Use offense to inform defense. Find flaws before the bad guys do.

Copyright SANS Institute
Author Retains Full Rights

This paper is from the SANS Penetration Testing site. Reposting is not permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Hacker Tools, Techniques, Exploits, and Incident Handling (SEC504)" at https://pen-testing.sans.org/events/
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
Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensic

Outline

1. Abstract ................................................................. 3
2. Requirements for System Examination for Incident Handling and Forensics ............................................. 3
   Incident Handling Six-Step Process ...................... 5
   Live CDs ................................................................. 10
3. Testing the Live CDs ..................................................... 11
   Testing Environment ................................................. 11
   Test Methodology and Criteria ............................. 11
4. Testing Results .......................................................... 20
   Live CDs Used for Live System Incident Handling .... 20
   Analysis of the Forensic Images ......................... 29
5. Summary ................................................................. 32
6. References ............................................................... 34
7. Appendix A Common Files Modified by the Live CDs on the Windows XP Virtual Machine ........................ 39
8. Appendix B Files Modified by the Live CDs on the Windows XP Virtual Machine ............................... 41
9. Appendix C Common Files Modified by the Live CDs on the RedHat 9 Linux Virtual Machine ................. 58
10. Appendix D Files Modified on the RedHat Linux 9 Virtual Machines ..................................................... 63
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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.

Ricky D. Smith
In either case, once the incident has been verified the incident handler will need to further examine the system to 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
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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.

![Diagram of 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

Ricky D. Smith
Pros and Cons of Using Linux and Windows  
Live CDs in Incident Handling and Forensic

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
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

