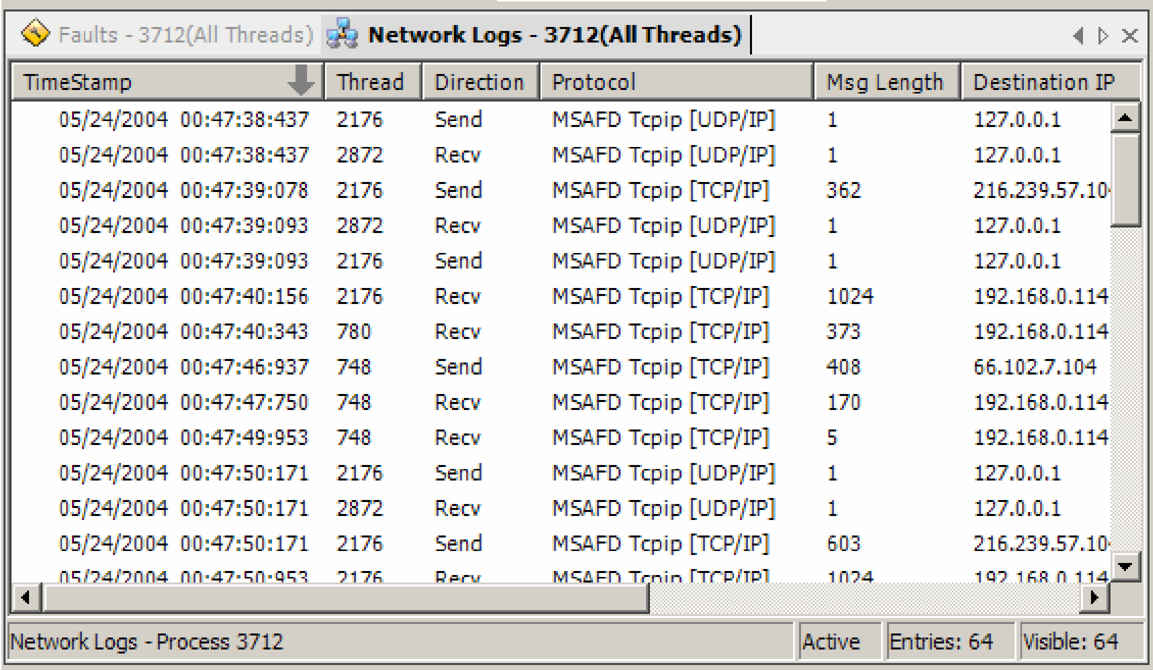
Thread – The thread number that called the API to send or receive the message.

Direction – If the message was sent or received.

Protocol – Which network protocol was used to communicate the message.

Msg Length – The complete message length in bytes.

Start of Msg – The first 8 bytes of the message


Faults - 3712(All Threads)
Network Logs - 3712(All Threads)
Network Logs - Process 3712
Active
Entries: 64
Visible: 64

TimeStamp	Thread	Direction	Protocol	Msg Length	Destination IP
05/24/2004 00:47:38:437	2176	Send	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:47:38:437	2872	Recv	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:47:39:078	2176	Send	MSAFD Tcpip [TCP/IP]	362	216.239.57.10
05/24/2004 00:47:39:093	2872	Recv	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:47:39:093	2176	Send	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:47:40:156	2176	Recv	MSAFD Tcpip [TCP/IP]	1024	192.168.0.114
05/24/2004 00:47:40:343	780	Recv	MSAFD Tcpip [TCP/IP]	373	192.168.0.114
05/24/2004 00:47:46:937	748	Send	MSAFD Tcpip [TCP/IP]	408	66.102.7.104
05/24/2004 00:47:47:750	748	Recv	MSAFD Tcpip [TCP/IP]	170	192.168.0.114
05/24/2004 00:47:49:953	748	Recv	MSAFD Tcpip [TCP/IP]	5	192.168.0.114
05/24/2004 00:47:50:171	2176	Send	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:47:50:171	2872	Recv	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:47:50:171	2176	Send	MSAFD Tcpip [TCP/IP]	603	216.239.57.10
05/24/2004 00:47:50:953	2176	Recv	MSAFD Tcpip [TCP/IP]	1024	192.168.0.114

To see the complete message highlight the network log entry and look at the Network message details. For more information on the Message Details see the Message Details Pane help item in the Holodeck Windows and Panes Section.

Export the network logs by right clicking any entry in the log and selecting Export Log to file, or click File >Export Logs to File… with the Network Logs Pane open.

Working with Reports

Reports Overview

Holodeck makes it easy to investigate application failures by organizing the logged API calls, Faults, Tests, Error Codes, Resource Dependencies, Resource Usage, and Return Values into easy to read pivot tables.

For more information regarding Holodeck's reporting feature see the following help topics:

Managing and Printing Reports

What's Contained in a Report

Working with Pivot Tables

Managing and Printing Reports

To create a report on all processes and threads in the current project right click the Reports node in the project pane and click Create a Report. This will create a report under the reports global node named Holodeck Report

Manipulating generated reports

To save a report Right-Click the report and click Save Report, this will allow you to save the report to a remote location to manipulate and compare different reports.

Note: If you create a report and want to share it with someone else you will need to send the html file plus its support files folder "reportname_files"

Renaming Reports do either:

1) To rename a report Right-Click the report and click Rename Report
2) Single click the name of the report you would like to rename.

Note: Rename a report before generating a new one to avoid overwriting the old report.

What's Contained in a Report

Each report Holodeck creates an easy to read summary of the log file created by the Application Under Test. This summary is displayed in a PivotTable which can be filtered, modified or manipulated however you see fit. The log summary is useful to see where the Application Under Test failed or which category of API calls are most frequently used.

API Log Summary Table - This report shows summary data for APIs logged by each process. Use this data to determine how many API calls were made for each category.

Faults Summary Table - This report shows summary data for the faults set for each process. Use this data to determine which faults were active at the time of report creation.

Tests Summary Table - This report shows summary data for the tests set for each process. Use this data to determine which tests were active at the time of report creation.

Error Codes Summary Table - This report shows summary data for the error codes set by APIs called from each process. Use this data to examine any API calls that set failure error codes.

Resource Dependencies Summary Table - This report summarizes the dependencies for each process. Use this data to see the number of dependencies as well as the number of times each dependency was touched. If you see a dependency with a very high hit-count this may be, or related to, a performance bug.

Resource Usage Summary Table - This report shows maximum and average resource usage for each process.

Return Values Summary Table - This report shows summary data for the values returned by APIs called from each process. Use this data to examine any API calls that returned failure error codes.

Working with Pivot Tables

The Holodeck report uses PivotTables which are interactive tables that quickly combine and compare large amounts of data. You can rotate its rows and columns to see different summaries of the data, and you can expand the details of the table to drill down on more important information.

You can drag irrelevant information out of the table to remove it from view. Filter the table views to show only pertinent information, by right clicking the table header and clicking AutoFilter. Sort your tables ascending or descending by right clicking the table header and clicking either Filter Ascending or descending.

Reorder your tables to view certain information near to one another by dragging and dropping entire rows from one place to the other, the PivotTable functionality will keep your information in order.

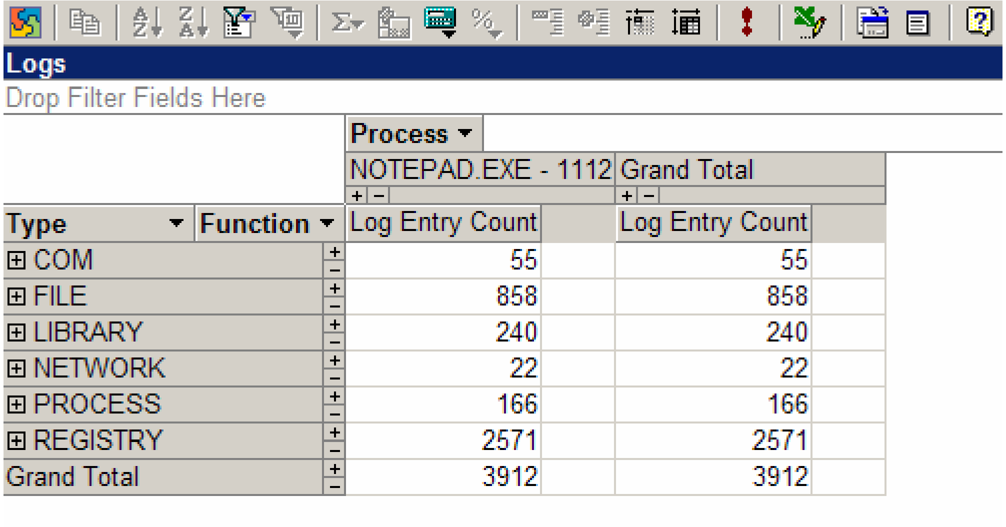
For more information about PivotTables please see this Microsoft Help Demo.

Reports Tables

API Log Summary Table

This report shows summary data for APIs logged by each process. Use this data to determine how many API calls were made for each category.

Drill down into each category to find which API calls failed, and a record of error codes, exceptions, return values and parameters.



Logs

Drop Filter Fields Here

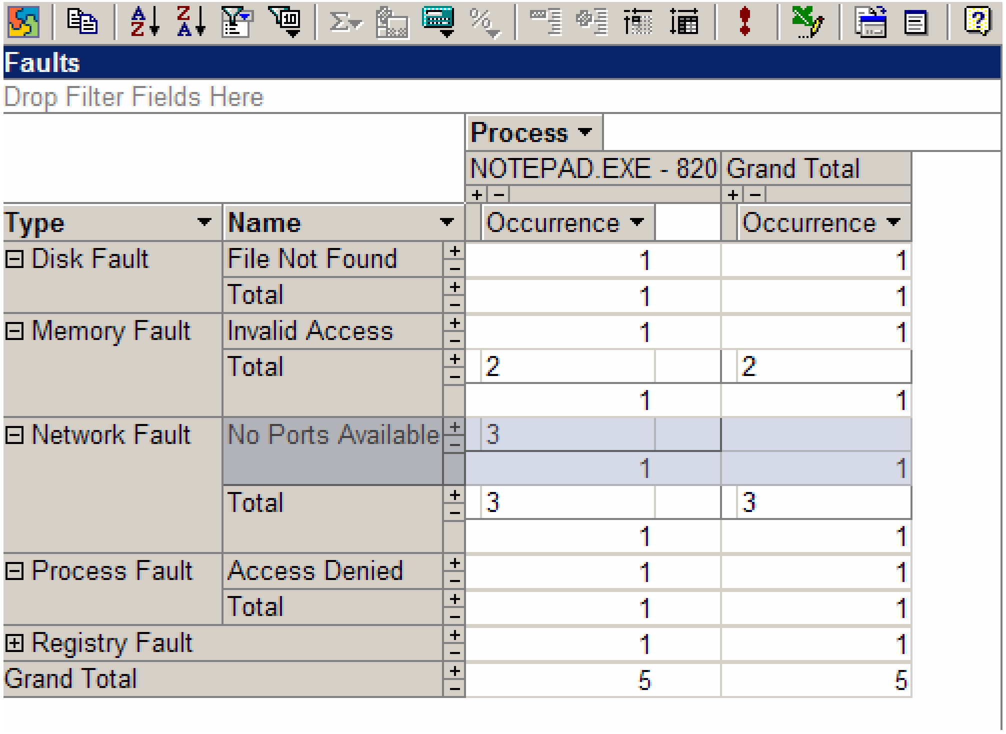
Process ▾

Type ▾	Function ▾	NOTEPAD.EXE - 1112 Log Entry Count	Grand Total Log Entry Count
⊞ COM		55	55
⊞ FILE		858	858
⊞ LIBRARY		240	240
⊞ NETWORK		22	22
⊞ PROCESS		166	166
⊞ REGISTRY		2571	2571
Grand Total		3912	3912

Faults Summary Table

This report shows summary data for the faults set for each process. Use this data to determine which faults were active at the time of report creation.

Expand fault types to find out which faults were set during the test.



Faults

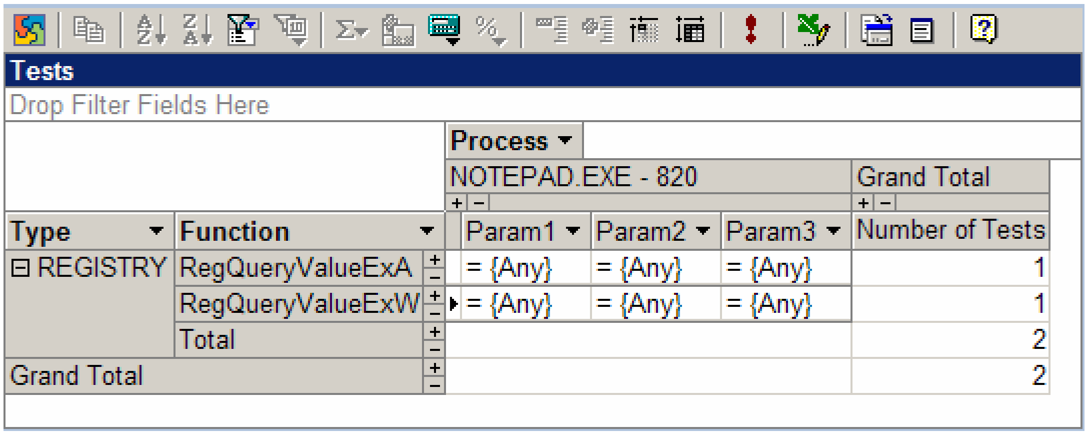
Drop Filter Fields Here

		Process	
		NOTEPAD.EXE - 820	Grand Total
Type	Name	Occurrence	Occurrence
⊟ Disk Fault	File Not Found	1	1
	Total	1	1
⊟ Memory Fault	Invalid Access	1	1
	Total	2 1	2 1
⊟ Network Fault	No Ports Available	3 1	 1
	Total	3 1	3 1
⊟ Process Fault	Access Denied	1	1
	Total	1	1
⊞ Registry Fault		1	1
Grand Total		5	5

Tests Summary Table

This report shows summary data for the tests set for each process. Use this data to determine which tests were active at the time of report creation.

Expand the type to find out which tests of each type were set in the test run. Expand the functions to find out the test details.



Tests

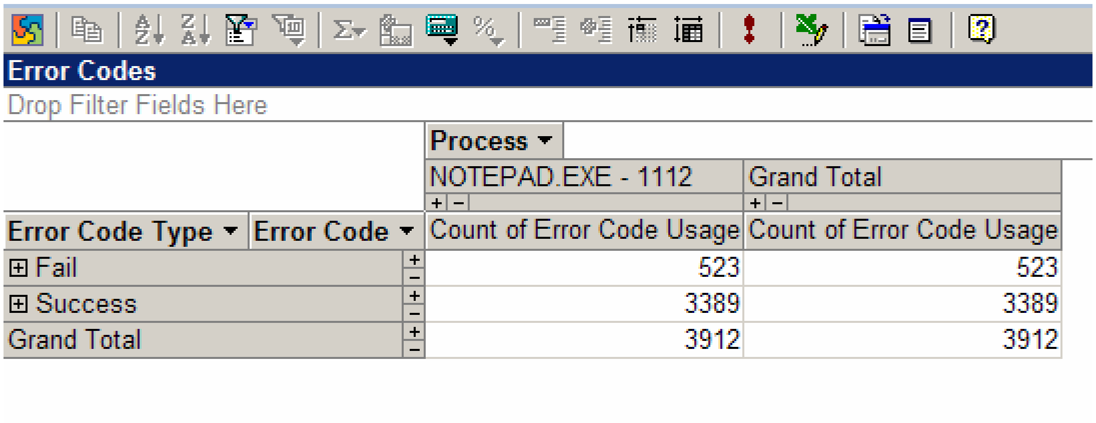
Drop Filter Fields Here

		Process			
		NOTEPAD.EXE - 820			Grand Total
Type	Function	Param1	Param2	Param3	Number of Tests
⊟ REGISTRY	RegQueryValueExA	= {Any}	= {Any}	= {Any}	1
	RegQueryValueExW	= {Any}	= {Any}	= {Any}	1
	Total				2
Grand Total					2

Error Codes Summary Table

This report shows summary data for the error codes set by APIs called from each process. Use this data to examine any API calls that set failure error codes.

Drill down into failure codes to find out why and when your application failed. Some failures are expected, but others may be unnoticed bugs.



Error Codes

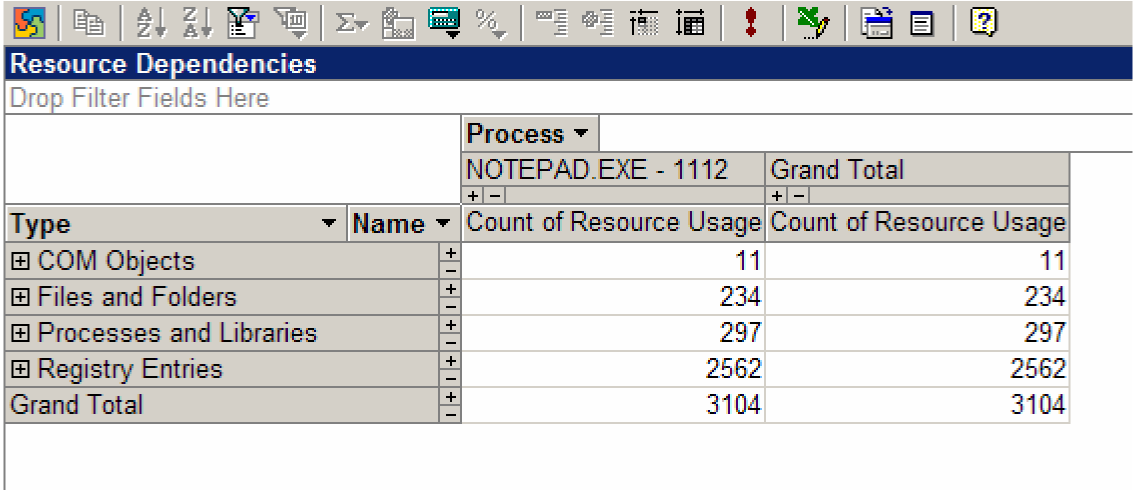
Drop Filter Fields Here

		Process	
		NOTEPAD.EXE - 1112	Grand Total
Error Code Type	Error Code	Count of Error Code Usage	Count of Error Code Usage
⊞ Fail		523	523
⊞ Success		3389	3389
Grand Total		3912	3912

Resource Dependencies Summary Table

This report summarizes the dependencies for each process. Use this data to see the number of dependencies as well as the number of times each dependency was touched. If you see a dependency with a very high hit-count this may be, or related to, a performance bug.

Investigate which resources your application uses the most. Some performance issues may be discovered if a resource is unnecessarily accessing a resource too many times.



Resource Dependencies

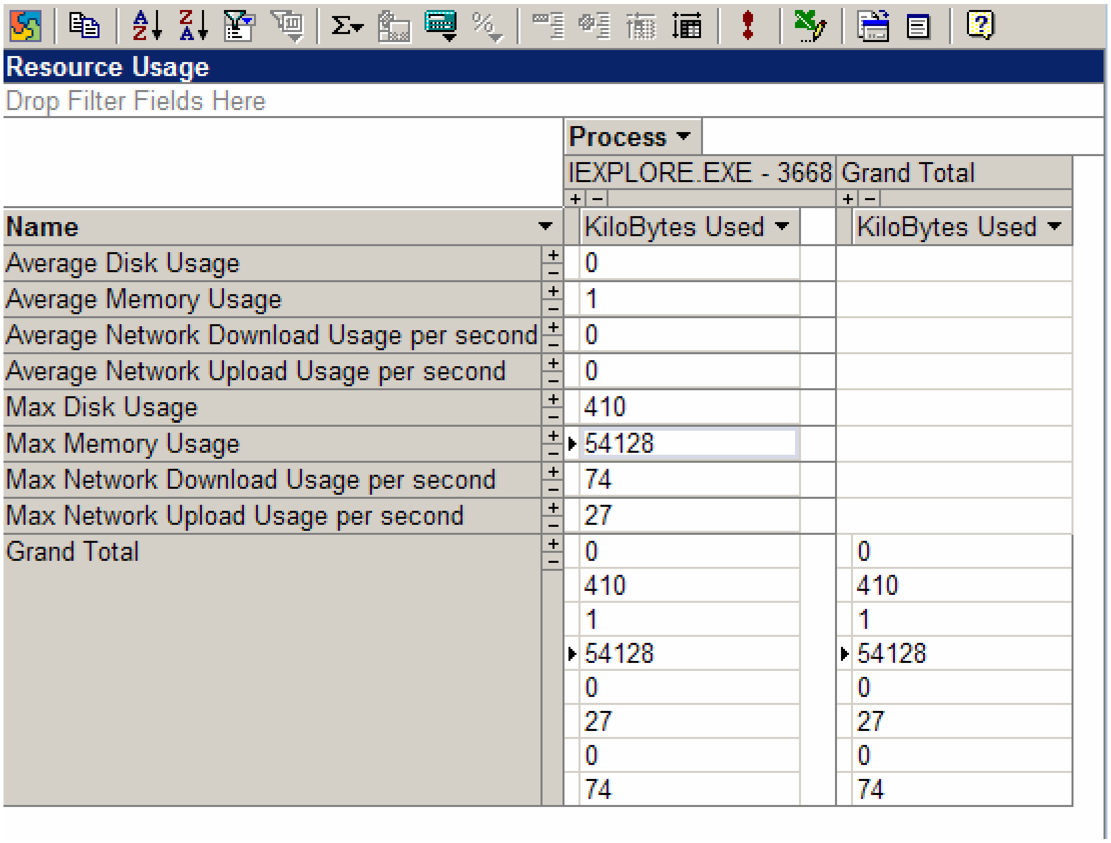
Drop Filter Fields Here

		Process	
		NOTEPAD.EXE - 1112	Grand Total
Type	Name	Count of Resource Usage	Count of Resource Usage
⊞ COM Objects		11	11
⊞ Files and Folders		234	234
⊞ Processes and Libraries		297	297
⊞ Registry Entries		2562	2562
Grand Total		3104	3104

Resource Usage Summary Table

This report shows maximum and average resource usage for each process.

Investigate which physical resources your application uses to find average and max disk, memory and network usage.



Resource Usage

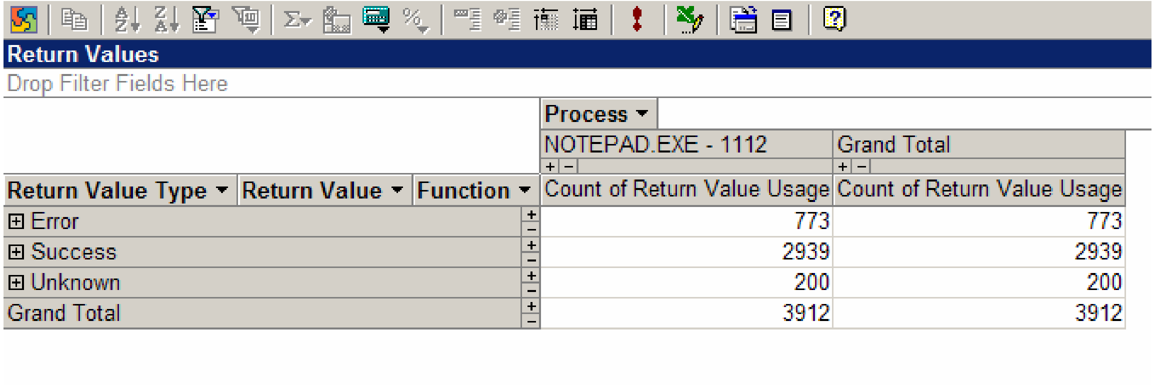
Drop Filter Fields Here

	Process	
	IEXPLORE.EXE - 3668	Grand Total
Name	KiloBytes Used	KiloBytes Used
Average Disk Usage	0	
Average Memory Usage	1	
Average Network Download Usage per second	0	
Average Network Upload Usage per second	0	
Max Disk Usage	410	
Max Memory Usage	54128	
Max Network Download Usage per second	74	
Max Network Upload Usage per second	27	
Grand Total	0 410 1 54128 0 27 0 74	0 410 1 54128 0 27 0 74

Return Values Summary Table

This report shows summary data for the values returned by APIs called from each process. Use this data to examine any API calls that returned failure error codes.

Many API functions use return values to report failures, use this in conjunction with the error codes to investigate unexpected failures.



