INITIAL RESPONSE AND FORENSIC DUPLICATION

INITIAL RESPONSE

- One of the first steps of any preliminary investigation is to obtain enough information to determine an appropriate response.

- The goal of an initial response is twofold: Confirm there is an incident, and then retrieve the system's volatile data that will no longer be there after you power off the system.

- Initial response is an investigative as well as a technical process!

CREATING A RESPONSE TOOLKIT

- For an initial response, you need to plan your approach to obtain all the information.

- Without affecting any potential evidence, you will be issuing commands with administrator rights on the victim system, you need to be particularly careful not to destroy or alter the evidence.

- The best way to meet this goal is to prepare a complete response toolkit.

GATHERING-THE-TOOLS

In all incident responses, regardless of the type of incident, it is critical to use trusted commands. For responding to Windows, we maintain aCDor two floppy disks that contain a minimum of the tools listed

Tool	Description	Source
cmd.exe	The command prompt for Windows NT and Windows 2000	Built in
PsLoggedOn	A utility that shows all users connected locally and remotely	www.foundstone.com
rasusers	A command that shows which users have remote-access privileges on the target system	NT Resource Kit (NTRK)
netstat	A system tool that enumerates all listening ports and all current connections to those ports	Built in

Fport	A utility that enumerates all processes that opened any TCP/IP ports on a Windows NT/2000 system	www.foundstone.com
PsList	A utility that enumerates all running processes on the target system	www.foundstone.com
ListDLLs	A utility that lists all running processes, their command-line arguments, and the dynamically linked libraries (DLLs) on which each process depends	www.foundstone.com
`nbtstat`	A system tool that lists the recent NetBIOS connections for approximately the last 10 minutes	Built in
`arp`	A system tool that shows the MAC addresses of systems that the target system has been communicating with, within the last minute	Built in
`kill`	A command that terminates a process	NTRK
`md5sum`	A utility that creates MD5 hashes for a given file	www.cygwin.com
`rmtshare`	A command that displays the shares accessible on a remote machine	NTRK

Preparing the Toolkit

We take several steps to prepare our toolkits for initial response:

- **Label the response toolkit media**
- Case number
- Time and date
- Name of the investigator who created the response media
- Name of the investigator using the response media
- Whether or not the response media (usually a floppy disk) contains output files or evidence from the victim system

OBTAINING VOLATILE DATA

- Now that you have a forensic toolkit and a methodology, you need to determine exactly which data to collect. At this point, you want to obtain the volatile data from the Windows
- NT/2000 system prior to turning off that system. At a minimum, we collect the following volatile data prior to forensic duplication:

- System date and time
- A list of the users who are currently logged on
- Time/date stamps for the entire file system
- A list of currently running processes
- A list of currently open sockets
- The applications listening on open sockets

VOLATILE DATA COLLECTION FROM WINDOWS SYSTEM

- Now that you know what to collect and how to document your response, you are ready to retrieve the volatile data.

- 1. Execute a trusted cmd.exe.
- 2. Record the system time and date.
- 3. Determine who is logged in to the system (and remote-access users,
- if applicable).
- 104 Incident Response & ComputerFor ensics
- 4. Record modification, creation, and access times of all files.
- 5. Determine open ports.
- 6. List applications associated with open ports.
- 7. List all running processes.
- 8. List current and recent connections.
- 9. Record the system time and date.

Collecting Volatile Data from a Linux System

- **Remotely Accessing the Linux Host via Secure Shell**

1) You will be collecting forensic evidence from this machine and storing it on the “VTELaunchpad.” You will need to reestablish the VTELaunchpad to listen for incoming connections.

2) You will want to save the collected data in a file called
C:\LinuxCollectiondata.txt or
C:\LinuxCollectiondata. cvs.