**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

Ricky D. Smith
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

of the target machines’ hard drives will be 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
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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
```

Ricky D. Smith
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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**

<table>
<thead>
<tr>
<th>Command and options</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>date /t</code></td>
<td>Identify the date of the start of the first responder process</td>
</tr>
<tr>
<td><code>time /t</code></td>
<td>Identify the time of the start of the first responder process</td>
</tr>
<tr>
<td><code>set</code></td>
<td>List the environmental variables</td>
</tr>
<tr>
<td><code>psinfo</code></td>
<td>Lists information about a system (Russinovich, 2006)</td>
</tr>
<tr>
<td><code>autorunsc.exe -a -c -d -e -s -w</code></td>
<td>Lists programs are configured to run during system bootup or login, and shows you the entries in the order Windows processes them (Russinovich &amp; Cogswell, 2006)</td>
</tr>
</tbody>
</table>
### Pros and Cons of Using Linux and Windows

#### Live CDs in Incident Handling and Forensic

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

**Live CDs in Incident Handling and Forensic**

<table>
<thead>
<tr>
<th>Commands and options</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>date</strong></td>
<td>Identify the date and time of the start of the first responder process</td>
</tr>
<tr>
<td><strong>set</strong></td>
<td>List the environmental variables</td>
</tr>
<tr>
<td><strong>mount -n /mnt/cdrom</strong></td>
<td>Mount the first responder CD</td>
</tr>
<tr>
<td><strong>/mnt/cdrom/bin/bash</strong></td>
<td>Start a known good shell from the first responder CD</td>
</tr>
<tr>
<td><strong>cd /mnt/cdrom/bin</strong></td>
<td>Move to the directory containing the known good binaries.</td>
</tr>
<tr>
<td><strong>PATH=&quot;/mnt/cdrom/bin&quot;</strong></td>
<td>Set the PATH variable to the location of the known good binaries.</td>
</tr>
</tbody>
</table>

**Table 2: Commands used for testing using the Linux live CDs on a live system**
### Pros and Cons of Using Linux and Windows

**Live CDs in Incident Handling and Forensic**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LD_LIBRARY_PATH=“/mnt/cdrom/lib”</strong></td>
<td>Set the <code>LD_LIBRARY_PATH</code> variable to the location of the known good libraries</td>
</tr>
<tr>
<td><strong>export PATH</strong></td>
<td>Make the <code>PATH</code> variable to be in the environment of subsequently executed commands</td>
</tr>
<tr>
<td><strong>export LD_LIBRARY_PATH</strong></td>
<td>Make the <code>LD_LIBRARY_PATH</code> variable to be in the environment of subsequently executed commands</td>
</tr>
<tr>
<td><strong>echo $PATH</strong></td>
<td>Verify the setting of the environment variable</td>
</tr>
<tr>
<td><strong>echo $LD_LIBRARY_PATH</strong></td>
<td>Verify the setting of the environment variable</td>
</tr>
<tr>
<td><strong>ls -la /mnt/cdrom/bin</strong></td>
<td>List the contents of the binaries used by the first responder</td>
</tr>
<tr>
<td><strong>ls -la /mnt/cdrom/lib</strong></td>
<td>List the contents of the libraries used by the first responder</td>
</tr>
<tr>
<td><strong>ifconfig -a</strong></td>
<td>List the current configuration of all network interfaces.</td>
</tr>
<tr>
<td><strong>netstat -a</strong></td>
<td>Symbolically displays the contents of various network-related data structures showing the address of any protocol control blocks associated with sockets</td>
</tr>
<tr>
<td><strong>netstat -arp</strong></td>
<td>Symbolically displays the contents of various network-related data structures showing the address of any protocol control blocks associated with sockets</td>
</tr>
</tbody>
</table>
### Pros and Cons of Using Linux and Windows

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>netstat</strong></td>
<td>Symbolically displays the contents of various network-related data structures showing</td>
</tr>
<tr>
<td><strong>route</strong></td>
<td>Display and manually manipulate the network routing tables</td>
</tr>
<tr>
<td><strong>arp</strong></td>
<td>Displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol</td>
</tr>
<tr>
<td><strong>w</strong></td>
<td>Prints a summary of the current activity on the system, including what each user is doing</td>