Return Values

Drop Filter Fields Here

			Process	
			NOTEPAD.EXE - 1112	Grand Total
Return Value Type	Return Value	Function	Count of Return Value Usage	Count of Return Value Usage
⊞ Error			773	773
⊞ Success			2939	2939
⊞ Unknown			200	200
Grand Total			3912	3912

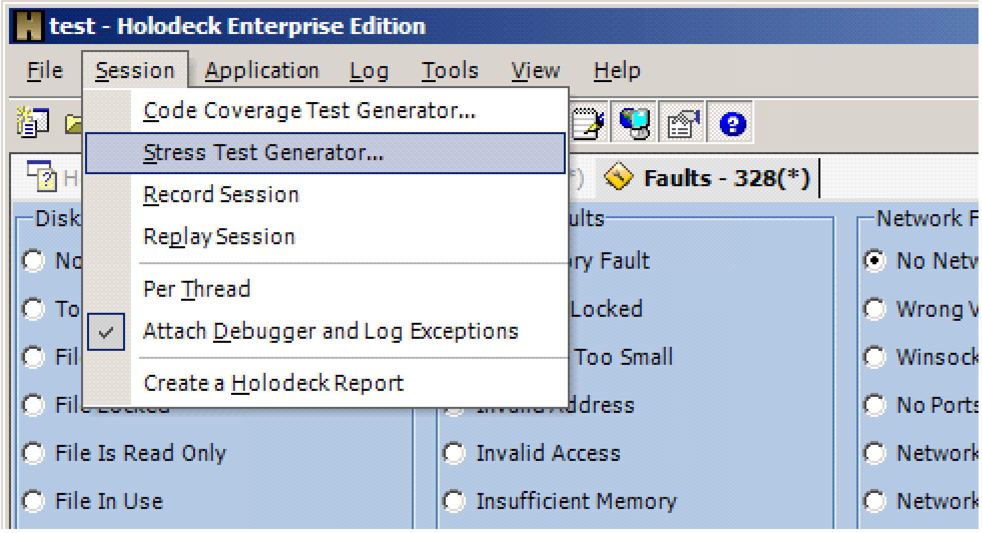
Using Automatic Test Generation

Introduction to Automatic Test Generation

Holodeck makes it easy to set and run different tests on the Application Under Test through the use of our Code Coverage Test Generator and Stress Test Generator. These help to test each line of code in the Application Under Test, and simulate stressful situations for your software. When using Holodeck to automatically test your application, turn off logging options that are unnecessary to test. Some Test Generation features may stop working if all logging is turned off, however the less logging used, the less system memory with be used which will allow stress testing to last longer.

1. Using Holodeck for Stress Test Generation

2. Using Holodeck for Code Coverage Test Generation

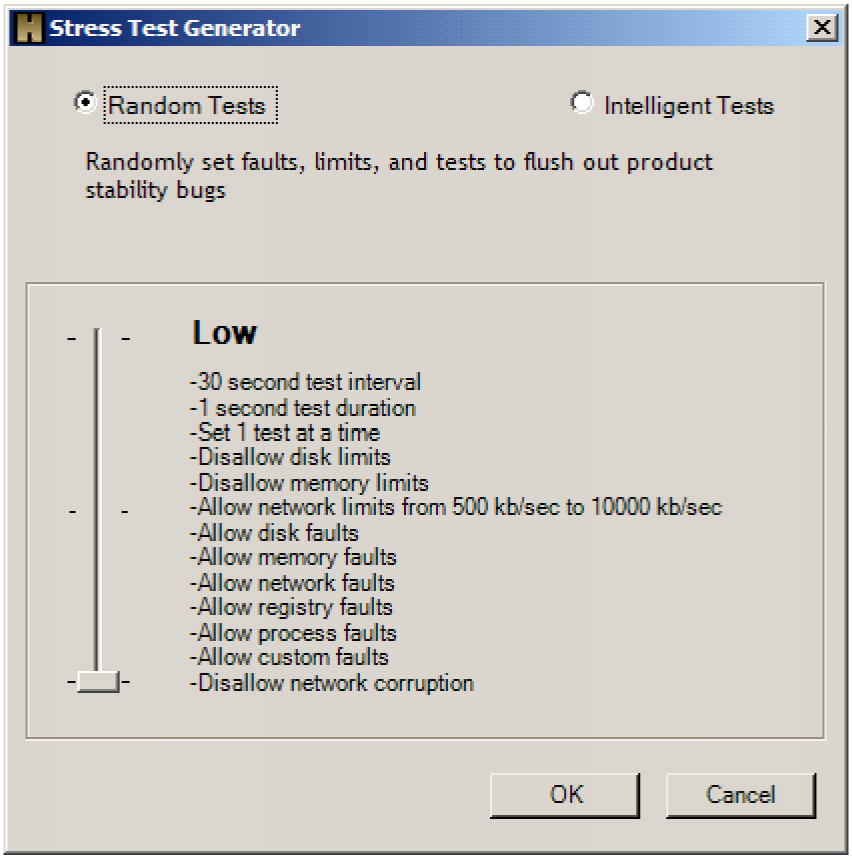


To ensure reproducibility of the bugs that you may find using Holodeck's Stress Test Generation and Code Coverage Test Generation you may want to record the test run. To record your test session simply start session recording before starting your test and stop recording the session once the tests have finished. See Recording and Replaying Sessions for help.

Creating Stress Test Generation

Using Holodeck's Stress Test Generation to test your application is a great way to ensure your software will continue to perform well even in stressful situations. Under Stress Testing Holodeck injects faults intermittently to cause stress failures to occur more rapidly than they would under normal circumstances.

Get to the Stress Test Generation dialog by clicking Session > Stress Test Generator… on the menu.



● Random Tests ○ Intelligent Tests

Randomly set faults, limits, and tests to flush out product stability bugs

Low

-30 second test interval
-1 second test duration
-Set 1 test at a time
-Disallow disk limits
-Disallow memory limits
-Allow network limits from 500 kb/sec to 10000 kb/sec
-Allow disk faults
-Allow memory faults
-Allow network faults
-Allow registry faults
-Allow process faults
-Allow custom faults
-Disallow network corruption

Holodeck can either set random or intelligent tests.

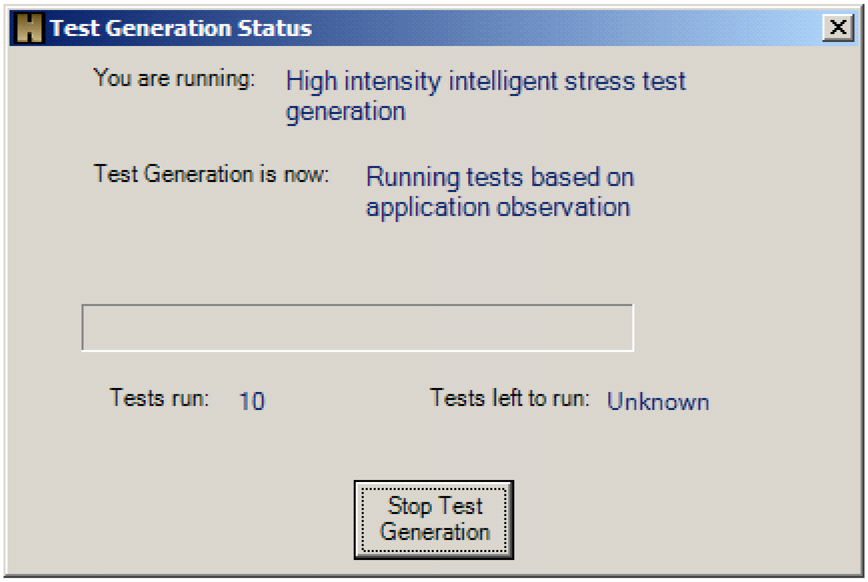
Random Tests:

Random tests starts setting tests, faults and limits as soon as Stress Testing is enabled. It randomly selects test, faults and limits within the specifications of the low, medium and high categories. While Stress Testing is running you can either attach an external test harness to run through an automated test set, or test by hand.

Intelligent Tests:

Holodeck begins the testing session by listening to the application. It sets tests, faults and limits based on what it has seen from the test run. Holodeck continues to listen to the application while further tests are made. While Stress Testing is running you can either attach an external test harness to run through an automated test set, or test by hand.

The test generation status dialog shows all the information having to do with the currently running Stress test. Since these tests can be run indefinitely there are an unknown number of tests left to run. While the tests are running look here for updates on what Holodeck is testing on your application.



You are running: High intensity intelligent stress test generation

Test Generation is now: Running tests based on application observation

Tests run: 10

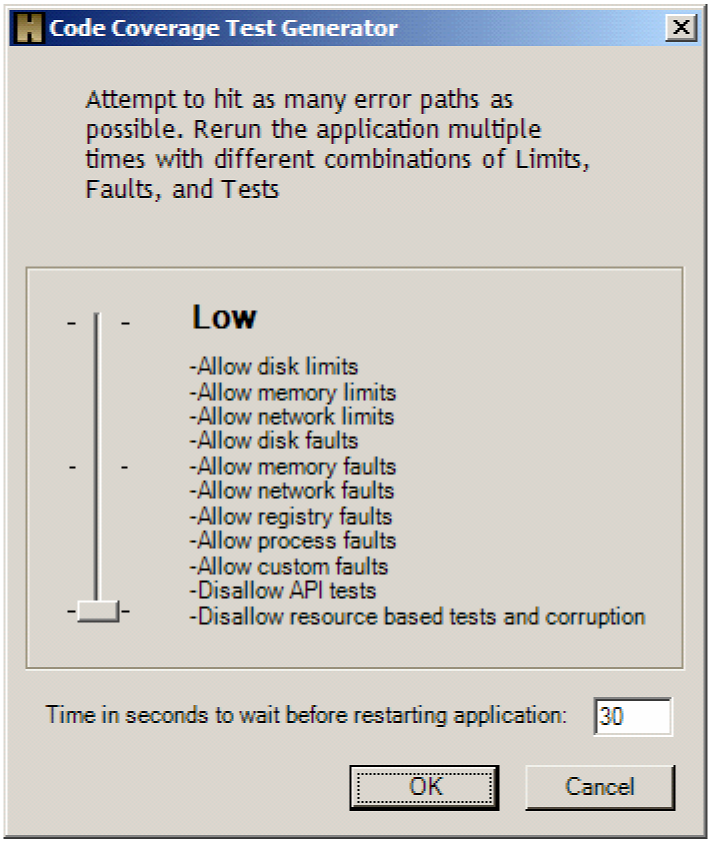
Tests left to run: Unknown

note: When stress test generation is run for multiple processes each time it creats a set of tests it will randomly select one of the processes to test.

Creating Code Coverage Generation

Code coverage test generation attempts to hit as many error paths as possible. It reruns the application multiple times, each time setting different combinations of Limits, Faults, and Tests. Each time the Application Under Test terminates, by way of the script terminating the Application gracefully or Holodeck finding a crashing bug, Holodeck will relaunch the Application Under Test and start the next test, until there are none left. Holodeck assumes that each testing script will close the application under test at the end of the test; this allows Holodeck to know when to start the next test.

To open the Code Coverage Test Generator click Test -> Code Coverage Test Generator… on the menu.



Code Coverage Test Generator

Attempt to hit as many error paths as possible. Rerun the application multiple times with different combinations of Limits, Faults, and Tests

Low

-Allow disk limits
-Allow memory limits
-Allow network limits
-Allow disk faults
-Allow memory faults
-Allow network faults
-Allow registry faults
-Allow process faults
-Allow custom faults
-Disallow API tests
-Disallow resource based tests and corruption

Time in seconds to wait before restarting application: 30

Initial Recording

The first thing Holodeck does when running Code Coverage Testing is record what the application is doing to create an intelligent test plan. Holodeck records resource usage and unique API calls until the application is terminated. It then uses the information found in the recording phase to build the next tests. Each time the application is restarted Holodeck sets a different single limit, fault or test.

Exact order of execution:

1) Set each fault one at a time

2) Set a limit

   a) For disk or memory

      i) Set a limit for max used – 1 byte

        ii) Set a limit for average used – 1 byte

        iii) Set a limit to minimum possible (0 bytes)

    b) For Network

        i) Set a limit to 50%

        ii) Set a limit to 0%

2) Set a test for each unique API call seen in the recording phase.

3) Resource faults are set targeting each dependency

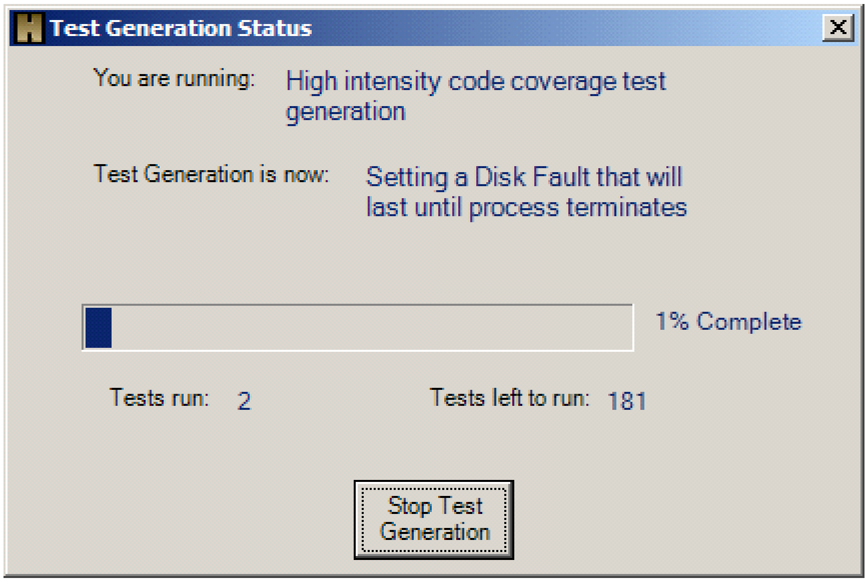
        i) Faults are either two of the following

            (1) Corruption of the Resource

            (2) Any one of the resource faults as found in the faults pane

Note: Test/limit/fault is set randomly between start and finish of the application running so that different code paths are hit

The test generation status dialog shows all the information having to do with the currently running test. This session of Code Coverage testing will run for 181 tests. Each time the application under test terminates, either from a crash or when the test harness closes, Holodeck will restart the application and set a new test.



You are running: High intensity code coverage test generation

Test Generation is now: Setting a Disk Fault that will last until process terminates

1% Complete

Tests run: 2

Tests left to run: 181

Modifying Testing Settings

You can change how Holodeck Stress and Code Coverage tests your application by modifying the TestGeneration.xml file found in the Test Generation folder in the Holodeck install directory (default: C:\Program Files\Security Innovation\Holodeck Enterprise Edition\Test Generation).

This XML file holds all the settings for how Holodeck tests your application. Before making any changes to this file it is recommended that you make a backup copy.

TestInterval – Time between setting individual tests, in milliseconds.

TestDuration – Time to enable each test, in milliseconds.

AllowNetworkLimit – Boolean, allow or disallow network limits.

AllowDiskLimit - Boolean, allow or disallow disk limits.

AllowMemoryLimit - Boolean, allow or disallow memory faults.

AllowNetworkFaults - Boolean, allow or disallow network faults.

AllowRegistryFaults - Boolean, allow or disallow registry faults.

AllowProcessFaults - Boolean, allow or disallow process faults.

AllowCustomFaults - Boolean, allow or disallow custom faults.

AllowDiskFaults - Boolean, allow or disallow disk faults.

AllowMemoryFaults - Boolean, allow or disallow memory faults.

AllowNetworkCorruption - Boolean, allow or disallow network corruption.

NumOverlappingTests – The number of tests allowed to execute at the same time.

NetworkLowRange – Lowest the network limit can be, in bytes per second.

NetworkHighRange - Highest the network limit can be, in bytes per second.

DiskLimitSet – set value 0 for at current usage, set value 1 for above current usage

DiskLimitMax – limits will be set from current usage to current usage plus this number

MemoryLimitSet– set value 0 for at current usage, set value 1 for above current usage

MemoryLimitMax– limits will be set from current usage to current usage plus this number.

Generating Network Corruption Faults

Using the Network Corruption Fault Wizard

Holodeck can inject faults into the Application Under Test that simulate network problems or network hardware problems. Holodeck also has faults related to the actual data being transmitted over the network. This help topic describes how network data corruption can be added to your project.

Often network traffic can become corrupted in transfer. Holodeck allows you to simulate these errors through network corruption faults.   Using this wizard you can simulate random corruption or find and replace interesting string to test network stream parsing.

Please see the following pages for more information on the network corruption fault wizard.

Creating a fault using Random Corruption

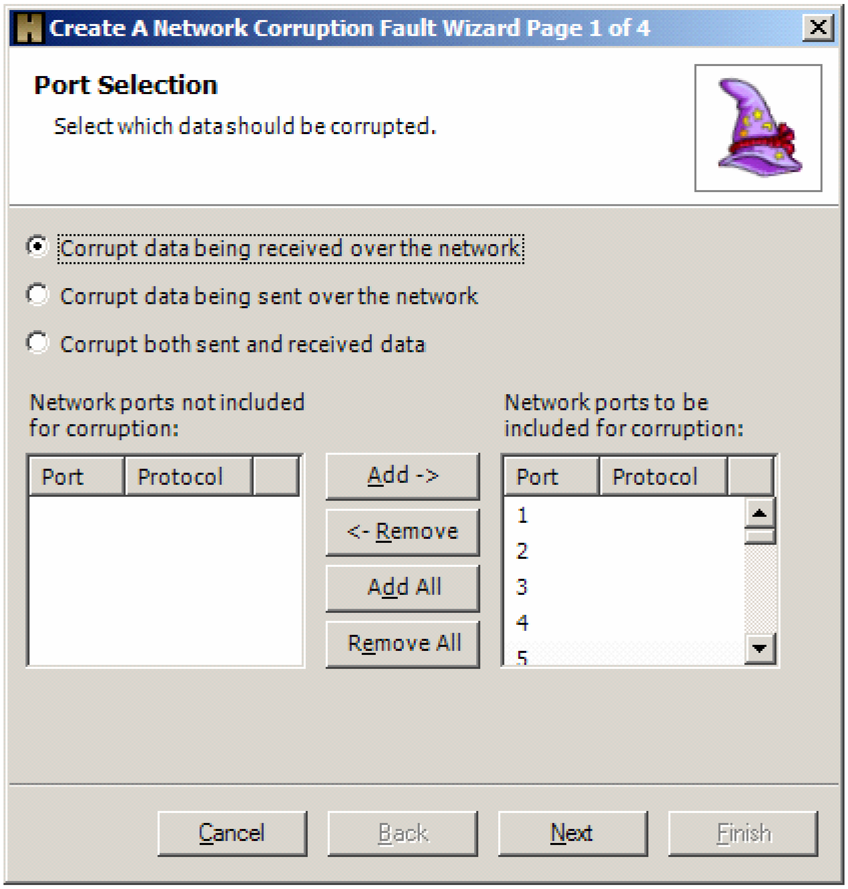
Creating a fault using Find and Replace Corruption

Creating a fault using Regular Expressions

Creating a fault using Random Corruption

Random Corruption is a good way of testing for the type of corruption that would happen as a result of common line noise.

First, since we only want to test the client only data being received over the network will be corrupted. However we do want to corrupt on all ports. To test a single port or protocol simply remove all the ports using the Remove all button, and select the port you would like to test by selecting it and adding it to the Ports to be included for corruption.



Create A Network Corruption Fault Wizard Page 1 of 4

Port Selection

Select which data should be corrupted.

● Corrupt data being received over the network

○ Corrupt data being sent over the network

○ Corrupt both sent and received data

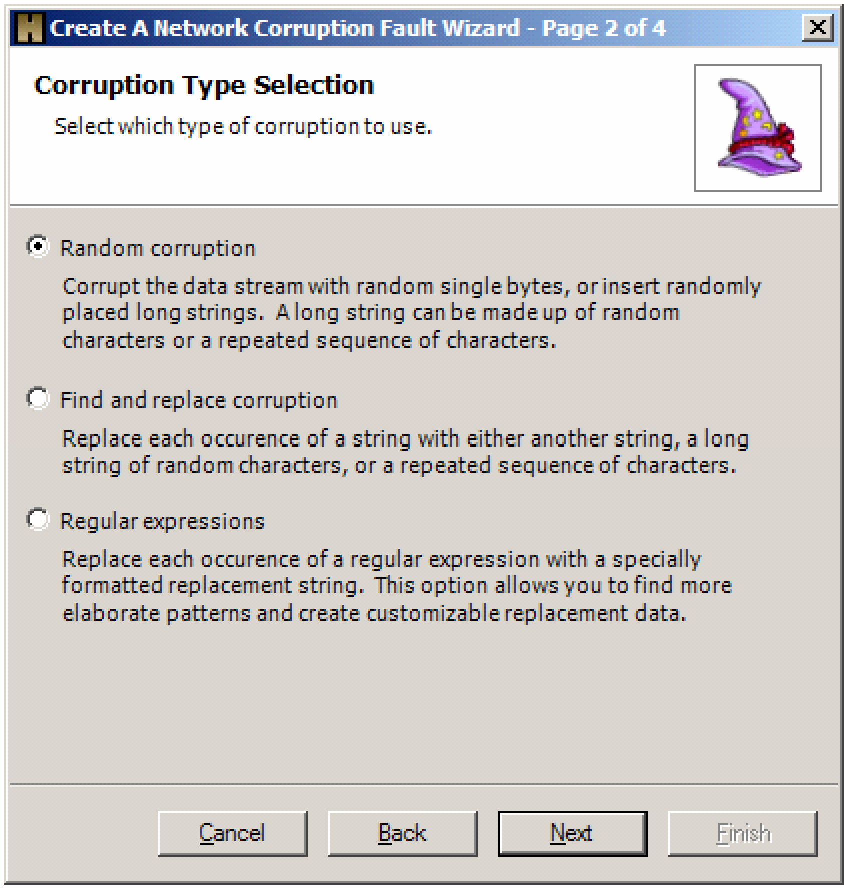
Network ports not included for corruption:

Port	Protocol

Network ports to be included for corruption:

Port	Protocol
1	
2	
3	
4	
5	

The Default Random Corruption should already be set.



Create A Network Corruption Fault Wizard - Page 2 of 4

Corruption Type Selection

Select which type of corruption to use.

● Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

○ Find and replace corruption

Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

○ Regular expressions

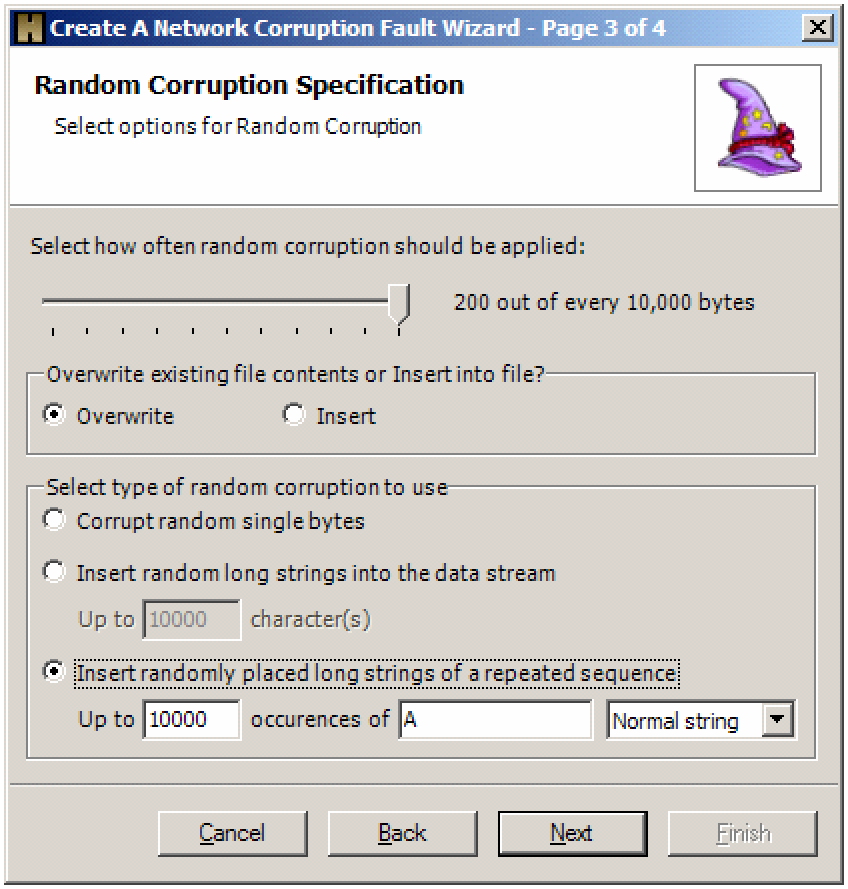
Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

Random Corruption can happen in a variety of ways.