- Steps:
- To connect to the compromised Linux host locate and doubleclick the ‘Putty.exe icon’ on the desktop of the VTELaunchpad. Putty is a very popular (and free) SSH client.
- Type ‘10.0.4.51’ in the Host name (IP Address) box withinthe Putty application and then click ‘Open’. Select Yes to accept the server key.
- Login with the following credentials: Username:root Password: tartans

3.2 Collecting data using a trusted Netstat command

1. From the command line on the "Linux Compromised" host it will be necessary to mount the CDROM containing a trusted forensics toolkit. The CD has been pre-loaded. To do this, type:

```
# mount /dev/cdrom  /mnt/cdrom
```

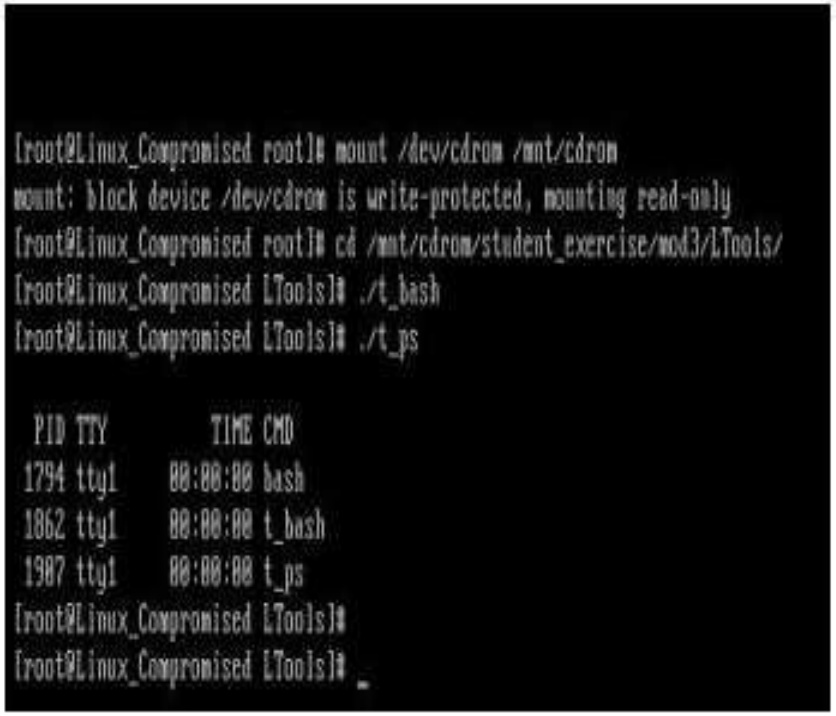

Figure 4

2. Now that the CDROM is mounted, you will need to load a trusted .bash shell from which to continue working. First, the current working directory needs to be changed to the newly mounted forensics toolkit CD. To do this, type:

```
# cd /mnt/cdrom/Tools/Linux/Forensics/
```

3. At this point load the trusted .bash shell from the CD. To do this, type:

```
# ./t_bash
```

4. Next, verify that the t_bash shell has been loaded and is the current location from which the collection is occurring. To do this, type:

```
# ./t_ps
```

Note the output from the t_ps command should indicate that the t_bash is running inside of bash. The PID #'s should be different in your screen.

5. Now that you are running commands from a trusted bash shell it is time to begin the collection of volatile data. From the trusted command shell, type:

```
# ./t_netstat -an | ./t_netcat 10.0.254.254 443
```

This syntax will execute 't_netstat' from the trusted CD and send the output from the command to the "VTE-Launchpad" which will write the data in the "C:\LinuxCollectiondata.txt" file.

6. You will need to wait approximately one minute for the command to be executed and data transferred to the VTE-Launchpad. Now close the open Netcat connections on both the "Linux Compromised" and "VTE-Launchpad". To do this, from the open trusted command shells press "Ctrl C". This will close the Netcat connections. You can now close the SSH connection to the compromised Linux host.

