Global Information Assurance Certification Paper

Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensics

GCIH Gold Certification

Author: Ricky D. Smith, rdsmith@mac.com

Adviser: Jim Purcell

Accepted: January 14th 2007

Outline

1. Abstract

This paper describes the examination of the use of five different live CDs in the six-step incident handling process and the subsequent forensic examination of the machines. A brief synopsis of the six step incident handling process to provide the background for the testing conducted. The first part of the examination will be an evaluation of the ability of the live CD to be used for incident response by a first responder. After the first response capability is evaluated, an examination of the capability of the live CDs to carry out the initial forensics imaging will be conducted. The test procedures used on a Windows XP and Linux machines are described including the sets of commands that simulate the first responder actions each operating system. The advantages and disadvantages of using each live CD for incident response and their effect on the forensic process are examined on the basis of the testing.

2. Requirements for System Examination for Incident Handling and Forensics

One of the first things that an incident handler takes for a potential computer incident is verifying that an incident has actually occurred. As part of the verification process, the incident handler will need to examine the system looking for the evidence of the incident. In some cases, this may be a simple as opening a web browser on another machine and pointing it at the suspect system to view a defaced web server. Other cases may require that the incident handler review multiple different aspects of the system, for example, the list of open files and the processes that opened those files.

In either case, once the incident has been verified the incident handler will need to further examine the system determine how the attacker compromised the system so that the vulnerability that was exploited can be mitigated during the system restoration. This will be a more thorough examination of the system that includes many more aspects of system. In this process the incident handler will also use other tools to examine the system for viruses, worms, spyware, or other malicious code, all of this is sometimes called malware.

Until now we have been talking about what the incident handler needs to do. Now we need to consider how the handler will go about doing some of these tasks and reasons for doing the tasks in a particular fashion. There are competing sets of priorities:

- the business process owners that want the system back up and supporting the business process,

- the security team that wants to fully understand the attack and how to prevent it, and

- the legal counsel or law enforcement agencies that may consider bringing civil suits or filing criminal charges against the attacker.

All of these priorities affect what the incident handler does and how it is done.

Generally for the business process owners, the priority is getting the system returned to service as quickly as possible without losing any data and without the attack succeeding again. They want to try cleaning the malware off the system, patching

the vulnerability, restoring any potentially compromised data from backup, and putting the system back in service. In other cases, like a root kit was installed, it may be backing up the data, re-installing the operating system, patching the vulnerability, restoring the data from backup and placing it back in service.

For the security team, the priority is to support the business process restoration but as part of that they need to understand what the attack was and why it succeeded in order to prevent its reoccurrence. Their concern in examining the system is minimizing the changes to the system to allow them to accurately follow the attacker's tracks as the system was compromised. With that information the security team can identify the vulnerability that allowed the compromise and methods to prevent the attack from succeeding again or mitigate the risk of the attack.

For the legal team that may be considering civil or criminal action against the attacker, the priority is to minimize any changes to the system to ensure that the evidence collected form the system will give them the best case against the attacker. Conversely, the legal team may also be concerned with the downstream liability and want to contain the attack and may not be concerned with preserving any evidence.

Incident Handling Six-Step Process

With an understanding of some of the issues and constraints that affect the incident handling process, a synopsis of the overall incident handling process is needed to understand where the use of live CDs fit in the process and the examination of

the use of these CDs in the investigation of events of interest, the indicators or evidence of incidents.

For most incident response or handling teams, the incident handling process is a six-step loop (*Incident Handling Step by Step*, 2006). For most incident handling teams, the team members may be investigating or working different incidents at different steps at the same time but they will all be following the same process shown in Figure 1. The different steps are discussed in the following sections.

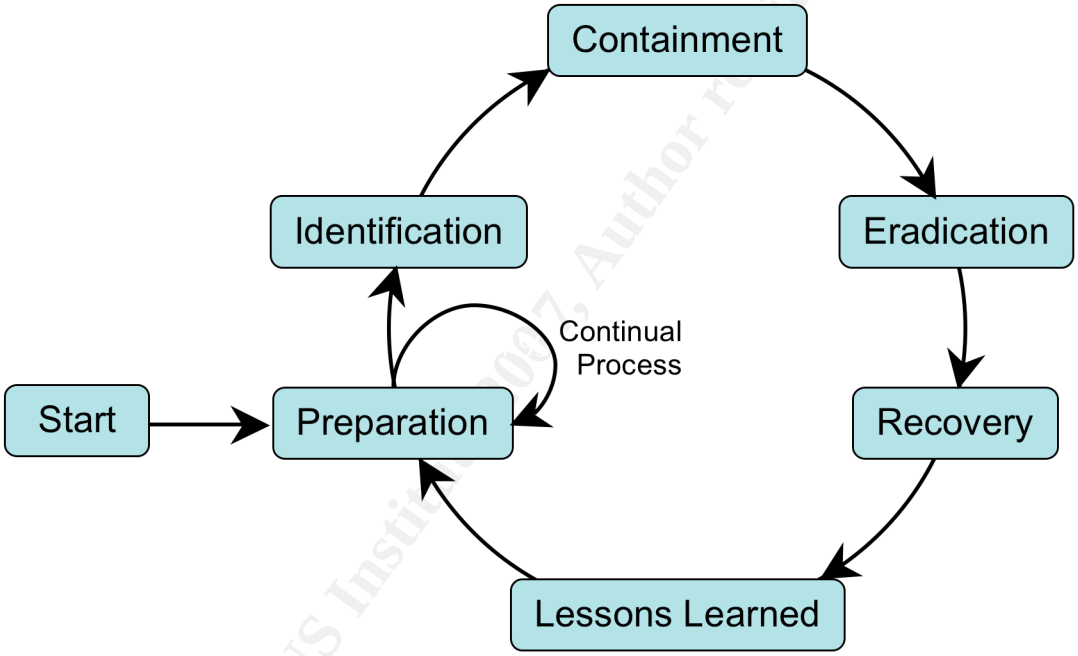

Figure 1: Six-Step Incident Handling Process Loop

Preparation

At the beginning of the loop is the Preparation Step. In this step the team writes, reviews and revises their policies, procedures and processes for investigating and handling incidents. There should also be time for training and learning

new skills that will enable them to better handle incidents. An important part of this step is building relationships with other organizations that may assist in the incident handling process. The organizations could be internal, such as the human resources and legal counsel departments, or outside agencies, such as law enforcement and other computer incident response teams. These relationships can be extremely beneficial during an incident as a source of information or assistance. This is the step where most incident handling teams would like to spend most of their time.

Identification

The second step of the process is Identification. In this step, a team of first responders is assigned to investigate a possible event of interest. A team of two or more is preferred for the investigation since different people will see different things and bring different views and those may contribute to a better understanding of the events. The first responders are trained to identify and conduct the initial investigation of events that may be incidents. First responders could be help desk personnel, system administrators working for other departments, or fully trained incident handlers.

The team will investigate an event to determine if it, or possibly a series of events, constitutes an incident. In this step the team may be only examining a specific system but generally will also be looking at logs from network devices, such as intrusion detection systems, routers, and firewalls, and other related systems. While trying to verify the incident, the incident handlers will try to minimize the changes they make to the system. Changes to the system by the team will impact their

own efforts to understand the attack and the forensic analysis of any evidence they collect. Once the events are classified as an incident, the team of first responders transitions the investigation over to fully trained incident handlers who will complete the rest of the process.

Containment

The next step is Containment where the incident handlers, in cooperation with the system owners and system administrators, begin making changes the system to restrict the spread of the attack. Examples of actions that may be taken are backing up the system data, unplugging the system from the network, changing the DNS name or IP address of the system, and pulling the power cord from the wall. The business risk, based on the criticality of the system as assessed by the system owner, and the severity of the attack will determine how drastic the actions will be in this step. Also the incident handlers should also be reviewing nearby systems, in network terms, and systems that have trust relationships with the suspect system.

Eradication

After the incident is contained, the next step is the removing the effects of the attack in the Eradication step. The actions taken in this step are dependent on the severity of the attack and the business criticality of the system. For example, if the incident was caused by easily removed and relatively benign spyware, then the eradication may be the installation of anti-spyware software and allowing it to remove the spyware. At the other end of the spectrum, if the attacker installed a rootkit after compromising the machine, the eradication could

involve wiping the disks and completely rebuilding the operating system.

Recovery

The next step is Recovery. This step restores the system back to its pre-incident functionality and verifies that the vulnerability that was exploited in the incident has been mitigated or eliminated. Full system functionality testing by the system owner should be conducted before placing the system back into production. Also the verification should include checking that all required patches have been installed, any necessary changes to the configuration of the machine has been made, and a vulnerability scan of the system conducted and the resulting findings mitigated.

Lessons Learned

The sixth step in the loop is Lessons Learned. In this step the incident handlers for an incident write a short report on the handling of that incident. They should analyze the incident to determine the parts of the incident handling process went well and those that didn't. They should also make any specific recommendations to improve the incident response policies, processes and procedures. The improvements in the incident handling process generated in the Lessons Learned step are fed back into the Preparation step. This way the other incident handlers and first responders will be trained on the improvements.

Live CDs

Live CDs are bootable CDs that have an operating system installed that can be run directly from the CD. Live CDs operate without installing any software on the hard drive of the system. Most live CDs are Linux based. Although there are some live CDs that are based on one of the 4.4BSD descendants (Wikipedia.org, 2007), e.g., the OliveBSD live CD that is based on OpenBSD 3.8 (Paderni, 2006).

One of the more popular live CD distributions is Knoppix (Knopper, 2006), which is based on Debian GNU/Linux. Numerous other specialized live CD distributions, such as Knoppix-STD (s-t-d.org, 2006) and Auditor (remote-exploit.org, 2006), are based on Knoppix. Other live CD distributions are based on Slackware Linux (Slackware.com, 2006) or Ubuntu Linux (Ubuntu.com, 2006). For a more complete list see FrozenTech's Live CD List (Brand, 2006).

For Windows live CDs, the selection is much more limited due to the licensing restrictions of Windows itself. The two most known options are Windows PE (Microsoft, 2004) from Microsoft and BartPE (Lagerweij, 2006). Windows PE is only available to purchasers of Microsoft's Software Assurance program. BartPE, however, can be built using the installation media for a licensed copy of Windows XP or Windows Server 2003.

The use of the live CDs will be covered in the context of the Investigation and Containment steps of the six-step incident handling process loop. The live CDs' capability to provide the known good tools used in these steps will be examined. The capability of the live CD to create a forensically sound image

of the target machines' hard drives will examined. In addition, the effect of the use of each live CDs on the modified-accessed-changed (MAC) timeline created from the forensic image of the hard drive will also be examined. (*Forensic and Investigative Essentials*, 2006)

3. Testing the Live CDs

Testing Environment

VMware virtual machines (VMs) will be used as the platform for the target machines for the testing of the effects of using the live CDs on the target machines. By using the snapshot features of VMware 5 (VMware.com, 2006), the state of the target machines can be reset back to the same point in the before testing each live CD on the target machine. There will be two target virtual machines, one machine running Windows XP SP2 and the other running RedHat Linux 9.

Once the testing with a live CD on the live system has been completed, the live CD will be used to create a forensically sound image of the virtual hard drive of the VM. The hard drive forensic images will be analyzed with the Autopsy Forensic Browser (Carrier, 2006) to create the MAC timeline for each image. The MAC time lines will be compared with various tools to examine the effect of the live CD used.

Test Methodology and Criteria

There will be three criteria for comparing the capabilities of live CDs. The two main criteria will be the effect of running a standard set of tools on the virtual machine in live system investigation and in a dead system investigation. The second

main criteria will be a comparison of the tools and utilities included on the CD. The third criteria will be an examination of the other capabilities of the CD.

To measure the effect of running the tools from the live CD, the live CD will be used as the tool the first responder will use to investigate the system. The simulation of the first responder actions will consist of:

- inserting the live CD in the system;
- starting a terminal or command prompt window from the live CD;
- running the commands in Table 1 for the suspect machine running Windows (First Responders – Windows, 2005) or in Table 2 for the suspect machine running RedHat Linux 9 (First Responders – Unix/Linux, 2005) and sending the data across the network using netcat (Hobbit, 1996);
- securing power Abruptly to the machine;
- rebooting the machine from the live CD; and
- imaging the hard drive using dd and sending the image across the network using netcat to the forensic workstation. (*Forensic and Investigative Essentials*, 2006)

On the Windows XP machines being imaged with the BartPE live CD using **dd.exe** (Syring, 2004):

dd.exe if=\\.\f: | nc 192.168.154.1 1234

On the Windows XP machines being imaged with one of the other live CDs:

dd if=/dev/hda | nc 192.168.154.1 1234

or for the RedHat Linux 9 machines:

dd if=/dev/sda | nc 192.168.154.1 1234

and on the forensics workstation:

nc -l -p 1234 | dd *<LiveCD name>-<machine OS>_data.img*

Once the first responder testing with a live CD has been completed, the virtual machines will be abruptly powered down and the virtual hard drive imaged with the live CD if possible. The hard drive images will be transferred to a forensics workstation for a limited analysis of the MAC timeline.

Table 1: Commands used for testing using the Windows live CDs on a live system

Command and options	Purpose
date /t	Identify the date of the start of the first responder process
time /t	Identify the time of the start of the first responder process
set	List the environmental variables
psinfo	Lists information about a system (Russinovich, 2006)
autorunsc.exe -a -c -d -e -s -w	Lists programs are configured to run during system bootup or login, and shows you the entries in the order Windows processes them (Russinovich & Cogswell, 2006)

ipconfig /all	List the current configuration of all network interface cards.
tasklist	Displays a list of application(s) and associated task(s)/process(es) currently running the local system.
tasklist /m	Displays all DLL modules loaded by each task.
tasklist /svc	Displays services in each process.
tasklist /v	Displays a list of application(s) and associated task(s)/process(es) currently running the local system and specifies that the verbose information is to be displayed.
pslist	Lists detailed information about processes (Russinovich, 2006)
pulist	Lists processes running on local or remote computers. (From Windows 2000 Resource Kit) (Microsoft.com, 2000)
pstat	Lists the status of threads, processes, and drivers that are currently running on the local machine. (From Windows XP Support Tools) (Microsoft.com, 2004)
net session	Displays information about all sessions with the local computer.
nbtstat -S	Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP) and lists sessions table with the destination IP addresses.
nbtstat -A test_machine_IP_address	Lists the remote machine's name table given its IP address.
attrib -r -h -s	Clears the read-only, hidden and system file attributes for all files in

C:\Windows\Tasks*	C:\Windows\Task.
at	Displays the scheduled commands and programs to run on the local machine at a specified time and date.
netstat -nao	Displays protocol statistics and current TCP/IP network connections including all connections and listening ports with addresses and port numbers in numerical form, and displays the owning process ID associated with each connection.
fport	Lists all open TCP/IP and UDP ports and maps them to the associated application (Foundstone.com, 2002)
cmdline	Lists processes on the system, including process IDs and full command lines (with all parameters) (DiamondCS.com, 2003)

Table 2: Commands used for testing using the Linux live CDs on a live system

Commands and options	Purpose
date	Identify the date and time of the start of the first responder process
set	List the environmental variables
mount -n /mnt/cdrom	Mount the first responder CD
/mnt/cdrom/bin/bash	Start a known good shell from the first responder CD
cd /mnt/cdrom/bin	Move to the directory containing the known good binaries.
PATH=”/mnt/cdrom/bin”	Set the **PATH** variable to the location of the known good binaries

LD_LIBRARY_PATH=”/mnt/cdrom/lib”	Set the **LD_LIBRARY_PATH** variable to the location of the known good libraries
export PATH	Make the **PATH** variable to be in the environment of subsequently executed commands
export LD_LIBRARY_PATH	Make the **LD_LIBRARY_PATH** variable to be in the environment of subsequently executed commands
echo $PATH	Verify the setting of the environment variable
echo $LD_LIBRARY_PATH	Verify the setting of the environment variable
ls -la /mnt/cdrom/bin	List the contents of the binaries used by the first responder
ls -la /mnt/cdrom/lib	List the contents of the libraries used by the first responder
ifconfig -a	List the current configuration of all network interfaces.
netstat -a	Symbolically displays the contents of various network-related data structures showing the address of any protocol control blocks associated with sockets
netstat -arp	Symbolically displays the contents of various network-related data structures showing the address of any protocol control blocks associated with sockets

	and the routing tables.
netstat -ap -inet	Symbolically displays the contents of various network-related data structures showing
route -n -v -ee	Display and manually manipulate the network routing tables
arp -v -n	Displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol
w	Prints a summary of the current activity on the system, including what each user is doing
who	Displays information about currently logged in users
last	Displays a list of all users logged in (and out) since */var/log/wtmp* was created.
who -Hi	Displays information about currently logged in users
finger -ls	Displays information about the system users
last -aix	Displays a list of all users logged in (and out) since */var/log/wtmp*
lastb -aix	Displays a list of all of the bad login attempts since */var/log/btmp* was created
ps -auxeww	Displays information about a selection

	of the active processes
ps -aux	Displays information about a selection of the active processes
top -b -n1	Provides a dynamic real-time view of a running system
lsof -i -n -P -l	Lists information about files opened by processes with the listing of all Internet and network files selected and the conversion of network numbers to host names, port numbers to port names, and user ID numbers to login names inhibited.
lsof -i	Lists information about files opened by processes with the listing of all Internet and network files selected
lsof -d rtd	Lists information about files opened by processes with the specified list of file descriptors that is, in this case, **rtd**, a root directory
lsof +M -i	Lists information about files opened by processes with the reporting of portmapper registrations for local TCP and UDP ports enabled.