Depending on the severity of the test you may opt to corrupt more data. Sending an extremely corrupted package may be rejected by the application early on, but is good for severe corruption smoke testing. On the other hand corrupting fewer bytes may allow the corrupted packet to masquerade as a legitimate packet and find bugs deeper in the network code.

Overwriting data in a file replaces already existing data, this includes any header or footer information your application may be looking for.

Inserting data into the packet can find buffer overflow bugs. It may also make it easier to find the corrupted string in memory if a error occurs.



Create A Network Corruption Fault Wizard - Page 3 of 4

Random Corruption Specification

Select options for Random Corruption

Select how often random corruption should be applied:

200 out of every 10,000 bytes

Overwrite existing file contents or Insert into file?

● Overwrite ○ Insert

Select type of random corruption to use

○ Corrupt random single bytes

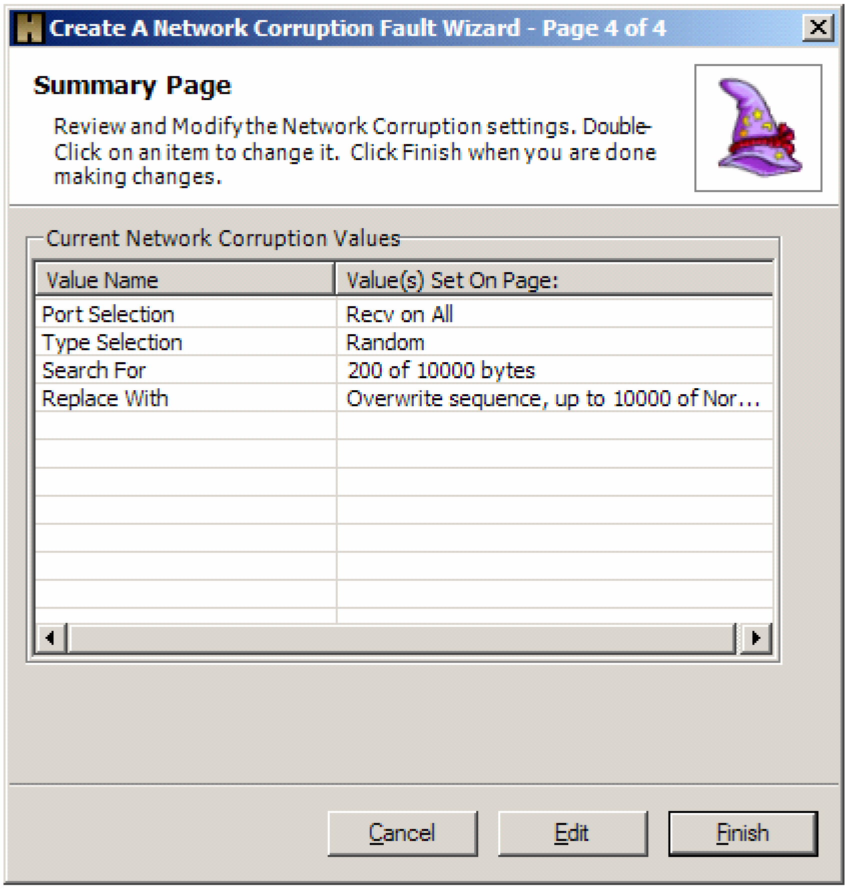
○ Insert random long strings into the data stream

Up to 10000 character(s)

● Insert randomly placed long strings of a repeated sequence

Up to 10000 occurences of A Normal string

The final page shows a summary of the corruption fault you just created. To edit any information on this page simply select it, and click edit. This will take you back to that page to make any necessary changes.



Summary Page

Review and Modify the Network Corruption settings. Double-Click on an item to change it. Click Finish when you are done making changes.

Current Network Corruption Values

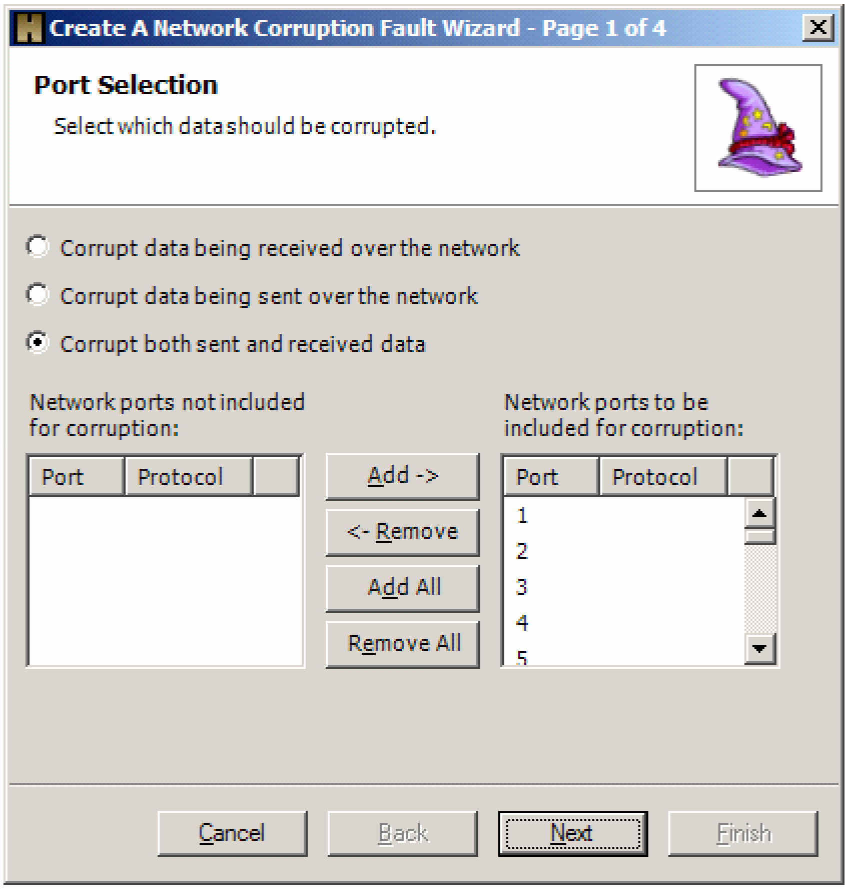
Value Name	Value(s) Set On Page:
Port Selection	Recv on All
Type Selection	Random
Search For	200 of 10000 bytes
Replace With	Overwrite sequence, up to 10000 of Nor…

Creating a fault using Find and Replace Corruption

In this topic we will discover how find and replace works. We will create a find and replace function to replace any occurrences of "coffee" with "decaf."

To begin, create a project using Internet Explorer as the Application Under Test, keep all logging as the defaults.

First set the fault to catch data being sent and received on all ports and protocols.


Create A Network Corruption Fault Wizard - Page 1 of 4

Port Selection

Select which data should be corrupted.

○ Corrupt data being received over the network

○ Corrupt data being sent over the network

● Corrupt both sent and received data

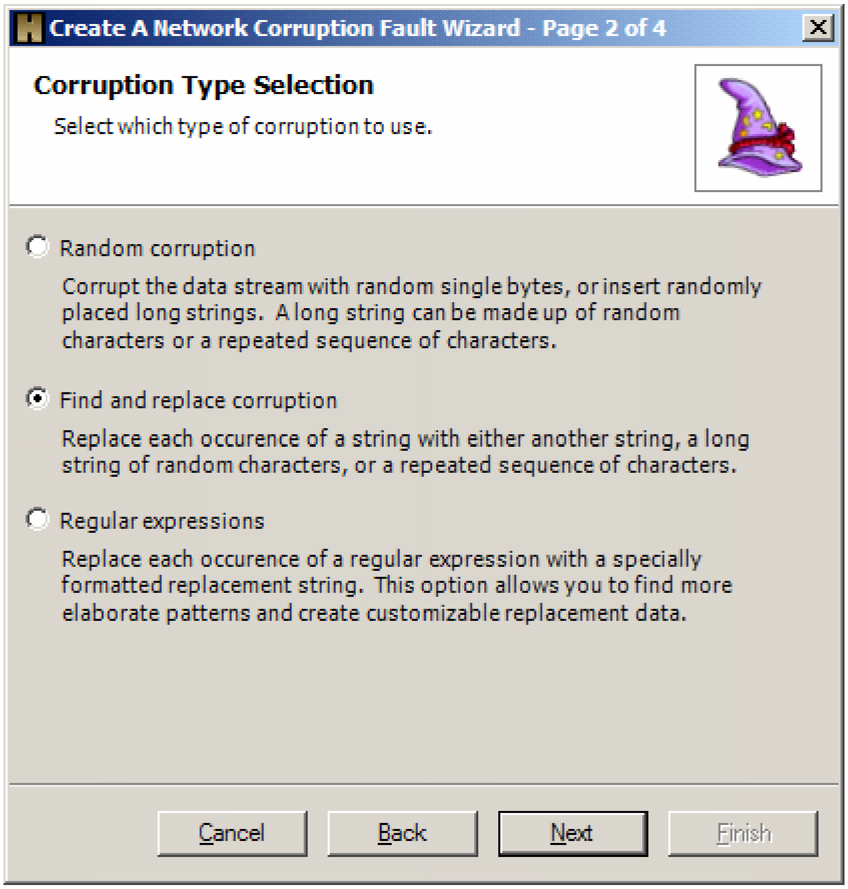
Network ports not included for corruption:

Port	Protocol

Network ports to be included for corruption:

Port	Protocol
1	
2	
3	
4	
5	

This is a simple find and replace fault.



Corruption Type Selection

Select which type of corruption to use.

○ Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

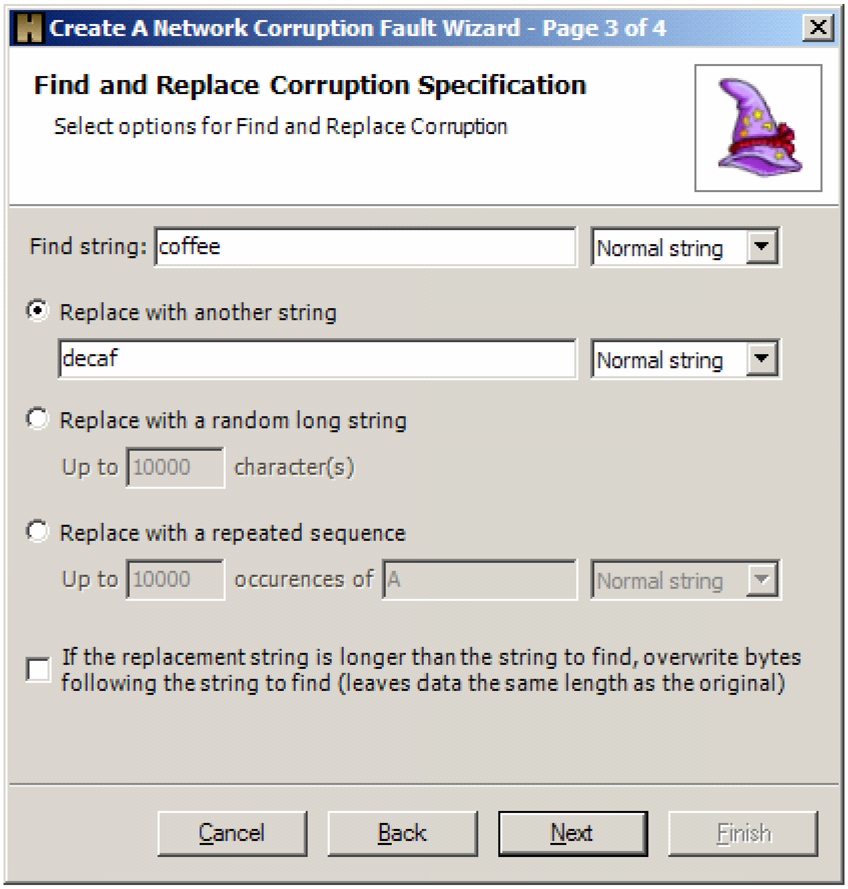
● Find and replace corruption

Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

○ Regular expressions

Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

On this page we have the option of replacing a normal string, an escaped string, or a hex string. Escaping and using hex strings can be useful for finding or replacing untypeable characters such as the line return, tab and other interesting characters. In this case we want to replace all occurrences of "coffee" with the word "decaf"



Create A Network Corruption Fault Wizard - Page 3 of 4

Find and Replace Corruption Specification

Select options for Find and Replace Corruption

Find string: coffee Normal string

● Replace with another string

decaf Normal string

○ Replace with a random long string

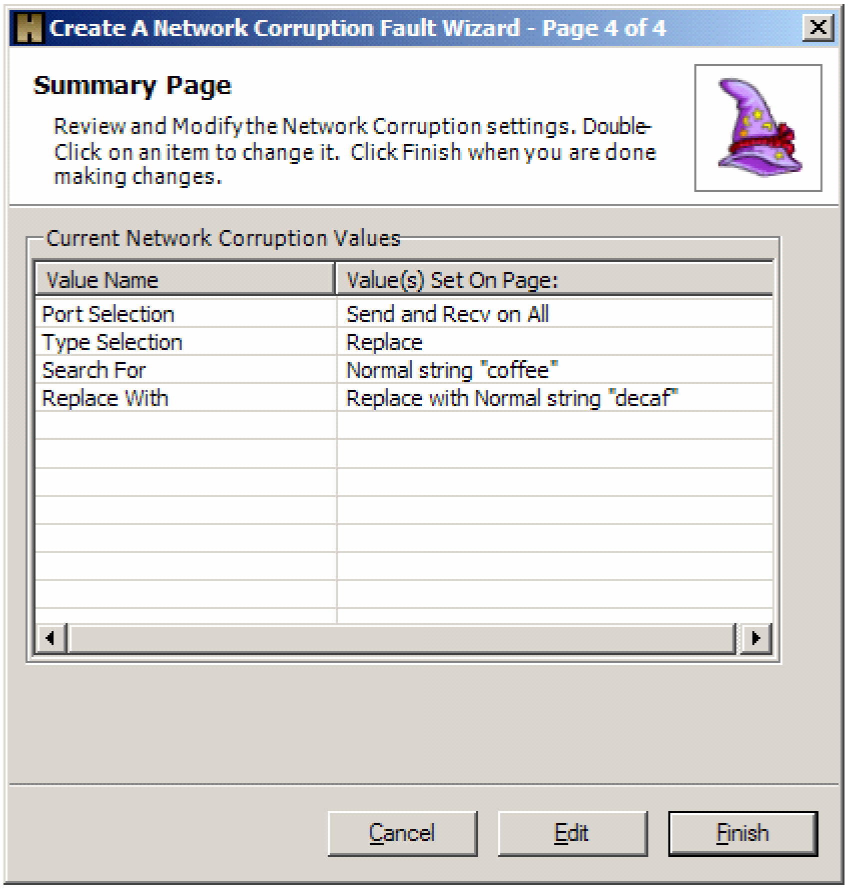
Up to 10000 character(s)

○ Replace with a repeated sequence

Up to 10000 occurences of A Normal string

□ If the replacement string is longer than the string to find, overwrite bytes following the string to find (leaves data the same length as the original)

The final page shows a summary of the corruption fault you just created. To edit any information on this page simply select it, and click edit. This will take you back to that page to make any necessary changes.



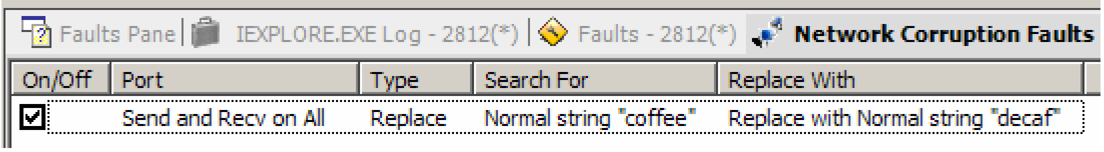
Summary Page

Review and Modify the Network Corruption settings. Double-Click on an item to change it. Click Finish when you are done making changes.

Current Network Corruption Values

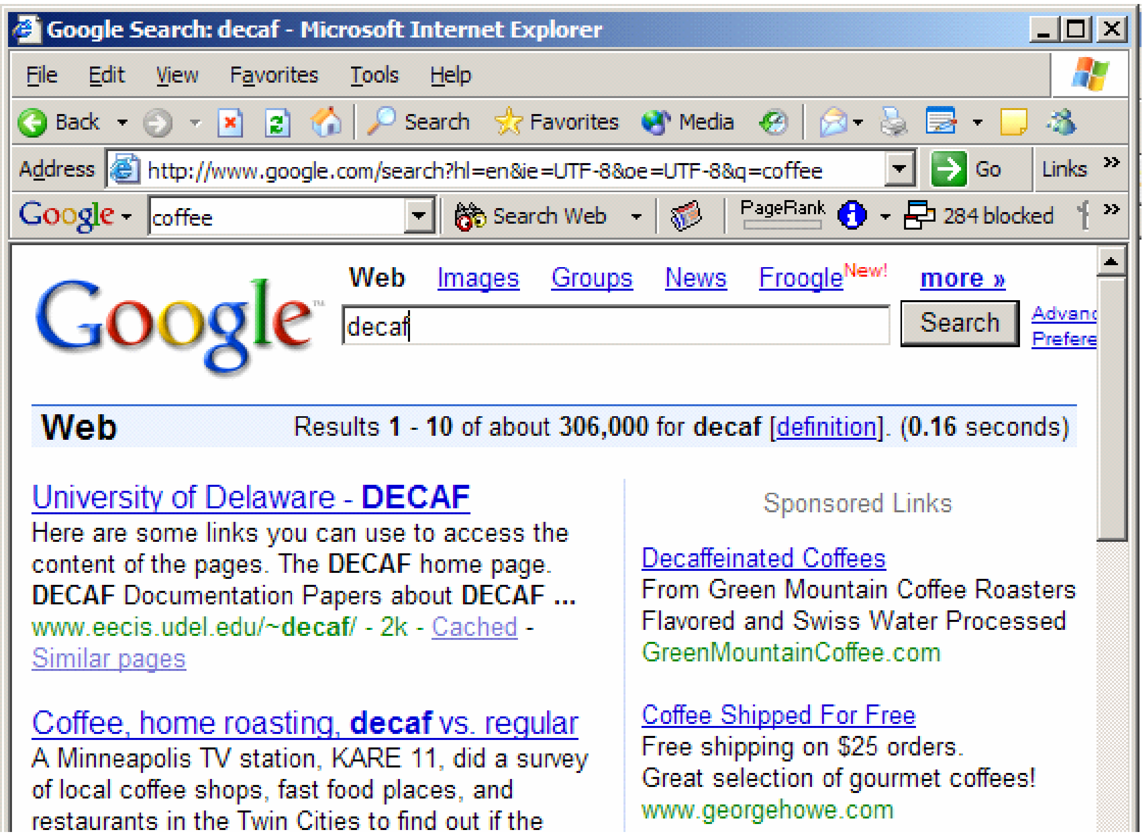
Value Name	Value(s) Set On Page:
Port Selection	Send and Recv on All
Type Selection	Replace
Search For	Normal string "coffee"
Replace With	Replace with Normal string "decaf"

In the network corruption pane of Holodeck we can see the fault has been set to search for the normal string "coffee" and replace it with the Normal string "decaf"



On/Off	Port	Type	Search For	Replace With
☑	Send and Recv on All	Replace	Normal string "coffee"	Replace with Normal string "decaf"

Return to Internet Explorer, and navigate to the Google Search Engine (www.google.com). Type "coffee" into the Search Box and click Search. The following is a screenshot of what should be displayed. Notice the search string in the address bar still shows coffee, since that was the string that was sent to Google before Holodeck intercepted it.



Google Search: decaf - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=coffee Go Links
Google coffee Search Web PageRank 284 blocked
Web Images Groups News Froogle New! more »
decaf
Search
Advanc
Prefere

Web Results **1** - **10** of about **306,000** for **decaf** [definition]. (**0.16** seconds)

University of Delaware - **DECAF**
Here are some links you can use to access the content of the pages. The **DECAF** home page. **DECAF** Documentation Papers about **DECAF** ...
www.eecis.udel.edu/~**decaf**/ - 2k - Cached - Similar pages

Coffee, home roasting, **decaf** vs. regular
A Minneapolis TV station, KARE 11, did a survey of local coffee shops, fast food places, and restaurants in the Twin Cities to find out if the

Sponsored Links

Decaffeinated Coffees
From Green Mountain Coffee Roasters Flavored and Swiss Water Processed
GreenMountainCoffee.com

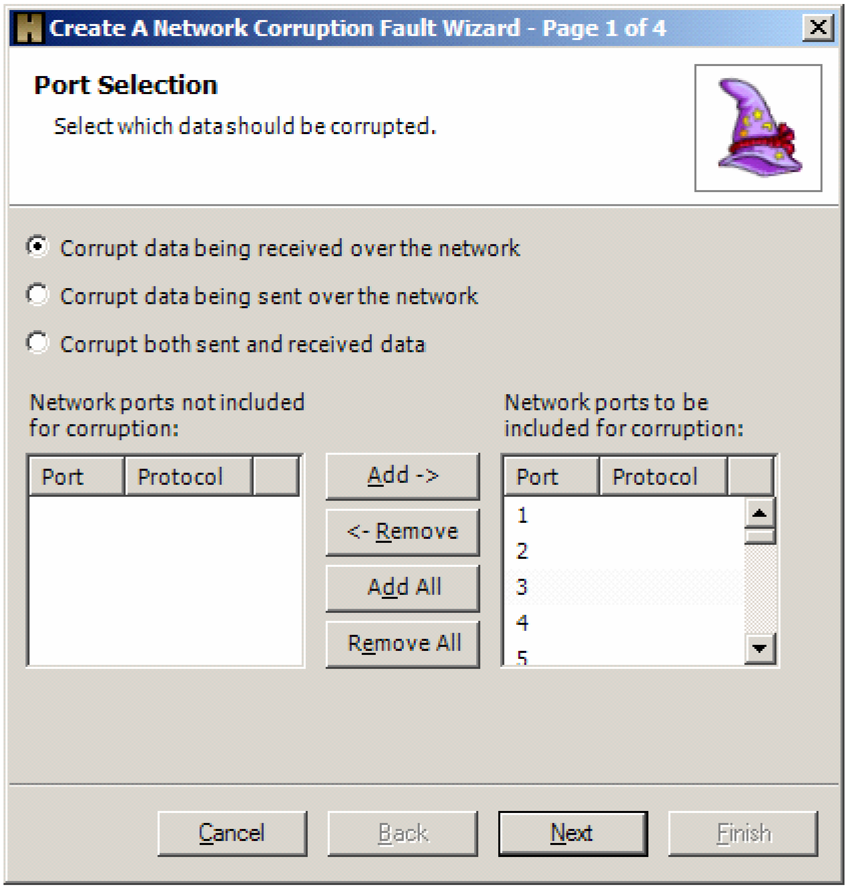
Coffee Shipped For Free
Free shipping on $25 orders. Great selection of gourmet coffees!
www.georgehowe.com

Creating a fault using Regular Expressions

In this topic we will discover how to find and replace network data using Regular Expressions and Replacement strings.

Note: Regular expressions only work with uncompressed data, some web pages may be compressed for better data transfer; Regular Expressions will not match on these pages.

Select all ports and protocols and only data being received over the network since we only want to test the client.



Create A Network Corruption Fault Wizard - Page 1 of 4

Port Selection

Select which data should be corrupted.