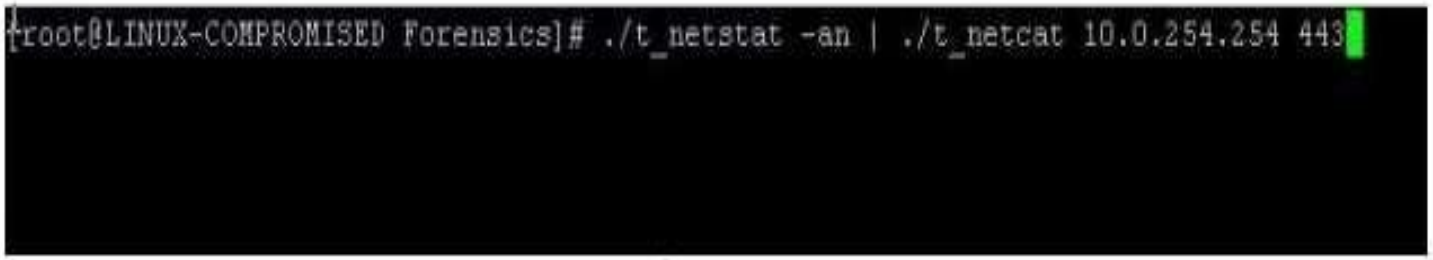

Figure 5

It may take Netcat several seconds, possibly a minute or two, to transfer the data to the remote collection system (VTE-Launchpad)

FORENSIC DUPLICATION

- Defination: **File that contains every bit of information from the source in a raw bit stream format.** A 5GB hard drive would result in a 5GB forensic duplicate. No extra data is stored within the file, except in the case where errors occurred in a read operation from the original.

- The forensic duplication of the target media provides the mirror image of the target system. This methodology provides due diligence when handling critical incidents.

- Generally, if the incident is severe or deleted material may need to be recovered, a forensic duplication is warranted.

IS FORENSIC DUPLICATION NECESSARY?

- Law enforcement generally prefers forensic "bit-for-bit, byte-for-byte" duplicates of target systems. If you are responding to an incident that can evolve into a corporate-wide issue with grave consequences, you may want to perform a forensic duplication.

- It is a good idea to have some policy that addresses when full duplication of a system is required.

- Eg: consider a sexual harassment suit or any investigation that can lead to the firing or demotion of an employee as grave enough to perform forensic duplication

Forensics Duplicates as Admissible Evidence

- Federal Rules of Evidence §1002 requires an original to prove the content of a writing, record, or photograph.

- Follows from the best evidence rule: Copying can introduce errors.

- F.R.E. §1001

If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".

- Federal Rules of Evidence § 1003

  A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

- As familiarity with digital data increases, behavior of the judicial system will increase in rationality.

QUALIFIED FORENSIC DUPLICATE

- A *qualified forensic duplicate is a file that contains every bit of information from the source,* but may be stored in an altered form. Two examples of altered forms are in-band hashes and empty sector compression.

- Some tools will read in a number of sectors from the source, generate a hash from that group of sectors, and write the sector group, followed by the hash value to the output file.

- This method works very well if something goes wrong during the duplication or restoration of the duplicate.

- Empty sector compression is a common method for minimizing the size of the output file. If the tool comes across 500 sectors, all filled with zeros, it will make a special entry in the output file that the restoration program will recognize.

RESTORED IMAGE

- A *restored image is what you get when you restore a forensic duplicate or a qualified forensic* duplicate to another storage medium. The restoration process is more complicated than it sounds.

- For eg: sector-to sector copy of file from source hard drive to
destination hard drive.

- Case I: If the destination hard drive is the same as the original hard drive, everything will work fine. The information in the partition table will match the geometry of the hard drive. Partition tables will be accurate; if the table says that partition 2 starts on cylinder 20, head 3, sector 0, that is where the data actually resides.

- Case II: Destination hard drive is not the same as the original hard drive.

- If you restore the forensic duplicate of a 2.1GB drive to a 20GB drive, for example, the geometries do not match. In fact, all of the data from the original drive may occupy only three cylinders of the 20GB destination drive. The partition that started on cylinder 20, head 3, sector 0 on the original drive may actually start on cylinder 2, head 9, and sector 0.

- The software would look in the wrong location and give inaccurate results.

FORENSIC DUPLICATION TOOL REQUIREMENTS

- The tool must have the ability to image every bit of data on the storage medium.
- The tool must create a forensic duplicate or mirror image of the original storage medium.
- The tool must handle read errors in a robust and graceful manner. If a process fails after repeated attempts, the error is noted and the imaging process continues. A placeholder may be put in the output file with the same dimensions as the portion of the input with errors. The contents of this placeholder must be documented in the tool's documentation.
- The tool must not make any changes to the source medium.
- The tool must have the ability to be held up to scientific and peer review.
- Results must be repeatable and verifiable by a third

- The most common tools used for obtaining a true forensic duplicate are built to run in a Unix operating environment.