Table 3: Live CDs to be tested

Distribution	**Version**	Source	**Description from website**
Helix	1.7	http://www.e-fense.com/helix/	Helix is a customized distribution of the Knoppix Live Linux CD. Helix is more than just a bootable live CD. You can still boot into a customized

			Linux environment that includes customized linux kernels, excellent hardware detection and many applications dedicated to Incident Response and Forensics. (e-fense.com, 2006)
Bart's Preinstalled Environment bootable live windows CD/DVD (BartPE)	Version 3.1.10a	http://www.nu2.nu/pebuilder/	Bart's PE Builder helps you build a "BartPE" (Bart Preinstalled Environment) bootable Windows CD-Rom or DVD from the original Windows XP or Windows Server 2003 installation/setup CD, very suitable for PC maintenance tasks. It will give you a complete Win32 environment with network support, a graphical user interface (800x600) and FAT/NTFS/CDFS filesystem support. (Lagerweij, 2006)
Forensic and Incident Response Environment Bootable CD (F.I.R.E.)	0.3.5b	http://biatchux.dmzs.com/	FIRE is a portable bootable cdrom based distribution with the goal of providing an immediate environment to perform forensic analysis, incident response, data recovery, virus scanning and vulnerability assessment. (Salusky, 2002)
Inside Security Rescue Toolkit (INSERT)	v1.3.6	http://www.inside-security.de/insert_en.html	INSERT is a complete, bootable linux system. It comes with a graphical user interface running the fluxbox window manager while still being sufficiently small to fit on a credit card-sized CD-ROM. (Inside Security IT Consulting GmbH, 2006)
Operator	3.3.20	http://www.us	Operator is a complete Linux (Debian)

		sysadmin.com/ operator/	distribution that runs from a single bootable CD and runs entirely in RAM. The Operator contains an extensive set of Open Source network security tools that can be used for monitoring and discovering networks. This virtually can turn any PC into a network security pen-testing device without having to install any software. Operator also contains a set of computer forensic and data recovery tools that can be used to assist you in data retrieval on the local system. (Barber, 2005)

4. Testing Results

Live CDs Used for Live System Incident Handling

This section discusses the each live CD including the pros and cons and other issues with using the live CD as a first responders' tool.

BartPE:

This is the hardest live CD to obtain since you must build the ISO image using your licensed copy of Widows XP. All tools that you want to use must be collected from the appropriate website before attempting to build the ISO. It took multiple trial versions to create the CD used that had all of the Windows tools and required DLLs available and running.

Pros:

It's very easy to customize since you are building your own ISO image to burn to the CD. The customization attempted for this evaluation was limited to the addition of tools for Windows. Further customization could be done to add Linux static binary tools and the addition of other device drivers.

When you insert the CD in a live system, a "Go" menu is created over the Start menu and it gives you access to the known-good command shell from the CD. From there, the known good tools can be used as a first responder.

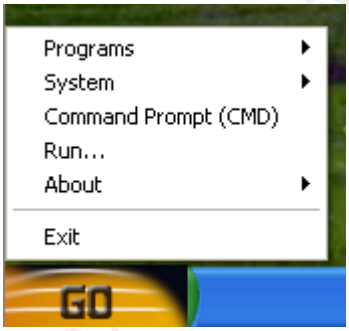

Figure 2: BartPE Go Menu

Cons:

There are no Linux binaries for incident response. For imaging the RedHat Linux 9 machine, there is no capability to access Linux partitions in the VMware machines because the drivers for the virtualized SCSI adapter are not on the BartPE CD, not to mention the fact that drivers for the EXT2 file system are not included. For the forensic imaging of the RedHat Linux 9 machine, the INSERT live CD was used to boot the machine and image the hard drive.

F.I.R.E.

Pros:

The F.I.R.E. interface launches upon insertion of the CD into a machine if autorun is enabled on the suspect machine. That allows quick access to the Forensic Command Shell. One of the advantages of the Forensic Command shell is its start-up script sets the PATH environment to the directory of the known good Windows executables on the F.I.R.E. live CD. This should help to minimize the effect of the live CD on the subsequent forensic analysis.

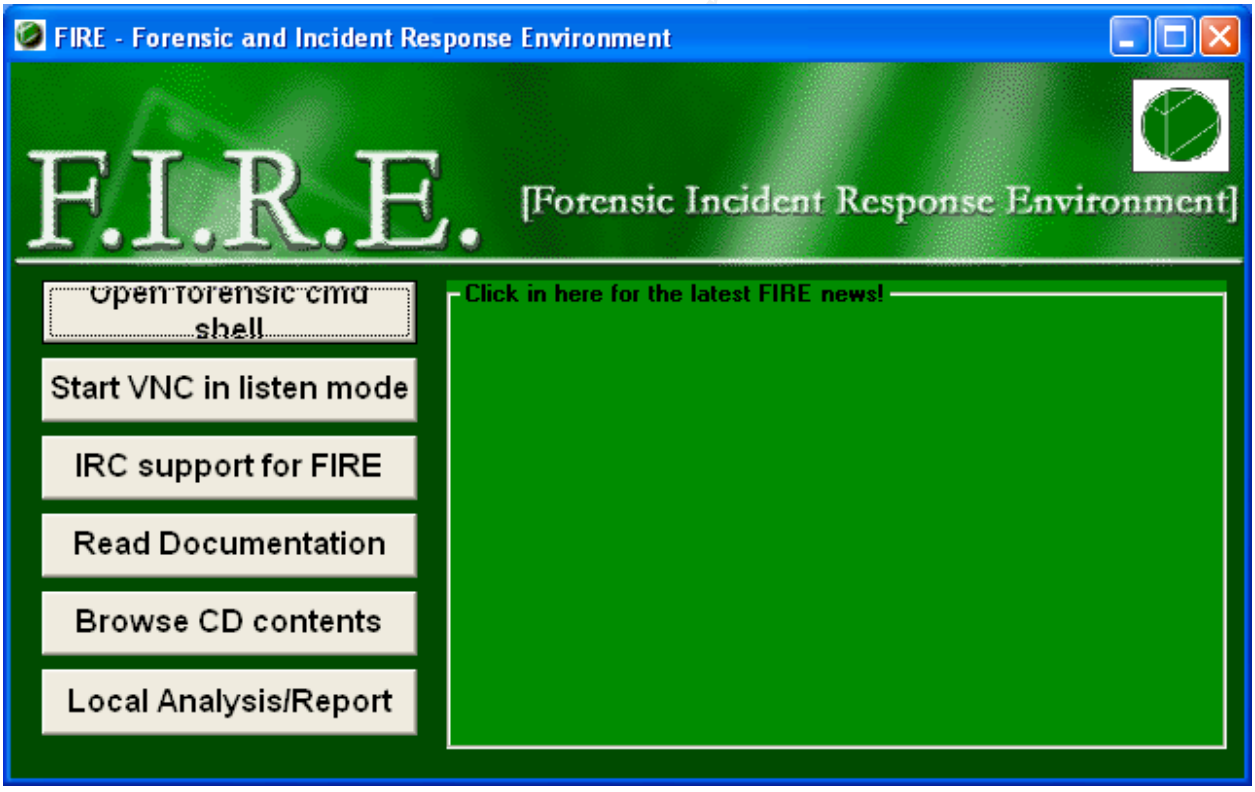

Figure 3: F.I.R.E. Pop-up Window

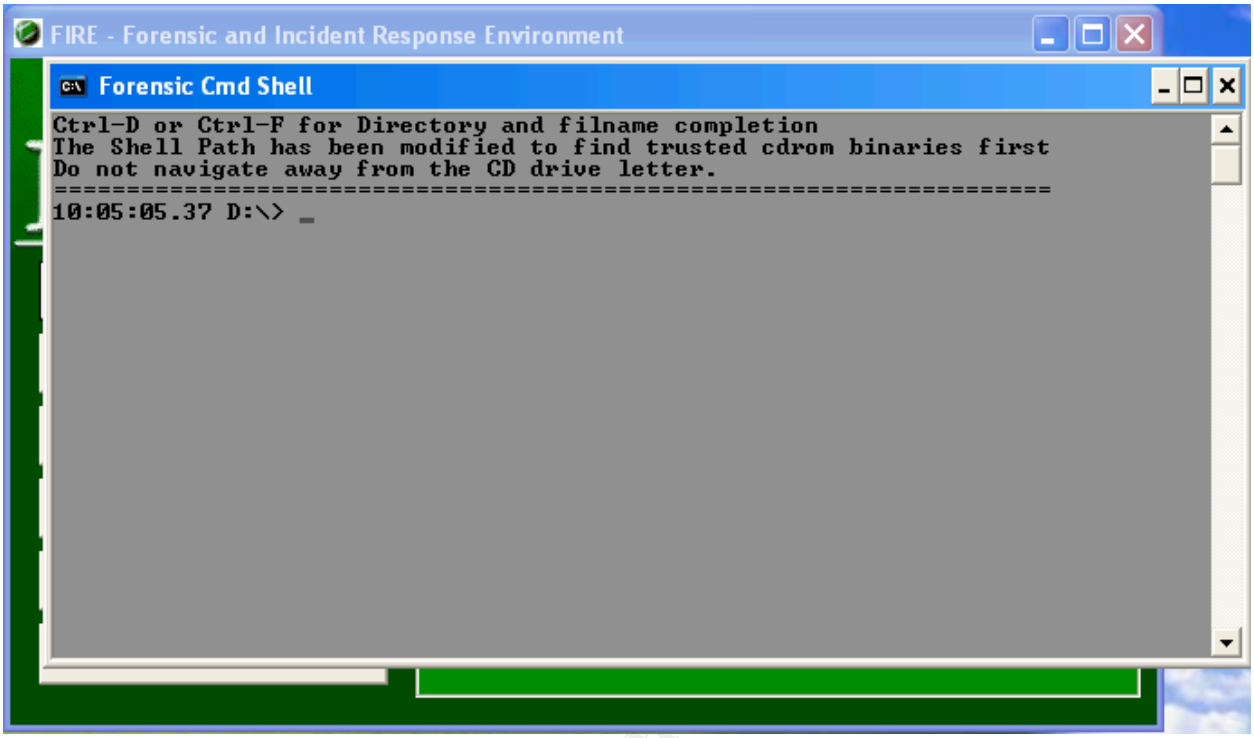

Figure 4: F.I.R.E. Command Shell

Cons:

Several of the tools selected for use on Windows machines were not available.

For the Linux machine, several of the static binary tools were missing or failed with a segmentation fault. The missing tools were: **finger**, **last**, **w**, **lastb**, and **ps**. The tools that failed were: **netstat**, **lsof**.

For imaging the RedHat Linux 9 machine, the SCSI hard drive that contained the Linux partitions in the VMware machines could not be accessed because the drivers for the virtualized SCSI adapter are not on the F.I.R.E. live CD. To image the RedHat Linux 9 machine, the INSERT LiveCD was used to boot the machine and image the hard drive.

Helix

The CD contains numerous other incident response and forensics tools and toolkits, including Autopsy Forensics Browser (Carrier, 2006) and the Windows Forensics Toolchest (WFT) (McDougal, 2006).

Pros:

The Helix splash screen launches upon insertion of the CD into a machine if autorun is enabled on the target machine. That allows quick access to a known good Command Prompt from the menu. Like the F.I.R.E. live CD, one of the advantages of the Forensic Command Prompt is it's start-up script sets the PATH environment to the directory of the known good Windows executables on the Helix live CD.

Figure 5: Helix Initial Screen

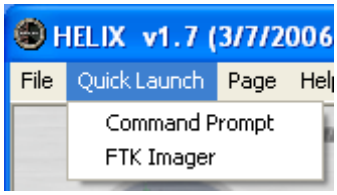

Figure 6: Accessing the Helix Command Prompt

The Helix CD also includes numerous other packages of tools that can automate the process to collect the first responder data and for the subsequent forensics examination.

Cons:

On the Windows XP machine there were several tools chosen for the testing that were not available, as shown in Figure 7.

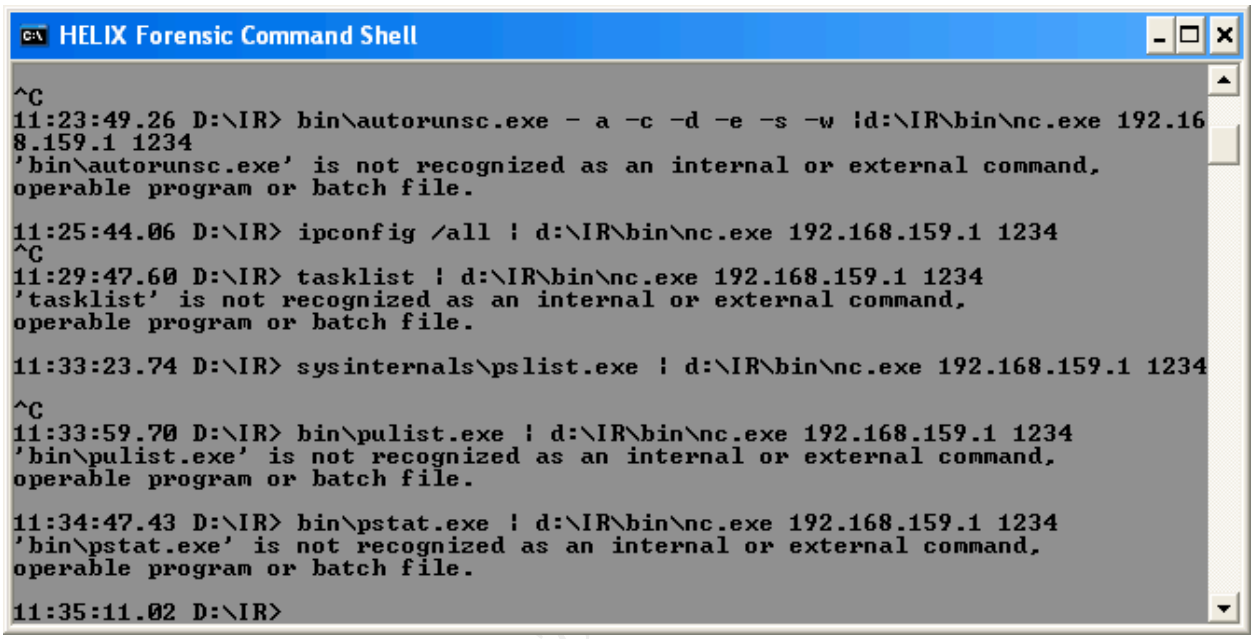

Figure 7: Some of Missing Tools on Helix Live CD

For the Linux machine, several of the static binary tools were missing or failed with a segmentation fault. The missing tools were: **finger**, **w**, and **lastb**. The tools that failed were: **netstat**, **top**, and **lsof**.

Similar to the BartPE and F.I.R.E. live CDs, the SCSI hard drive could not be accessed due to the lack of SCSI adapter drivers. The INSERT LiveCD was used to boot the machine and image the hard drive.

INSERT

INSERT worked well within its limitations. One thing to note for the INSERT live CD, the netcat binary is “netcat” not “nc” as it is on most Linux machines.

Pros:

When used to boot the RedHat Linux machines, it recognized and had the drivers for the SCSI adapter in the RedHat Linux virtual machine.

The ISO includes the captive NTFS drivers (Kratochvil, 2006) for mounting the Windows NTFS partitions but does not mount them by default.

Cons:

No Windows tools for the first responder, however, it is capable of imaging the Windows VM hard drive. If the CD is inserted in a running machine, the autorun opens a browser window containing the index.html from the root directory of the CD.

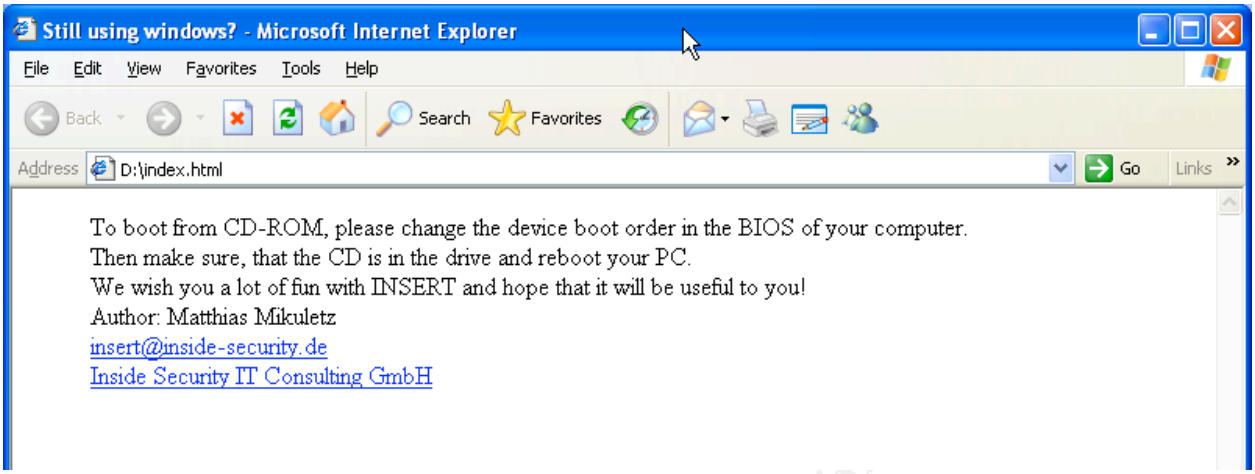

Figure 8: INSERT Autorun Web Page

No Linux tools for the first responder, however, it does have the drivers for the SCSI adapter used in the RedHat virtual machine and is capable of imaging the Linux drive.

Operator

The Operator CD is similar to the INSERT CD in functionality being tested. Although, the Operator CD does not have an automatically opening HTML file when the CD is inserted in the live machine.

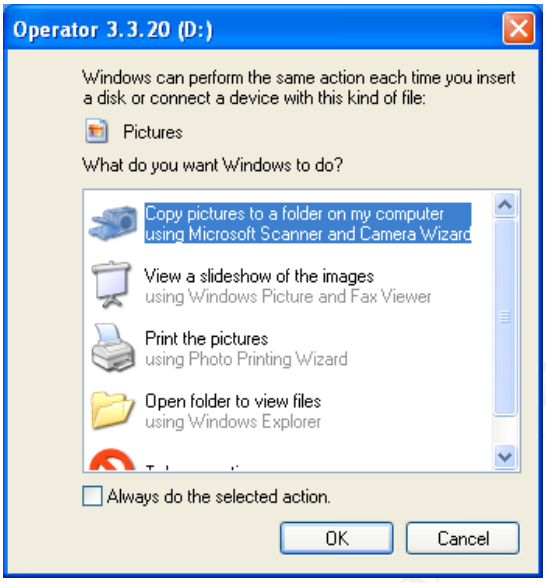

Figure 9: Results of Inserting the Operator Live CD in the Windows XP Machine

Pros:

When used to boot the RedHat Linux machines, it recognized and had the drivers for the SCSI adapter in the RedHat Linux machine.