● Corrupt data being received over the network

○ Corrupt data being sent over the network

○ Corrupt both sent and received data

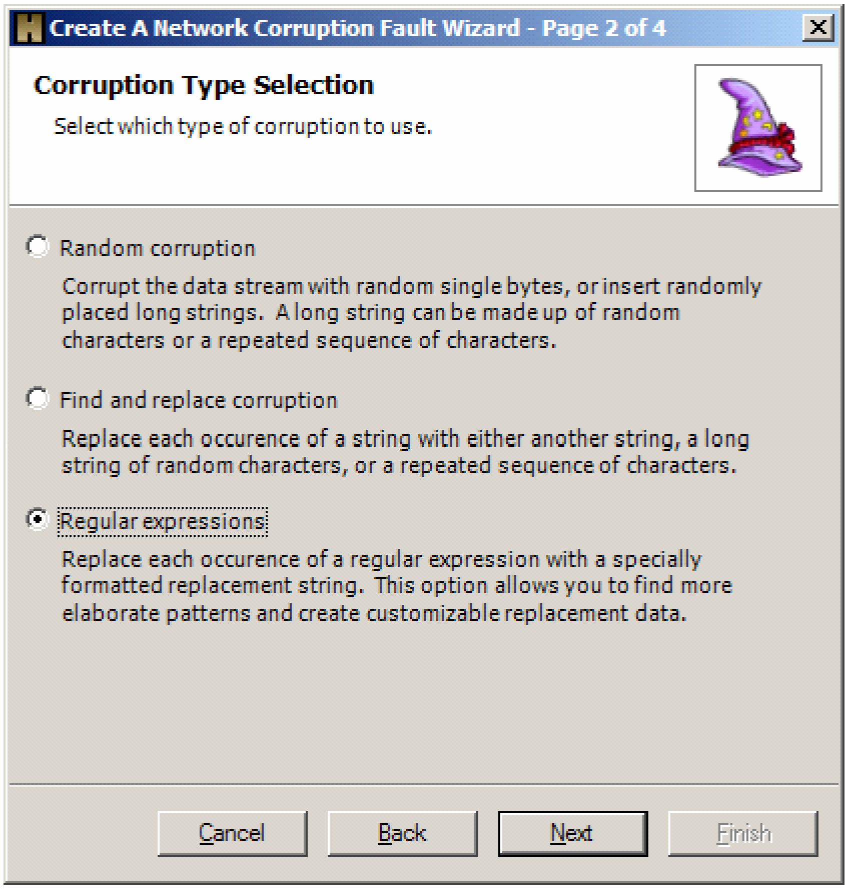
Network ports not included for corruption:

Port	Protocol

Network ports to be included for corruption:

Port	Protocol
1	
2	
3	
4	
5	

Select Regular Expressions as the method of corruption



Create A Network Corruption Fault Wizard - Page 2 of 4

Corruption Type Selection

Select which type of corruption to use.

○ Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

○ Find and replace corruption

Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

● Regular expressions

Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

Create a regular expression so match on the domain of any URL (iegwww.google.com, or slashdot.org) and replace it with 1000 to 5000 of the letter ‘A’.

The regular expression to match any domain is as follows:

```
([wW]{3,}\.)?([abcefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXY
Z]+)\.(com|net|org)
```

`([wW]{3,}\.)?` - this part matches an optional capital or lowercase "www."

`([abcefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]+)` – this part matches any length string consisting of upper or lowercase alphabet letters, greater than 1 (eg. "abc", "aRdfpQ", etc.)

`\.(com|net|org)` – this part matches a period followed by any one of the following, "com", "net", or "org"

The expansion string to expand between 1000 and 5000 ‘A’s is as follows:

```
$S1000,5000,A$
```

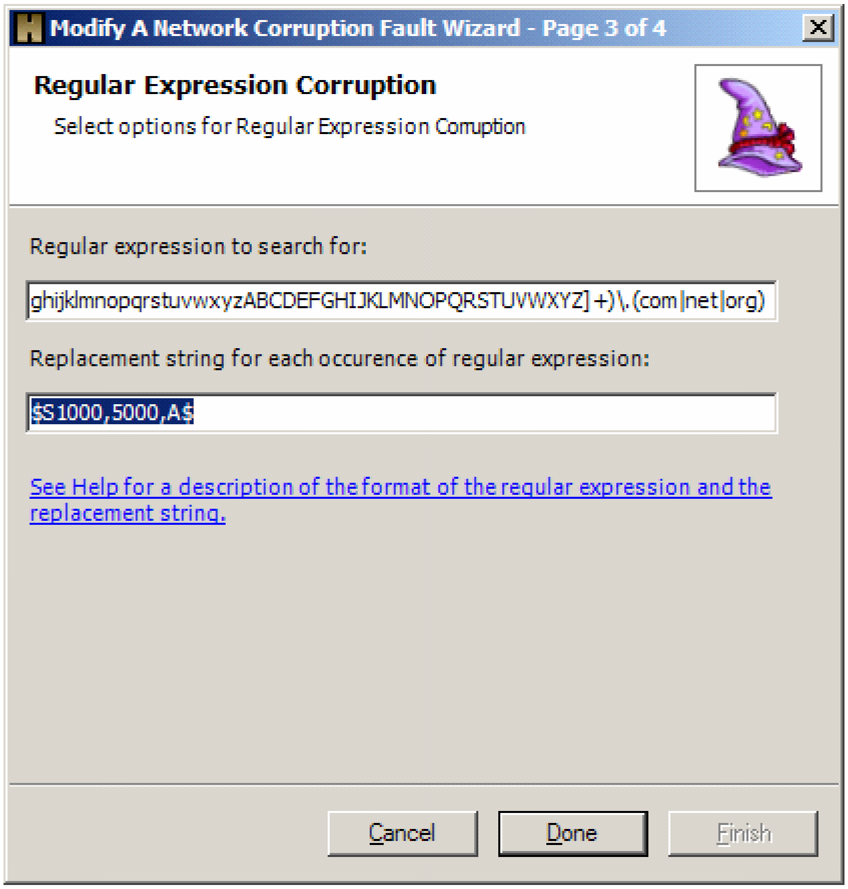
`S` – shows this will expand to a string

`1000` – the minimum number of repetitions

`5000` – the maximum number of repetitions

`A` – the string to expand

By enclosing this string in '`$`' Holodeck knows this is a string to expand.



Modify A Network Corruption Fault Wizard - Page 3 of 4

Regular Expression Corruption

Select options for Regular Expression Corruption

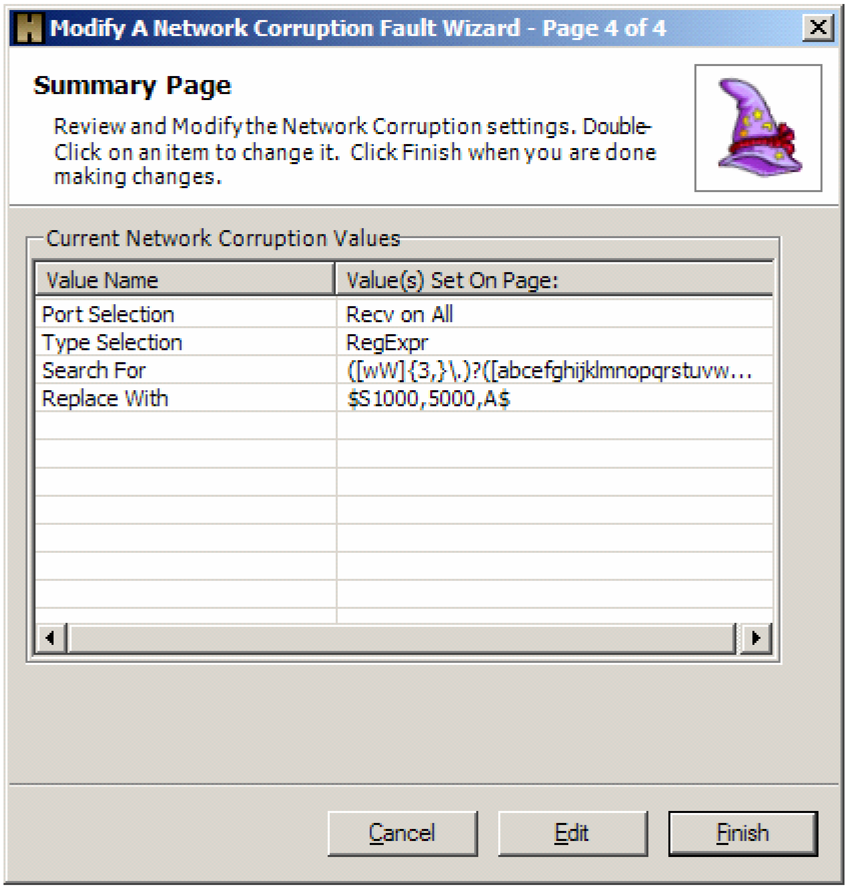
Regular expression to search for:

```
ghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]+)\.(com|net|org)
```

Replacement string for each occurence of regular expression:

```
$S1000,5000,A$
```

See Help for a description of the format of the regular expression and the replacement string.



Summary Page

Review and Modify the Network Corruption settings. Double-Click on an item to change it. Click Finish when you are done making changes.

Current Network Corruption Values

Value Name	Value(s) Set On Page:
Port Selection	Recv on All
Type Selection	RegExpr
Search For	([wW]{3,}\.)?([abcefghijklmnopqrstuvw...
Replace With	$S1000,5000,A$

Generating File Corruption

File Corruption Overview

When you create a File corruption fault Holodeck does not corrupt the original file, but rather when the Application Under Test attempts to access that file it redirects the Application Under Test to a corrupted version of the file. This is useful because it allows you to corrupt a single file many different ways to test all aspects of file processing.

Please see the following pages for more information on File Corruption:

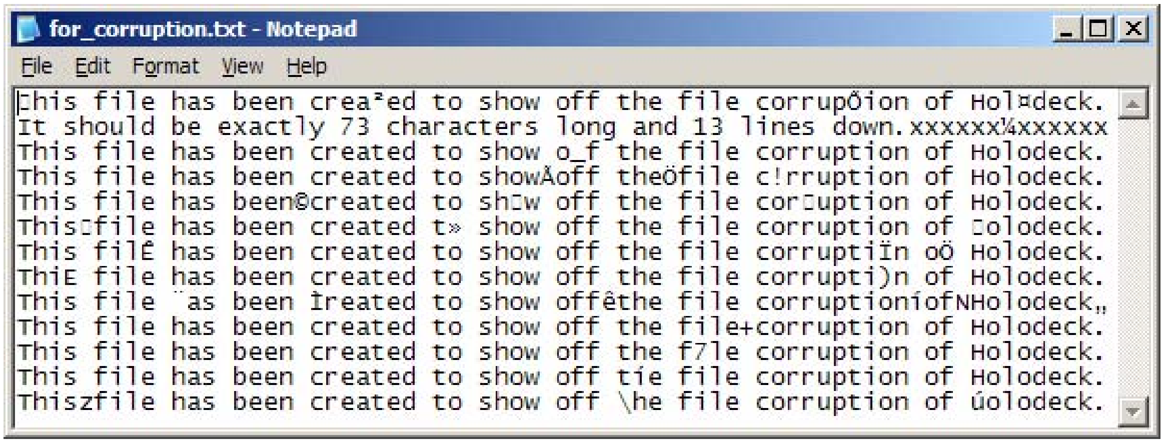
Create a File Corruption Fault using Random Corruption

Create a File Corruption Fault using Find and Replace

Create a File Corruption Fault with Regular Expressions

To create a file corruption fault click Application > "Create a New File Corruption Fault…" This will bring up the file corruption wizard.

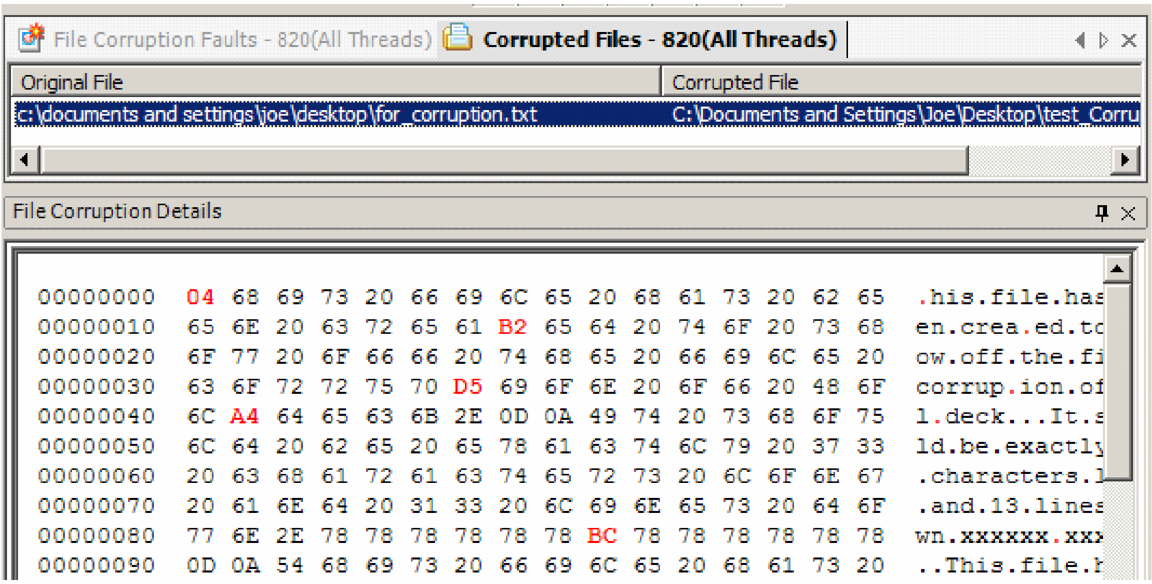
Example of a corrupted file:



```
□his file has been crea²ed to show off the file corrupÕion of Hol¤deck.
It should be exactly 73 characters long and 13 lines down.xxxxxx¼xxxxxx
This file has been created to show o_f the file corruption of Holodeck.
This file has been created to showÅoff theÖfile c!rruption of Holodeck.
This file has been©created to sh□w off the file cor□uption of Holodeck.
This□file has been created t» show off the file corruption of □olodeck.
This filÊ has been created to show off the file corruptiÏn oÖ Holodeck.
ThiE file has been created to show off the file corrupti)n of Holodeck.
This file ¨as been İreated to show offêthe file corruptioníofNHolodeck„
This file has been created to show off the file+corruption of Holodeck.
This file has been created to show off the f7le corruption of Holodeck.
This file has been created to show off tíe file corruption of Holodeck.
Thiszfile has been created to show off \he file corruption of úolodeck.
```

The original file remains untouched; Holodeck creates a new file in the Corrupted Files directory, the redirects the application to that file. All changes are stored in an XML file with the same name as the corrupted file.

In the image below a corrupted file has been selected in the Corrupted Files Pane after the application had tried to access it. Holodeck then generated the corrupted file and added an entry in the Corrupted Files Pane. Selecting the corrupted file will load the corrupted file, with all corruption changes highlighted, in the File Corruption Details Pane.


File Corruption Faults - 820(All Threads)
Corrupted Files - 820(All Threads)
File Corruption Details

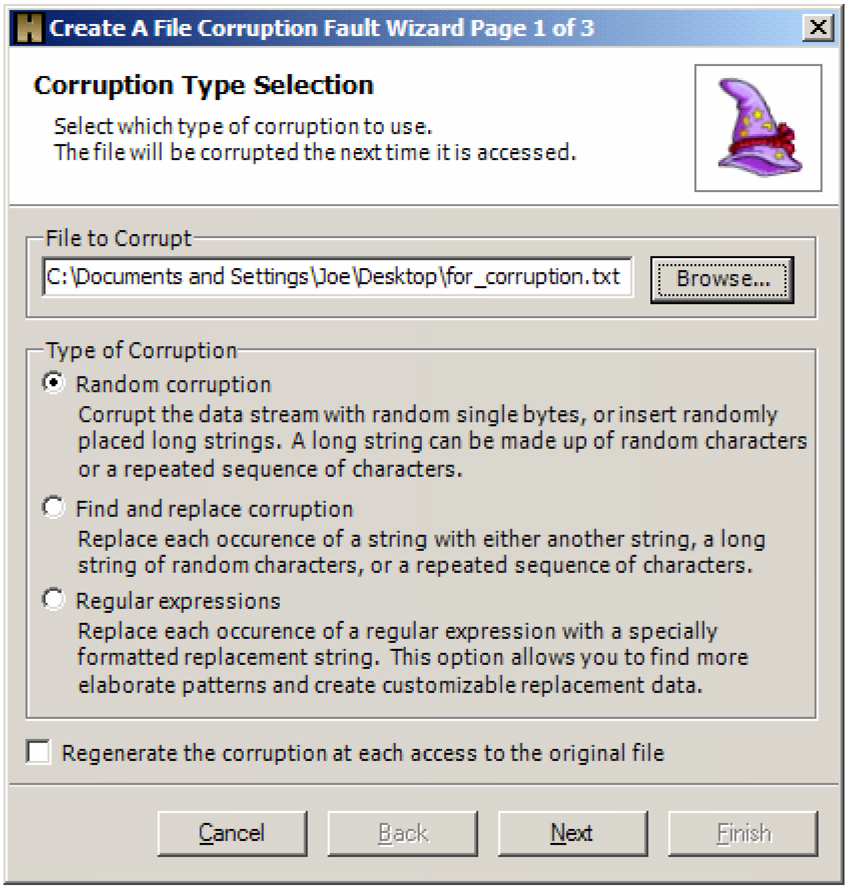
Original File	Corrupted File
c:\documents and settings\joe\desktop\for_corruption.txt	C:\Documents and Settings\Joe\Desktop\test_Corru

```
00000000  04 68 69 73 20 66 69 6C 65 20 68 61 73 20 62 65  .his.file.has
00000010  65 6E 20 63 72 65 61 B2 65 64 20 74 6F 20 73 68  en.crea.ed.to
00000020  6F 77 20 6F 66 66 20 74 68 65 20 66 69 6C 65 20  ow.off.the.fi
00000030  63 6F 72 72 75 70 D5 69 6F 6E 20 6F 66 20 48 6F  corrup.ion.of
00000040  6C A4 64 65 63 6B 2E 0D 0A 49 74 20 73 68 6F 75  l.deck...It.s
00000050  6C 64 20 62 65 20 65 78 61 63 74 6C 79 20 37 33  ld.be.exactly
00000060  20 63 68 61 72 61 63 74 65 72 73 20 6C 6F 6E 67  .characters.l
00000070  20 61 6E 64 20 31 33 20 6C 69 6E 65 73 20 64 6F  .and.13.lines
00000080  77 6E 2E 78 78 78 78 78 78 BC 78 78 78 78 78 78  wn.xxxxxx.xxx
00000090  0D 0A 54 68 69 73 20 66 69 6C 65 20 68 61 73 20  ..This.file.h
```

Create a File Corruption Fault using Random Corruption

Select the file you wish to corrupt by browsing to it using the Browse… button or type it directly into the "File to Corrupt" text box. Select Random Corruption as the type of corruption. This is a good way to flush out file parsing bugs, Holodeck generates completely random bytes which also generates many unprintable and unexpected characters.

Holodeck creates a copy of the file to be corrupted and corrupts file on the first access, then uses that same file each time it is accessed unless "Regenerate the corruption at each access to the original file" is checked. Check this checkbox for better overall testing when using any kind of random corruption, uncheck this checkbox for help reproducing bugs.



Create A File Corruption Fault Wizard Page 1 of 3

Corruption Type Selection

Select which type of corruption to use.
The file will be corrupted the next time it is accessed.

File to Corrupt: C:\Documents and Settings\Joe\Desktop\for_corruption.txt

Type of Corruption

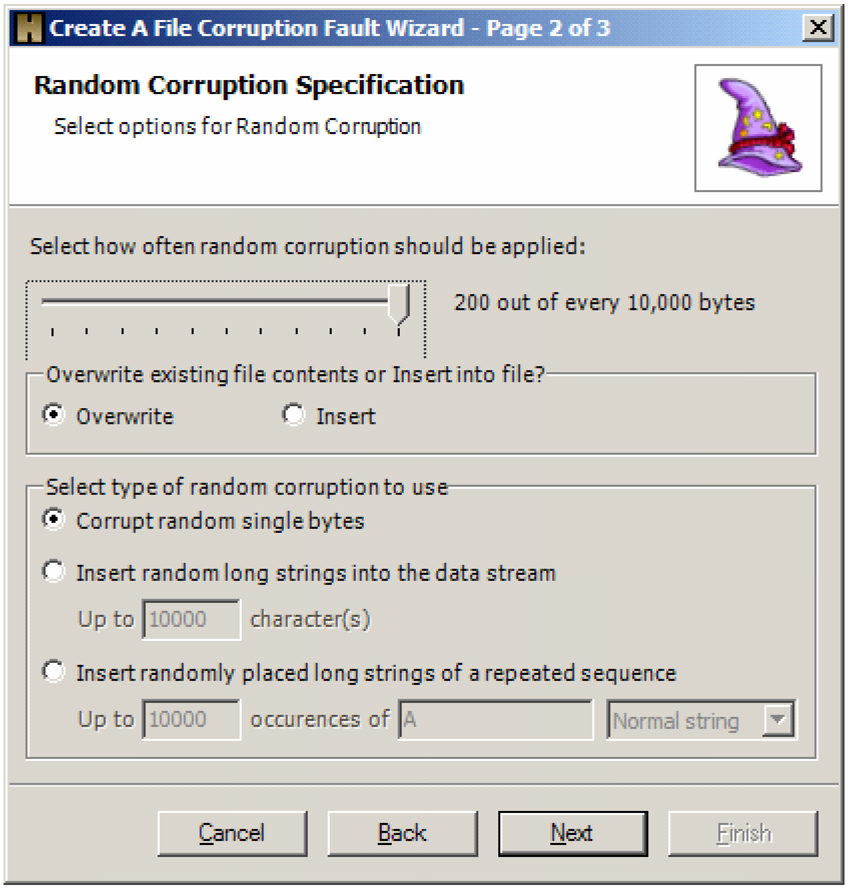
● Random corruption
Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

○ Find and replace corruption
Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

○ Regular expressions
Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

□ Regenerate the corruption at each access to the original file

In this case we want to corrupt the file as much as possible, to flush out easy file parsing bugs. More corruption will also be easier to find in the application once it has opened the file. We could opt to insert random characters into the file instead of overwriting them. Sometimes it is useful to insert a repeating character into the file for easy discovery within the application.



Random Corruption Specification

Select options for Random Corruption

Select how often random corruption should be applied:

200 out of every 10,000 bytes

Overwrite existing file contents or Insert into file?

● Overwrite ○ Insert

Select type of random corruption to use

● Corrupt random single bytes

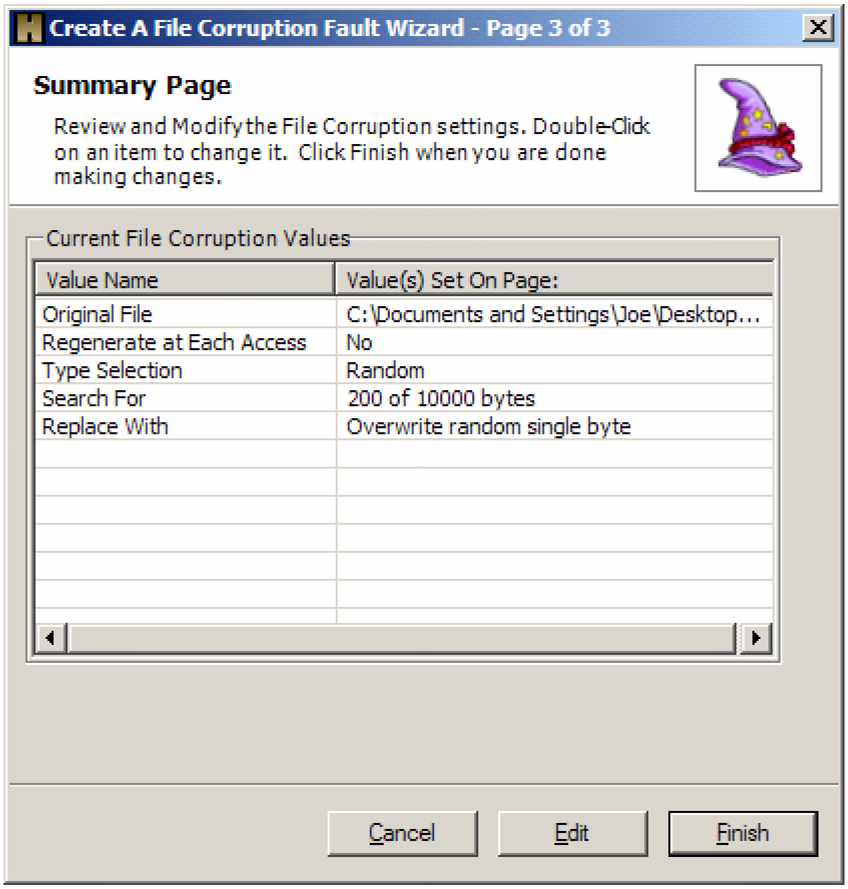
○ Insert random long strings into the data stream

Up to 10000 character(s)

○ Insert randomly placed long strings of a repeated sequence

Up to 10000 occurences of A Normal string

The Summary Page shows all the information about the wizard pertaining to this File Corruption Fault. You can go back and change any part of the fault by highlighting the value name and clicking edit. This will return you to the page in the wizard so you can change the options.



Summary Page

Review and Modify the File Corruption settings. Double-Click on an item to change it. Click Finish when you are done making changes.