- One tool, dd, is part of the GNU software suite. This was improved upon by programmers at the DoD Computer Forensics Lab and re-released as dcfldd. The command-line parameters for dd and dcfldd are nearly identical, and the core data transfer code has not been altered. If your team has validated the operation of dd, very little work will be required to validate the new features.

- Another tool that we will look at here is the Open Data Duplicator from openforensics.org. One of the strong points of this new Unix tool is that it allows an

PERFORMING A DUPLICATION WITH "dd"

- In certain situations, duplications will be stored in a series of files that are sized to fit on a particular media type (such as CDs or DVDs) or file system type (such as files under 2.1GB).

- This is that we call a *segmented image. The following is a bash shell script that will create a* true forensic duplicate of a hard drive and store the image on a local storage hard drive

BASH SCRIPT

- #!/bin/bash
- # Bash script for duplicating hard drives with dd
- # Set source device name here
- source=/dev/hdc
- # Set output file name here
- output_name=/mnt/RAID_1/dd_Image
- # Set output file size here
- output_size=2048k;
- ####
- count=1
- while (dd if=$source of=$output_name.$count
  bs=$output_size \
- count=1 skip=$(($count-1)) conv=noerror,notrunc);
- do printf "#"; count=$((count+1)); done
- ####
- echo "Done. Verify the image with md5sum."

DUPLICATING WITH THE OPEN DATA DUPLICATOR (ODD)

- The Open Data Duplicator (ODD) is a new open-source tool. This tool follows a client/ server model that allows the investigator to perform forensic duplications on a number of computer systems simultaneously over a local LAN.
- There are three portions of the ODD package:
- **Bootable CD-ROMs** These are similar to the Trinux Linux distribution.
- **Server-side application** The server will perform most of the processing of the duplicate image, including the calculation of hashes, string searches, and the storage of the true forensic duplication.
- **Client-side application** This portion may be run locally if you are duplicating drives on a forensic

We have installed ODD on Red Hat Linux 7.3 and started the ODD server application. The first screen asks for the location of the ODD server. In this example, we are running everything on the same forensic workstation, so we can choose Detect Server

Figure 7-1. ODD startup screen

The second screen, shown in Figure 7-2, shows the devices that were detected by ODD. Notice that there is a text-entry box for specifying a file, which you can use to direct ODD to duplicate certain partitions if necessary.

Figure 7-2. ODD device detection

The next screen lists the processing options available on the server. The most important items are the Image Store Plugin and Compressed Image Store Plugin options, which will produce the true forensic duplicate image. We suggest using the Compressed Image Store plug-in only if you are low on storage space.