</tr>
<tr>
<td><strong>who</strong></td>
<td>Displays information about currently logged in users</td>
</tr>
<tr>
<td><strong>last</strong></td>
<td>Displays a list of all users logged in (and out) since <code>/var/log/wtmp</code> was created.</td>
</tr>
<tr>
<td><strong>who -Hi</strong></td>
<td>Displays information about currently logged in users</td>
</tr>
<tr>
<td><strong>finger</strong></td>
<td>Displays information about the system users</td>
</tr>
<tr>
<td><strong>last -aix</strong></td>
<td>Displays a list of all users logged in (and out) since <code>/var/log/wtmp</code></td>
</tr>
<tr>
<td><strong>lastb -aix</strong></td>
<td>Displays a list of all of the bad login attempts since <code>/var/log/btmp</code> was created</td>
</tr>
<tr>
<td><strong>ps -auxeww</strong></td>
<td>Displays information about a selection</td>
</tr>
</tbody>
</table>
### Pros and Cons of Using Linux and Windows

#### Live CDs in Incident Handling and Forensic Analysis

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ps -aux</strong></td>
<td>Displays information about a selection of the active processes</td>
</tr>
<tr>
<td><strong>top -b -n1</strong></td>
<td>Provides a dynamic real-time view of a running system</td>
</tr>
<tr>
<td><strong>ls/of -i -n -P -l</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>ls/of</strong> -i</td>
<td>Lists information about files opened by processes with the listing of all Internet and network files selected</td>
</tr>
<tr>
<td><strong>ls/of -d rt/d</strong></td>
<td>Lists information about files opened by processes with the specified list of file descriptors that is, in this case, rt/d, a root directory</td>
</tr>
<tr>
<td><strong>ls/of +M -i</strong></td>
<td>Lists information about files opened by processes with the reporting of portmapper registrations for local TCP and UDP ports enabled.</td>
</tr>
</tbody>
</table>

#### Table 3: Live CDs to be tested

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Version</th>
<th>Source</th>
<th>Description from website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helix</td>
<td>1.7</td>
<td><a href="http://www.e-fense.com/helix/">http://www.e-fense.com/helix/</a></td>
<td>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</td>
</tr>
</tbody>
</table>
### Pros and Cons of Using Linux and Windows

<table>
<thead>
<tr>
<th>Bart's Preinstalled Environment bootable live windows CD/DVD (BartPE)</th>
<th>Version 3.1.10a</th>
<th><a href="http://www.nu2.nu/pebuilder/">http://www.nu2.nu/pebuilder/</a></th>
<th>Bart's PE Builder helps you build a &quot;BartPE&quot; (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)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic and Incident Response Environment Bootable CD (F.I.R.E.)</td>
<td>0.3.5b</td>
<td><a href="http://biatchux.dmzs.com/">http://biatchux.dmzs.com/</a></td>
<td>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)</td>
</tr>
<tr>
<td>Inside Security Rescue Toolkit (INSERT)</td>
<td>v1.3.6</td>
<td><a href="http://www.inside-security.de/insert_en.html">http://www.inside-security.de/insert_en.html</a></td>
<td>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)</td>
</tr>
<tr>
<td>Operator</td>
<td>3.3.20</td>
<td><a href="http://www.us">http://www.us</a> Operator</td>
<td>Operator is a complete Linux (Debian)</td>
</tr>
</tbody>
</table>

Ricky D. Smith
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

| 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:**

Ricky D. Smith
Pros and Cons of Using Linux and Windows

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](image)

**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.

Ricky D. Smith
Pros and Cons of Using Linux and Windows
Live CDs in Incident Handling and Forensic

**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.

![F.I.R.E. Pop-up Window](image)

*Figure 3: F.I.R.E. Pop-up Window*
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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.

Ricky D. Smith

Figure 4: F.I.R.E. Command Shell
Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensic

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.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

Figure 5: Helix Initial Screen

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.

Ricky D. Smith
Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensic 

Cons:

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