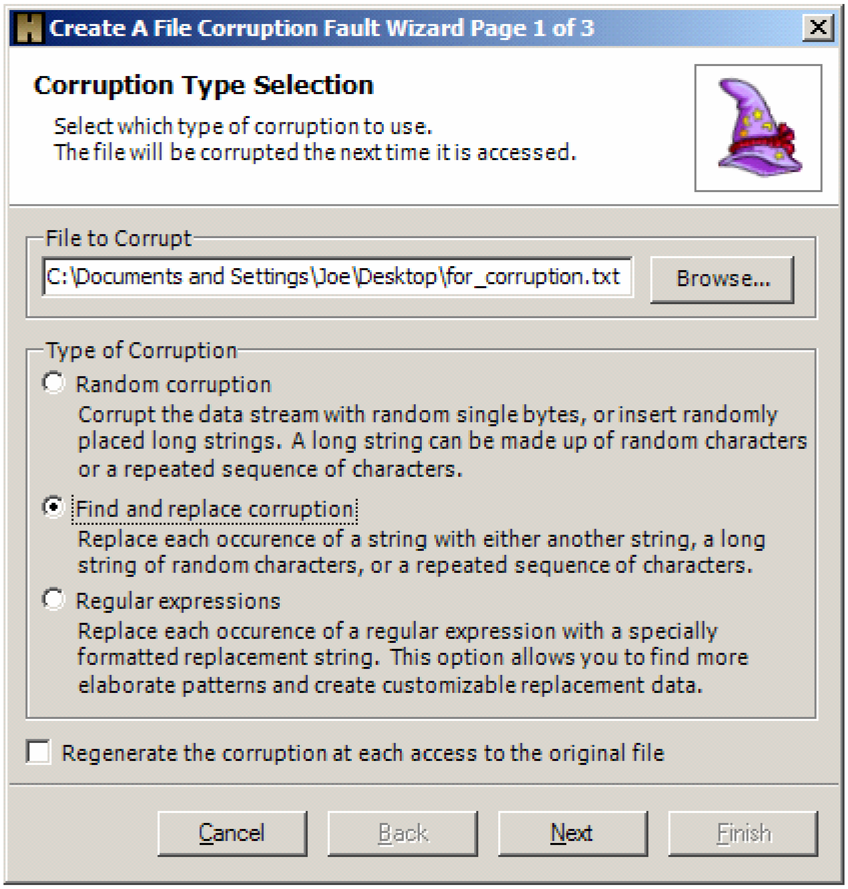
Current File Corruption Values

Value Name	Value(s) Set On Page:
Original File	C:\Documents and Settings\Joe\Desktop...
Regenerate at Each Access	No
Type Selection	Random
Search For	200 of 10000 bytes
Replace With	Overwrite random single byte

Create a File Corruption Fault using Find and Replace

Select the file you wish to corrupt by browsing to it using the Browse… button or type it directly into the "File to Corrupt" text box. Select Find and Replace as the type of corruption. This is a good way to focus your corruption to a single word, escaped string, or hex string.

Holodeck creates a copy of the file to be corrupted and corrupts file on the first access, then uses that same file each time it is accessed unless "Regenerate the corruption at each access to the original file" is checked. Check this checkbox for better overall testing when using any kind of random corruption, uncheck this checkbox for help reproducing bugs or if you are performing the same find and replace corruption.



Create A File Corruption Fault Wizard Page 1 of 3

Corruption Type Selection

Select which type of corruption to use.
The file will be corrupted the next time it is accessed.

File to Corrupt

C:\Documents and Settings\Joe\Desktop\for_corruption.txt

Type of Corruption

○ Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

● Find and replace corruption

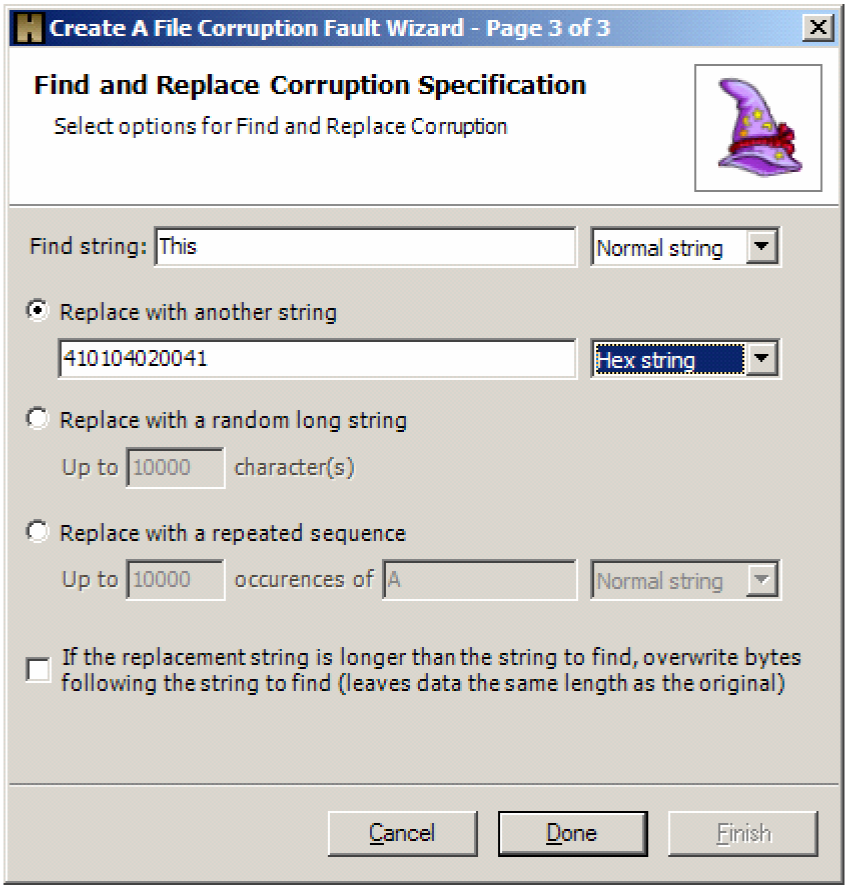
Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

○ Regular expressions

Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

☐ Regenerate the corruption at each access to the original file

In this case we want to search for any occurrence of the normal string "This" and replace it with a number of unprintable Hex characters. The example here shows a string of five unprintable characters preceded and followed by the Hex value 41, which represents ‘A’. I did this so that if the program parses the string properly, I will have a starting and ending place. If an error occurs I will be able to find the character that caused the error.



Create A File Corruption Fault Wizard - Page 3 of 3

Find and Replace Corruption Specification

Select options for Find and Replace Corruption

Find string: This — Normal string

● Replace with another string

410104020041 — Hex string

○ Replace with a random long string

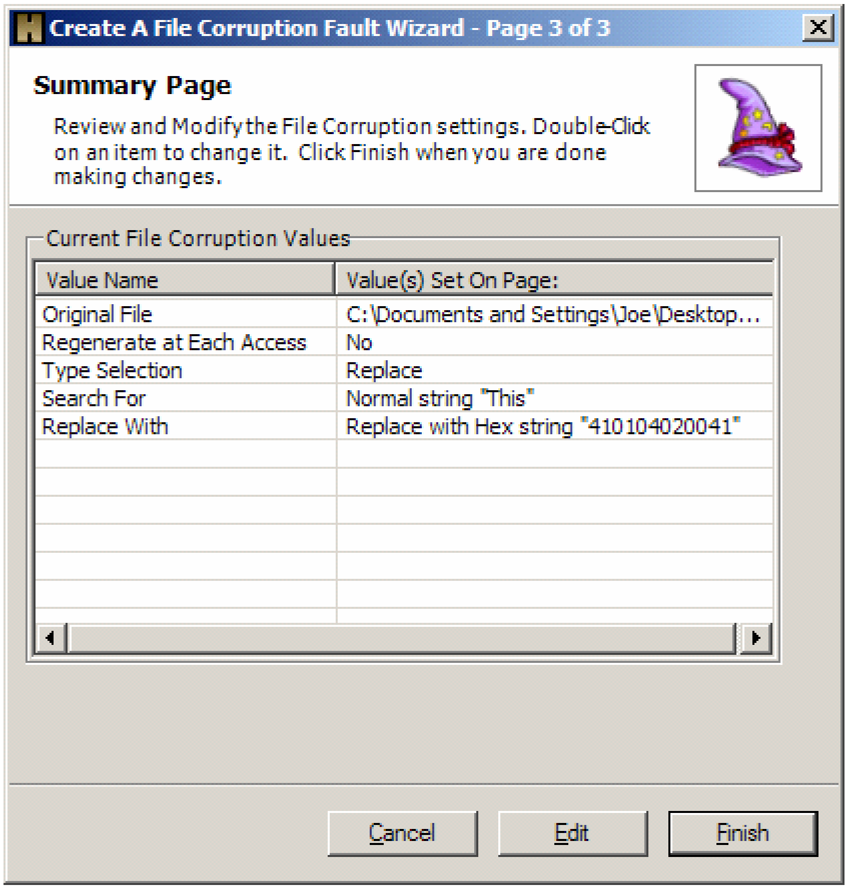
Up to 10000 character(s)

○ Replace with a repeated sequence

Up to 10000 occurences of A — Normal string

□ If the replacement string is longer than the string to find, overwrite bytes following the string to find (leaves data the same length as the original)

The final page shows a summary of the corruption fault you just created. To edit any information on this page simply select it, and click edit. This will take you back to that page to make any necessary changes.



Summary Page

Review and Modify the File Corruption settings. Double-Click on an item to change it. Click Finish when you are done making changes.

Current File Corruption Values

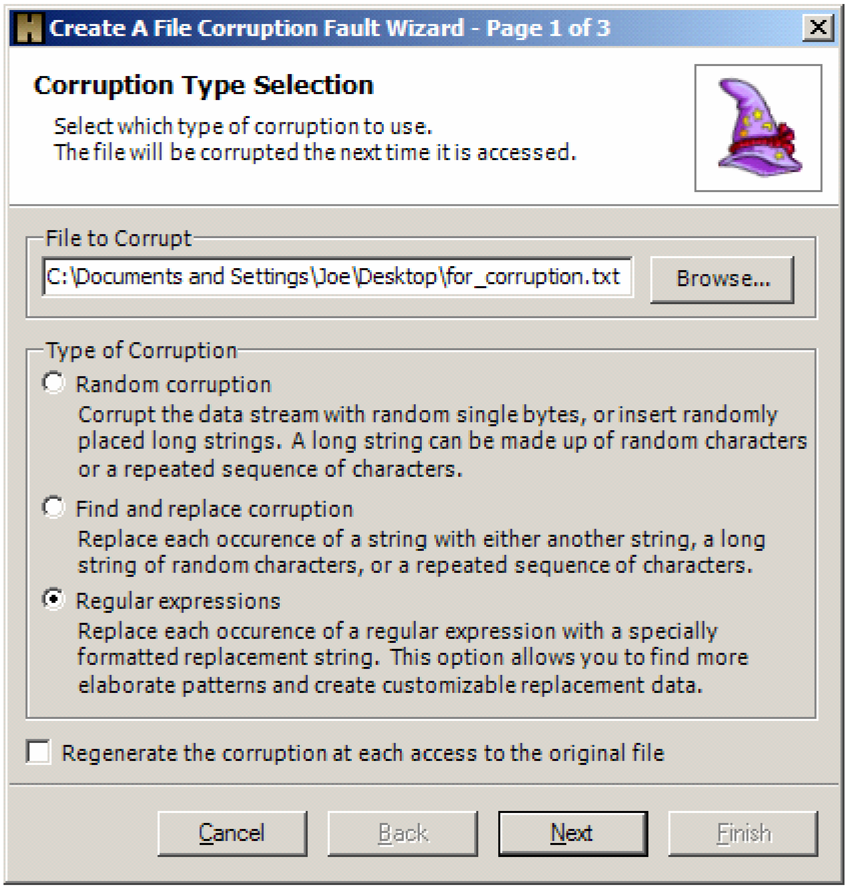
Value Name	Value(s) Set On Page:
Original File	C:\Documents and Settings\Joe\Desktop...
Regenerate at Each Access	No
Type Selection	Replace
Search For	Normal string "This"
Replace With	Replace with Hex string "410104020041"

Create a File Corruption Fault with Regular Expressions

Select the file you wish to corrupt by browsing to it using the Browse… button or type it directly into the "File to Corrupt" text box.

Select Regular expressions. This will allow you to search for a number of different strings, and replace them with normal strings or with expansion strings. This is very useful for matching on filenames, web addresses, or other well formed, but unique, strings.

Holodeck creates a copy of the file to be corrupted and corrupts file on the first access, then uses that same file each time it is accessed unless "Regenerate the corruption at each access to the original file" is checked. Check this checkbox for better overall testing when using any kind of random corruption, uncheck this checkbox for help reproducing bugs or if you are performing the same find and replace corruption.



Create A File Corruption Fault Wizard - Page 1 of 3

Corruption Type Selection

Select which type of corruption to use.
The file will be corrupted the next time it is accessed.

File to Corrupt

C:\Documents and Settings\Joe\Desktop\for_corruption.txt

Type of Corruption

○ Random corruption

Corrupt the data stream with random single bytes, or insert randomly placed long strings. A long string can be made up of random characters or a repeated sequence of characters.

○ Find and replace corruption

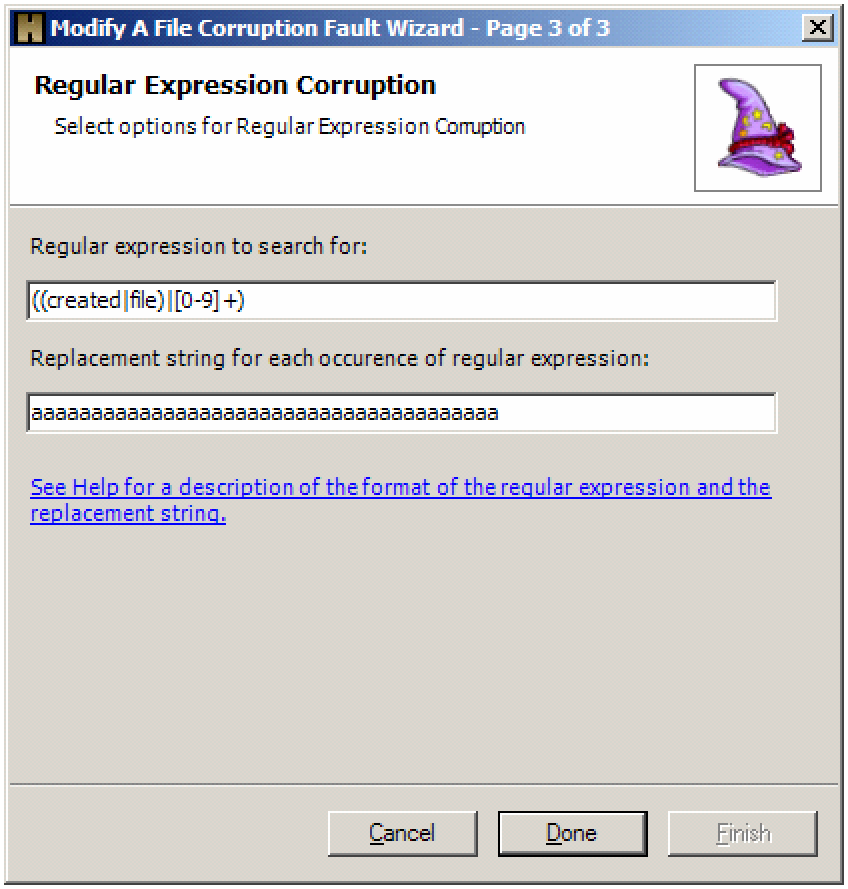
Replace each occurence of a string with either another string, a long string of random characters, or a repeated sequence of characters.

● Regular expressions

Replace each occurence of a regular expression with a specially formatted replacement string. This option allows you to find more elaborate patterns and create customizable replacement data.

□ Regenerate the corruption at each access to the original file

This regular expression: ((created|file)|[0-9]+) will match the word "created" or the word "file" or a string of numbers of any length. My file contains all three of these things so Holodeck will replace any of these occurrences with the long string of ‘a’s below.



Modify A File Corruption Fault Wizard - Page 3 of 3

Regular Expression Corruption

Select options for Regular Expression Corruption

Regular expression to search for:

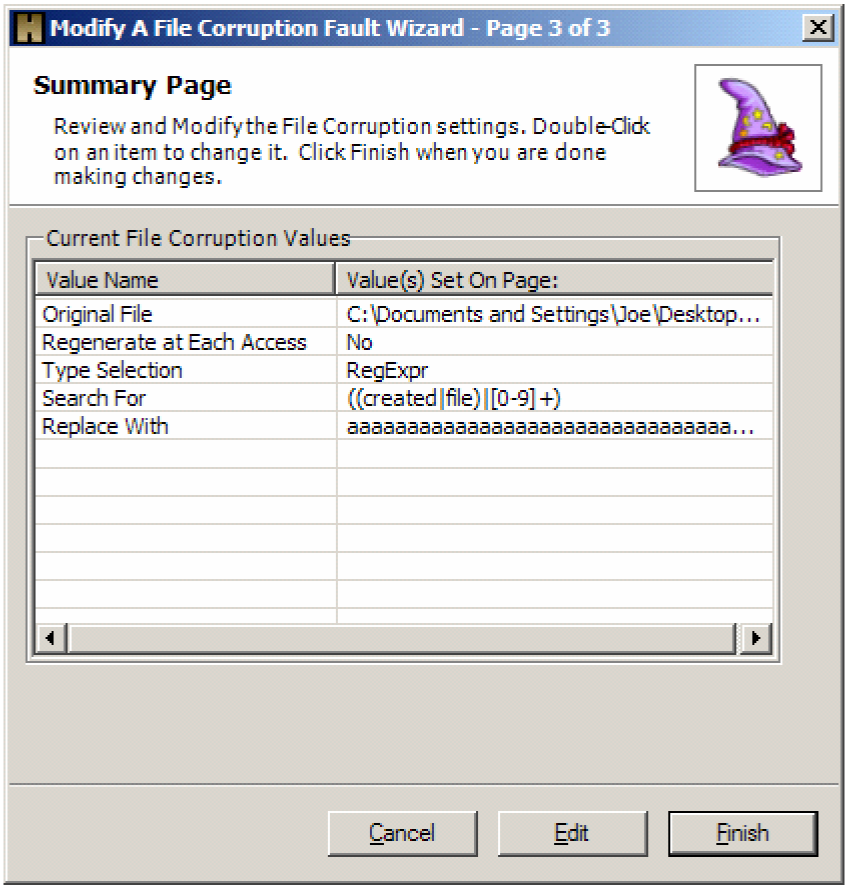
((created|file)|[0-9]+)

Replacement string for each occurence of regular expression:

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

See Help for a description of the format of the regular expression and the replacement string.

The final page shows a summary of the corruption fault you just created. To edit any information on this page simply select it, and click edit. This will take you back to that page to make any necessary changes.



Summary Page

Review and Modify the File Corruption settings. Double-Click on an item to change it. Click Finish when you are done making changes.

Current File Corruption Values

Value Name	Value(s) Set On Page:
Original File	C:\Documents and Settings\Joe\Desktop...
Regenerate at Each Access	No
Type Selection	RegExpr
Search For	((created|file)|[0-9]+)
Replace With	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...

Regular Expressions and Replacement Strings

Using regular expressions

Regular expressions can be helpful while trying to match a well formed string, that may change over time. Regular expressions are used in matching data being sent over the network in the network corruption faults as well as use in file corruption faults.

Note: to replace a string please see the Using replacement strings section.

Regular expression examples:

Match any IP address, with optional port number:
`[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+((:[0-9]+)?)`

`[0-9]+ –` represents a random number between 0 and 9 the following ‘+’ means there can be a string of 1 or more of these numbers.

`\. –` Since ‘.’ character is a reserved character it must be escaped, escape reserved characters by using the ‘\’

`((:[0-9]+)?)` – This section matches a colon first, then a string of random numbers, the final '?' makes this entire section optional.

Match a sequence of 10 or more consecutive "A" characters:

`A{10,}` – An sequence of the preceeding group is represented by {min, max} this regular expression matches a sequence of 10 or more of the character 'A'. If you leave a number for the max out of the expression Holodeck assumes any length.

Match any domain is as follows:

```
([wW]{3,}\.)?([abcefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXY
Z]+)\.(com|net|org)
```

`([wW]{3,}\.)?` - this part matches an optional capital or lowercase "www."

`([abcefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]+)` – this part matches any length string consisting of upper or lowercase alphabet letters, greater than 1 (eg. "abc", "aRdfpQ", etc.)

`\.(com|net|org)` – this part matches a period followed by any one of the following, "com", "net", or "org"

Regular Expression Definition:

All characters except "(", ")", "{", "}", "$", "\", "?", "/", ".", "*", "+", "^", and "|" can be used normally. C escape sequences are defined. To use a reserved character, place a "\" character in front of it (for example, "\+" represents a literal "+" character).

The "." character matches any single character.

A "*" after an expression matches repetition of zero or more times, whereas a "+" character represents repetition of one or more times. A range of repetition counts can be specified with {}, i.e. "a{2,5}" matches between 2 and 5 repetitions of "a".

A "?" following an expression makes it optional (can be present exactly zero or one times).

A "|" between two expressions represents an either-or match. The expression "get|set" will match either "get" or "set".

Character sets can be enclosed in []. The expression "[Gg]et" would match either "Get" or "get".

Sub-expressions can be enclosed in (). These sub-expressions can be referred to directly in the replacement string by numerical order starting at one.

Nonprintable characters can be represented with a C-style octal or hexadecimal escape sequences, i.e. "\0123" for octal or "\xAB" for hexadecimal.

Null characters can be matched using "\x00".

Regular expressions match the string closest to the start of the buffer first, and the length of the matched string second.

Using replacement strings

Replacement strings are useful when trying to insert a string into a stream of data that might have to be formed in a precise manner. This is useful for trying to create an improper string that will be checked as correct by the first or second string checking statements. These replacement strings replace whatever is found when using find and replace corruption or regular expression corruption.

Replacement string examples:

Replace with a random long string of between 500 and 1000 characters, followed by a string of 100 "A" characters:

`$R500,1000$$S100,100,A$ -` This will replace the matched string (regular expression, or find and replace string) with a random string followed by a 100 ‘A’ characters.

`$R500,1000$` - the first ‘R’ tells Holodeck to use Random strings, and expand it from 500 to 1000 characters long.

`$S100,100,A$` - the first ‘S’ tells Holodeck to use the following string and expand it exactly 100 times, since the minimum and maximum are the same.

Duplicate the matched string 500 times:
`$S500,500,$$&$ -` The first ‘S’ tells Holodeck to use the following string.

`$& -` expands to the previously matched string (from the find and replace or regular expression corruption.)

Insert 100 random characters just before the matched string

`$R100,100$$&`

`$R100,100$ -` expands to exactly 100 random characters.

`$& -` expands to the previously matches string (from the find and replace or regular expression corruption)

Replacement strings definition:

All characters except "(", ")", "$", "\", "?", ",", and "/" can be used normally. C escape sequences are defined, as well as the following expansions:

$` Expands to all data from the end of the previous match to the start of the current match.

$& Expands to all of the current match.

$0 Expands to the entire current match.

$N (N is 0-9) Expands to matched sub-expression N.

$Rmin,max$ Expands to a random string of between min and max characters.

$Smin,max,seq$ Expands to a string of between min and max repetitions of character sequence seq.

?Ntrue:false If subexpression N has matched, expand true expression, otherwise expand false expression (or nothing if false expression is not specified).

\/ Expands to a normal / character

Multiple Threads and Processes

Dealing with Multiple Processes

This option is available if you check the Process Chaining option on the last page of the Holodeck Project Setup Wizard. If the application spawns multiple processes, or if you choose to test multiple applications simultaneously Holodeck will allow you to set faults, tests etc for each process.

The features of Holodeck can be focused to test and log a single process, or all processes the Application Under Test spawns. Once process chaining has been set Holodeck will automatically attach to any new processes that are created by the process you are testing.

To test multiple applications at the same time select File > New Test Application, this will bring up the New Test Application Wizard to select an additional Application Under Test. You can specify different APIs to log for each Application Under Test, by selecting the functions under Log > Functions Logged…

Each new process the Application Under Test spawns can be treated like its own application. You can set limits, faults, and tests on each new process, as well as viewing resources specific to that process.

Working with Multi-threaded applications

Holodeck will automatically track any new threads that are created by the process you are testing. If Holodeck is in Per-Thread mode each new thread will show up in the Project Pane as a child of its parent process. This can be extremely useful for testing specific threads, such as threads in charge of reading a file or parsing incoming network traffic.

To turn on Per-Thread mode click Session > Per Thread from the Menu.

Each new thread the application spawns can be treated like its own application, allowing you to set limits, faults, and tests on each thread individually. Each fault, limit, or test set on a single thread will only apply to that thread, however, setting a fault, limit or test on the main process node will create that fault, limit or test for all Threads of that process.