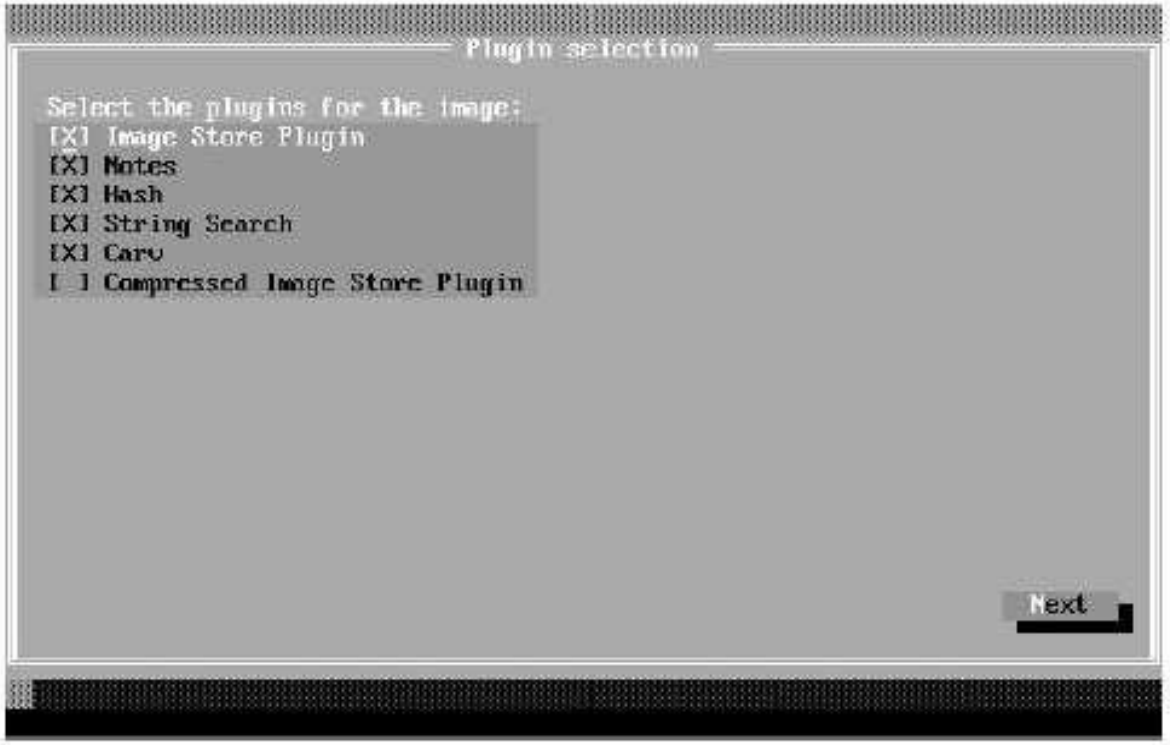

Figure 7-3. ODD plug-in selection

Figure 7-4 shows the requested information for the Notes plug- in. Here, you supply information such as the case number, the computer's date and time, the actual date and time, and the system description.