Cons:

No Windows or Linux tools for the first responder, however, it is capable of imaging the Windows and the Linux hard drives.

Analysis of the Forensic Images

The hard drive images taken from the target machines with the live CDs were analyzed using Autopsy to create a File Activity Timeline for each hard drive. The timelines for each target operating system, Windows XP and RedHat Linux 9, were compared to determine which live CD creates the biggest signature. To ease the process of analysis only the files that

were changed after the approximate time that the virtual machine was suspended were used to create a signature for that live CD. For the Windows XP system, the time was Sun Oct 01 2006 04:06:38.

For the RedHat Linux 9 system, the approximate time of suspending the virtual machine was Sun Oct 01 2006 06:40:10. Slight differences existed between the timelines before that time. However, those differences were due to deleted files appearing at different locations in the timeline.

Comparison of the Windows XP Timelines

Not surprisingly, the live CDs with the lowest interaction with the live system, i.e., those with no Windows first responder tools, produced the smallest number of changes in the timeline. The converse is also true for the live CDs that had a large number of first responder tools, e.g., F.I.R.E. and Helix. The BartPE live CD had the largest number of Windows first responder tools had the largest effect on the hard drive.

Table 4: Windows Results

Live CD	Number of Timeline entries
Operator	86
INSERT	163
Helix	327
FIRE	343
BartPE	459

Reviewing the files listed in the File Activity Timeline for the period of interest, there were 79 files that were common to all of the live CDs, see Appendix A for the list of files. The BartPE live CD had the largest number of Windows first responder tools had the largest effect on the hard drive. The difference between Operator and INSERT, the two live CDs with no first responder tools, is due to autorun opening of the browser with the INSERT HTML file.

Comparison of the RedHat Linux 9 Timelines

For the two live CDs that were able to image the hard drive on the RedHat Linux machine, the files that were modified while the system running were almost exactly the same. This is probably a result of the GUI running for the period of time it took to insert the CD in the live system, the CD to automount and then securing power to the system.

Table 5: Linux Results

Live CD	Number of Timeline entries
BartPE	376
Operator	377
INSERT	384
FIRE	410
Helix	764

A review of the differences of between the signatures of the live CDs showed that the large delta between the Helix live CD and the rest was caused by the Helix CD accessing 360 files

in the /usr/lib/locale directory. If those 360 files are taken out of the analysis, there are 369 modified files that are common to all five live CD signatures, these are listed in Appendix C. Two files that were deleted, at inodes 290894 and 290964, are included in the list. For the modified files that were not common, there were several that were in the signature for three of the five, F.I.R.E, Helix, and INSERT, but not by the other two. Appendix D lists the modified files that are not common amount all five live CDs.

Table 6: Linux Results with Common Files Removed

Live CD	Number of Timeline entries
BartPE	7
Operator	8
INSERT	15
Helix	35
FIRE	41

5. Summary

The use of live CDs as a first responders' tool has several advantages. They provide known good tools to the first responders. They may also provide additional tools that may not exist on the standard machine. However, the choice of live CD to use depends on the environment that it will be used in.

For a Windows environment, the Helix live CD will be the best choice unless a customized BartPE live CD is created for the environment. The F.I.R.E live CD would also be a good

choice, but it's not recommended since it doesn't appear to be currently maintained.

In a Linux-centric environment, the Helix live CD is again probably the best choice. The next best choice would be a customized live CD that included static binaries for the versions of the Linux kernel that are in use in the environment, i.e., 2.4 and 2.6.

In some cases it might be better to have two CDs for first responders, one with the known good tools for live system investigation and another CD for dead system investigation that is bootable with the necessary devices drivers to image the machines and access the drives.

If the option exists to customize the CD, scripts and approved procedures can be added to the live CD to standardize "actions" taken by the first responder. Other additions to the customized live CD that may be required are drivers for devices that exist in the environment but not on the standard version of the live CD.

In any case that a live CD is used as a first responders' tool in the six-step incident handling process, it will affect the forensics of the computer. All of the live CDs change the state of the machine being examined to some degree. The actions taken and tools used by the first responders and incident handlers must be recorded. The forensics expert needs the record to differentiate between the attackers' actions and the incident response process.

6. References

Barber, J. (2005, October 1). Operator v3.3.20 [Computer Software]. Retrieved January 5, 2007, from US Sysadmin Web site: http://www.ussysadmin.com/operator/

Brand, N. (2006, December 30). The LiveCD List. Retrieved January 3, 2007, from FrozenTech Web site: http://www.frozentech.com/content/livecd.php

Carrier, B. (2006, September 1). Autopsy Forensic Browser. Retrieved January 4, 2007, from The Sleuth Kit Web site: http://www.sleuthkit.org/autopsy/

DiamondCS.com. (2003). CmdLine - Freeware Console Tool for Windows to show all processes and commandline parameters. Retrieved January 5, 2007, from DiamondCS Web site: http://www.diamondcs.com.au/index.php?page=console-cmdline

e-fense.com. (2006). Helix - Incident Response & Computer Forensics Live CD by e-fense, Inc. [Computer Software]. Retrieved January 3, 2007, from e-fense™, Inc. Web site: http://www.e-fense.com/helix/

First Responders – Unix/Linux Stay Sharp Course Book (Security 552), (2005). Bethesda, MD: SANS Institute.

First Responders – Windows Stay Sharp Course Book (Security 551), (2005). Bethesda, MD: SANS Institute.

Forensic and Investigative Essentials. (2006) In R. Lee (Ed.), *Security 508 System Forensics, Investigation & Response*.

Bethesda, MD: SANS Institute.

Foundstone.com. (2002). Intrusion Detection Tools: Fport v2.0 [Computer Software]. Retrieved January 5, 2007, from Foundstone, a division of McAfee, Inc. Web site: http://www.foundstone.com/index.htm?subnav=home/navigation.htm&subcontent=/search/index_search.htm%3Fq%3Dfport

Hobbit. (1996, March 20). Netcat (Version 1.10 for Unix and Version 1.11 for NT) [Computer Software]. Retrieved January 3, 2007, from VulnWatch: vulnerability disclosure list Web site: http://www.vulnwatch.org/netcat/

Incident Handling Step by Step and Computer Crime Investigation. (2006). In E. Skoudis (Ed.), *Security 504 Hacker Techniques, Exploits & Incident Handling*. Bethesda, MD: SANS Institute.

Inside Security IT Consulting GmbH. (2006, February 22). Inside Security Rescue Toolkit - INSERT (Version 1.3.6) [Computer Software]. Retrieved January 5, 2007, from Inside Security Web site: http://www.inside-security.de/insert_en.html

Knopper, K (2006). KNOPPIX - Live Linux Filesystem On CD. Retrieved January 3, 2007, from knoppix.org Web site: http://www.knopper.net/knoppix/index-en.html

Kratochvil, J. (2006, February 28). Jan Kratochvil: Captive: The first free NTFS read/write filesystem for GNU/Linux. Retrieved January 5, 2007, from Jan Kratochvil: Project List Web site: http://www.jankratochvil.net/project/captive/

Lagerweij, B. (2006, February 17). Bart's Preinstalled Environment (BartPE) bootable live windows CD/DVD. Retrieved

January 3, 2007, from nu2.nu Web site: http://www.nu2.nu/pebuilder/

McDougal, M. (2006, September 1). Windows Forensic Toolchest (WFT). Retrieved January 4, 2007, from Fool Moon Software & Security Web site: http://www.foolmoon.net/security/wft/

Microsoft.com. (2004, August 10). Windows XP Service Pack 2 Support Tools [Computer Software]. Retrieved January 5, 2007, from Microsoft TechNet Web site: http://www.microsoft.com/downloads/details.aspx?FamilyID=49AE8576-9BB9-4126-9761-BA8011FABF38&displaylang=en

Microsoft.com. (2004, June 30). Windows Preinstallation Environment Overview. Retrieved January 3, 2007, from microsoft.com Web site: http://www.microsoft.com/whdc/system/winpreinst/WindowsPE_over.mspx

Microsoft.com. (2000, October 18). Windows 2000 Resource Kit Tool : PUList (pulist.exe) [Computer Software]. Retrieved January 5, 2007, from Microsoft TechNet Web site: http://www.microsoft.com/downloads/details.aspx?FamilyID=9b9da78d-f7d1-4b8a-8a31-3bb725c7a069&DisplayLang=en

Paderni, G. (2006, February 18). OliveBSD - OpenBSD Live CD. Retrieved January 12, 2007, from OliveBSD - OpenBSD Live CD Web site: http://g.paderni.free.fr/olivebsd/

Remote-exploit.org, (2006). Auditor - Remote-exploit.org. Retrieved January 3, 2007, from remote-exploit.org Web site: http://www.remote-exploit.org/index.php/Auditor

Russinovich, M. (2006, December 4). PsInfo v1.74 [Computer Software]. Retrieved January 5, 2007, from Microsoft TechNet: Windows SysInternals Web site: http://www.microsoft.com/technet/sysinternals/utilities/psinfo.mspx

Russinovich, M. (2006, December 4). PsList v1.28 [Computer Software]. Retrieved January 5, 2007, from Microsoft TechNet: Windows SysInternals Web site: http://www.microsoft.com/technet/sysinternals/ProcessesAndThreads/PsList.mspx

Russinovich, M. & Cogswell, B. (2006, November 1). AutoRuns for Windows v8.54 [Computer Software]. Retrieved January 5, 2007, from Microsoft TechNet: Windows SysInternals Web site: http://www.microsoft.com/technet/sysinternals/ProcessesAndThreads/Autoruns.mspx

Salusky, W. (2002, November 29). F.I.R.E. Forensic and Incident Response Environment Bootable CD (Version 0.3.5b) [Computer Software]. Retrieved January 4, 2007, from F.I.R.E. Forensic and Incident Response Environment Bootable CD Web site: http://fire.dmzs.com

Slackware.com, (2006). The Slackware Linux Project. Retrieved January 3, 2007, from The Slackware Linux Project Web site: http://www.slackware.com

S-T-D.org, (2006). S-T-D. Retrieved January 3, 2007, from STD 0.1 security tools distribution Web site: http://www.s-t-d.org/index.html

Syring, K. M. (2004, April 30). GNU utilities for Win32 [Computer software]. Retrieved January 3, 2007, from Native win32 ports of some GNU utilities Web site: http://unxutils.sourceforge.net

Ubuntu.com. (2006). Ubuntu: Linux for human beings. Retrieved January 3, 2007, from Ubuntu Web site: http://www.ubuntu.com/

VMware.com. (2006). VMware Workstation virtual machine for Linux, Windows & More: VMware - VMware. Retrieved January 3, 2007, from VMware: Virtualization, Virtual Machine & Virtual Server Consolidation - VMware Web site: http://www.vmware.com/products/ws/

Wikipedia.org, (2007, January 6). Berkeley Software Distribution - Wikipedia, the free encyclopedia. Retrieved January 12, 2007, from Wikipedia.org Web site: http://en.wikipedia.org/wiki/Berkeley_Software_Distribution

7. Appendix A Common Files Modified by the Live CDs on the Windows XP Virtual Machine

```
1175-144-1 C:/Documents and
   Settings/test/Local
   Settings/Temp/VMwareDnD
124-144-5 C:/WINDOWS/WinSxS
124-144-5 C:/WINDOWS/WinSxS
   (deleted-realloc)
15510-128-3
   C:/WINDOWS/system32/setupapi.dll
15526-128-3
   C:/WINDOWS/system32/oleaut32.dll
15531-128-3
   C:/WINDOWS/system32/ntdll.dll
15541-128-3
   C:/WINDOWS/system32/kernel32.dll
15542-128-3
   C:/WINDOWS/system32/imagehlp.dll
15549-128-3
   C:/WINDOWS/system32/comctl32.dll
15550-128-3
   C:/WINDOWS/system32/cmd.exe
15553-128-3
   C:/WINDOWS/system32/advapi32.dll
15555-128-3
   C:/WINDOWS/system32/xpsp2res.dll
15613-128-3
   C:/WINDOWS/system32/wintrust.dll
15622-128-3
   C:/WINDOWS/system32/winmm.dll
15624-128-3
   C:/WINDOWS/system32/SET1D8.tmp
   (deleted-realloc)
15624-128-3
   C:/WINDOWS/system32/winlogon.exe
15653-128-3
   C:/WINDOWS/system32/SET1ED.tmp
   (deleted-realloc)
15653-128-3
   C:/WINDOWS/system32/version.dll
15660-128-3
   C:/WINDOWS/system32/SET1F3.tmp
   (deleted-realloc)
15660-128-3
   C:/WINDOWS/system32/uxtheme.dll
15664-128-3
   C:/WINDOWS/system32/SET1F6.tmp
   (deleted-realloc)
15664-128-3
   C:/WINDOWS/system32/userenv.dll
15665-128-3
   C:/WINDOWS/system32/SET1F7.tmp
   (deleted-realloc)
15665-128-3
   C:/WINDOWS/system32/user32.dll
15772-128-3
   C:/WINDOWS/system32/SET24F.tmp
   (deleted-realloc)
15772-128-3
   C:/WINDOWS/system32/shlwapi.dll
15775-128-3
   C:/WINDOWS/system32/SET251.tmp
   (deleted-realloc)
15775-128-3
   C:/WINDOWS/system32/shimeng.dll
15778-128-3
   C:/WINDOWS/system32/SET254.tmp
   (deleted-realloc)
15778-128-3
   C:/WINDOWS/system32/shell32.dll
15820-128-3
   C:/WINDOWS/system32/rundll32.exe
15827-128-3
   C:/WINDOWS/system32/rsaenh.dll
15829-128-3
   C:/WINDOWS/system32/rpcss.dll
15831-128-3
   C:/WINDOWS/system32/rpcrt4.dll
15831-128-3
   C:/WINDOWS/system32/SET27A.tmp
   (deleted-realloc)
15913-128-3
   C:/WINDOWS/system32/ole32.dll
15913-128-3
   C:/WINDOWS/system32/SET2BE.tmp
   (deleted-realloc)
16018-128-3
   C:/WINDOWS/system32/msvcrt.dll
16018-128-3
   C:/WINDOWS/system32/SET312.tmp
   (deleted-realloc)
16107-128-3
   C:/WINDOWS/system32/msacm32.dll
16107-128-3
   C:/WINDOWS/system32/SET362.tmp
   (deleted-realloc)
16209-128-3
   C:/WINDOWS/system32/imapi.exe
16247-128-3
   C:/WINDOWS/system32/gdi32.dll
```

```
16247-128-3
   C:/WINDOWS/system32/SET3E2.tmp
   (deleted-realloc)
16383-128-3
   C:/WINDOWS/system32/crypt32.dll
16383-128-3
   C:/WINDOWS/system32/SET456.tmp
   (deleted-realloc)
16392-128-3
   C:/WINDOWS/system32/comres.dll
16392-128-3
   C:/WINDOWS/system32/SET45C.tmp
   (deleted-realloc)
17163-144-1
   C:/WINDOWS/WinSxS/x86_Microsoft.
   Windows.Common-
   Controls_6595b64144ccf1df_6.0.26
   00.2180_x-ww_a84f1ff9
17164-128-3
   C:/WINDOWS/WinSxS/x86_Microsoft.
   Windows.Common-
   Controls_6595b64144ccf1df_6.0.26
   00.2180_x-
   ww_a84f1ff9/comctl32.dll
17166-128-4
   C:/WINDOWS/WinSxS/Manifests/x86_
   Microsoft.Windows.Common-
   Controls_6595b64144ccf1df_6.0.26
   00.2180_x-ww_a84f1ff9.Manifest
17168-128-4
   C:/WINDOWS/WinSxS/Policies/x86_p
   olicy.6.0.Microsoft.Windows.Comm
   on-Controls_6595b64144ccf1df_x-
   ww_5ddad775/6.0.2600.2180.Policy
1726-128-3
   C:/WINDOWS/system32/wbem/wbemcon
   s.dll
180-128-3
   C:/WINDOWS/system32/clbcatq.dll
2615-144-6 C:/Program
   Files/VMware/VMware Tools
2619-144-1 C:/Documents and
   Settings/test/Local
   Settings/Temp/VMwareDnD/000069da
2708-128-3
   C:/WINDOWS/AppPatch/acgenral.dll
271-128-4
   C:/WINDOWS/Prefetch/RUNDLL32.EXE
   -451FC2C0.pf
28-144-6 C:/WINDOWS
29-144-7 C:/WINDOWS/system32
2963-128-3
   C:/WINDOWS/system32/msasn1.dll
2963-128-3
   C:/WINDOWS/system32/SET35D.tmp
   (deleted-realloc)
3328-128-4 C:/Documents and
   Settings/test/NTUSER.DAT.LOG
3330-128-3
   C:/WINDOWS/system32/config/syste
   m.LOG
3331-128-0
   C:/WINDOWS/system32/config/softw
   are.LOG
3387-144-6
   C:/WINDOWS/WinSxS/Policies/x86_p
   olicy.6.0.Microsoft.Windows.Comm
   on-Controls_6595b64144ccf1df_x-
   ww_5ddad775
401-128-3
   C:/WINDOWS/system32/actxprxy.dll
401-128-3
   C:/WINDOWS/system32/SET4A2.tmp
   (deleted-realloc)
5188-144-6 C:/WINDOWS/Registration
5472-144-1 C:/WINDOWS/Tasks
6165-128-4
   C:/WINDOWS/WindowsShell.Manifest
6165-128-4
   C:/WINDOWS/WindowsShell.Manifest
   (deleted-realloc)
72-144-1 C:/WINDOWS/Temp
87-144-5 C:/WINDOWS/AppPatch
921-128-4
   C:/WINDOWS/Prefetch/IMAPI.EXE-
   0BF740A4.pf
9631-128-3
   C:/WINDOWS/system32/wbem/Logs/wb
   emess.log
```