To change limits, set faults etc. expand the thread by clicking the ‘+’ sign next to the thread.

Double clicking an active log node in the Project Pane will open a log pane that will show just entries for the thread you chose.

Exceptions and mini-dumps

Exceptions Overview

Holodeck catches all exceptions your application produces. Exceptions are routed through Holodeck first, as a first chance exception, then passed back to the application to handle. If the application does not handle the exception it is logged as a second chance exception.

View the Exception in a debugger by right clicking an exception in the Exception Pane and selecting "View Exception in Debugger." If you have a debugger attached to the application the debugger may catch the second chance exception allowing you to handle the exception in other ways. If source code is available your debugger may be able to use the exception information provided by Holodeck to step into the exception causing function.

Mini-dump Overview

You can save the mini-dump information for debugging the application at a later time. The mini-dump file is a snapshot of the computer state at the time of the crash. Matching images must be available because mini-dump files store very little information; they store only some of the volatile information at the time of the crash. They do not store the basic code streams that the computer loaded into memory. Instead, to save space, the mini-dump file stores only the name and time stamp of the images loaded on the crashing computer.

To examine the code that was running on the crashing computer, the debugger must be given access to the same binaries that the crashing computer was running. The debugger uses the name and time stamp stored in the mini-dump file to uniquely match and load the binaries when the developer wants to debug the crash.

Recording and replaying sessions

Introduction to recoding and replaying

You can create a Recorded Session while testing the Application Under Test using Holodeck by using the **Record Session** Functionality. This will allow you to reproduce a test or bug more precisely than trying to remember and write down steps. Recorded Sessions are global to your entire project, so they will record changes to all of the process and threads being tested by Holodeck.

While recording Holodeck records each change in Holodeck including when faults, tests, limits etc are set and lifted. Recording does not save UI changes, input, or any changes from a test harness.

Holodeck records every application in the current Holodeck Session, however, if no changes are made to the application it will not interfere with the recording of the other applications.

Creating a recorded session

A Recorded Session can be created by any of the following methods

1) From the Project Pane
a) Right Click the Recorded Sessions node in the Project Pane
b) Click Create a Recorded Session
2) From the Menu
a) Click Session -> Record Session

Once a Recorded Session has been started Holodeck will log every change within Holodeck, faults, limits, tests, etc are all recorded in the recordedSession.xml file. Holodeck does not record UI testing, or input that must be handled by the test harness.

When you are finished recording your test session stop recording by…
1) Click Session -> Stop Recording
2) Right click the newly created test and click Stop Recording

Note: when recording a session Holodeck records all changes made in Holodeck to all applications for the current session.

Replaying a recorded session

Replaying a recorded session and ensure Holodeck sets and lifts the same hostile environments every time it is run. Use this every time test scripts are run so you can ensure reproducibility of bugs, and ensure you are testing the same things on each different build.

When a recorded session is replayed Holodeck will set each fault, test, limit etc. according to the logs coming in, as it was set when recording.

1) Right click the Recorded Session you would like to replay and select Replay from the menu.
2) Select the Recorded Session you would like to replay and select Replay Session from the Tests Menu
3) This will start the recorded session; Holodeck will automatically restart the Application Under Test and begin the repro steps exactly as they were recorded. Playing a Recorded session will set all the faults, limits, tests, etc. that were set while recording at the same relative time to application start.

Add Holodeck Intercepts

Add Holodeck Intercepts

Holodeck Intercepts Manager

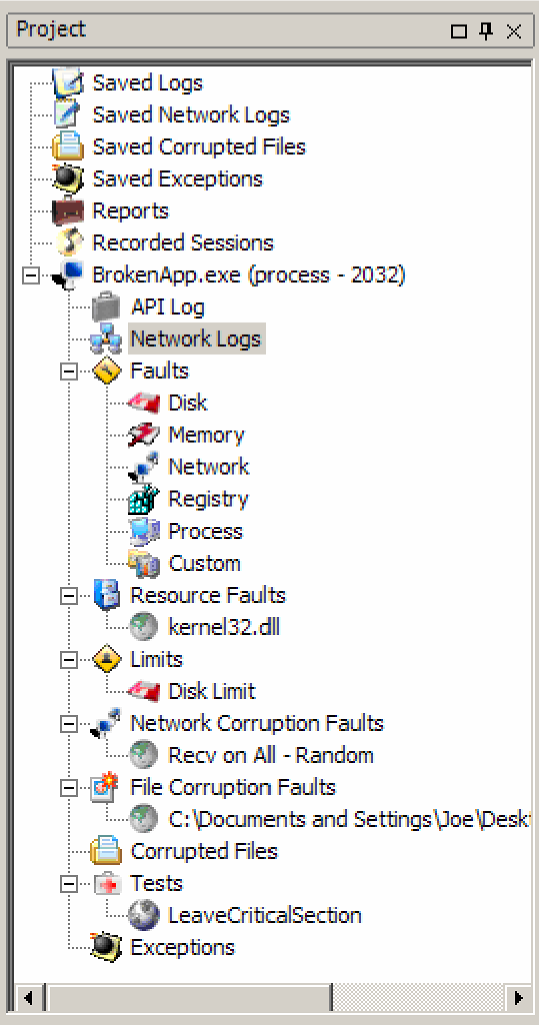
Holodeck Windows and Panes

Project Pane

The Project Pane will help you to display and organize your project entries into a tree view. The majority of the information about your project will be displayed here.

Double clicking on any node brings into focus the corresponding UI, for instance double clicking on the faults node will bring up the faults pane.

Show the Project Pane by clicking Project Pane button on the Project Toolbar, or click View > "Project Pane"



Global Nodes contain information that pertains to the entire session.

Saved Logs – API Logs which have been previously saved can be reviewed here.

Saved Network Logs – Network Logs which have been previously saved can be reviewed here.

Saved Corrupted Files – Corrupted Files which have been previously saved can be reviewed here.

Saved Exceptions – Exceptions which have been previously saved can be reviewed here.

Reports – View all reports created for this session.

Recorded Sessions – View and replay all Recorded Sessions for this session.

All nodes under a Process node contain information that pertains to the process.

If the Application Under Test has multiple threads or processes, each new thread or process will show up here, as a new node with its own Active Log, Resources, Faults, Limits and Tests.

Log Pane – View all the API function logs Holodeck has created.

Network Logs Pane – View the packets intercepted over the network.

Faults Pane – View and set faults.

Resource Faults Pane – View faults currently enabled, and create new ones.

Limits Pane – View and create hardware resource limits.

Network Corruption Faults Pane – View Network corruption currently enabled.

File Corruption Faults Pane – View File corruption currently enabled.

Corrupted Files Pane – View the Files that Holodeck has corrupted based on File Corruption Faults.

Test Pane – View the scheduled test currently enabled for your application.

Exception Pane – View the exceptions your application has produced and save mini-dump files.

Viewing with per-process granularity:

1) There are two scenarios in which Holodeck will show multiple processes.
    a) Testing two applications at the same time.
    b) The Test application spawns a child process.
        i) Process Chaining must be turned on from the project wizard for Holodeck to follow the child processes

For more information on testing multiple processes see the Dealing with Multiple Processes help topic.

Viewing with per-thread granularity:

1) If your test application spawns new threads while running Holodeck will automatically begin logging these threads

2) By selecting the new thread you can view the active log for that thread, view the resources used by that specific thread, and set faults, limits or tests.

To turn on per-thread functionality Click Session > Per Thread.

When in per-thread mode, Holodeck automatically separates all relevant nodes in the project pane by ThreadID. This allows you to set faults and test to be specific to a single thread; you can also view API logs, Network Logs and Exceptions on a per-thread level.

You can still set faults and tests to span an entire application, simply select the fault or tests node directly under the application node in the project pane. To view API logs, Network logs or Exceptions generated by the entire application, select the node directly under the application node in the Project Pane.

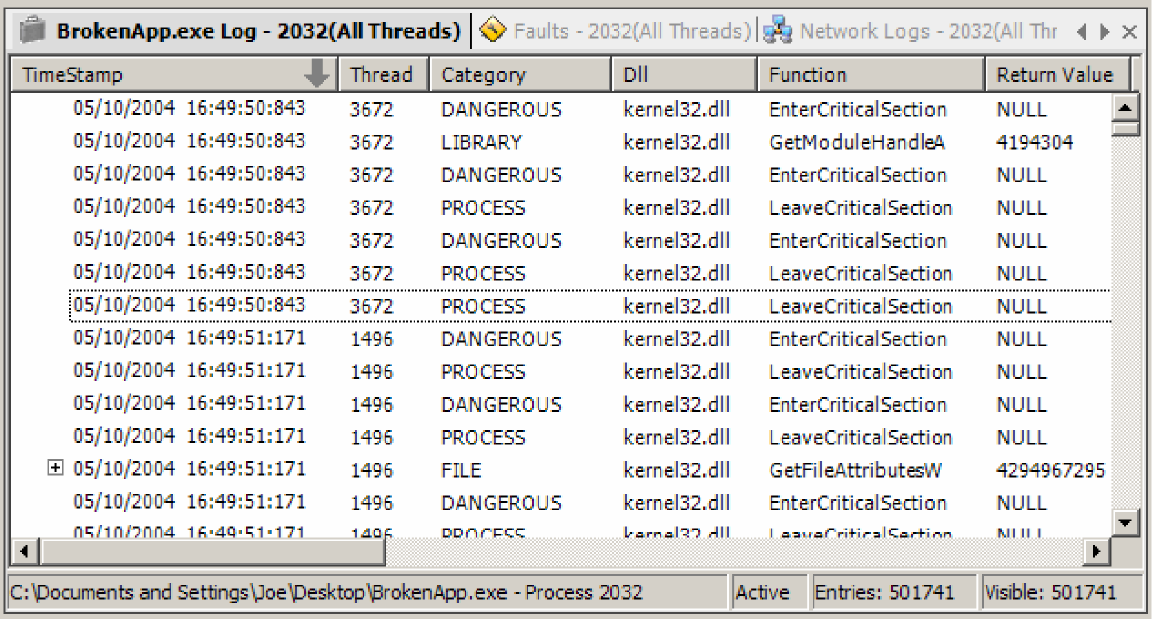
Log Pane

As soon as you begin the Application Under Test Holodeck will start to log the API calls you have selected. The log pane will hold any logs you are currently viewing. Each log will be titled by the application you are currently working with, in the format Appname processID(threadID) where All Threads for threadID means the log applies to all threads in this process.

In the below example for the log on the left Notepad is the Application Under Test 2788 is its process ID, and this log is for all the threads in the process.

In the below example for the log on the right Notepad is still the Application Under Test, 2788 is its process ID, and this log only covers the API calls for the thread 2792.

Show the Log Pane by double-clicking the API node in the Project pane.



BrokenApp.exe Log - 2032(All Threads) | Faults - 2032(All Threads) | Network Logs - 2032(All Thr

TimeStamp	Thread	Category	Dll	Function	Return Value
05/10/2004 16:49:50:843	3672	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL
05/10/2004 16:49:50:843	3672	LIBRARY	kernel32.dll	GetModuleHandleA	4194304
05/10/2004 16:49:50:843	3672	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL
05/10/2004 16:49:50:843	3672	PROCESS	kernel32.dll	LeaveCriticalSection	NULL
05/10/2004 16:49:50:843	3672	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL
05/10/2004 16:49:50:843	3672	PROCESS	kernel32.dll	LeaveCriticalSection	NULL
05/10/2004 16:49:50:843	3672	PROCESS	kernel32.dll	LeaveCriticalSection	NULL
05/10/2004 16:49:51:171	1496	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL
05/10/2004 16:49:51:171	1496	PROCESS	kernel32.dll	LeaveCriticalSection	NULL
05/10/2004 16:49:51:171	1496	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL
05/10/2004 16:49:51:171	1496	PROCESS	kernel32.dll	LeaveCriticalSection	NULL
⊞ 05/10/2004 16:49:51:171	1496	FILE	kernel32.dll	GetFileAttributesW	4294967295
05/10/2004 16:49:51:171	1496	DANGEROUS	kernel32.dll	EnterCriticalSection	NULL
05/10/2004 16:49:51:171	1496	PROCESS	kernel32.dll	LeaveCriticalSection	NULL

C:\Documents and Settings\Joe\Desktop\BrokenApp.exe - Process 2032 | Active | Entries: 501741 | Visible: 501741

By default Holodeck will display the following information in the log pane: TimeStamp, Thread, Category, DLL, Function, Return Value, Error Code, Exception, and a list of parameters.

For more information on working with logs, please see the Logs Overview in the Holodeck In Depth Section.

Network Logs Pane

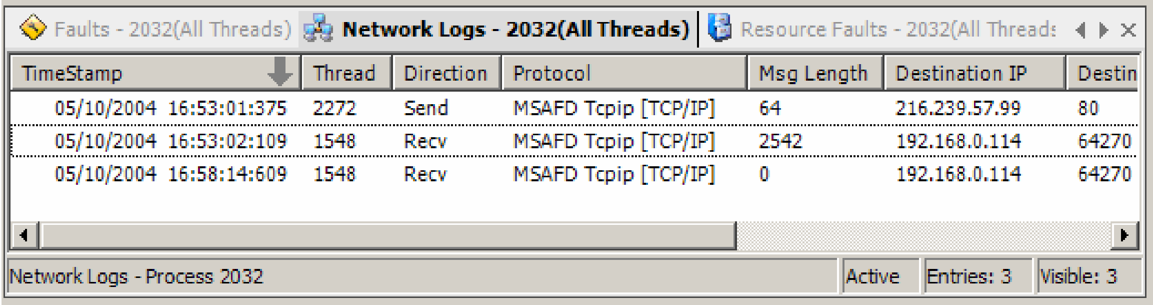
Holodeck automatically intercepts all messages sent and received over the network. These messages can be found in the network logs pane.

Select which columns are displayed by right clicking and selecting "Select Visible Columns…

View the message details of a network message by opening the Network Message Details Pane

Export the contents of the Network logs by right clicking the Network Logs node in the Project Pane and selecting "Export Log to File"

Show the Network Logs pane by double-clicking on the Network Logs node in the Project Pane.



Faults - 2032(All Threads) | Network Logs - 2032(All Threads) | Resource Faults - 2032(All Thread:

TimeStamp	Thread	Direction	Protocol	Msg Length	Destination IP	Destin
05/10/2004 16:53:01:375	2272	Send	MSAFD Tcpip [TCP/IP]	64	216.239.57.99	80
05/10/2004 16:53:02:109	1548	Recv	MSAFD Tcpip [TCP/IP]	2542	192.168.0.114	64270
05/10/2004 16:58:14:609	1548	Recv	MSAFD Tcpip [TCP/IP]	0	192.168.0.114	64270

Network Logs - Process 2032 | Active | Entries: 3 | Visible: 3

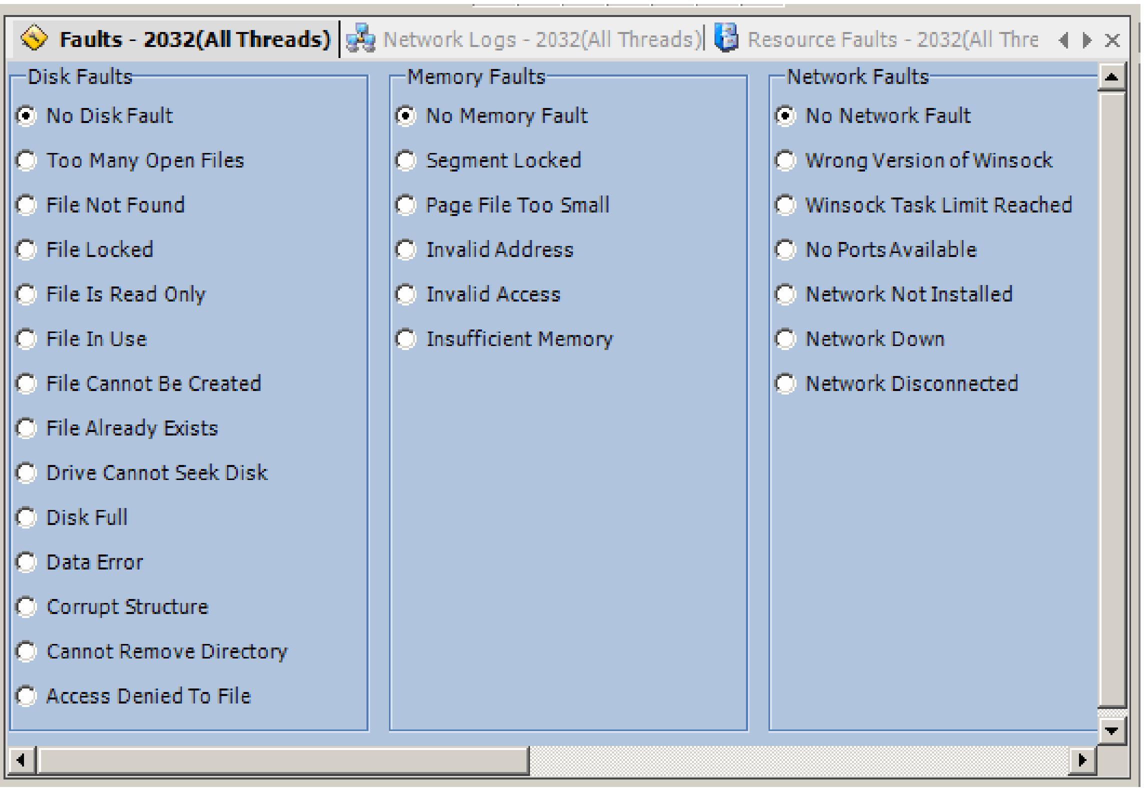
For more information regarding the Network Logs see the help topic within Holodeck in Depth

Faults Pane

The Faults Pane shows all available "out of the box" faults Holodeck ships with. Use these faults to simulate different hardware and software failures, easily and precisely. To enable each fault simply select a bullet at the right of the fault you would like to enable. Holodeck supports one fault per category.

Holodeck shows the Faults Pane once the application under test has finished loading.

To view the Faults Pane otherwise, double click the Faults node or a Faults Category node in the Project Pane.


Faults - 2032(All Threads)
Network Logs - 2032(All Threads)
Resource Faults - 2032(All Thre

Disk Faults

- ● No Disk Fault
- ○ Too Many Open Files
- ○ File Not Found
- ○ File Locked
- ○ File Is Read Only
- ○ File In Use
- ○ File Cannot Be Created
- ○ File Already Exists
- ○ Drive Cannot Seek Disk
- ○ Disk Full
- ○ Data Error
- ○ Corrupt Structure
- ○ Cannot Remove Directory
- ○ Access Denied To File

Memory Faults

- ● No Memory Fault
- ○ Segment Locked
- ○ Page File Too Small
- ○ Invalid Address
- ○ Invalid Access
- ○ Insufficient Memory

Network Faults

- ● No Network Fault
- ○ Wrong Version of Winsock
- ○ Winsock Task Limit Reached
- ○ No Ports Available
- ○ Network Not Installed
- ○ Network Down
- ○ Network Disconnected

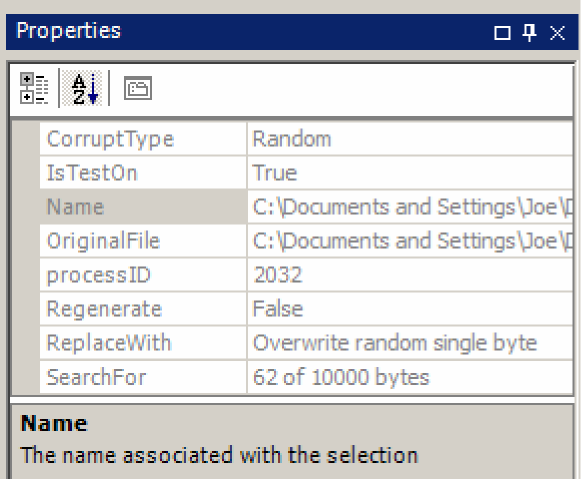
See the Faults Overview for more information concerning faults.

Properties Pane

The purpose of the property pane is to provide you with information regarding selected UI objects. Look here for additional information about the UI you are currently working with

General Layout - The property pane toolbox window provides information in an expandable tree-view using a table. Each table can be expanded or collapsed using the +/- button in the upper left hand corner.

Show the Properties Pane by clicking the Show/Hide Property Pane button on the Project toolbar or Click View > "Properties Pane" from the menu.



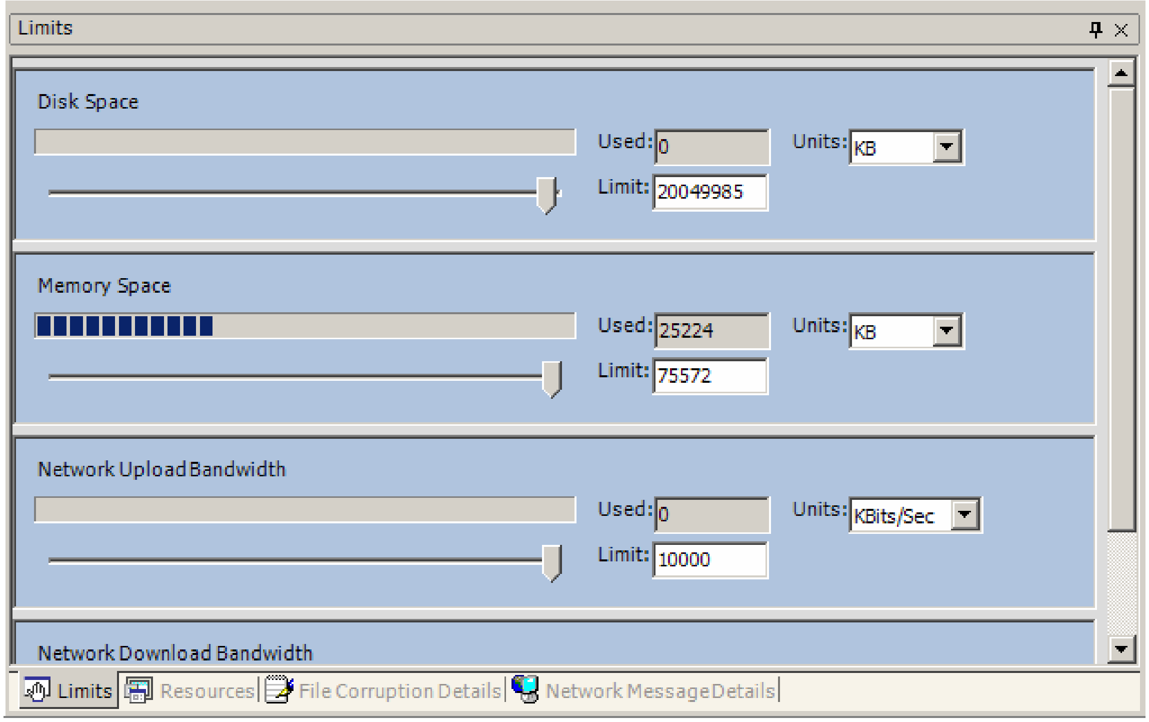
CorruptType	Random
IsTestOn	True
Name	C:\Documents and Settings\Joe\
OriginalFile	C:\Documents and Settings\Joe\
processID	2032
Regenerate	False
ReplaceWith	Overwrite random single byte
SearchFor	62 of 10000 bytes

Name
The name associated with the selection

Limits Pane

The Limits Pane allows you to limit the amount of a resource your application has available to it. For instance, using Holodeck you could simulate a computer with a smaller Hard Drive, Less RAM, or a slower internet connection.

Show the limits pane by clicking the Show/Hide Limits Pane Node on the Project toolbar or by clicking View > Limits Pane from the Menu.



Disk Space
Used: 0
Units: KB
Limit: 20049985

Memory Space
Used: 25224
Units: KB
Limit: 75572

Network Upload Bandwidth
Used: 0
Units: KBits/Sec
Limit: 10000

Network Download Bandwidth

To find out more about Limits check out the Limits overview in the Holodeck in depth section.