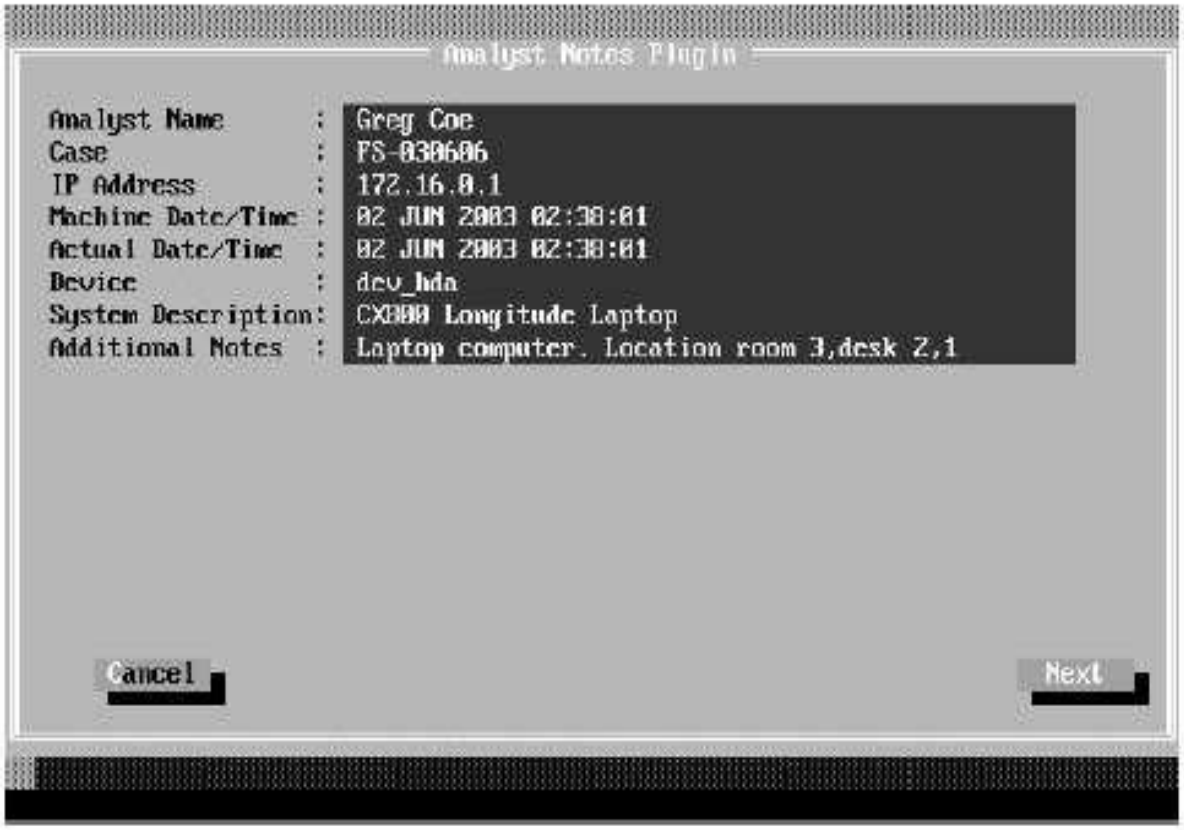

Figure 7-4. ODD Notes plug-in

The Carv plug-in will extract a certain number of bytes from the incoming data stream, based on file headers. For example, we have selected gif and jpg for extraction in Figure 7-5. Once the duplication has completed, the carved files may be found in a directory on the ODD serv

Figure 7-5. ODD Carv plug-in

A QUALIFIED FORENSIC DUPLICATE OF A HARD DRIVE

- One of the first things that a beginning examiner must learn is to never boot from the evidence drive.
- Many items on the evidence media can be altered, starting from the moment the BIOS executes the boot block on the hard drive.
- During the initial boot process, file access timestamps, partition information, the Registry, configuration files, and essential log files may be changed in a matter of seconds.

CREATING A BOOT DISK

- Imaging system requires a clean operating environment. When using a DOS application, such as SafeBack or EnCase, this means that you must create an MS DOS boot disk. Using MS DOS 6.22 or Windows 95/98, the following command will format and copy the system files to a floppy:

C:\format a:\ /s

- The first file processed by the computer is IO.SYS. The code in IO.SYS loads the contents of MSDOS.SYS and begins to initialize device drivers, tests and resets the hardware, and loads the command interpreter, COMMAND.COM

- During the process of loading device drivers, if a disk or partition connected to the machine uses compression software, such as DriveSpace or DoubleSpace, IO.SYS loads the DRVSPACE.BIN driver file.

- You do not want this to happen when performing a forensic duplication. As the driver loads,it will mount the compressed volume and present the operating system with an uncompressed view of the file system.

- When it mounts the compressed volume, it changes thetime/date stamps on the compressed file, which means that the evidence will be

CREATING A QUALIFIED FORENSIC DUPLICATE WITH SAFEBACK

- SafeBack, offered by New Technologies Inc. (NTI), can make a qualified forensic duplicate of any hard drive that is accessible through a system's drive controllers.
- Creating a duplicate of a computer system with SafeBack is fairly straightforward. It offers four modes of operation:
- The Backup function produces a forensically sound image file of the source media.
- The Restore function restores forensically sound image files.
- The Verify function verifies the checksum values within an image file.
- The Copy function performs the Backup and Restore operations in one action.

CREATING A QUALIFIED FORENSIC DUPLICATE WITH ENCASE

- Most popular forensic tool suite available commercially.
- Its popularity is based primarily on the easy- to-navigate GUI interface.
- A flexiblescripting language is included, allowing the examiner to customize the types of searches performed by the tool.
- Perhaps the most valuable feature is the preview option.

- During the first stages of an investigation, you can use the preview function to quickly ascertain whether a computer system is material to the issue being investigated.
- To use the preview option, boot the suspect computer system with an EnCase boot disk.
- Instead of acquiring an image, you connect to the suspect computer through a parallel cable or a network connection with a copy of EnCase running on your forensic workstation.
- Once the connection is established, the analysis process is the same as if you were working on an EnCase image file.

- EnCase will present you with a series of options and text-entry fields that will be placed in the header of the qualified forensic duplicate.
- You will be asked for the following information:
- Location of the qualified duplicate
- Case number
- Examiner's name
- Evidence number
- Description of the evidence being acquired
- Verification of the current date and time
- Any other notes or comments that you wish to make