```
11:23:49.26 D:\IR> bin\autorunsc.exe -a -o -d -e -w \d:\IR\bin\nc.exe 192.168.159.1 1234
'bin\autorunsc.exe' is not recognized as an internal or external command, operable program or batch file.
11:25:44.06 D:\IR> ipconfig /all | d:\IR\bin\nc.exe 192.168.159.1 1234
'ipconfig' is not recognized as an internal or external command, operable program or batch file.
11:29:47.60 D:\IR> tasklist | d:\IR\bin\nc.exe 192.168.159.1 1234
'tasklist' is not recognized as an internal or external command, operable program or batch file.
11:33:23.74 D:\IR> sysinternals\pslist.exe | d:\IR\bin\nc.exe 192.168.159.1 1234
'pslist.exe' is not recognized as an internal or external command, operable program or batch file.
11:35:59.70 D:\IR> bin\pulist.exe | d:\IR\bin\nc.exe 192.168.159.1 1234
'pulist.exe' is not recognized as an internal or external command, operable program or batch file.
11:34:47.43 D:\IR> bin\pstat.exe | d:\IR\bin\nc.exe 192.168.159.1 1234
'pstat.exe' is not recognized as an internal or external command, operable program or batch file.
```

**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.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

**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.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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 8: INSERT Autorun Web Page**

To boot from CD-ROM, please change the device boot order in the BIOS of your computer. Then make sure, that the CD is in the drive and reboot your PC.

We wish you a lot of fun with INSERT and hope that it will be useful to you.

Author: Matthias Mukulez
insert@inside-security.de
Inside Security IT Consulting GmbH
Pros and Cons of Using Linux and Windows
Live CDs in Incident Handling and Forensic

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
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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**

<table>
<thead>
<tr>
<th>Live CD</th>
<th>Number of Timeline entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>86</td>
</tr>
<tr>
<td>INSERT</td>
<td>163</td>
</tr>
<tr>
<td>Helix</td>
<td>327</td>
</tr>
<tr>
<td>FIRE</td>
<td>343</td>
</tr>
<tr>
<td>BartPE</td>
<td>459</td>
</tr>
</tbody>
</table>

Ricky D. Smith
Pros and Cons of Using Linux and Windows  
Live CDs in Incident Handling and Forensic Investigation

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>
<thead>
<tr>
<th>Live CD</th>
<th>Number of Timeline entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>376</td>
</tr>
<tr>
<td>Operator</td>
<td>377</td>
</tr>
<tr>
<td>INSERT</td>
<td>384</td>
</tr>
<tr>
<td>FIRE</td>
<td>410</td>
</tr>
<tr>
<td>Helix</td>
<td>764</td>
</tr>
</tbody>
</table>

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.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic Analysis

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

<table>
<thead>
<tr>
<th>Live CD</th>
<th>Number of Timeline entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>7</td>
</tr>
<tr>
<td>Operator</td>
<td>8</td>
</tr>
<tr>
<td>INSERT</td>
<td>15</td>
</tr>
<tr>
<td>Helix</td>
<td>35</td>
</tr>
<tr>
<td>FIRE</td>
<td>41</td>
</tr>
</tbody>
</table>

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
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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.

Ricky D. Smith
6. References


Ricky D. Smith
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

Bethesda, MD: SANS Institute.


Ricky D. Smith
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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


http://www.microsoft.com/whdc/system/winpreinst/WindowsPE_over.mspx


Ricky D. Smith
Pros and Cons of Using Linux and Windows
Live CDs in Incident Handling and Forensic


Pros and Cons of Using Linux and Windows


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

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/msvcrtdll.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

Ricky D. Smith

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

Ricky D. Smith
## 8. Appendix B Files Modified by the Live CDs on the Windows XP Virtual Machine

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>1076-128-4 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP</td>
</tr>
<tr>
<td>BartPE</td>
<td>1077-128-3 C:/Program Files/WIndows NT/Accessories/wordpad.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>1106-128-4 C:/WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf</td>
</tr>
<tr>
<td>BartPE</td>
<td>1399-128-3 C:/Program Files/Common Files/System/Ole DB/oledb32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1399-128-3 C:/Program Files/Common Files/System/Ole DB/SET4PB.tmp (deleted-realloc)</td>
</tr>
<tr>
<td>BartPE</td>
<td>1399-128-3 C:/WINDOWS/system32/msrd3x40.dll (deleted-realloc)</td>
</tr>
<tr>
<td>BartPE</td>
<td>1422-128-3 C:/WINDOWS/system32/msxml3r.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1544-128-3 C:/WINDOWS/system32/ntlanui2.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys</td>
</tr>
<tr>
<td>BartPE</td>
<td>15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys (deleted-realloc)</td>
</tr>
<tr>
<td>BartPE</td>
<td>15496-128-3 C:/WINDOWS/system32/drivers/acpi.sys</td>
</tr>
<tr>
<td>BartPE</td>
<td>15498-128-3 C:/WINDOWS/system32/winspool.drv</td>
</tr>
<tr>
<td>BartPE</td>
<td>15501-128-3 C:/WINDOWS/system32/userinit.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15512-128-3 C:/WINDOWS/system32/services.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15512-128-3 C:/WINDOWS/system32/services.exe (deleted-realloc)</td>
</tr>
<tr>
<td>BartPE</td>