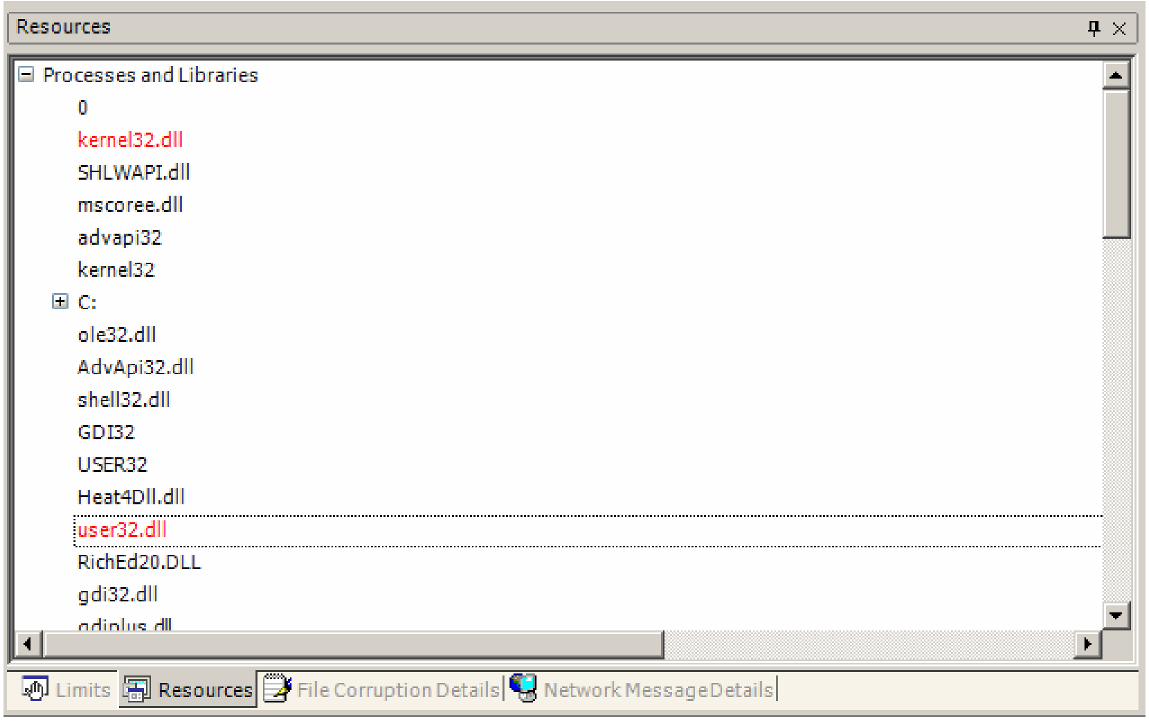
Resource Pane

Holodeck can also track external file, library, and registry resources and log every read, write, update, or access the Application Under Test makes. The resource pane shows al these resources in an easy to read tree view.

To show what resources the Application Under Test is using make sure the resources pane is open by clicking View and verifying there is a check mark by Resource Pane. From here you can view exactly which resources the Application Under Test is using. You can change which resources are displayed by clicking the different nodes in the Project pane.

You can set a resource fault easily by finding the resource in the treeview right clicking and selecting the desired fault. When a fault has been set for a resource the text will be displayed in red.

Show the Resource Pane by clicking the Show/Hide button on the Project toolbar or click View > "Project Pane" on the menu.



```
⊟ Processes and Libraries
      0
      kernel32.dll
      SHLWAPI.dll
      mscoree.dll
      advapi32
      kernel32
   ⊞ C:
      ole32.dll
      AdvApi32.dll
      shell32.dll
      GDI32
      USER32
      Heat4Dll.dll
      user32.dll
      RichEd20.DLL
      gdi32.dll
      gdiplus.dll
```

Holodeck automatically combines the registry paths from multiple registry API calls to give you the full path, even if that was not what was used in the last API call. Holodeck also combines file paths to give you the full file path.

Jump to the last log entry that touched a resource by right clicking the resource in the resource pane and selecting "Select most recent log entry"

Export a complete list of which resources your application has accessed by clicking File > "Export Resource to File…"

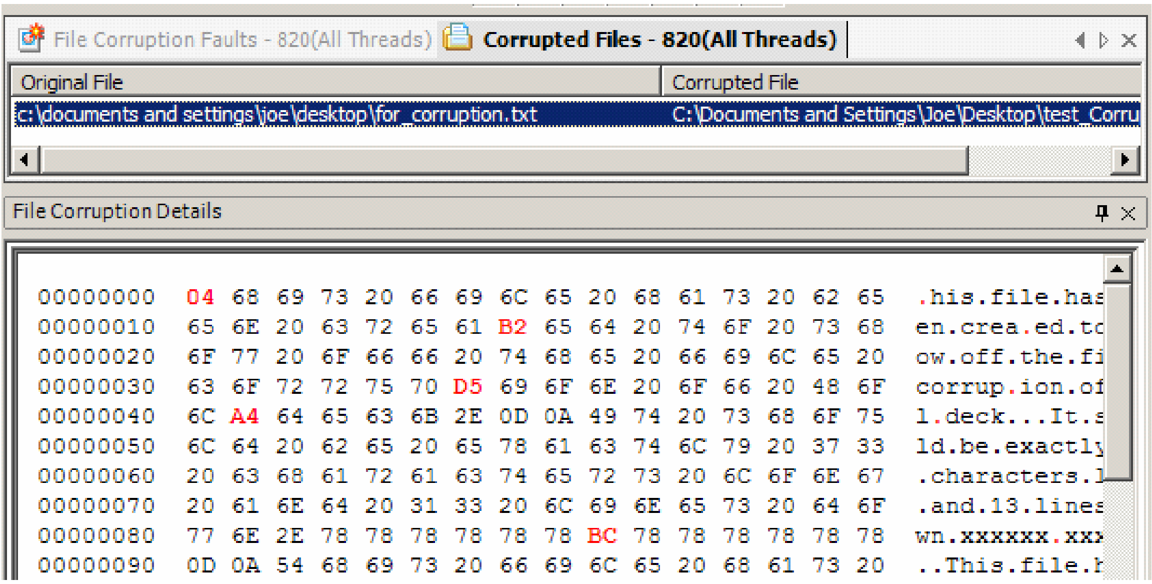
For more information please see the Resource Fault Overview help topic in the Holodeck in Depth Section.

File Corruption Details Pane

The file corruption details pane shows exactly how a file has been corrupted. All changes Holodeck has made to a file through the file corruption faults will show up here. Holodeck will highlight any changes made in red. The center column is a hexadecimal display of the file, and how it has been changed by Holodeck; use this display to see changes in characters that may not be able to be able to be displayed. The right column shows the file in its ASCII representation so it is easy to read.

You must select an item from the Corrupted Files Pane to show the File Corruption Details Pane.

To show the File Corruption Details Pane double-click a Corrupted file in the Corrupted Files Pane.


File Corruption Faults - 820(All Threads)
Corrupted Files - 820(All Threads)
File Corruption Details

Original File	Corrupted File
c:\documents and settings\joe\desktop\for_corruption.txt	C:\Documents and Settings\Joe\Desktop\test_Corru

```
00000000  04 68 69 73 20 66 69 6C 65 20 68 61 73 20 62 65  .his.file.has
00000010  65 6E 20 63 72 65 61 B2 65 64 20 74 6F 20 73 68  en.crea.ed.to
00000020  6F 77 20 6F 66 66 20 74 68 65 20 66 69 6C 65 20  ow.off.the.fi
00000030  63 6F 72 72 75 70 D5 69 6F 6E 20 6F 66 20 48 6F  corrup.ion.of
00000040  6C A4 64 65 63 6B 2E 0D 0A 49 74 20 73 68 6F 75  l.deck...It.s
00000050  6C 64 20 62 65 20 65 78 61 63 74 6C 79 20 37 33  ld.be.exactly
00000060  20 63 68 61 72 61 63 74 65 72 73 20 6C 6F 6E 67  .characters.l
00000070  20 61 6E 64 20 31 33 20 6C 69 6E 65 73 20 64 6F  .and.13.lines
00000080  77 6E 2E 78 78 78 78 78 78 BC 78 78 78 78 78 78  wn.xxxxxx.xxx
00000090  0D 0A 54 68 69 73 20 66 69 6C 65 20 68 61 73 20  ..This.file.h
```

Test Pane

When you use the Create a Scheduled Test Wizard to create a test it will show up in the test pane.

To show the Test Pane double click the Tests Node in the Project Pane.

On/Off – Turn this test on or off without interrupting other processing.

Target Thread – The thread this test will be testing on. A zero in this field means the test applies to all threads.

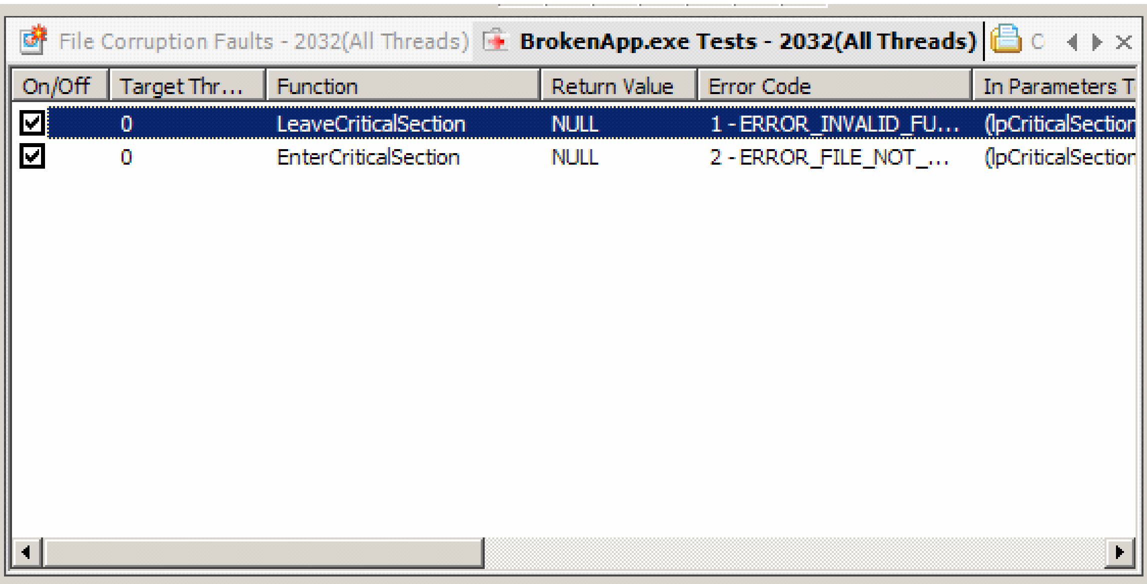
Function – The function to test.

Return Value – The value the test function will return.

Error Code – Upon return the function will set this as the last error

In Parameters to match – The in Parameters to match based on your specifications

Out Parameters to Change – If the in parameter specification has been met, out parameters will be changed to this.

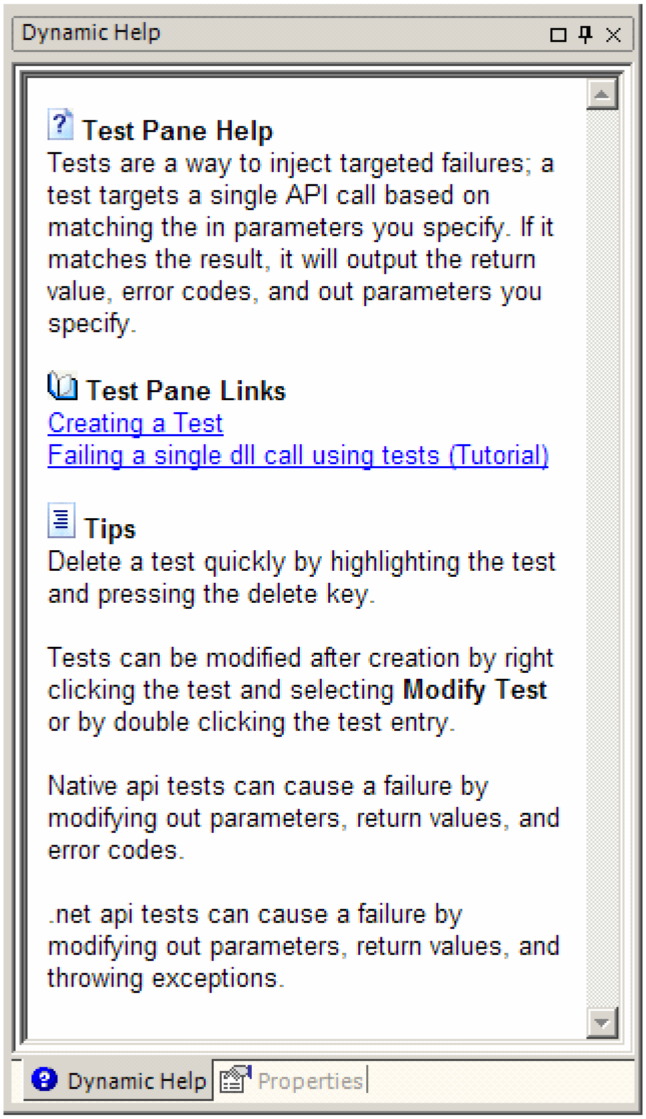

File Corruption Faults - 2032(All Threads)
BrokenApp.exe Tests - 2032(All Threads)
C

On/Off	Target Thr...	Function	Return Value	Error Code	In Parameters T
☑	0	LeaveCriticalSection	NULL	1 - ERROR_INVALID_FU...	(lpCriticalSection
☑	0	EnterCriticalSection	NULL	2 - ERROR_FILE_NOT_...	(lpCriticalSection

Dynamic Help Pane

The dynamic help pane will change to display help related to the pane that is currently selected. A brief introduction, links to useful help topics and quick tips will be displayed in this pane. Follow one of the provided links to learn more about the task at hand.

To show the Dynamic Help pane click the Show/Hide Dynamic Help button on the Project toolbar or click View > Dynamic Help on the menu.



Test Pane Help

Tests are a way to inject targeted failures; a test targets a single API call based on matching the in parameters you specify. If it matches the result, it will output the return value, error codes, and out parameters you specify.

Test Pane Links

Creating a Test

Failing a single dll call using tests (Tutorial)

Tips

Delete a test quickly by highlighting the test and pressing the delete key.

Tests can be modified after creation by right clicking the test and selecting **Modify Test** or by double clicking the test entry.

Native api tests can cause a failure by modifying out parameters, return values, and error codes.

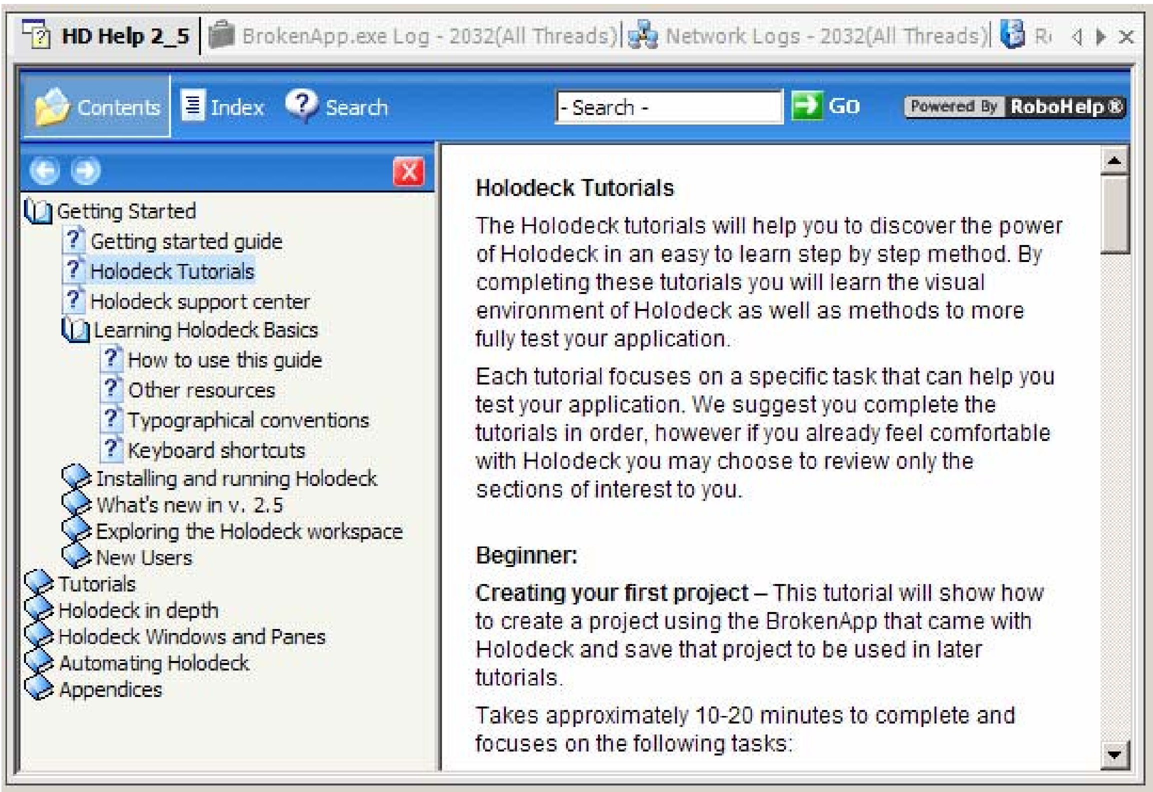
.net api tests can cause a failure by modifying out parameters, return values, and throwing exceptions.

Help Pane

The Help pane is the central pane that shows the main help topics. To print a help topic right click anywhere in main, lower right frame and select "Print…"

The complete help documentation in PDF form is available in the help directory or for download here.

Show the Help pane by selecting Help > "Help Topics…" from the menu.



Holodeck Tutorials

The Holodeck tutorials will help you to discover the power of Holodeck in an easy to learn step by step method. By completing these tutorials you will learn the visual environment of Holodeck as well as methods to more fully test your application.

Each tutorial focuses on a specific task that can help you test your application. We suggest you complete the tutorials in order, however if you already feel comfortable with Holodeck you may choose to review only the sections of interest to you.

Beginner:

Creating your first project – This tutorial will show how to create a project using the BrokenApp that came with Holodeck and save that project to be used in later tutorials.

Takes approximately 10-20 minutes to complete and focuses on the following tasks:

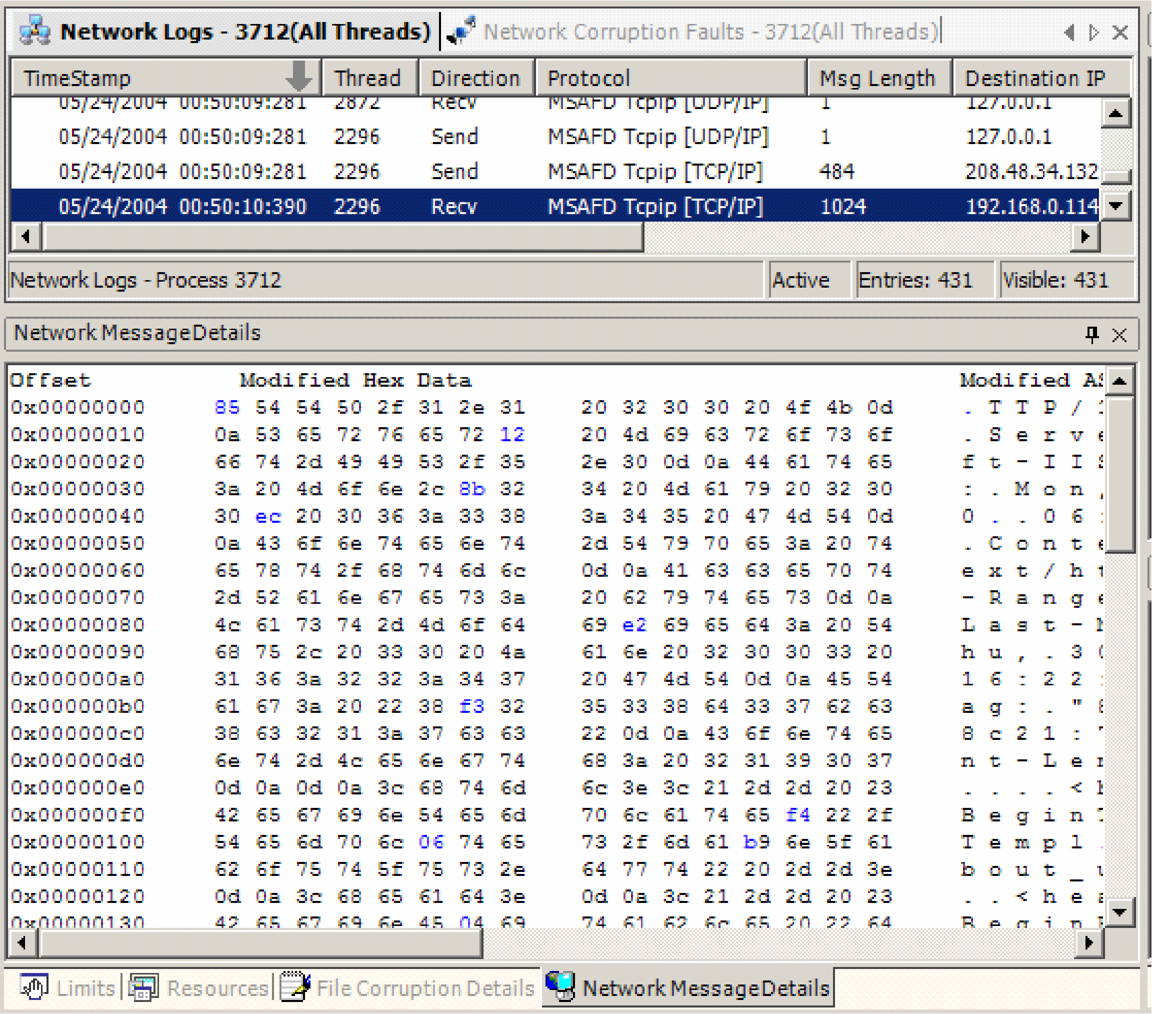
Network Message Details Pane

This pane contains the details of the network message of the highlighted network log entry. Both the original packet and the corrupted packet are shown side by side. The offset, Hex Data and the ascii representation are shown for each packet. Any modification Holodeck has made to the packet through a Network Corruption Fault is highlighted in blue in the modified packet on the left. Modifications made to the packet are highlighted in red in the original packet data on the right.

This data is accessible through the Network logs pane. Find a packet you are interested in, and double click it. This will bring up the entire packet information into the Network Message Details Pane.

You must select an item from the network logs pane to view Network Message Details data.

Show the Network Logs Pane by double-clicking the Network Logs Node in the Project Pane.