8. Appendix B Files Modified by the Live CDs on the Windows XP Virtual Machine

Live CD	File
BartPE	1076-128-4 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP
BartPE	1077-128-3 C:/Program Files/Windows NT/Accessories/wordpad.exe
BartPE	1106-128-4 C:/WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf
BartPE	1399-128-3 C:/Program Files/Common Files/System/Ole DB/oledb32.dll
BartPE	1399-128-3 C:/Program Files/Common Files/System/Ole DB/SET4FB.tmp (deleted-realloc)
BartPE	1399-128-3 C:/WINDOWS/system32/msrd3x40.dll (deleted-realloc)
BartPE	1422-128-3 C:/WINDOWS/system32/msxml3r.dll
BartPE	1544-128-3 C:/WINDOWS/system32/ntlanui2.dll
BartPE	15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys
BartPE	15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys (deleted-realloc)
BartPE	15496-128-3 C:/WINDOWS/system32/drivers/acpi.sys
BartPE	15498-128-3 C:/WINDOWS/system32/winspool.drv
BartPE	15501-128-3 C:/WINDOWS/system32/userinit.exe
BartPE	15512-128-3 C:/WINDOWS/system32/services.exe
BartPE	15512-128-3 C:/WINDOWS/system32/services.exe (deleted-realloc)
BartPE	15517-128-3 C:/WINDOWS/system32/samlib.dll
BartPE	15518-128-3 C:/WINDOWS/system32/rshx32.dll
BartPE	15520-128-3 C:/WINDOWS/system32/rasman.dll
BartPE	15523-128-3 C:/WINDOWS/system32/rasapi32.dll
BartPE	15524-128-3 C:/WINDOWS/system32/printui.dll
BartPE	15525-128-3 C:/WINDOWS/system32/perfctrs.dll
BartPE	15533-128-3 C:/WINDOWS/system32/msv1_0.dll
BartPE	15563-128-3 C:/WINDOWS/system32/wzcsapi.dll
BartPE	15564-128-3 C:/WINDOWS/system32/wzcdlg.dll
BartPE	15565-128-3 C:/WINDOWS/system32/wtsapi32.dll
BartPE	15568-128-3 C:/WINDOWS/system32/wsock32.dll
BartPE	15571-128-3 C:/WINDOWS/system32/wshtcpip.dll
BartPE	15576-128-3 C:/WINDOWS/system32/wshext.dll
BartPE	15579-128-3 C:/WINDOWS/system32/ws2help.dll
BartPE	15581-128-3 C:/WINDOWS/system32/ws2_32.dll
BartPE	15595-128-3 C:/WINDOWS/system32/wmpshell.dll
BartPE	15601-128-3 C:/WINDOWS/system32/wmi.dll
BartPE	15608-128-3 C:/WINDOWS/system32/wlnotify.dll
BartPE	15610-128-3 C:/WINDOWS/system32/wldap32.dll
BartPE	15615-128-3 C:/WINDOWS/system32/winsta.dll
BartPE	15616-128-3 C:/WINDOWS/system32/winsrv.dll
BartPE	15619-128-3 C:/WINDOWS/system32/winrnr.dll
BartPE	15627-128-3 C:/WINDOWS/system32/wininet.dll
BartPE	15630-128-3 C:/WINDOWS/system32/wiashext.dll
BartPE	15641-128-3 C:/WINDOWS/system32/webcheck.dll
BartPE	15677-128-3 C:/WINDOWS/system32/upnp.dll
BartPE	15695-128-3 C:/WINDOWS/system32/themeui.dll

Live CD	File
BartPE	15709-128-3 C:/WINDOWS/system32/tapi32.dll
BartPE	15715-128-3 C:/WINDOWS/system32/syncui.dll
BartPE	15719-128-3 C:/WINDOWS/system32/svchost.exe
BartPE	15723-128-3 C:/WINDOWS/system32/stobject.dll
BartPE	15748-128-3 C:/WINDOWS/system32/spoolsv.exe
BartPE	15760-128-3 C:/WINDOWS/system32/slayerxp.dll
BartPE	15768-128-3 C:/WINDOWS/system32/shscrap.dll
BartPE	15770-128-3 C:/WINDOWS/system32/shmgrate.exe
BartPE	15771-128-3 C:/WINDOWS/system32/shmedia.dll
BartPE	15774-128-3 C:/WINDOWS/system32/shimgvw.dll
BartPE	15777-128-3 C:/WINDOWS/system32/shfolder.dll
BartPE	15780-128-3 C:/WINDOWS/system32/shdocvw.dll
BartPE	15784-128-3 C:/WINDOWS/system32/sfc_os.dll
BartPE	15786-128-3 C:/WINDOWS/system32/sfc.dll
BartPE	15791-128-3 C:/WINDOWS/system32/sensapi.dll
BartPE	15793-128-3 C:/WINDOWS/system32/sens.dll
BartPE	15795-128-3 C:/WINDOWS/system32/sendmail.dll
BartPE	15798-128-3 C:/WINDOWS/system32/secur32.dll
BartPE	1580-128-3 C:/WINDOWS/system32/wbem/wmiutils.dll
BartPE	15804-128-3 C:/WINDOWS/system32/scrobj.dll
BartPE	15821-128-3 C:/WINDOWS/system32/rtutils.dll
BartPE	15833-128-3 C:/WINDOWS/system32/riched20.dll
BartPE	15835-128-3 C:/WINDOWS/system32/resutils.dll
BartPE	15838-128-3 C:/WINDOWS/system32/remotepg.dll
BartPE	15840-128-3 C:/WINDOWS/system32/regsvr32.exe
BartPE	15856-128-3 C:/WINDOWS/system32/rcbdyctl.dll
BartPE	15866-128-3 C:/WINDOWS/system32/rasadhlp.dll
BartPE	15869-128-3 C:/WINDOWS/system32/query.dll
BartPE	15884-128-3 C:/WINDOWS/system32/psapi.dll
BartPE	15900-128-3 C:/WINDOWS/system32/photowiz.dll
BartPE	15901-128-3 C:/WINDOWS/system32/perfproc.dll
BartPE	15902-128-3 C:/WINDOWS/system32/perfos.dll
BartPE	15904-128-3 C:/WINDOWS/system32/perfdisk.dll
BartPE	15905-128-3 C:/WINDOWS/system32/pdh.dll
BartPE	15937-128-3 C:/WINDOWS/system32/occache.dll
BartPE	15942-128-3 C:/WINDOWS/system32/ntshrui.dll
BartPE	15948-128-3 C:/WINDOWS/system32/ntmarta.dll
BartPE	15957-128-3 C:/WINDOWS/system32/ntdsapi.dll
BartPE	15960-128-3 C:/WINDOWS/system32/notepad.exe
BartPE	15970-128-3 C:/WINDOWS/system32/netshell.dll
BartPE	15976-128-3 C:/WINDOWS/system32/netplwiz.dll
BartPE	15983-128-3 C:/WINDOWS/system32/netcfgx.dll
BartPE	15985-128-3 C:/WINDOWS/system32/netapi32.dll
BartPE	15994-128-3 C:/WINDOWS/system32/ncobjapi.dll
BartPE	15996-128-3 C:/WINDOWS/system32/mydocs.dll
BartPE	15999-128-3 C:/WINDOWS/system32/mtxclu.dll

Live CD	File
BartPE	16008-128-3 C:/WINDOWS/system32/mswsock.dll
BartPE	16020-128-3 C:/WINDOWS/system32/msvcp60.dll
BartPE	16033-128-3 C:/WINDOWS/system32/mstask.dll
BartPE	16046-128-3 C:/WINDOWS/system32/mspatcha.dll
BartPE	16065-128-3 C:/WINDOWS/system32/msimg32.dll
BartPE	16069-128-3 C:/WINDOWS/system32/msieftp.dll
BartPE	16086-128-3 C:/WINDOWS/system32/msdtcuiu.dll
BartPE	16088-128-3 C:/WINDOWS/system32/msdtcprx.dll
BartPE	16109-128-3 C:/WINDOWS/system32/mprapi.dll
BartPE	16111-128-3 C:/WINDOWS/system32/mpr.dll
BartPE	16124-128-3 C:/WINDOWS/system32/mmsys.cpl
BartPE	16126-128-3 C:/WINDOWS/system32/mmcshext.dll
BartPE	16128-128-3 C:/WINDOWS/system32/mmcbase.dll
BartPE	16136-128-3 C:/WINDOWS/system32/mfc42u.dll
BartPE	16147-128-3 C:/WINDOWS/system32/lsass.exe
BartPE	16156-128-3 C:/WINDOWS/system32/loadperf.dll
BartPE	1616-128-3 C:/WINDOWS/system32/wbem/wmiprvse.exe
BartPE	16190-128-3 C:/WINDOWS/system32/iphlpapi.dll
BartPE	16202-128-3 C:/WINDOWS/system32/inetmib1.dll
BartPE	16218-128-3 C:/WINDOWS/system32/iedkcs32.dll
BartPE	16221-128-3 C:/WINDOWS/system32/ie4uinit.exe
BartPE	1622-128-3 C:/WINDOWS/system32/wbem/wmiprov.dll
BartPE	16235-128-3 C:/WINDOWS/system32/hnetcfg.dll
BartPE	1624-128-3 C:/WINDOWS/system32/perfnet.dll
BartPE	16251-128-3 C:/WINDOWS/system32/fontext.dll
BartPE	16263-128-3 C:/WINDOWS/system32/esent.dll
BartPE	1628-128-3 C:/WINDOWS/system32/perfts.dll
BartPE	16283-128-3 C:/WINDOWS/system32/dsuiext.dll
BartPE	16286-128-3 C:/WINDOWS/system32/dssec.dll
BartPE	16287-128-3 C:/WINDOWS/system32/dsquery.dll
BartPE	16315-128-3 C:/WINDOWS/system32/docprop2.dll
BartPE	16318-128-3 C:/WINDOWS/system32/dnsapi.dll
BartPE	16342-128-3 C:/WINDOWS/system32/dfsshlex.dll
BartPE	16369-128-3 C:/WINDOWS/system32/cscui.dll
BartPE	16372-128-3 C:/WINDOWS/system32/cscdll.dll
BartPE	16378-128-3 C:/WINDOWS/system32/cryptnet.dll
BartPE	16379-128-3 C:/WINDOWS/system32/cryptext.dll
BartPE	1668-128-3 C:/WINDOWS/system32/wbem/wmiapsrv.exe
BartPE	16758-128-3 C:/WINDOWS/system32/wups.dll
BartPE	16762-128-3 C:/WINDOWS/system32/wuaueng.dll
BartPE	16763-128-3 C:/WINDOWS/system32/wuaucpl.cpl
BartPE	16765-128-3 C:/WINDOWS/system32/wuauclt.exe
BartPE	16780-128-3 C:/WINDOWS/system32/winhttp.dll
BartPE	16783-128-3 C:/WINDOWS/system32/twext.dll
BartPE	1682-128-3 C:/WINDOWS/system32/wbem/wmiaprpl.dll
BartPE	1683-128-3 C:/WINDOWS/system32/wbem/wmiapres.dll

Live CD	File
BartPE	16842-128-3 C:/WINDOWS/system32/extmgr.dll
BartPE	16897-128-3 C:/WINDOWS/system32/drivers/mssmbios.sys
BartPE	16900-128-3 C:/WINDOWS/system32/drivers/intelppm.sys
BartPE	16901-128-3 C:/WINDOWS/system32/drivers/http.sys
BartPE	1691-128-3 C:/WINDOWS/system32/rasctrs.dll
BartPE	1696-128-3 C:/WINDOWS/system32/wbem/wbemsvc.dll
BartPE	1703-128-3 C:/WINDOWS/system32/wbem/wbemprox.dll
BartPE	1735-128-3 C:/WINDOWS/system32/wbem/wbemcomn.dll
BartPE	175-128-3 C:/WINDOWS/Fonts/vgaoem.fon
BartPE	1765-128-3 C:/WINDOWS/system32/rsvpperf.dll
BartPE	1813-128-3 C:/WINDOWS/system32/drivers/etc/services
BartPE	1816-128-3 C:/WINDOWS/system32/wbem/mofd.dll
BartPE	1832-128-3 C:/WINDOWS/system32/wbem/framedyn.dll
BartPE	1833-128-3 C:/WINDOWS/system32/wbem/fastprox.dll
BartPE	185-128-3 C:/WINDOWS/system32/cfgmgr32.dll
BartPE	1878-128-3 C:/WINDOWS/system32/wbem/cimwin32.dll
BartPE	1924-128-3 C:/WINDOWS/system32/tapiperf.dll
BartPE	193-128-3 C:/WINDOWS/system32/cdfview.dll
BartPE	1993-128-3 C:/WINDOWS/system32/utildll.dll
BartPE	2141-128-3 C:/WINDOWS/Media/Windows XP Ding.wav
BartPE	214-128-4 C:/WINDOWS/WindowsUpdate.log
BartPE	222-128-3 C:/WINDOWS/Fonts/dosapp.fon
BartPE	224-128-3 C:/WINDOWS/Fonts/ega40woa.fon
BartPE	225-128-3 C:/WINDOWS/Fonts/cga80woa.fon
BartPE	226-128-3 C:/WINDOWS/Fonts/cga40woa.fon
BartPE	230-144-5 C:/WINDOWS/Prefetch
BartPE	240-128-3 C:/WINDOWS/Fonts/sserife.fon
BartPE	256-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP
BartPE	257-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP
BartPE	2574-128-3 C:/Program Files/Outlook Express/wabfind.dll
BartPE	2576-128-3 C:/Program Files/Outlook Express/setup50.exe
BartPE	258-128-1 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING.VER
BartPE	2614-144-1 C:/Program Files/VMware
BartPE	26-144-2 C:/$Extend/$Reparse:$R
BartPE	2621-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf
BartPE	2622-128-4 C:/WINDOWS/Prefetch/NU2MENU.EXE-0BF39A50.pf
BartPE	2623-128-4 C:/WINDOWS/Prefetch/NC.EXE-13FCD38B.pf
BartPE	2625-128-3 C:/WINDOWS/system32/CatRoot2/tmp.edb
BartPE	2626-128-1 C:/WINDOWS/system32/wbem/Logs/wbemprox.log
BartPE	2628-128-4 C:/WINDOWS/Prefetch/PSINFO.EXE-2865B84E.pf
BartPE	2629-128-4 C:/WINDOWS/Prefetch/WMIAPSRV.EXE-1E2270A5.pf
BartPE	2630-144-1 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache
BartPE	2633-144-1 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache/MetaData
BartPE	2635-144-1 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache/Content
BartPE	2637-128-5 C:/Documents and Settings/test/Application

Live CD	File
	Data/Microsoft/CryptnetUrlCache/MetaData/3C83474D61E624A4F9844DF935AFE217
BartPE	2639-128-4 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache/Content/3C83474D61E624A4F9844DF935AFE217
BartPE	2640-128-4 C:/WINDOWS/Prefetch/AUTORUNSC.EXE-0B526252.pf
BartPE	2641-128-4 C:/WINDOWS/Prefetch/IPCONFIG.EXE-319C45AD.pf
BartPE	2651-128-4 C:/WINDOWS/Prefetch/TASKLIST.EXE-1EDF9DC5.pf
BartPE	2654-128-4 C:/WINDOWS/Prefetch/PSLIST.EXE-24B5729E.pf
BartPE	2664-128-4 C:/WINDOWS/Prefetch/PULIST.EXE-2C9B24D0.pf
BartPE	2665-128-4 C:/WINDOWS/Prefetch/PSTAT.EXE-03795CAD.pf
BartPE	2667-128-4 C:/WINDOWS/Prefetch/NET1.EXE-254DD783.pf
BartPE	2674-128-4 C:/WINDOWS/Prefetch/NET.EXE-1E6CB345.pf
BartPE	2681-128-4 C:/WINDOWS/Prefetch/NBTSTAT.EXE-322DB66D.pf
BartPE	2688-128-4 C:/WINDOWS/Prefetch/ATTRIB.EXE-3786FA3B.pf
BartPE	2716-128-3 C:/Program Files/NetMeeting/nmwb.dll
BartPE	272-128-3 C:/WINDOWS/system32/drivers/etc/hosts
BartPE	2733-128-3 C:/Program Files/NetMeeting/conf.exe
BartPE	2738-128-4 C:/WINDOWS/Prefetch/AT.EXE-30E857C6.pf
BartPE	2739-128-4 C:/WINDOWS/Prefetch/NETSTAT.EXE-26674FF9.pf
BartPE	2741-128-4 C:/WINDOWS/Prefetch/FPORT.EXE-047242F3.pf
BartPE	275-128-3 C:/WINDOWS/system32/CatRoot2/edb.log
BartPE	280-128-3 C:/WINDOWS/system32/CatRoot2/edb.chk
BartPE	2803-128-3 C:/WINDOWS/PCHealth/HelpCtr/Binaries/msinfo.dll
BartPE	2809-128-4 C:/WINDOWS/Prefetch/CMDLINE.EXE-13480A5C.pf
BartPE	282-128-3 C:/WINDOWS/system32/netmsg.dll
BartPE	289-128-4 C:/WINDOWS/Prefetch/WMIPRVSE.EXE-28F301A9.pf
BartPE	2950-128-3 C:/WINDOWS/system32/ntbackup.exe
BartPE	298-144-1 C:/WINDOWS/SoftwareDistribution/DataStore
BartPE	299-144-1 C:/WINDOWS/SoftwareDistribution/DataStore/Logs
BartPE	300-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log
BartPE	30-144-5 C:/WINDOWS/system32/config
BartPE	302-128-3 C:/WINDOWS/system32/stdole2.tlb
BartPE	307-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk
BartPE	308-128-4 C:/WINDOWS/SoftwareDistribution/DataStore/DataStore.edb
BartPE	31-144-6 C:/WINDOWS/system32/drivers
BartPE	313-128-3 C:/WINDOWS/system32/accwiz.exe
BartPE	314-128-3 C:/WINDOWS/system32/cabview.dll
BartPE	3170-128-3 C:/Program Files/VMware/VMware Tools/hook.dll
BartPE	317-128-3 C:/WINDOWS/system32/cabinet.dll
BartPE	321-128-3 C:/WINDOWS/system32/browseui.dll
BartPE	33-144-1 C:/WINDOWS/system32/ras
BartPE	3325-128-3 C:/WINDOWS/repair/setup.log
BartPE	3326-144-5 C:/Documents and Settings/test
BartPE	3339-128-10 C:/boot.ini
BartPE	3345-144-6 C:/Documents and Settings
BartPE	3347-144-6 C:/Documents and Settings/All Users
BartPE	3421-144-5 C:/WINDOWS/system32/CatRoot2