<td>15517-128-3 C:/WINDOWS/system32/samlib.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15518-128-3 C:/WINDOWS/system32/rshx32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15520-128-3 C:/WINDOWS/system32/rasman.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15523-128-3 C:/WINDOWS/system32/rasapi32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15524-128-3 C:/WINDOWS/system32/printui.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15525-128-3 C:/WINDOWS/system32/perfctrs.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15533-128-3 C:/WINDOWS/system32/msvl_0.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15563-128-3 C:/WINDOWS/system32/wzcsapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15564-128-3 C:/WINDOWS/system32/wzcdig.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15565-128-3 C:/WINDOWS/system32/wtsapi32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15568-128-3 C:/WINDOWS/system32/wsock32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15571-128-3 C:/WINDOWS/system32/wshcpipe.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15576-128-3 C:/WINDOWS/system32/wshext.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15579-128-3 C:/WINDOWS/system32/ws2help.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15581-128-3 C:/WINDOWS/system32/ws2_32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15595-128-3 C:/WINDOWS/system32/wmpshell.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15601-128-3 C:/WINDOWS/system32/wmi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15608-128-3 C:/WINDOWS/system32/wlnotify.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15610-128-3 C:/WINDOWS/system32/wldap32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15615-128-3 C:/WINDOWS/system32/winsta.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15616-128-3 C:/WINDOWS/system32/winsrv.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15619-128-3 C:/WINDOWS/system32/winrnr.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15627-128-3 C:/WINDOWS/system32/wininet.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15630-128-3 C:/WINDOWS/system32/wiashext.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15641-128-3 C:/WINDOWS/system32/webcheck.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15677-128-3 C:/WINDOWS/system32/upnp.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15695-128-3 C:/WINDOWS/system32/themeui.dll</td>
</tr>
</tbody>
</table>
## Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>15709-128-3 C:/WINDOWS/system32/tapi32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15715-128-3 C:/WINDOWS/system32/syncui.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15719-128-3 C:/WINDOWS/system32/svchost.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15723-128-3 C:/WINDOWS/system32/stobject.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15748-128-3 C:/WINDOWS/system32/spoolsv.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15760-128-3 C:/WINDOWS/system32/slayerxp.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15768-128-3 C:/WINDOWS/system32/shscrap.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15770-128-3 C:/WINDOWS/system32/shmgrate.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15771-128-3 C:/WINDOWS/system32/shmedia.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15774-128-3 C:/WINDOWS/system32/shimgvw.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15777-128-3 C:/WINDOWS/system32/shfolder.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15780-128-3 C:/WINDOWS/system32/shdocvw.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15781-128-3 C:/WINDOWS/system32/sfcs.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15782-128-3 C:/WINDOWS/system32/sfcs.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15791-128-3 C:/WINDOWS/system32/sensapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15793-128-3 C:/WINDOWS/system32/sens.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15795-128-3 C:/WINDOWS/system32/sendmail.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15798-128-3 C:/WINDOWS/system32/secur32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1580-128-3 C:/WINDOWS/system32/wbem/wmiutils.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15804-128-3 C:/WINDOWS/system32/scrobj.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15821-128-3 C:/WINDOWS/system32/rtutils.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15833-128-3 C:/WINDOWS/system32/riched20.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15835-128-3 C:/WINDOWS/system32/resutils.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15838-128-3 C:/WINDOWS/system32/remotepg.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15840-128-3 C:/WINDOWS/system32/regsrvr32.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15856-128-3 C:/WINDOWS/system32/rcbdyct1.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15866-128-3 C:/WINDOWS/system32/rapidhlp.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15869-128-3 C:/WINDOWS/system32/query.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15884-128-3 C:/WINDOWS/system32/psapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15900-128-3 C:/WINDOWS/system32/photowiz.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15901-128-3 C:/WINDOWS/system32/perfproc.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15902-128-3 C:/WINDOWS/system32/perfos.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15904-128-3 C:/WINDOWS/system32/perfdisk.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15905-128-3 C:/WINDOWS/system32/psapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15937-128-3 C:/WINDOWS/system32/occache.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15942-128-3 C:/WINDOWS/system32/ntshru1.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15948-128-3 C:/WINDOWS/system32/ntmarta.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15957-128-3 C:/WINDOWS/system32/ntdsapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15960-128-3 C:/WINDOWS/system32/notepad.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>15970-128-3 C:/WINDOWS/system32/ntshell.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15976-128-3 C:/WINDOWS/system32/netplwiz.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15983-128-3 C:/WINDOWS/system32/netcfgdx.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15985-128-3 C:/WINDOWS/system32/netapi32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15994-128-3 C:/WINDOWS/system32/ncobjapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15995-128-3 C:/WINDOWS/system32/mydocs.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15996-128-3 C:/WINDOWS/system32/mtxclu.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>15999-128-3 C:/WINDOWS/system32/mtxclu.dll</td>
</tr>
</tbody>
</table>