Network Logs - 3712(All Threads) | Network Corruption Faults - 3712(All Threads)

TimeStamp	Thread	Direction	Protocol	Msg Length	Destination IP
05/24/2004 00:50:09:281	2872	Recv	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:50:09:281	2296	Send	MSAFD Tcpip [UDP/IP]	1	127.0.0.1
05/24/2004 00:50:09:281	2296	Send	MSAFD Tcpip [TCP/IP]	484	208.48.34.132
05/24/2004 00:50:10:390	2296	Recv	MSAFD Tcpip [TCP/IP]	1024	192.168.0.114

Network Logs - Process 3712 | Active | Entries: 431 | Visible: 431

Network MessageDetails

```
Offset           Modified Hex Data                                         Modified AS
0x00000000      85 54 54 50 2f 31 2e 31   20 32 30 30 20 4f 4b 0d    . T T P /
0x00000010      0a 53 65 72 76 65 72 12   20 4d 69 63 72 6f 73 6f    . S e r v
0x00000020      66 74 2d 49 49 53 2f 35   2e 30 0d 0a 44 61 74 65    f t - I I
0x00000030      3a 20 4d 6f 6e 2c 8b 32   34 20 4d 61 79 20 32 30    : . M o n
0x00000040      30 ec 20 30 36 3a 33 38   3a 34 35 20 47 4d 54 0d    0 . . 0 6
0x00000050      0a 43 6f 6e 74 65 6e 74   2d 54 79 70 65 3a 20 74    . C o n t
0x00000060      65 78 74 2f 68 74 6d 6c   0d 0a 41 63 63 65 70 74    e x t / h
0x00000070      2d 52 61 6e 67 65 73 3a   20 62 79 74 65 73 0d 0a    - R a n g
0x00000080      4c 61 73 74 2d 4d 6f 64   69 e2 69 65 64 3a 20 54    L a s t -
0x00000090      68 75 2c 20 33 30 20 4a   61 6e 20 32 30 30 33 20    h u , . 3
0x000000a0      31 36 3a 32 32 3a 34 37   20 47 4d 54 0d 0a 45 54    1 6 : 2 2
0x000000b0      61 67 3a 20 22 38 f3 32   35 33 38 64 33 37 62 63    a g : . "
0x000000c0      38 63 32 31 3a 37 63 63   22 0d 0a 43 6f 6e 74 65    8 c 2 1 :
0x000000d0      6e 74 2d 4c 65 6e 67 74   68 3a 20 32 31 39 30 37    n t - L e
0x000000e0      0d 0a 0d 0a 3c 68 74 6d   6c 3e 3c 21 2d 2d 20 23    . . . . <
0x000000f0      42 65 67 69 6e 54 65 6d   70 6c 61 74 65 f4 22 2f    B e g i n
0x00000100      54 65 6d 70 6c 06 74 65   73 2f 6d 61 b9 6e 5f 61    T e m p l
0x00000110      62 6f 75 74 5f 75 73 2e   64 77 74 22 20 2d 2d 3e    b o u t _
0x00000120      0d 0a 3c 68 65 61 64 3e   0d 0a 3c 21 2d 2d 20 23    . . < h e
0x00000130      42 65 67 69 6e 45 04 69   74 61 62 6c 65 20 22 64    B e g i n
```

File Corruption Faults Pane

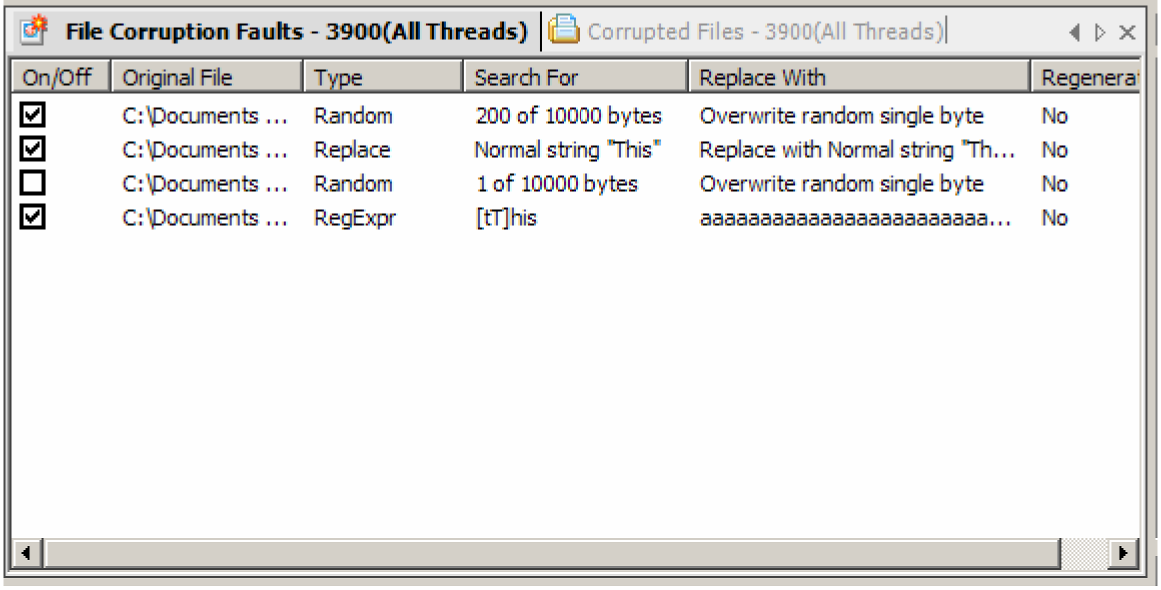
Each File Corruption Fault you create will show up as an item in this pane. You can turn faults on or off by toggling the checkmark beside each fault. Double click a fault to edit its corruption properties. Modify which columns are shown by right clicking anywhere in the pane and clicking "Select Visible Columns."

To create a new fault from the File Corruption Faults Pane right click anywhere in the pane and select "Create a new Fault"

When a file is accessed by the application under test it will show up in the Corrupted Files Pane

Turn a File Corruption Fault on or off quickly by toggling the check in the On/Off Column.

Show the File Corruption Faults pane by double-clicking the File Corruption Faults Node in the Project Pane.



File Corruption Faults - 3900(All Threads)
Corrupted Files - 3900(All Threads)

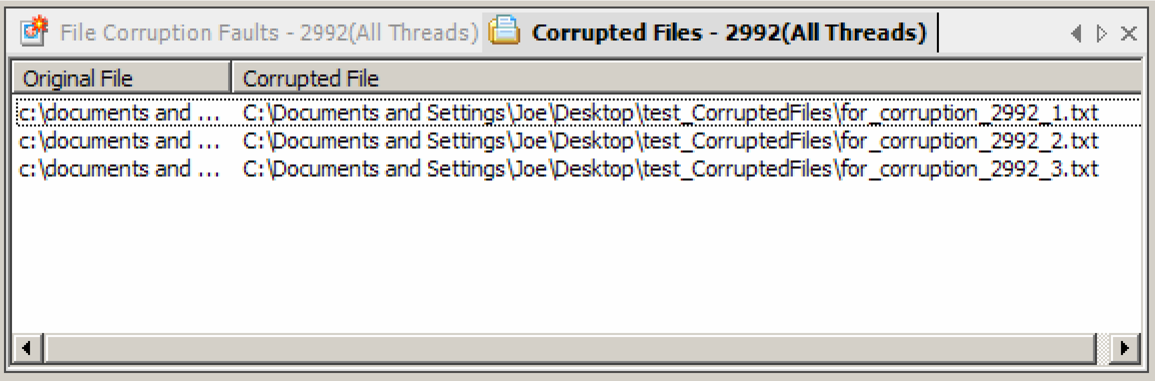
On/Off	Original File	Type	Search For	Replace With	Regenera
☑	C:\Documents ...	Random	200 of 10000 bytes	Overwrite random single byte	No
☑	C:\Documents ...	Replace	Normal string "This"	Replace with Normal string "Th...	No
□	C:\Documents ...	Random	1 of 10000 bytes	Overwrite random single byte	No
☑	C:\Documents ...	RegExpr	[tT]his	aaaaaaaaaaaaaaaaaaaaaaaa...	No

Corrupted Files Pane

Through the Corrupted Files Pane Holodeck allows you to save the original file, save the corrupted file, save the file corruption details, and delete the corrupted file. Saving the corrupted file is useful for reproducing file parsing bugs since Holodeck may not corrupt the file the same each time.

You can also save the corruption details to a HTML file by right clicking the corrupted file and selecting "Save HTML details." Saving the HTML details of a corrupted file exports the offset, hex value, and ascii representation of the file. Before each modification to the original file a red x is displayed; any other modification to the file is represented in both the hex values and ASCII in blue text. This is also good file to attach to a bug report since it may contain unprintable characters that will help a developer track down and fix the reported bug.

Show the Corrupted Files Pane by double-clicking on the Corrupted Files Node in the Project Pane.


File Corruption Faults - 2992(All Threads)
Corrupted Files - 2992(All Threads)

Original File	Corrupted File
c:\documents and ...	C:\Documents and Settings\Joe\Desktop\test_CorruptedFiles\for_corruption_2992_1.txt
c:\documents and ...	C:\Documents and Settings\Joe\Desktop\test_CorruptedFiles\for_corruption_2992_2.txt
c:\documents and ...	C:\Documents and Settings\Joe\Desktop\test_CorruptedFiles\for_corruption_2992_3.txt

Resource Faults Pane

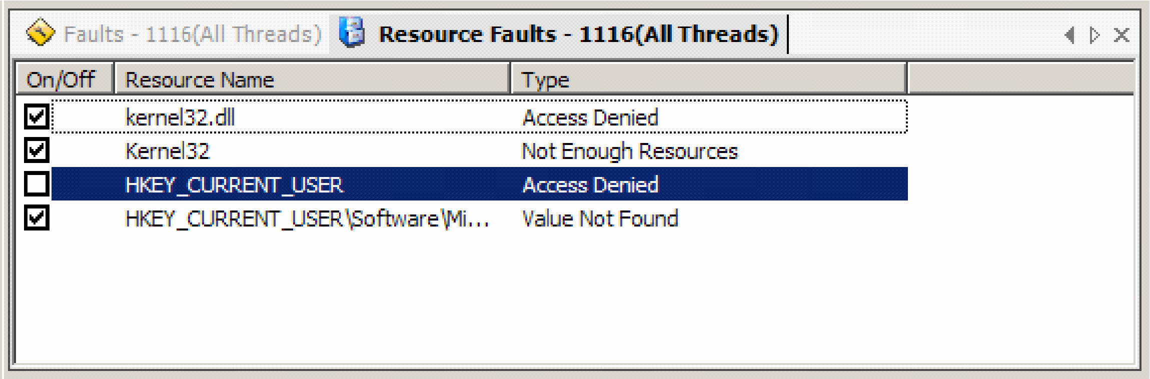
The resource faults pane gives you access to each Resource Fault that has been created. Through it you can add, remove, disable, modify, or copy resource faults. Access these fault operations by right clicking a fault

Add a fault by right clicking anywhere in the Resource Faults Pane and selecting "Create a new Resource Faults."

Select which columns are visible in this pane by right clicking anywhere in the pane and selecting "Select Visible Columns"

Turn a Resource Fault on or off quickly by toggling the check in the On/Off Column.

To show the Resource Faults pane double-click the Resource Faults Node in the Project Pane.


Faults - 1116(All Threads)
Resource Faults - 1116(All Threads)

On/Off	Resource Name	Type
☑	kernel32.dll	Access Denied
☑	Kernel32	Not Enough Resources
□	HKEY_CURRENT_USER	Access Denied
☑	HKEY_CURRENT_USER\Software\Mi...	Value Not Found

Network Corruption Faults Pane

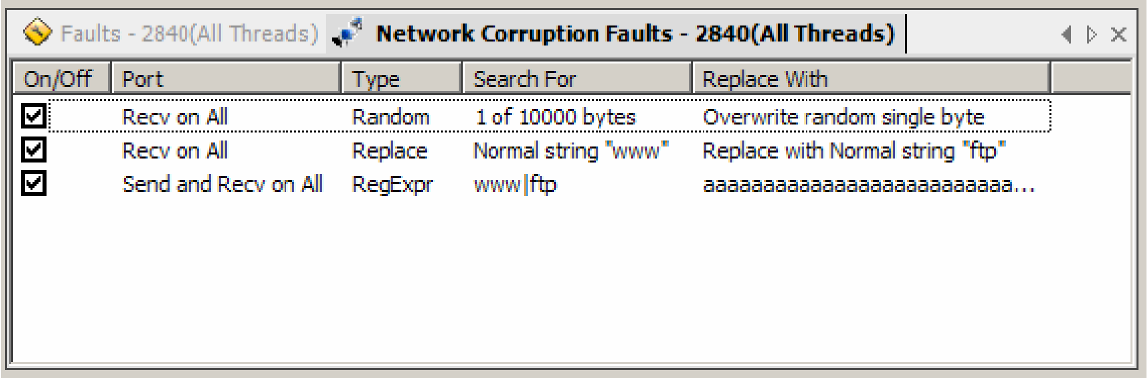
The Network Corruption Faults Pane allows you to copy, modify, delete, and create new network corruption faults. To modify, copy or delete a fault right click the fault and select the correct operation from the Right-Click menu.

To Create a new fault by right clicking anywhere in the Network Corruption Faults Pane and selecting "Create a new Fault"

Choose which columns are visible by right clicking anywhere in pane and clicking "Select Visible Columns."

Turn a Network Corruption Fault on or off quickly by toggling the check in the On/Off Column.

To show the Network Corruption Faults pane double-click the Network Corruption Faults node in the Project Pane.


Faults - 2840(All Threads)
Network Corruption Faults - 2840(All Threads)

On/Off	Port	Type	Search For	Replace With
☑	Recv on All	Random	1 of 10000 bytes	Overwrite random single byte
☑	Recv on All	Replace	Normal string "www"	Replace with Normal string "ftp"
☑	Send and Recv on All	RegExpr	www|ftp	aaaaaaaaaaaaaaaaaaaaaaaaa...

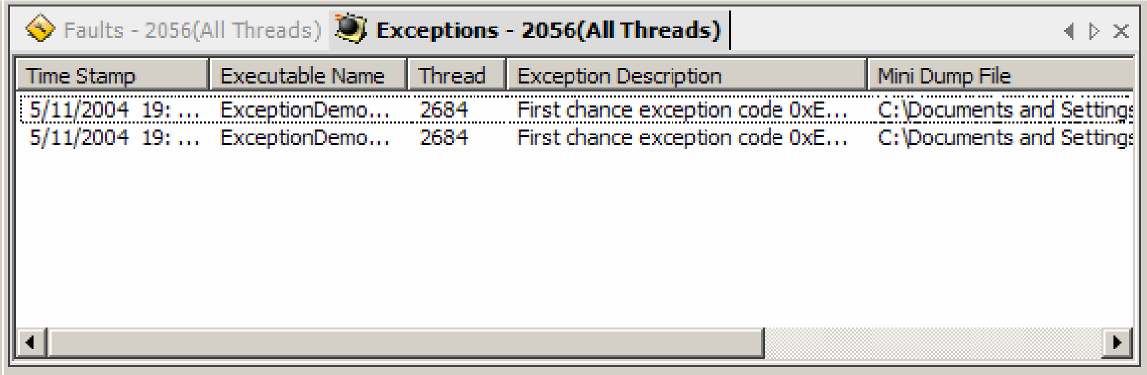
Exception Pane

Holodeck catches all exceptions your application produces. Exceptions are routed through Holodeck first, as a first chance exception, then passed back to the application to handle. If the application does not handle the exception it is logged as a second chance exception.

View the Exception in a debugger by right clicking an exception in the Exception Pane and selecting "View Exception in Debugger." For more information on debugging Exceptions please see the Exceptions Overview.

You can save the mini-dump information for debugging the application at a later time. The mini-dump file is a snapshot of the computer state at the time of the crash. For more information on debugging using the mini-dump file please see the Mini-dump Overview.

To show the Exception pane double-click the Exception node in the Project Pane.



Time Stamp	Executable Name	Thread	Exception Description	Mini Dump File
5/11/2004 19: ...	ExceptionDemo...	2684	First chance exception code 0xE...	C:\Documents and Settings
5/11/2004 19: ...	ExceptionDemo...	2684	First chance exception code 0xE...	C:\Documents and Settings

Automated Testing with Holodeck

Introduction to Automating Holodeck

This section includes more advanced topics about HD such as Recording and replying sessions, using HD with other test frameworks, using with a command line, and the customizing and extension of HD.

Recording and replaying sessions can be very helpful when trying to reproduce a crash found using Holodeck.

If you already have an automated test framework in use you can use Holodeck to test your applications further. You can use the test framework to record the session or to catch errors as they happen.

Holodeck can be run by on the command line, which makes it easy to launch with test scripts.

To insert your own custom intercepts for testing custom dlls or functions Holodeck has included the Custom Intercept Generator which will walk you through the process of creating an impostor dll.

HoloScript is a tool built on top of the HeatAPI that can be used to create new Holodeck interception frameworks.

HEAT (The Hostile Environment for Application Testing) is the foundation upon which Holodeck has been built.

Using Holodeck with other Automated Test Frameworks

Using Holodeck with other Automated Test Frameworks

Holodeck can be used in conjunction with your already existing Automated Test Frameworks to increase the probability of finding bugs. Holodeck can be used for ad-hoc testing by manipulating tests, faults, limits in the UI while running your test framework. Holodeck can also be used in a lab environment or stress test environment. For stress testing Holodeck expects a stress test harness to launch it, telling it the stress options and Application Under Test on the command line. For code coverage testing Holodeck expects to be launched by a test harness as well. If there is a crash in the Application Under Test the harness is responsible to do the right thing (launch debugger, record crash, etc).

Using Holodeck as a command-line utility

Introduction to using Holodeck as a command-line Utility

Usage

HolodeckGui [startwizard_option] [project_option] <options>

[startwizard_option] choices

/addnewintercepts	starts the 'Add Holodeck Intercepts' wizard on startup
/customtestproject	starts the 'Create a custom test project' wizard on startup

[project_option] choices

projectfile.hdp	loads the specified project file on startup
/launch:exefilename	launches the specified exe with default options*
/attach:<process_id>	attaches to the specified processID with default options*
/launchservice:servicename	launches the specified service with default options*
/attachservice:servicename	attachs to the specified running service with default options*

<options> choices*

/randomstress:[low,medium,high]	starts the random test generator with the specified intensity
/intelligentstress:[low,medium,high]	starts the intelligent test generator with the specified intensity
/codecoverage:[low,medium,high][,timeout]	starts the code coverage generator with the specified intensity and optional timeout in seconds
/record	starts recording the session on startup
/silent	starts Holodeck in slient mode, messages are logged to ErrorLog.txt

***Default Options:**

Pause on start	false

Process chaining	true
Inherit settings	true
Attach debugger	true
Logging options	same defaults as in New Project Wizard

Examples:

```
HolodeckGui myproject.hdp

HolodeckGui myproject.hdp /codecoverage:low

HolodeckGui myproject.hdp /codecoverage:high,15

HolodeckGui myproject.hdp /record

HolodeckGui /launch:c:\windows\notepad.exe

HolodeckGui /attach:2146 /randomstress:high

HolodeckGui /launchservice:"Indexing Service"

HolodeckGui /attachservice:"ClipBook" /record /slientÿÿÿÿÿ
```

Code Coverage testing from the command-line

Code coverage test generation attempts to hit as many error paths as possible. It reruns the application multiple times, each time setting different combinations of Limits, Faults, and Tests. Each time the Application Under Test terminates, by way of the script terminating the Application gracefully or Holodeck finding a crashing bug, Holodeck will relaunch the Application Under Test and start the next test, until there are none left. Holodeck assumes that each testing script will close the application under test at the end of the test; this allows Holodeck to know when to start the next test.

To turn on Code Coverage testing from the command-line use the /codecoverage switch followed by colon (:) high, medium, or low.

Example: `HolodeckGui.exe projectName /codecoverage:high`

1) **High**

a) Allow network limits

b) Allow disk limits

c) Allow memory limits

d) Allow all faults

e) Allow all tests

2) **Medium**

a) Allow network limits

b) Allow disk limits

c) Allow memory limits

d) Allow all faults

e) Allow resource based tests

f) Disallow all other tests

3) **Low**

a) Allow network limits

b) Allow disk limits

c) Allow memory limits

d) Disallow all faults

e) Disallow all tests

Initial Recording

The first thing Holodeck does when running Code Coverage Testing is record what the Application Under Test is doing to create an intelligent test plan. Holodeck records resource usage and unique API calls until the Application Under Test is terminated. It then uses the information found in the recording phase to build the next tests.

Exact order of execution:

1) Set each fault one at a time
a) For disk or memory
i) Set a limit for max used – 1 byte
ii) iSet a limit for average used – 1 byte
iii) iiSet a limit to minimum possible (0 bytes)
b) For Network
i) Set a limit to 50%
ii) iSet a limit to 0%
2) Set a test for each unique API call seen in the recording phase.

Stress testing from the command-line

Using Holodeck's Stress Test Generation to test your application is a great way to ensure your software will continue to perform well even in stressful situations. This is useful for server side applications or applications that must perform well in multi-user environments. Holodeck will perform a random or intelligent test for a short period of time, if the test crashes the application under test Holodeck will restart the application and continue testing with the next test.

Random Tests – Randomly set faults, limits, and tests will be set at a given interval, at a given test duration, to flush out stability bugs.

To turn on Random Stress testing from the command-line use the /randomstress switch followed by colon (:) high, medium, or low.

Example: `HolodeckGui.exe projectName /randomstress:high`

1) **High –** test the Application Under Test with a very hostile environment

a) Every 15 seconds a random test will occur
b) Each Test will last two seconds
c) Holodeck will set five tests each time
d) Allow network limits from 0% to 25% of throughput
e) Allow disk limits down to the amount currently being used by the Application Under Test
f) Allow memory limits down to the amount currently being used by the Application Under Test
g) Allow all faults

2) **Medium –** test the Application Under Test with a semi hostile environment

a) Every 15 seconds a random test will occur
b) Each Test will last two seconds
c) Holodeck will set one test each time
d) Allow network limits from 25% to 75% of throughput
e) Allow disk limits down to one kilobyte over the amount currently being used by the Application Under Test
f) Allow memory limits down to one kilobyte over the amount currently being used by the Application Under Test
g) Allow all faults

3) **Low –** test the Application Under Test with some tests and faults

a) Every 30 seconds a random test will occur
b) Each test will last one second
c) Holodeck will set one test each time
d) Allow network limits from 75% to 100% of throughput
e) No disk limits will be set
f) No memory limits will be set
g) Allow all faults

Intelligent Tests – Create tests based on observation of API calls made by the application under test

To turn on Intelligent Stress testing from the command-line use the /intelligentstress switch followed by colon (:) high, medium, or low.

Example: `HolodeckGui.exe projectName /intelligentstress:high`

1) **High**

a) Each test will occur at 15 second intervals
b) Holodeck will set five tests at a time

2) **Medium**

a) Each test will occur at 30 second intervals
b) Holodeck will set two tests at a time

3) **Low**

a) Each test will occur at 60 second intervals
b) Holodeck will set only one test at a time

Using Recorded Sessions from the command-line

Recording each session is a very good idea when running Holodeck from the command line, especially if it is run using the silent switch.

To enable recording of the session on the command line use the `/record` switch.

Example: `HolodeckGui.exe projectName /record`

This will create a recordedSession.xml file in the recorded session folder. This will allow you to replay the session to reproduce any errors Holodeck finds for a developer or bug triage team.

For more information on recording and replaying sessions please see the Introduction to recoding and replaying section in the Holodeck in Depth Section.

Running Holodeck silently

You can run Holodeck minimized and without any UI notifications. You can run Holodeck more smoothly, especially in a test harness situation, if the UI notifications are suppressed. To test your application without any UI, and with as little memory as possible other Automated Testing options might be better such as the Custom Intercept Generator, HoloScript, and HEAT.

To run Holodeck silently use the /silent switch.

Example: `HolodeckGui.exe projectName /silent`

Create a Custom Test Project

Create a Custom Test Project Wizard

Using HoloScript

Using HoloScript

Using HEAT (Hostile Environment for Application Testing)

Using HEAT

Appendices

About fault injection

Same as Help docs in 2.1 updated to 2.5 specs.

How to Break Software

Same as Help docs in 2.1 updated to 2.5 specs.

How to Break Software Security

Same as Help docs in 2.1 updated to 2.5 specs.

API Call Categories

Same as Help docs in 2.1 updated to 2.5 specs.

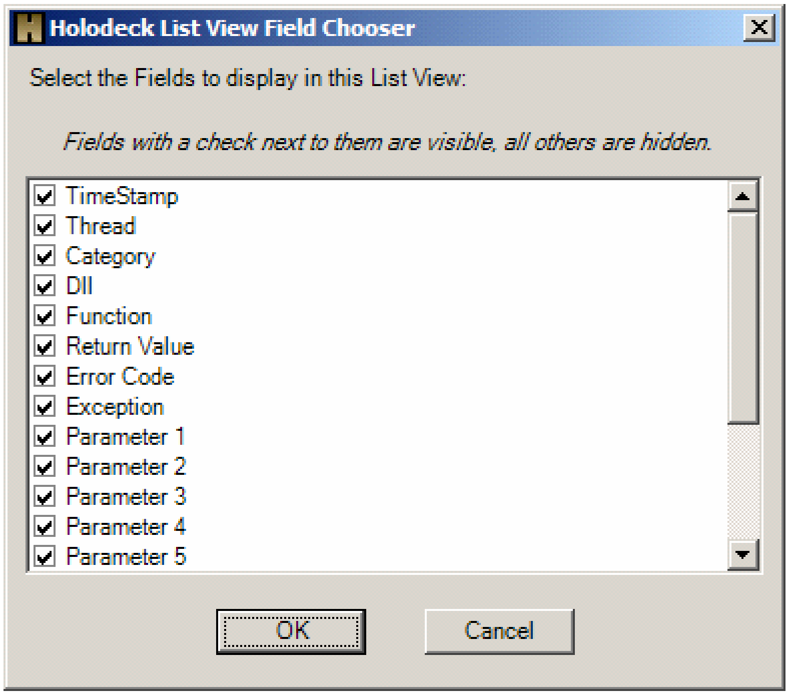
Error Codes

Exception Codes

Same as Help docs in 2.1 updated to 2.5 specs.

Field Chooser

The Field Chooser allows you to select which columns are visible in the currently displayed pane with selectable columns. To access the Field Choose open the pane you wish to change and click View > "Filed Chooser"



Holodeck List View Field Chooser

Select the Fields to display in this List View:

Fields with a check next to them are visible, all others are hidden.

- ☑ TimeStamp
- ☑ Thread
- ☑ Category
- ☑ Dll
- ☑ Function
- ☑ Return Value
- ☑ Error Code
- ☑ Exception
- ☑ Parameter 1
- ☑ Parameter 2
- ☑ Parameter 3
- ☑ Parameter 4
- ☑ Parameter 5

Index