Live CD	File
BartPE	342-128-3 C:/WINDOWS/system32/perfc009.dat
BartPE	3422-144-1 C:/WINDOWS/system32/CatRoot2/{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
BartPE	3429-128-3 C:/WINDOWS/system32/CatRoot2/{127D0A1D-4EF2-11D1-8608-00C04FC295EE}/catdb
BartPE	3430-128-1 C:/WINDOWS/system32/CatRoot/{127D0A1D-4EF2-11D1-8608-00C04FC295EE}/TimeStamp
BartPE	3431-128-1 C:/WINDOWS/system32/CatRoot2/{127D0A1D-4EF2-11D1-8608-00C04FC295EE}/TimeStamp
BartPE	343-128-3 C:/WINDOWS/system32/perfh009.dat
BartPE	3433-144-1 C:/WINDOWS/system32/CatRoot2/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
BartPE	3437-128-3 C:/WINDOWS/system32/CatRoot2/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/catdb
BartPE	3438-128-4 C:/Program Files/VMware/VMware Tools/VMwareService.exe
BartPE	3441-128-4 C:/Program Files/VMware/VMware Tools/VMwareTray.exe
BartPE	344-128-3 C:/WINDOWS/system32/console.dll
BartPE	3442-128-4 C:/Program Files/VMware/VMware Tools/VMwareUser.exe
BartPE	3509-144-6 C:/Documents and Settings/All Users/Start Menu
BartPE	3510-128-1 C:/Documents and Settings/All Users/Start Menu/desktop.ini
BartPE	3511-144-5 C:/Documents and Settings/All Users/Start Menu/Programs
BartPE	3512-128-1 C:/Documents and Settings/All Users/Start Menu/Programs/desktop.ini
BartPE	3513-144-1 C:/Documents and Settings/All Users/Start Menu/Programs/Startup
BartPE	3514-128-1 C:/Documents and Settings/All Users/Start Menu/Programs/Startup/desktop.ini
BartPE	3787-144-6 C:/Program Files
BartPE	3788-144-6 C:/Program Files/Common Files
BartPE	398-128-3 C:/WINDOWS/system32/activeds.dll
BartPE	413-128-3 C:/WINDOWS/msagent/agentpsh.dll
BartPE	43-144-1 C:/WINDOWS/system32/drivers/etc
BartPE	4491-144-1 C:/Documents and Settings/All Users/Application Data/Microsoft/Network/Connections/Pbk
BartPE	45-144-6 C:/WINDOWS/inf
BartPE	459-128-3 C:/WINDOWS/system32/atl.dll
BartPE	4912-128-3 C:/WINDOWS/system32/hticons.dll
BartPE	49-144-5 C:/WINDOWS/msagent
BartPE	5224-144-5 C:/WINDOWS/system32/wbem/Logs
BartPE	5224-144-5 C:/WINDOWS/system32/wbem/Logs
BartPE	5231-128-3 C:/WINDOWS/system32/wbem/Logs/wmiprov.log
BartPE	5234-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.DATA
BartPE	5235-128-3 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.BTR
BartPE	5250-144-5 C:/Program Files/Common Files/System
BartPE	5271-144-6 C:/Program Files/Common Files/System/Ole DB
BartPE	528-128-3 C:/WINDOWS/system32/appwiz.cpl
BartPE	5304-144-1 C:/Documents and Settings/test/Start Menu
BartPE	5306-144-6 C:/Program Files/Outlook Express
BartPE	533-128-3 C:/WINDOWS/system32/apphelp.dll
BartPE	5378-128-3 C:/Program Files/Movie Maker/wmmres.dll
BartPE	5451-128-3 C:/Program Files/Internet Explorer/Connection Wizard/icwres.dll
BartPE	546-128-3 C:/WINDOWS/system32/advpack.dll

Live CD	File
BartPE	574-128-3 C:/WINDOWS/system32/adsldpc.dll
BartPE	5846-128-3 C:/WINDOWS/system32/zipfldr.dll
BartPE	61-144-6 C:/WINDOWS/system32/wbem
BartPE	653-128-3 C:/WINDOWS/system32/deskadp.dll
BartPE	654-128-3 C:/WINDOWS/system32/deskmon.dll
BartPE	655-128-3 C:/WINDOWS/system32/deskperf.dll
BartPE	685-128-3 C:/WINDOWS/system32/diskcopy.dll
BartPE	711-128-3 C:/WINDOWS/system32/docprop.dll
BartPE	742-128-3 C:/WINDOWS/system32/dskquoui.dll
BartPE	860-128-3 C:/WINDOWS/explorer.exe
BartPE	895-128-3 C:/WINDOWS/inf/unregmp2.exe
BartPE	906-128-3 C:/WINDOWS/system32/icmui.dll
BartPE	9580-144-6 C:/System Volume Information
BartPE	9629-128-3 C:/WINDOWS/system32/clusapi.dll
BartPE	9636-144-5 C:/Documents and Settings/test/Start Menu/Programs
BartPE	9637-144-1 C:/Documents and Settings/test/Start Menu/Programs/Startup
BartPE	9646-144-6 C:/Documents and Settings/test/Local Settings
BartPE	9661-144-6 C:/Documents and Settings/test/Application Data/Microsoft
BartPE	9664-144-1 C:/Documents and Settings/test/Application Data/Microsoft/SystemCertificates/My/CTLs
BartPE	9665-144-1 C:/Documents and Settings/test/Application Data/Microsoft/SystemCertificates/My/CRLs
BartPE	9666-144-1 C:/Documents and Settings/test/Application Data/Microsoft/SystemCertificates/My/Certificates
BartPE	9681-128-3 C:/Documents and Settings/test/Start Menu/Programs/Startup/desktop.ini
BartPE	9683-128-3 C:/Documents and Settings/test/Start Menu/Programs/desktop.ini
BartPE	9697-128-3 C:/Documents and Settings/test/Start Menu/desktop.ini
BartPE	982-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP
FIRE	1076-128-4 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP
FIRE	1106-128-4 C:/WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf
FIRE	1329-128-3 C:/WINDOWS/Fonts/arialbd.ttf
FIRE	1383-128-3 C:/WINDOWS/system32/msls31.dll
FIRE	15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys
FIRE	15474-128-3 C:/WINDOWS/system32/drivers/fastfat.sys
FIRE	15496-128-3 C:/WINDOWS/system32/drivers/acpi.sys
FIRE	15498-128-3 C:/WINDOWS/system32/winspool.drv
FIRE	15503-128-3 C:/WINDOWS/system32/ulib.dll
FIRE	15517-128-3 C:/WINDOWS/system32/samlib.dll
FIRE	15520-128-3 C:/WINDOWS/system32/rasman.dll
FIRE	15523-128-3 C:/WINDOWS/system32/rasapi32.dll
FIRE	15525-128-3 C:/WINDOWS/system32/perfctrs.dll
FIRE	15533-128-3 C:/WINDOWS/system32/msv1_0.dll
FIRE	15545-128-3 C:/WINDOWS/system32/dhcpcsvc.dll
FIRE	15561-128-3 C:/WINDOWS/system32/wzcsvc.dll
FIRE	15563-128-3 C:/WINDOWS/system32/wzcsapi.dll
FIRE	15564-128-3 C:/WINDOWS/system32/wzcdlg.dll
FIRE	15565-128-3 C:/WINDOWS/system32/wtsapi32.dll

Live CD	File
FIRE	15568-128-3 C:/WINDOWS/system32/wsock32.dll
FIRE	15571-128-3 C:/WINDOWS/system32/wshtcpip.dll
FIRE	15579-128-3 C:/WINDOWS/system32/ws2help.dll
FIRE	15581-128-3 C:/WINDOWS/system32/ws2_32.dll
FIRE	15601-128-3 C:/WINDOWS/system32/wmi.dll
FIRE	15610-128-3 C:/WINDOWS/system32/wldap32.dll
FIRE	15615-128-3 C:/WINDOWS/system32/winsta.dll
FIRE	15616-128-3 C:/WINDOWS/system32/winsrv.dll
FIRE	15619-128-3 C:/WINDOWS/system32/winrnr.dll
FIRE	15627-128-3 C:/WINDOWS/system32/wininet.dll
FIRE	15669-128-3 C:/WINDOWS/system32/urlmon.dll
FIRE	15677-128-3 C:/WINDOWS/system32/upnp.dll
FIRE	15709-128-3 C:/WINDOWS/system32/tapi32.dll
FIRE	15754-128-3 C:/WINDOWS/system32/snmpapi.dll
FIRE	15777-128-3 C:/WINDOWS/system32/shfolder.dll
FIRE	15780-128-3 C:/WINDOWS/system32/shdocvw.dll
FIRE	15781-128-3 C:/WINDOWS/system32/shdoclc.dll
FIRE	15784-128-3 C:/WINDOWS/system32/sfc_os.dll
FIRE	15786-128-3 C:/WINDOWS/system32/sfc.dll
FIRE	15798-128-3 C:/WINDOWS/system32/secur32.dll
FIRE	1580-128-3 C:/WINDOWS/system32/wbem/wmiutils.dll
FIRE	15821-128-3 C:/WINDOWS/system32/rtutils.dll
FIRE	15833-128-3 C:/WINDOWS/system32/riched20.dll
FIRE	15835-128-3 C:/WINDOWS/system32/resutils.dll
FIRE	15866-128-3 C:/WINDOWS/system32/rasadhlp.dll
FIRE	15869-128-3 C:/WINDOWS/system32/query.dll
FIRE	15884-128-3 C:/WINDOWS/system32/psapi.dll
FIRE	15901-128-3 C:/WINDOWS/system32/perfproc.dll
FIRE	15902-128-3 C:/WINDOWS/system32/perfos.dll
FIRE	15904-128-3 C:/WINDOWS/system32/perfdisk.dll
FIRE	15948-128-3 C:/WINDOWS/system32/ntmarta.dll
FIRE	15957-128-3 C:/WINDOWS/system32/ntdsapi.dll
FIRE	15970-128-3 C:/WINDOWS/system32/netshell.dll
FIRE	15974-128-3 C:/WINDOWS/system32/netrap.dll
FIRE	15977-128-3 C:/WINDOWS/system32/netman.dll
FIRE	15983-128-3 C:/WINDOWS/system32/netcfgx.dll
FIRE	15985-128-3 C:/WINDOWS/system32/netapi32.dll
FIRE	15987-128-3 C:/WINDOWS/system32/net1.exe
FIRE	15994-128-3 C:/WINDOWS/system32/ncobjapi.dll
FIRE	15999-128-3 C:/WINDOWS/system32/mtxclu.dll
FIRE	16008-128-3 C:/WINDOWS/system32/mswsock.dll
FIRE	16020-128-3 C:/WINDOWS/system32/msvcp60.dll
FIRE	16024-128-3 C:/WINDOWS/system32/msvbvm60.dll
FIRE	16046-128-3 C:/WINDOWS/system32/mspatcha.dll
FIRE	16065-128-3 C:/WINDOWS/system32/msimg32.dll
FIRE	16077-128-3 C:/WINDOWS/system32/mshtml.dll

Live CD	File
FIRE	16086-128-3 C:/WINDOWS/system32/msdtcuiu.dll
FIRE	16088-128-3 C:/WINDOWS/system32/msdtcprx.dll
FIRE	16109-128-3 C:/WINDOWS/system32/mprapi.dll
FIRE	16111-128-3 C:/WINDOWS/system32/mpr.dll
FIRE	16130-128-3 C:/WINDOWS/system32/mlang.dll
FIRE	16136-128-3 C:/WINDOWS/system32/mfc42u.dll
FIRE	16156-128-3 C:/WINDOWS/system32/loadperf.dll
FIRE	16160-128-3 C:/WINDOWS/system32/licwmi.dll
FIRE	1616-128-3 C:/WINDOWS/system32/wbem/wmiprvse.exe
FIRE	16162-128-3 C:/WINDOWS/system32/licdll.dll
FIRE	16190-128-3 C:/WINDOWS/system32/iphlpapi.dll
FIRE	16202-128-3 C:/WINDOWS/system32/inetmib1.dll
FIRE	1622-128-3 C:/WINDOWS/system32/wbem/wmiprov.dll
FIRE	16235-128-3 C:/WINDOWS/system32/hnetcfg.dll
FIRE	1624-128-3 C:/WINDOWS/system32/perfnet.dll
FIRE	16263-128-3 C:/WINDOWS/system32/esent.dll
FIRE	1628-128-3 C:/WINDOWS/system32/perfts.dll
FIRE	16318-128-3 C:/WINDOWS/system32/dnsapi.dll
FIRE	16357-128-3 C:/WINDOWS/system32/dbghelp.dll
FIRE	16385-128-3 C:/WINDOWS/system32/credui.dll
FIRE	1668-128-3 C:/WINDOWS/system32/wbem/wmiapsrv.exe
FIRE	16758-128-3 C:/WINDOWS/system32/wups.dll
FIRE	16762-128-3 C:/WINDOWS/system32/wuaueng.dll
FIRE	16763-128-3 C:/WINDOWS/system32/wuaucpl.cpl
FIRE	16765-128-3 C:/WINDOWS/system32/wuauclt.exe
FIRE	16780-128-3 C:/WINDOWS/system32/winhttp.dll
FIRE	1682-128-3 C:/WINDOWS/system32/wbem/wmiaprpl.dll
FIRE	1683-128-3 C:/WINDOWS/system32/wbem/wmiapres.dll
FIRE	16897-128-3 C:/WINDOWS/system32/drivers/mssmbios.sys
FIRE	16900-128-3 C:/WINDOWS/system32/drivers/intelppm.sys
FIRE	16901-128-3 C:/WINDOWS/system32/drivers/http.sys
FIRE	1691-128-3 C:/WINDOWS/system32/rasctrs.dll
FIRE	1696-128-3 C:/WINDOWS/system32/wbem/wbemsvc.dll
FIRE	1703-128-3 C:/WINDOWS/system32/wbem/wbemprox.dll
FIRE	17128-128-3 C:/WINDOWS/system32/dpcdll.dll
FIRE	1735-128-3 C:/WINDOWS/system32/wbem/wbemcomn.dll
FIRE	175-128-3 C:/WINDOWS/Fonts/vgaoem.fon
FIRE	1765-128-3 C:/WINDOWS/system32/rsvpperf.dll
FIRE	1813-128-3 C:/WINDOWS/system32/drivers/etc/services
FIRE	1816-128-3 C:/WINDOWS/system32/wbem/mofd.dll
FIRE	1832-128-3 C:/WINDOWS/system32/wbem/framedyn.dll
FIRE	1833-128-3 C:/WINDOWS/system32/wbem/fastprox.dll
FIRE	185-128-3 C:/WINDOWS/system32/cfgmgr32.dll
FIRE	1878-128-3 C:/WINDOWS/system32/wbem/cimwin32.dll
FIRE	1924-128-3 C:/WINDOWS/system32/tapiperf.dll
FIRE	1928-128-3 C:/WINDOWS/system32/tasklist.exe

Live CD	File
FIRE	1993-128-3 C:/WINDOWS/system32/utildll.dll
FIRE	214-128-4 C:/WINDOWS/WindowsUpdate.log
FIRE	222-128-3 C:/WINDOWS/Fonts/dosapp.fon
FIRE	224-128-3 C:/WINDOWS/Fonts/ega40woa.fon
FIRE	225-128-3 C:/WINDOWS/Fonts/cga80woa.fon
FIRE	226-128-3 C:/WINDOWS/Fonts/cga40woa.fon
FIRE	230-144-5 C:/WINDOWS/Prefetch
FIRE	240-128-3 C:/WINDOWS/Fonts/sserife.fon
FIRE	256-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP
FIRE	257-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP
FIRE	258-128-1 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING.VER
FIRE	2621-128-3 C:/Documents and Settings/test/Local Settings/Temp/~DF375.tmp
FIRE	2622-128-4 C:/WINDOWS/Prefetch/FIRE.EXE-28F7DF6F.pf
FIRE	2623-128-4 C:/WINDOWS/Prefetch/CMD.EXE-339B0F65.pf
FIRE	2625-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf
FIRE	2626-128-4 C:/WINDOWS/Prefetch/NC.EXE-27A8D0F4.pf
FIRE	2628-128-4 C:/WINDOWS/Prefetch/IPCONFIG.EXE-28418EC3.pf
FIRE	2629-128-4 C:/WINDOWS/Prefetch/PSINFO.EXE-21A4D93B.pf
FIRE	2630-128-4 C:/WINDOWS/Prefetch/WMIAPSRV.EXE-1E2270A5.pf
FIRE	2633-128-4 C:/WINDOWS/Prefetch/TASKLIST.EXE-10D94B23.pf
FIRE	2635-128-4 C:/WINDOWS/Prefetch/PSLIST.EXE-25551EEB.pf
FIRE	2637-128-4 C:/WINDOWS/Prefetch/NET1.EXE-029B9DB4.pf
FIRE	2639-128-4 C:/WINDOWS/Prefetch/NET.EXE-338CD3B1.pf
FIRE	2640-128-4 C:/WINDOWS/Prefetch/NBTSTAT.EXE-1CFCA700.pf
FIRE	2641-128-4 C:/WINDOWS/Prefetch/ATTRIB.EXE-39EAFB02.pf
FIRE	2651-128-4 C:/WINDOWS/Prefetch/AT.EXE-2770DD18.pf
FIRE	2654-128-4 C:/WINDOWS/Prefetch/NETSTAT.EXE-3B985F66.pf
FIRE	2664-128-4 C:/WINDOWS/Prefetch/FPORT.EXE-23BFDE24.pf
FIRE	272-128-3 C:/WINDOWS/system32/drivers/etc/hosts
FIRE	282-128-3 C:/WINDOWS/system32/netmsg.dll
FIRE	289-128-4 C:/WINDOWS/Prefetch/WMIPRVSE.EXE-28F301A9.pf
FIRE	292-128-3 C:/WINDOWS/system32/wpa.dbl
FIRE	298-144-1 C:/WINDOWS/SoftwareDistribution/DataStore
FIRE	299-144-1 C:/WINDOWS/SoftwareDistribution/DataStore/Logs
FIRE	300-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log
FIRE	30-144-5 C:/WINDOWS/system32/config
FIRE	307-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk
FIRE	308-128-4 C:/WINDOWS/SoftwareDistribution/DataStore/DataStore.edb
FIRE	31-144-6 C:/WINDOWS/system32/drivers
FIRE	3170-128-3 C:/Program Files/VMware/VMware Tools/hook.dll
FIRE	317-128-3 C:/WINDOWS/system32/cabinet.dll
FIRE	3325-128-3 C:/WINDOWS/repair/setup.log
FIRE	3326-144-5 C:/Documents and Settings/test
FIRE	3339-128-10 C:/boot.ini
FIRE	342-128-3 C:/WINDOWS/system32/perfc009.dat
FIRE	343-128-3 C:/WINDOWS/system32/perfh009.dat

Live CD	File
FIRE	3787-144-6 C:/Program Files
FIRE	398-128-3 C:/WINDOWS/system32/activeds.dll
FIRE	43-144-1 C:/WINDOWS/system32/drivers/etc
FIRE	459-128-3 C:/WINDOWS/system32/atl.dll
FIRE	466-128-3 C:/WINDOWS/system32/attrib.exe
FIRE	471-128-3 C:/WINDOWS/system32/at.exe
FIRE	477-128-3 C:/WINDOWS/system32/asycfilt.dll
FIRE	5224-144-5 C:/WINDOWS/system32/wbem/Logs
FIRE	5225-128-1 C:/WINDOWS/system32/wbem/Logs/FrameWork.log
FIRE	5231-128-3 C:/WINDOWS/system32/wbem/Logs/wmiprov.log
FIRE	5234-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.DATA
FIRE	5235-128-3 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.BTR
FIRE	5244-144-6 C:/Program Files/Internet Explorer
FIRE	533-128-3 C:/WINDOWS/system32/apphelp.dll
FIRE	546-128-3 C:/WINDOWS/system32/advpack.dll
FIRE	574-128-3 C:/WINDOWS/system32/adsldpc.dll
FIRE	61-144-6 C:/WINDOWS/system32/wbem
FIRE	9629-128-3 C:/WINDOWS/system32/clusapi.dll
FIRE	9647-144-1 C:/Documents and Settings/test/Local Settings/Temporary Internet Files
FIRE	9648-144-1 C:/Documents and Settings/test/Local Settings/Temporary Internet Files/Content.IE5
FIRE	9653-144-5 C:/Documents and Settings/test/Local Settings/Temp
FIRE	9654-144-1 C:/Documents and Settings/test/Local Settings/History
FIRE	9655-144-1 C:/Documents and Settings/test/Local Settings/History/History.IE5
FIRE	9659-144-1 C:/Documents and Settings/test/Cookies
FIRE	9706-128-4 C:/Documents and Settings/test/Local Settings/Temporary Internet Files/Content.IE5/index.dat
FIRE	9708-128-4 C:/Documents and Settings/test/Local Settings/History/History.IE5/index.dat
FIRE	9713-128-4 C:/Documents and Settings/test/Cookies/index.dat
FIRE	982-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP
Helix	1076-128-4 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP
Helix	1106-128-4 C:/WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf
Helix	1329-128-3 C:/WINDOWS/Fonts/arialbd.ttf
Helix	15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys
Helix	15496-128-3 C:/WINDOWS/system32/drivers/acpi.sys
Helix	15498-128-3 C:/WINDOWS/system32/winspool.drv
Helix	15503-128-3 C:/WINDOWS/system32/ulib.dll
Helix	15517-128-3 C:/WINDOWS/system32/samlib.dll
Helix	15520-128-3 C:/WINDOWS/system32/rasman.dll
Helix	15523-128-3 C:/WINDOWS/system32/rasapi32.dll
Helix	15525-128-3 C:/WINDOWS/system32/perfctrs.dll
Helix	15533-128-3 C:/WINDOWS/system32/msv1_0.dll
Helix	15545-128-3 C:/WINDOWS/system32/dhcpcsvc.dll
Helix	15561-128-3 C:/WINDOWS/system32/wzcsvc.dll
Helix	15563-128-3 C:/WINDOWS/system32/wzcsapi.dll
Helix	15564-128-3 C:/WINDOWS/system32/wzcdlg.dll

Live CD	File
Helix	15565-128-3 C:/WINDOWS/system32/wtsapi32.dll
Helix	15568-128-3 C:/WINDOWS/system32/wsock32.dll
Helix	15571-128-3 C:/WINDOWS/system32/wshtcpip.dll
Helix	15579-128-3 C:/WINDOWS/system32/ws2help.dll
Helix	15581-128-3 C:/WINDOWS/system32/ws2_32.dll
Helix	15601-128-3 C:/WINDOWS/system32/wmi.dll
Helix	15610-128-3 C:/WINDOWS/system32/wldap32.dll
Helix	15615-128-3 C:/WINDOWS/system32/winsta.dll
Helix	15616-128-3 C:/WINDOWS/system32/winsrv.dll
Helix	15619-128-3 C:/WINDOWS/system32/winrnr.dll
Helix	15627-128-3 C:/WINDOWS/system32/wininet.dll
Helix	15643-128-3 C:/WINDOWS/system32/wdmaud.drv
Helix	15669-128-3 C:/WINDOWS/system32/urlmon.dll
Helix	15677-128-3 C:/WINDOWS/system32/upnp.dll
Helix	15709-128-3 C:/WINDOWS/system32/tapi32.dll
Helix	15754-128-3 C:/WINDOWS/system32/snmpapi.dll
Helix	15777-128-3 C:/WINDOWS/system32/shfolder.dll
Helix	15784-128-3 C:/WINDOWS/system32/sfc_os.dll
Helix	15786-128-3 C:/WINDOWS/system32/sfc.dll
Helix	15798-128-3 C:/WINDOWS/system32/secur32.dll
Helix	1580-128-3 C:/WINDOWS/system32/wbem/wmiutils.dll
Helix	15821-128-3 C:/WINDOWS/system32/rtutils.dll
Helix	15835-128-3 C:/WINDOWS/system32/resutils.dll
Helix	15866-128-3 C:/WINDOWS/system32/rasadhlp.dll
Helix	15869-128-3 C:/WINDOWS/system32/query.dll
Helix	15884-128-3 C:/WINDOWS/system32/psapi.dll
Helix	15901-128-3 C:/WINDOWS/system32/perfproc.dll
Helix	15902-128-3 C:/WINDOWS/system32/perfos.dll
Helix	15904-128-3 C:/WINDOWS/system32/perfdisk.dll
Helix	15911-128-3 C:/WINDOWS/system32/olepro32.dll
Helix	1593-128-3 C:/WINDOWS/system32/oledlg.dll
Helix	15948-128-3 C:/WINDOWS/system32/ntmarta.dll
Helix	15957-128-3 C:/WINDOWS/system32/ntdsapi.dll
Helix	15970-128-3 C:/WINDOWS/system32/netshell.dll
Helix	15974-128-3 C:/WINDOWS/system32/netrap.dll
Helix	15977-128-3 C:/WINDOWS/system32/netman.dll
Helix	15983-128-3 C:/WINDOWS/system32/netcfgx.dll
Helix	15985-128-3 C:/WINDOWS/system32/netapi32.dll
Helix	15987-128-3 C:/WINDOWS/system32/net1.exe
Helix	15994-128-3 C:/WINDOWS/system32/ncobjapi.dll
Helix	15999-128-3 C:/WINDOWS/system32/mtxclu.dll
Helix	16008-128-3 C:/WINDOWS/system32/mswsock.dll
Helix	16020-128-3 C:/WINDOWS/system32/msvcp60.dll
Helix	16046-128-3 C:/WINDOWS/system32/mspatcha.dll
Helix	16065-128-3 C:/WINDOWS/system32/msimg32.dll
Helix	16086-128-3 C:/WINDOWS/system32/msdtcuiu.dll

Live CD	File
Helix	16088-128-3 C:/WINDOWS/system32/msdtcprx.dll
Helix	16109-128-3 C:/WINDOWS/system32/mprapi.dll
Helix	16132-128-3 C:/WINDOWS/system32/midimap.dll
Helix	16136-128-3 C:/WINDOWS/system32/mfc42u.dll
Helix	16156-128-3 C:/WINDOWS/system32/loadperf.dll
Helix	1616-128-3 C:/WINDOWS/system32/wbem/wmiprvse.exe
Helix	16190-128-3 C:/WINDOWS/system32/iphlpapi.dll
Helix	16202-128-3 C:/WINDOWS/system32/inetmib1.dll
Helix	1622-128-3 C:/WINDOWS/system32/wbem/wmiprov.dll
Helix	16235-128-3 C:/WINDOWS/system32/hnetcfg.dll
Helix	1624-128-3 C:/WINDOWS/system32/perfnet.dll
Helix	16263-128-3 C:/WINDOWS/system32/esent.dll
Helix	1628-128-3 C:/WINDOWS/system32/perfts.dll
Helix	16290-128-3 C:/WINDOWS/system32/dsound.dll
Helix	16318-128-3 C:/WINDOWS/system32/dnsapi.dll
Helix	16357-128-3 C:/WINDOWS/system32/dbghelp.dll
Helix	16385-128-3 C:/WINDOWS/system32/credui.dll
Helix	1668-128-3 C:/WINDOWS/system32/wbem/wmiapsrv.exe
Helix	16758-128-3 C:/WINDOWS/system32/wups.dll
Helix	16762-128-3 C:/WINDOWS/system32/wuaueng.dll
Helix	16763-128-3 C:/WINDOWS/system32/wuaucpl.cpl
Helix	16765-128-3 C:/WINDOWS/system32/wuauclt.exe
Helix	16780-128-3 C:/WINDOWS/system32/winhttp.dll
Helix	1682-128-3 C:/WINDOWS/system32/wbem/wmiaprpl.dll
Helix	1683-128-3 C:/WINDOWS/system32/wbem/wmiapres.dll
Helix	16897-128-3 C:/WINDOWS/system32/drivers/mssmbios.sys
Helix	16900-128-3 C:/WINDOWS/system32/drivers/intelppm.sys
Helix	16901-128-3 C:/WINDOWS/system32/drivers/http.sys
Helix	1691-128-3 C:/WINDOWS/system32/rasctrs.dll
Helix	1696-128-3 C:/WINDOWS/system32/wbem/wbemsvc.dll
Helix	1703-128-3 C:/WINDOWS/system32/wbem/wbemprox.dll
Helix	1735-128-3 C:/WINDOWS/system32/wbem/wbemcomn.dll
Helix	175-128-3 C:/WINDOWS/Fonts/vgaoem.fon
Helix	1765-128-3 C:/WINDOWS/system32/rsvpperf.dll
Helix	1813-128-3 C:/WINDOWS/system32/drivers/etc/services
Helix	1816-128-3 C:/WINDOWS/system32/wbem/mofd.dll
Helix	1833-128-3 C:/WINDOWS/system32/wbem/fastprox.dll
Helix	1924-128-3 C:/WINDOWS/system32/tapiperf.dll
Helix	1993-128-3 C:/WINDOWS/system32/utildll.dll
Helix	2141-128-3 C:/WINDOWS/Media/Windows XP Ding.wav
Helix	214-128-4 C:/WINDOWS/WindowsUpdate.log
Helix	222-128-3 C:/WINDOWS/Fonts/dosapp.fon
Helix	224-128-3 C:/WINDOWS/Fonts/ega40woa.fon
Helix	225-128-3 C:/WINDOWS/Fonts/cga80woa.fon
Helix	226-128-3 C:/WINDOWS/Fonts/cga40woa.fon
Helix	230-144-5 C:/WINDOWS/Prefetch

Live CD	File
Helix	240-128-3 C:/WINDOWS/Fonts/sserife.fon
Helix	256-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP
Helix	257-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP
Helix	258-128-1 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING.VER
Helix	2621-144-1 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1
Helix	2622-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/Arial_1.TFT
Helix	2623-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/Arial_1.FON
Helix	2625-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/Denmark.TFT
Helix	2626-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/Denmark.FON
Helix	2628-128-4 C:/WINDOWS/Prefetch/HELIX.EXE-2AC0706C.pf
Helix	2629-128-4 C:/WINDOWS/Prefetch/LS.EXE-0EACACF4.pf
Helix	2630-128-4 C:/WINDOWS/Prefetch/CMD.EXE-31FFA378.pf
Helix	2633-128-4 C:/WINDOWS/Prefetch/MORE.EXE-1CE4AB20.pf
Helix	2635-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf
Helix	2637-128-4 C:/WINDOWS/Prefetch/NC.EXE-22B21017.pf
Helix	2639-128-1 C:/WINDOWS/system32/wbem/Logs/wbemprox.log
Helix	2640-128-4 C:/WINDOWS/Prefetch/PSINFO.EXE-3ADEAEEF.pf
Helix	2641-128-4 C:/WINDOWS/Prefetch/WMIAPSRV.EXE-1E2270A5.pf
Helix	2651-128-4 C:/WINDOWS/Prefetch/IPCONFIG.EXE-2A403659.pf
Helix	2654-128-4 C:/WINDOWS/Prefetch/PSLIST.EXE-372E693F.pf
Helix	2664-128-4 C:/WINDOWS/Prefetch/NET1.EXE-029B9DB4.pf
Helix	2665-128-4 C:/WINDOWS/Prefetch/NET.EXE-02C522BD.pf
Helix	2667-128-4 C:/WINDOWS/Prefetch/NBTSTAT.EXE-1F49A3E4.pf
Helix	2674-128-4 C:/WINDOWS/Prefetch/ATTRIB.EXE-2DD00289.pf
Helix	2681-128-4 C:/WINDOWS/Prefetch/AT.EXE-0432F398.pf
Helix	2688-128-4 C:/WINDOWS/Prefetch/NETSTAT.EXE-10EBC1A8.pf
Helix	272-128-3 C:/WINDOWS/system32/drivers/etc/hosts
Helix	2738-128-4 C:/WINDOWS/Prefetch/FPORT.EXE-287E45A5.pf
Helix	2739-128-4 C:/WINDOWS/Prefetch/CMDLINE.EXE-1D2AD11F.pf
Helix	277-128-3 C:/WINDOWS/system32/msacm32.drv
Helix	282-128-3 C:/WINDOWS/system32/netmsg.dll
Helix	289-128-4 C:/WINDOWS/Prefetch/WMIPRVSE.EXE-28F301A9.pf
Helix	2935-128-3 C:/WINDOWS/system32/ksuser.dll
Helix	298-144-1 C:/WINDOWS/SoftwareDistribution/DataStore
Helix	299-144-1 C:/WINDOWS/SoftwareDistribution/DataStore/Logs
Helix	300-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log
Helix	30-144-5 C:/WINDOWS/system32/config
Helix	307-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk
Helix	308-128-4 C:/WINDOWS/SoftwareDistribution/DataStore/DataStore.edb
Helix	31-144-6 C:/WINDOWS/system32/drivers
Helix	3170-128-3 C:/Program Files/VMware/VMware Tools/hook.dll
Helix	317-128-3 C:/WINDOWS/system32/cabinet.dll
Helix	33-144-1 C:/WINDOWS/system32/ras
Helix	3326-144-5 C:/Documents and Settings/test

Live CD	File
Helix	3345-144-6 C:/Documents and Settings
Helix	3347-144-6 C:/Documents and Settings/All Users
Helix	342-128-3 C:/WINDOWS/system32/perfc009.dat
Helix	343-128-3 C:/WINDOWS/system32/perfh009.dat
Helix	380-128-3 C:/WINDOWS/Fonts/verdanab.ttf
Helix	398-128-3 C:/WINDOWS/system32/activeds.dll
Helix	43-144-1 C:/WINDOWS/system32/drivers/etc
Helix	4466-128-3 C:/WINDOWS/system32/drivers/es1371mp.sys
Helix	4491-144-1 C:/Documents and Settings/All Users/Application Data/Microsoft/Network/Connections/Pbk
Helix	459-128-3 C:/WINDOWS/system32/atl.dll
Helix	463-128-3 C:/WINDOWS/system32/atmfd.dll
Helix	5224-144-5 C:/WINDOWS/system32/wbem/Logs
Helix	5224-144-5 C:/WINDOWS/system32/wbem/Logs
Helix	5231-128-3 C:/WINDOWS/system32/wbem/Logs/wmiprov.log
Helix	5234-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.DATA
Helix	5235-128-3 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.BTR
Helix	533-128-3 C:/WINDOWS/system32/apphelp.dll
Helix	546-128-3 C:/WINDOWS/system32/advpack.dll
Helix	574-128-3 C:/WINDOWS/system32/adsldpc.dll
Helix	61-144-6 C:/WINDOWS/system32/wbem
Helix	9629-128-3 C:/WINDOWS/system32/clusapi.dll
Helix	9653-144-5 C:/Documents and Settings/test/Local Settings/Temp
Helix	982-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP
INSERT	1298-128-3 C:/WINDOWS/Fonts/times.ttf
INSERT	1383-128-3 C:/WINDOWS/system32/msls31.dll
INSERT	15616-128-3 C:/WINDOWS/system32/winsrv.dll
INSERT	15627-128-3 C:/WINDOWS/system32/wininet.dll
INSERT	15669-128-3 C:/WINDOWS/system32/urlmon.dll
INSERT	15671-128-3 C:/WINDOWS/system32/url.dll
INSERT	15717-128-3 C:/WINDOWS/system32/sxs.dll
INSERT	15780-128-3 C:/WINDOWS/system32/shdocvw.dll
INSERT	15781-128-3 C:/WINDOWS/system32/shdoclc.dll
INSERT	15798-128-3 C:/WINDOWS/system32/secur32.dll
INSERT	15833-128-3 C:/WINDOWS/system32/riched20.dll
INSERT	16063-128-3 C:/WINDOWS/system32/msimtf.dll
INSERT	16073-128-3 C:/WINDOWS/system32/msi.dll
INSERT	16077-128-3 C:/WINDOWS/system32/mshtml.dll
INSERT	16077-128-3 C:/WINDOWS/system32/mshtml.dll
INSERT	16095-128-3 C:/WINDOWS/system32/msctf.dll
INSERT	16130-128-3 C:/WINDOWS/system32/mlang.dll
INSERT	16206-128-3 C:/WINDOWS/system32/imm32.dll
INSERT	16369-128-3 C:/WINDOWS/system32/cscui.dll
INSERT	16372-128-3 C:/WINDOWS/system32/cscdll.dll
INSERT	17131-128-3 C:/Program Files/Messenger/msmsgs.exe
INSERT	175-128-3 C:/WINDOWS/Fonts/vgaoem.fon
INSERT	222-128-3 C:/WINDOWS/Fonts/dosapp.fon

Live CD	File
INSERT	224-128-3 C:/WINDOWS/Fonts/ega40woa.fon
INSERT	225-128-3 C:/WINDOWS/Fonts/cga80woa.fon
INSERT	226-128-3 C:/WINDOWS/Fonts/cga40woa.fon
INSERT	230-144-5 C:/WINDOWS/Prefetch
INSERT	2621-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf
INSERT	2622-144-1 C:/Documents and Settings/test/Local Settings/History/History.IE5/MSHist012006111220061113
INSERT	2623-128-3 C:/Documents and Settings/test/Local Settings/History/History.IE5/MSHist012006111220061113/index.dat
INSERT	2625-128-4 C:/WINDOWS/Prefetch/IEXPLORE.EXE-27122324.pf
INSERT	270-128-1 C:/Documents and Settings/test/Local Settings/Temporary Internet Files/desktop.ini
INSERT	2794-128-3 C:/Program Files/Internet Explorer/iexplore.exe
INSERT	2794-128-3 C:/Program Files/Internet Explorer/iexplore.exe
INSERT	281-128-1 C:/Documents and Settings/test/Local Settings/History/desktop.ini
INSERT	302-128-3 C:/WINDOWS/system32/stdole2.tlb
INSERT	3170-128-3 C:/Program Files/VMware/VMware Tools/hook.dll
INSERT	321-128-3 C:/WINDOWS/system32/browseui.dll
INSERT	325-128-3 C:/WINDOWS/system32/browselc.dll
INSERT	3326-144-5 C:/Documents and Settings/test
INSERT	3345-144-6 C:/Documents and Settings
INSERT	3347-144-6 C:/Documents and Settings/All Users
INSERT	3519-128-1 C:/Documents and Settings/All Users/Documents/desktop.ini
INSERT	3787-144-6 C:/Program Files
INSERT	5244-144-6 C:/Program Files/Internet Explorer
INSERT	533-128-3 C:/WINDOWS/system32/apphelp.dll
INSERT	854-128-3 C:/WINDOWS/notepad.exe
INSERT	860-128-3 C:/WINDOWS/explorer.exe
INSERT	9646-144-6 C:/Documents and Settings/test/Local Settings
INSERT	9647-144-1 C:/Documents and Settings/test/Local Settings/Temporary Internet Files
INSERT	9648-144-1 C:/Documents and Settings/test/Local Settings/Temporary Internet Files/Content.IE5
INSERT	9654-144-1 C:/Documents and Settings/test/Local Settings/History
INSERT	9655-144-1 C:/Documents and Settings/test/Local Settings/History/History.IE5
INSERT	9657-144-6 C:/Documents and Settings/test/Favorites
INSERT	9659-144-1 C:/Documents and Settings/test/Cookies
INSERT	9706-128-4 C:/Documents and Settings/test/Local Settings/Temporary Internet Files/Content.IE5/index.dat
INSERT	9708-128-4 C:/Documents and Settings/test/Local Settings/History/History.IE5/index.dat
INSERT	9711-144-5 C:/Documents and Settings/test/Favorites/Links
INSERT	9713-128-4 C:/Documents and Settings/test/Cookies/index.dat
INSERT	9727-128-1 C:/Documents and Settings/test/My Documents/desktop.ini
INSERT	9772-128-1 C:/Documents and Settings/test/Favorites/Desktop.ini
INSERT	9796-144-1 C:/Documents and Settings/test/Local Settings/Application Data/Microsoft/CD Burning
INSERT	9832 <INSERT_WXP_data.img-MSHist012005022320050224-dead-9832>
Operator	15635-128-3 C:/WINDOWS/system32/wiaacmgr.exe

Live CD	File
Operator	15774-128-3 C:/WINDOWS/system32/shimgvw.dll
Operator	15884-128-3 C:/WINDOWS/system32/psapi.dll
Operator	2621 <Operator_WXP_data.img-2cg8crtk.TMP-dead-2621>
Operator	325-128-3 C:/WINDOWS/system32/browselc.dll
Operator	325-128-3 C:/WINDOWS/system32/SET483.tmp (deleted-realloc)

9. Appendix C Common Files Modified by the Live CDs on the RedHat 9 Linux Virtual Machine

```
/2/bin/bash
/2/bin/cut
/2/bin/egrep
/2/bin/grep
/2/bin/mount
/2/bin/sh -> bash
/2/bin/stty
/2/dev/cdrom -> /dev/scd0
/2/etc/.nsswitch.conf.swx (deleted-
   realloc)
/2/etc/bashrc
/2/etc/DIR_COLORS.xterm
/2/etc/fonts/fonts.conf
/2/etc/fstab
/2/etc/fstab.NEW (deleted-realloc)
/2/etc/gnome-vfs-2.0/modules
/2/etc/gnome-vfs-2.0/modules/default-
   modules.conf
/2/etc/gnome-vfs-2.0/modules/extra-
   modules.conf
/2/etc/gnome-vfs-2.0/modules/font-
   method.conf
/2/etc/gnome-vfs-2.0/modules/help-
   methods.conf
/2/etc/gnome-vfs-2.0/modules/mapping-
   modules.conf
/2/etc/gnome-vfs-2.0/modules/mapping-
   modules.conf;40012009 (deleted-
   realloc)
/2/etc/gnome-vfs-2.0/modules/ssl-
   modules.conf
/2/etc/group
/2/etc/gtk-2.0/gdk-pixbuf.loaders
/2/etc/gtk-2.0/gtk.immodules
/2/etc/gtk-2.0/gtkrc
/2/etc/gtk-2.0/gtkrc;40012009 (deleted-
   realloc)
/2/etc/host.conf
/2/etc/hosts
/2/etc/inputrc
/2/etc/ld.so.cache
/2/etc/modules.conf
/2/etc/mtab
/2/etc/mtab~ (deleted-realloc)
/2/etc/nsswitch.conf
/2/etc/pango/pango.modules
/2/etc/passwd
/2/etc/profile.d
/2/etc/profile.d/atrpms.sh
/2/etc/profile.d/colorls.sh
/2/etc/profile.d/colorls.sh;43cc0503
   (deleted-realloc)
/2/etc/profile.d/glib2.sh
/2/etc/profile.d/gnome-ssh-askpass.sh
/2/etc/profile.d/gnome-ssh-
   askpass.sh;43cc0503 (deleted-
   realloc)
/2/etc/profile.d/lang.sh
/2/etc/profile.d/less.sh
/2/etc/profile.d/vim.sh
/2/etc/profile.d/which-2.sh
/2/etc/resolv.conf
/2/etc/sysconfig/i18n
/2/etc/termcap
/2/lib/ld-2.3.2.so
/2/lib/ld-linux.so.2 -> ld-2.3.2.so
/2/lib/libcrypt.so.1 -> libcrypt-
   2.3.2.so
/2/lib/libcrypt-2.3.2.so
/2/lib/libcrypto.so.0.9.7a
/2/lib/libcrypto.so.4 ->
   libcrypto.so.0.9.7a
/2/lib/libdl.so.2 -> libdl-2.3.2.so
/2/lib/libdl-2.3.2.so
/2/lib/libnsl.so.1 -> libnsl-2.3.2.so
/2/lib/libnsl-2.3.2.so
/2/lib/libnss_files.so.2 ->
   libnss_files-2.3.2.so
/2/lib/libnss_files-2.3.2.so
/2/lib/libresolv.so.2 -> libresolv-
   2.3.2.so
/2/lib/libresolv-2.3.2.so
/2/lib/libssl.so.0.9.7a
/2/lib/libssl.so.4 -> libssl.so.0.9.7a
/2/lib/libtermcap.so.2 ->
   libtermcap.so.2.0.8
/2/lib/libtermcap.so.2.0.8
/2/lib/libutil.so.1 -> libutil-2.3.2.so
/2/lib/libutil-2.3.2.so
/2/lib/modules/2.4.20-
   31.9/kernel/fs/udf/udf.o
/2/lib/modules/2.4.20-
   31.9/kernel/fs/udf/udf.o;43cc0503
   (deleted-realloc)
/2/lib/modules/2.4.20-31.9/modules.dep
/2/lib/tls/libc.so.6 -> libc-2.3.2.so
/2/lib/tls/libc-2.3.2.so
/2/lib/tls/libm.so.6 -> libm-2.3.2.so
/2/lib/tls/libm-2.3.2.so
/2/lib/tls/libpthread.so.0 ->
   libpthread-0.34.so
/2/lib/tls/libpthread-0.34.so
/2/lib/tls/librt.so.1 -> librt-2.3.2.so
/2/lib/tls/librt-2.3.2.so
/2/root
/2/root/.bash_history
/2/root/.bashrc
/2/root/.fonts.cache-1
/2/root/.fonts.cache-1.LCK (deleted)
/2/root/.fonts.cache-1.NEW (deleted-
   realloc)
/2/root/.gconfd/lock/0t1159698850ut6013
   86u0p1937r240480261k3221215772
   (deleted-realloc)
```

```
/2/root/.gconfd/lock/ior
/2/root/.gconfd/saved_state
/2/root/.gconfd/saved_state.tmp
   (deleted-realloc)
/2/root/.gnome2_private
/2/root/.ICEauthority
/2/root/.Xauthority
/2/sbin/consoletype
/2/sbin/insmod
/2/sbin/modprobe -> insmod
/2/tmp
/2/tmp/.ICE-unix/1864
/2/tmp/.X11-unix/X0
/2/tmp/orbit-root
/2/tmp/orbit-root/bonobo-activation-
   server-ior
/2/tmp/orbit-root/linc-791-0-
   5ac978b7ee03
/2/tmp/orbit-root/linc-793-0-
   474550d04dfa3
/2/usr/bin/dircolors
/2/usr/bin/gnome-terminal
/2/usr/bin/id
/2/usr/bin/perl
/2/usr/bin/perl5.8.0
/2/usr/bin/tput
/2/usr/bin/wc
/2/usr/kerberos/lib/libcom_err.so.3 ->
   libcom_err.so.3.0
/2/usr/kerberos/lib/libcom_err.so.3.0
/2/usr/kerberos/lib/libgssapi_krb5.so.2
   -> libgssapi_krb5.so.2.2
/2/usr/kerberos/lib/libgssapi_krb5.so.2
   .2
/2/usr/kerberos/lib/libgssapi_krb5.so.2
   .2;43cc0503 (deleted-realloc)
/2/usr/kerberos/lib/libk5crypto.so.3 ->
   libk5crypto.so.3.0
/2/usr/kerberos/lib/libk5crypto.so.3.0
/2/usr/kerberos/lib/libkrb5.so.3 ->
   libkrb5.so.3.1
/2/usr/kerberos/lib/libkrb5.so.3.1
/2/usr/lib/gconv/ARMSCII-8.so
/2/usr/lib/gconv/BIG5.so
/2/usr/lib/gconv/BIG5HKSCS.so
/2/usr/lib/gconv/CP1250.so
/2/usr/lib/gconv/CP1251.so
/2/usr/lib/gconv/CP1252.so
/2/usr/lib/gconv/CP1253.so
/2/usr/lib/gconv/CP1254.so
/2/usr/lib/gconv/CP1255.so
/2/usr/lib/gconv/CP1256.so
/2/usr/lib/gconv/CP1257.so
/2/usr/lib/gconv/CP1258.so
/2/usr/lib/gconv/ECMA-CYRILLIC.so
/2/usr/lib/gconv/EUC-CN.so
/2/usr/lib/gconv/EUC-JP.so
/2/usr/lib/gconv/EUC-KR.so
/2/usr/lib/gconv/EUC-TW.so
/2/usr/lib/gconv/GB18030.so
/2/usr/lib/gconv/GBK.so
/2/usr/lib/gconv/gconv-modules.cache
/2/usr/lib/gconv/gconv-
   modules.cache.IxlGsm (deleted-
   realloc)
/2/usr/lib/gconv/GEORGIAN-ACADEMY.so
/2/usr/lib/gconv/IBM850.so
/2/usr/lib/gconv/IBM852.so
/2/usr/lib/gconv/IBM855.so
/2/usr/lib/gconv/IBM857.so
/2/usr/lib/gconv/IBM862.so
/2/usr/lib/gconv/IBM864.so
/2/usr/lib/gconv/IBM866.so
/2/usr/lib/gconv/ISO-2022-JP.so
/2/usr/lib/gconv/ISO-2022-KR.so
/2/usr/lib/gconv/ISO8859-1.so
/2/usr/lib/gconv/ISO8859-10.so
/2/usr/lib/gconv/ISO8859-13.so
/2/usr/lib/gconv/ISO8859-14.so
/2/usr/lib/gconv/ISO8859-15.so
/2/usr/lib/gconv/ISO8859-16.so
/2/usr/lib/gconv/ISO8859-2.so
/2/usr/lib/gconv/ISO8859-3.so
/2/usr/lib/gconv/ISO8859-4.so
/2/usr/lib/gconv/ISO8859-5.so
/2/usr/lib/gconv/ISO8859-6.so
/2/usr/lib/gconv/ISO8859-7.so
/2/usr/lib/gconv/ISO8859-8.so
/2/usr/lib/gconv/ISO8859-9.so
/2/usr/lib/gconv/JOHAB.so
/2/usr/lib/gconv/KOI8-R.so
/2/usr/lib/gconv/KOI8-U.so
/2/usr/lib/gconv/libCNS.so
/2/usr/lib/gconv/libGB.so
/2/usr/lib/gconv/libJIS.so
/2/usr/lib/gconv/libKSC.so
/2/usr/lib/gconv/MAC-UK.so
/2/usr/lib/gconv/SJIS.so
/2/usr/lib/gconv/TCVN5712-1.so
/2/usr/lib/gconv/TIS-620.so
/2/usr/lib/gconv/UHC.so
/2/usr/lib/gconv/UTF-16.so
/2/usr/lib/gconv/UTF-7.so
/2/usr/lib/gconv/VISCII.so
/2/usr/lib/gtk-
   2.0/2.2.0/engines/libbluecurve.so
/2/usr/lib/gtk-
   2.0/2.2.0/loaders/libpixbufloader-
   png.so
/2/usr/lib/libart_lgpl_2.so.2 ->
   libart_lgpl_2.so.2.3.11
/2/usr/lib/libart_lgpl_2.so.2.3.11
/2/usr/lib/libatk-1.0.so.0 -> libatk-
   1.0.so.0.200.0
/2/usr/lib/libatk-1.0.so.0.200.0
/2/usr/lib/libaudiofile.so.0 ->
   libaudiofile.so.0.0.2
/2/usr/lib/libaudiofile.so.0.0.2
/2/usr/lib/libbonobo-2.so.0 ->
   libbonobo-2.so.0.0.0
/2/usr/lib/libbonobo-2.so.0.0.0
/2/usr/lib/libbonobo-activation.so.4 ->
   libbonobo-activation.so.4.0.0
```

```
/2/usr/lib/libbonobo-
   activation.so.4.0.0
/2/usr/lib/libbonoboui-2.so.0 ->
   libbonoboui-2.so.0.0.0
/2/usr/lib/libbonoboui-2.so.0.0.0
/2/usr/lib/libesd.so.0 ->
   libesd.so.0.2.28
/2/usr/lib/libesd.so.0.2.28
/2/usr/lib/libexpat.so.0 ->
   libexpat.so.0.4.0
/2/usr/lib/libexpat.so.0.4.0
/2/usr/lib/libfontconfig.so.1 ->
   libfontconfig.so.1.0
/2/usr/lib/libfontconfig.so.1.0
/2/usr/lib/libfreetype.so.6 ->
   libfreetype.so.6.3.2
/2/usr/lib/libfreetype.so.6.3.2
/2/usr/lib/libgconf-2.so.4 -> libgconf-
   2.so.4.1.0
/2/usr/lib/libgconf-2.so.4.1.0
/2/usr/lib/libgdk_pixbuf-2.0.so.0 ->
   libgdk_pixbuf-2.0.so.0.200.1
/2/usr/lib/libgdk_pixbuf-2.0.so.0.200.1
/2/usr/lib/libgdk-x11-2.0.so.0 ->
   libgdk-x11-2.0.so.0.200.1
/2/usr/lib/libgdk-x11-2.0.so.0.200.1
/2/usr/lib/libglade-2.0.so.0 ->
   libglade-2.0.so.0.0.1
/2/usr/lib/libglade-2.0.so.0.0.1
/2/usr/lib/libglib-2.0.so.0 -> libglib-
   2.0.so.0.200.1
/2/usr/lib/libglib-2.0.so.0.200.1
/2/usr/lib/libgmodule-2.0.so.0 ->
   libgmodule-2.0.so.0.200.1
/2/usr/lib/libgmodule-2.0.so.0.200.1
/2/usr/lib/libgnome-2.so.0 -> libgnome-
   2.so.0.200.0
/2/usr/lib/libgnome-2.so.0.200.0
/2/usr/lib/libgnomecanvas-2.so.0 ->
   libgnomecanvas-2.so.0.200.0
/2/usr/lib/libgnomecanvas-2.so.0.200.0
/2/usr/lib/libgnomeui-2.so.0 ->
   libgnomeui-2.so.0.200.0
/2/usr/lib/libgnomeui-2.so.0.200.0
/2/usr/lib/libgnomevfs-2.so.0 ->
   libgnomevfs-2.so.0.0.0
/2/usr/lib/libgnomevfs-2.so.0.0.0
/2/usr/lib/libgobject-2.0.so.0 ->
   libgobject-2.0.so.0.200.1
/2/usr/lib/libgobject-2.0.so.0.200.1
/2/usr/lib/libgthread-2.0.so.0 ->
   libgthread-2.0.so.0.200.1
/2/usr/lib/libgthread-2.0.so.0.200.1
/2/usr/lib/libgtk-x11-2.0.so.0 ->
   libgtk-x11-2.0.so.0.200.1
/2/usr/lib/libgtk-x11-2.0.so.0.200.1
/2/usr/lib/libjpeg.so.62 ->
   libjpeg.so.62.0.0
/2/usr/lib/libjpeg.so.62.0.0
/2/usr/lib/liblinc.so.1 ->
   liblinc.so.1.0.0
/2/usr/lib/liblinc.so.1.0.0
/2/usr/lib/libncurses.so.5 ->
   libncurses.so.5.3
/2/usr/lib/libncurses.so.5.3
/2/usr/lib/libORBit-2.so.0 -> libORBit-
   2.so.0.0.0
/2/usr/lib/libORBit-2.so.0.0.0
/2/usr/lib/libORBitCosNaming-2.so.0 ->
   libORBitCosNaming-2.so.0.0.0
/2/usr/lib/libORBitCosNaming-2.so.0.0.0
/2/usr/lib/libpango-1.0.so.0 ->
   libpango-1.0.so.0.200.1
/2/usr/lib/libpango-1.0.so.0.200.1
/2/usr/lib/libpangoft2-1.0.so.0 ->
   libpangoft2-1.0.so.0.200.1
/2/usr/lib/libpangoft2-1.0.so.0.200.1
/2/usr/lib/libpangox-1.0.so.0 ->
   libpangox-1.0.so.0.200.1
/2/usr/lib/libpangox-1.0.so.0.200.1
/2/usr/lib/libpangoxft-1.0.so.0 ->
   libpangoxft-1.0.so.0.200.1
/2/usr/lib/libpangoxft-1.0.so.0.200.1
/2/usr/lib/libpng12.so.0 ->
   libpng12.so.0.1.2.2
/2/usr/lib/libpng12.so.0.1.2.2
/2/usr/lib/libpopt.so.0 ->
   libpopt.so.0.0.0
/2/usr/lib/libpopt.so.0.0.0
/2/usr/lib/libstartup-notification-
   1.so.0 -> libstartup-notification-
   1.so.0.0.0
/2/usr/lib/libstartup-notification-
   1.so.0.0.0
/2/usr/lib/libvte.so.4 ->
   libvte.so.4.0.0
/2/usr/lib/libvte.so.4.0.0
/2/usr/lib/libxml2.so.2 ->
   libxml2.so.2.5.4
/2/usr/lib/libxml2.so.2.5.4
/2/usr/lib/libz.so.1 -> libz.so.1.1.4
/2/usr/lib/libz.so.1.1.4
/2/usr/lib/locale/locale-archive
/2/usr/lib/locale/locale-archive.EVaYTH
   (deleted-realloc)
/2/usr/lib/mozilla-
   1.2.1/defaults/profile (deleted-
   realloc)
/2/usr/lib/pango/1.2.0/modules/pango-
   basic-xft.so
/2/usr/lib/perl5/5.8.0/i386-linux-
   thread-multi/Config.pm
/2/usr/lib/perl5/5.8.0/i386-linux-
   thread-multi/CORE/libperl.so
/2/usr/lib/vte/gnome-pty-helper
/2/usr/lib/vte/gnome-pty-
   helper;40012009 (deleted-realloc)
/2/usr/lib/X11 -> ../X11R6/lib/X11
/2/usr/local/lib/libpcre.so.0 ->
   libpcre.so.0.0.1
/2/usr/local/lib/libpcre.so.0.0.1
/2/usr/share/fonts/afms/adobe
/2/usr/share/fonts/afms/adobe/pagd8a.af
   m
```

```
/2/usr/share/fonts/afms/adobe/pagdo8a.a
   fm
/2/usr/share/fonts/afms/adobe/pagk8a.af
   m
/2/usr/share/fonts/afms/adobe/pagko8a.a
   fm
/2/usr/share/fonts/afms/adobe/pbkd8a.af
   m
/2/usr/share/fonts/afms/adobe/pbkdi8a.a
   fm
/2/usr/share/fonts/afms/adobe/pbkl8a.af
   m
/2/usr/share/fonts/afms/adobe/pbkli8a.a
   fm
/2/usr/share/fonts/afms/adobe/pcrb8a.af
   m
/2/usr/share/fonts/afms/adobe/pcrbo8a.a
   fm
/2/usr/share/fonts/afms/adobe/pcrr8a.af
   m
/2/usr/share/fonts/afms/adobe/pcrro8a.a
   fm
/2/usr/share/fonts/afms/adobe/phvb8a.af
   m
/2/usr/share/fonts/afms/adobe/phvb8an.a
   fm
/2/usr/share/fonts/afms/adobe/phvbo8a.a
   fm
/2/usr/share/fonts/afms/adobe/phvbo8an.
   afm
/2/usr/share/fonts/afms/adobe/phvl8a.af
   m
/2/usr/share/fonts/afms/adobe/phvlo8a.a
   fm
/2/usr/share/fonts/afms/adobe/phvr8a.af
   m
/2/usr/share/fonts/afms/adobe/phvr8an.a
   fm
/2/usr/share/fonts/afms/adobe/phvro8a.a
   fm
/2/usr/share/fonts/afms/adobe/phvro8an.
   afm
/2/usr/share/fonts/afms/adobe/pncb8a.af
   m
/2/usr/share/fonts/afms/adobe/pncbi8a.a
   fm
/2/usr/share/fonts/afms/adobe/pncr8a.af
   m
/2/usr/share/fonts/afms/adobe/pncri8a.a
   fm
/2/usr/share/fonts/afms/adobe/pplb8a.af
   m
/2/usr/share/fonts/afms/adobe/pplbi8a.a
   fm
/2/usr/share/fonts/afms/adobe/pplr8a.af
   m
/2/usr/share/fonts/afms/adobe/pplri8a.a
   fm
/2/usr/share/fonts/afms/adobe/psyr.afm
/2/usr/share/fonts/afms/adobe/ptmb8a.af
   m
/2/usr/share/fonts/afms/adobe/ptmbi8a.a
   fm
/2/usr/share/fonts/afms/adobe/ptmr8a.af
   m
/2/usr/share/fonts/afms/adobe/ptmri8a.a
   fm
/2/usr/share/fonts/afms/adobe/putb8a.af
   m
/2/usr/share/fonts/afms/adobe/putbi8a.a
   fm
/2/usr/share/fonts/afms/adobe/putr8a.af
   m
/2/usr/share/fonts/afms/adobe/putri8a.a
   fm
/2/usr/share/fonts/afms/adobe/pzcmi8a.a
   fm
/2/usr/share/fonts/afms/adobe/pzdr.afm
/2/usr/share/fonts/afms/adobe/pzdr.afm;
   40012009 (deleted-realloc)
/2/usr/share/fonts/bitmap-
   fonts/fonts.cache-1
/2/usr/share/fonts/default/fonts.cache-
   1
/2/usr/share/fonts/default/ghostscript/
   fonts.cache-1
/2/usr/share/icons/Bluecurve/cursors/le
   ft_ptr
/2/usr/share/icons/Bluecurve/cursors/xt
   erm
/2/usr/share/icons/Bluecurve/cursors/xt
   erm;40012009 (deleted-realloc)
/2/usr/share/icons/Bluecurve/index.them
   e
/2/usr/share/icons/Bluecurve/index.them
   e;40012009 (deleted-realloc)
/2/usr/share/icons/default/index.theme
/2/usr/share/icons/default/index.theme;
   43cc0503 (deleted-realloc)
/2/usr/share/icons/gnome/index.theme
/2/usr/share/locale/locale.alias
/2/usr/share/pixmaps/gnome-terminal.png
/2/usr/share/redhat-config-
   network/netconfpkg/gui/exception.py
   (deleted-realloc)
/2/usr/share/redhat-config-
   network/netconfpkg/gui/exception.pyc
   (deleted-realloc)
/2/usr/share/redhat-config-
   network/netconfpkg/gui/exception.pyo
   (deleted-realloc)
/2/usr/share/terminfo/x/xterm
/2/usr/share/themes/Bluecurve/gtk-
   2.0/gtkrc
/2/usr/share/themes/Bluecurve/gtk-
   2.0/iconrc
/2/usr/share/themes/Bluecurve/gtk-
   2.0/iconrc;40012009 (deleted-
   realloc)
/2/usr/share/themes/Default/gtk-2.0-
   key/gtkrc
/2/usr/share/themes/Default/gtk-2.0-
   key/gtkrc;40012009 (deleted-realloc)
```

```
/2/usr/share/vte/termcap/xterm
/2/usr/share/vte/termcap/xterm;40012009
   (deleted-realloc)
/2/usr/X11R6/lib/libICE.so.6 ->
   libICE.so.6.3
/2/usr/X11R6/lib/libICE.so.6.3
/2/usr/X11R6/lib/libSM.so.6 ->
   libSM.so.6.0
/2/usr/X11R6/lib/libSM.so.6.0
/2/usr/X11R6/lib/libX11.so.6 ->
   libX11.so.6.2
/2/usr/X11R6/lib/libX11.so.6.2
/2/usr/X11R6/lib/libXcursor.so.1 ->
   libXcursor.so.1.0
/2/usr/X11R6/lib/libXcursor.so.1.0
/2/usr/X11R6/lib/libXext.so.6 ->
   libXext.so.6.4
/2/usr/X11R6/lib/libXext.so.6.4
/2/usr/X11R6/lib/libXft.so.2 ->
   libXft.so.2.1.1
/2/usr/X11R6/lib/libXft.so.2.1.1
/2/usr/X11R6/lib/libXi.so.6 ->
   libXi.so.6.0
/2/usr/X11R6/lib/libXi.so.6.0
/2/usr/X11R6/lib/libXrandr.so.2 ->
   libXrandr.so.2.0
/2/usr/X11R6/lib/libXrandr.so.2.0
/2/usr/X11R6/lib/libXrender.so.1 ->
   libXrender.so.1.2.2
/2/usr/X11R6/lib/libXrender.so.1.2.2
/2/usr/X11R6/lib/X11/fonts/OTF
/2/usr/X11R6/lib/X11/fonts/Type1/fonts.
   cache-1
/2/usr/X11R6/lib/X11/fonts/Type1/l04701
   3t.pfa
/2/usr/X11R6/lib/X11/fonts/Type1/l04801
   3t.pfa
/2/usr/X11R6/lib/X11/locale/en_US.UTF-
   8/XI18N_OBJS
/2/usr/X11R6/lib/X11/locale/en_US.UTF-
   8/XLC_LOCALE
/2/usr/X11R6/lib/X11/locale/en_US.UTF-
   8/XLC_LOCALE;43cc0503 (deleted-
   realloc)
/2/usr/X11R6/lib/X11/locale/lib/common/
   xlcUTF8Load.so.2
/2/usr/X11R6/lib/X11/locale/lib/common/
   xlcUTF8Load.so.2;43cc0503 (deleted-
   realloc)
/2/usr/X11R6/lib/X11/locale/locale.alia
   s
/2/usr/X11R6/lib/X11/locale/locale.dir
/2/var/log/messages
<liveCD_RHL_data.img-dead-290894>
<liveCD_RHL_data.img-dead-290964>
```

10. Appendix D Files Modified on the RedHat Linux 9 Virtual Machines

Note: For this list, the files in /usr/lib/locale for the Helix live CD have been removed.

Live CD	File Name
BartPE	/2/bin/ls
BartPE	/2/etc/localtime
BartPE	/2/tmp/orbit-root/linc-96f-0-1aa79962a5c27
BartPE	/2/usr/lib/perl5/5.8.0/CGI/Carp.pm.newcgi (deleted-realloc)
BartPE	/2/usr/share/icons/Bluecurve/cursors/top_side
BartPE	/2/var/log/wtmp
BartPE	/2/var/run/utmp
FIRE	/2/bin/basename
FIRE	/2/bin/basename;43cc0503 (deleted-realloc)
FIRE	/2/bin/sed
FIRE	/2/bin/sleep
FIRE	/2/bin/uname
FIRE	/2/etc/cron.hourly
FIRE	/2/etc/cups/certs
FIRE	/2/etc/cups/certs/0
FIRE	/2/etc/localtime
FIRE	/2/etc/rc.d/init.d/functions
FIRE	/2/etc/services
FIRE	/2/etc/sysconfig/init
FIRE	/2/etc/sysconfig/network
FIRE	/2/etc/sysconfig/networking/ifcfg-lo
FIRE	/2/etc/sysconfig/network-scripts/ifcfg-eth0
FIRE	/2/etc/sysconfig/network-scripts/ifcfg-lo -> ../networking/ifcfg-lo
FIRE	/2/etc/sysconfig/network-scripts/network-functions
FIRE	/2/lib/libc.so.6 -> libc-2.3.2.so
FIRE	/2/lib/libc-2.3.2.so
FIRE	/2/lib/modules/2.4.20-31.9/kernel/fs/nls/nls_iso8859-1.o
FIRE	/2/mnt
FIRE	/2/root/.gconfd
FIRE	/2/root/.gconfd/saved_state.orig (deleted)
FIRE	/2/sbin/dhclient-script
FIRE	/2/sbin/ifconfig
FIRE	/2/tmp/orbit-root/linc-96f-0-41d7400fa0924
FIRE	/2/usr
FIRE	/2/usr/bin
FIRE	/2/usr/bin/expr
FIRE	/2/usr/bin/nc
FIRE	/2/usr/bin/run-parts

Live CD	File Name
FIRE	/2/usr/lib/perl5/5.8.0/CGI/Carp.pm.newcgi (deleted)
FIRE	/2/usr/lib/perl5/5.8.0/CGI/Cookie.pm.newcgi (deleted-realloc)
FIRE	/2/usr/share/icons/Bluecurve/24x24/stock/gtk-copy.png
FIRE	/2/usr/share/icons/Bluecurve/24x24/stock/gtk-paste.png
FIRE	/2/var/log/cron
FIRE	/2/var/log/wtmp
FIRE	/2/var/run/utmp
FIRE	/2/var/run/utmp
FIRE	/2/var/spool/at
FIRE	<FIRE_RHL_data-INSERT.img-dead-160262>
Helix	/2/bin/basename
Helix	/2/bin/basename;43cc0503 (deleted-realloc)
Helix	/2/bin/sed
Helix	/2/bin/uname
Helix	/2/etc/cups/certs
Helix	/2/etc/cups/certs/0
Helix	/2/etc/localtime
Helix	/2/etc/rc.d/init.d/functions
Helix	/2/etc/services
Helix	/2/etc/sysconfig/init
Helix	/2/etc/sysconfig/network
Helix	/2/etc/sysconfig/networking/ifcfg-lo
Helix	/2/etc/sysconfig/network-scripts/ifcfg-lo -> ../networking/ifcfg-lo
Helix	/2/etc/sysconfig/network-scripts/network-functions
Helix	/2/lib/libc.so.6 -> libc-2.3.2.so
Helix	/2/lib/libc-2.3.2.so
Helix	/2/lib/modules/2.4.20-31.9/kernel/fs/nls/nls_iso8859-1.o
Helix	/2/mnt
Helix	/2/root/.gconfd
Helix	/2/root/.gconfd/saved_state.orig (deleted)
Helix	/2/sbin/dhclient-script
Helix	/2/tmp/orbit-root/linc-96f-0-6ee10ee6b1032
Helix	/2/usr
Helix	/2/usr/bin/expr
Helix	/2/usr/bin/nc
Helix	/2/usr/lib/perl5/5.8.0/CGI/Carp.pm.newcgi (deleted)
Helix	/2/usr/lib/perl5/5.8.0/CGI/Cookie.pm.newcgi (deleted-realloc)
Helix	/2/usr/share/icons/Bluecurve/cursors/top_side
Helix	/2/usr/share/terminfo/d/dumb
Helix	/2/var/log/wtmp
Helix	/2/var/log/wtmp
Helix	/2/var/run/utmp
Helix	/2/var/run/utmp
Helix	/2/var/spool/at
Helix	<Helix_RHL_data-INSERT.img-dead-160262>
INSERT	/2/bin/ls

Live CD	File Name
INSERT	/2/etc/cups/certs
INSERT	/2/etc/cups/certs/0
INSERT	/2/lib/modules/2.4.20-31.9/kernel/fs/nls/nls_iso8859-1.o
INSERT	/2/root/.gconfd
INSERT	/2/root/.gconfd/saved_state.orig (deleted)
INSERT	/2/tmp/orbit-root/linc-96f-0-3a26b301d2f93
INSERT	/2/usr/bin/dir
INSERT	/2/usr/lib/perl5/5.8.0/CGI/Carp.pm.newcgi (deleted)
INSERT	/2/usr/lib/perl5/5.8.0/CGI/Cookie.pm.newcgi (deleted-realloc)
INSERT	/2/usr/share/icons/Bluecurve/cursors/top_side
INSERT	/2/var/log/wtmp
INSERT	/2/var/run/utmp
INSERT	/2/var/spool/at
INSERT	<INSERT_RHL_data.img-dead-160262>
Operator	/2/bin/ls
Operator	/2/lib/modules/2.4.20-31.9/kernel/fs/nls/nls_iso8859-1.o
Operator	/2/mnt
Operator	/2/tmp/orbit-root/linc-96f-0-7815d2608c14c
Operator	/2/usr/lib/perl5/5.8.0/CGI/Carp.pm.newcgi (deleted-realloc)
Operator	/2/usr/share/icons/Bluecurve/cursors/top_side
Operator	/2/var/log/wtmp
Operator	/2/var/run/utmp