### Pros and Cons of Using Linux and Windows

**Live CDs in Incident Handling and Forensic**

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>16008-128-3 C:/WINDOWS/system32/mswsock.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16020-128-3 C:/WINDOWS/system32/msvcp60.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16033-128-3 C:/WINDOWS/system32/mstask.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16046-128-3 C:/WINDOWS/system32/mspatcha.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16065-128-3 C:/WINDOWS/system32/msimg32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16069-128-3 C:/WINDOWS/system32/msieftp.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16086-128-3 C:/WINDOWS/system32/msdtcuiu.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16088-128-3 C:/WINDOWS/system32/msdtcprx.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16109-128-3 C:/WINDOWS/system32/mprapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16111-128-3 C:/WINDOWS/system32/mp.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16124-128-3 C:/WINDOWS/system32/mmsys.cpl</td>
</tr>
<tr>
<td>BartPE</td>
<td>16126-128-3 C:/WINDOWS/system32/mmcshext.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16128-128-3 C:/WINDOWS/system32/mmcbase.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16136-128-3 C:/WINDOWS/system32/mfc42u.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16147-128-3 C:/WINDOWS/system32/1sass.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>16156-128-3 C:/WINDOWS/system32/loadperf.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1616-128-3 C:/WINDOWS/system32/wbem/wmiprvse.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>1618-128-3 C:/WINDOWS/system32/iphlpapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16202-128-3 C:/WINDOWS/system32/inetmibl.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16218-128-3 C:/WINDOWS/system32/iedkcs32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16221-128-3 C:/WINDOWS/system32/ie4uinit.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>1622-128-3 C:/WINDOWS/system32/wbem/wmiprov.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16235-128-3 C:/WINDOWS/system32/hnetcfg.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1624-128-3 C:/WINDOWS/system32/perfnet.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16251-128-3 C:/WINDOWS/system32/fontext.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16263-128-3 C:/WINDOWS/system32/esent.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1628-128-3 C:/WINDOWS/system32/perftime.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16283-128-3 C:/WINDOWS/system32/dsuext.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16286-128-3 C:/WINDOWS/system32/dssec.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16287-128-3 C:/WINDOWS/system32/dsquery.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1631-128-3 C:/WINDOWS/system32/docprop2.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16318-128-3 C:/WINDOWS/system32/dnsapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16342-128-3 C:/WINDOWS/system32/dfsshlex.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16369-128-3 C:/WINDOWS/system32/cscui.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16372-128-3 C:/WINDOWS/system32/cscdll.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16378-128-3 C:/WINDOWS/system32/cryptnet.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16379-128-3 C:/WINDOWS/system32/cryptext.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1668-128-3 C:/WINDOWS/system32/wbem/wmiapsrv.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>16755-128-3 C:/WINDOWS/system32/wups.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16762-128-3 C:/WINDOWS/system32/wuaeng.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16763-128-3 C:/WINDOWS/system32/wuaucpl.cpl</td>
</tr>
<tr>
<td>BartPE</td>
<td>16765-128-3 C:/WINDOWS/system32/wuauctl.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>16780-128-3 C:/WINDOWS/system32/winhttp.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16783-128-3 C:/WINDOWS/system32/twext.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1682-128-3 C:/WINDOWS/system32/wbem/wmiaprpl.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1683-128-3 C:/WINDOWS/system32/wbem/wmiapres.dll</td>
</tr>
</tbody>
</table>

---

**Ricky D. Smith**

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
### Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>16842-128-3 C:/WINDOWS/system32/extmgdr.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>16897-128-3 C:/WINDOWS/system32/drivers/msasmbios.sys</td>
</tr>
<tr>
<td>BartPE</td>
<td>16900-128-3 C:/WINDOWS/system32/drivers/intelppm.sys</td>
</tr>
<tr>
<td>BartPE</td>
<td>16901-128-3 C:/WINDOWS/system32/drivers/http.sys</td>
</tr>
<tr>
<td>BartPE</td>
<td>1691-128-3 C:/WINDOWS/system32/rasctrs.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1696-128-3 C:/WINDOWS/system32/wbem/wbemsvc.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1703-128-3 C:/WINDOWS/system32/wbem/wbemprox.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1735-128-3 C:/WINDOWS/system32/wbem/wbemcomm.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>175-128-3 C:/WINDOWS/Fonts/vgaem.fon</td>
</tr>
<tr>
<td>BartPE</td>
<td>1765-128-3 C:/WINDOWS/system32/rsvpperf.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1813-128-3 C:/WINDOWS/system32/drivers/etc/services</td>
</tr>
<tr>
<td>BartPE</td>
<td>1816-128-3 C:/WINDOWS/system32/wbem/mofd.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1832-128-3 C:/WINDOWS/system32/wbem/framedyn.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1833-128-3 C:/WINDOWS/system32/wbem/fastprox.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>185-128-3 C:/WINDOWS/system32/cfgmgr32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1878-128-3 C:/WINDOWS/system32/wbem/cimwin32.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1924-128-3 C:/WINDOWS/system32/tapiperf.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>193-128-3 C:/WINDOWS/system32/cdfview.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>1993-128-3 C:/WINDOWS/system32/utilldll.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>2141-128-3 C:/WINDOWS/Media/Windows XP Ding.wav</td>
</tr>
<tr>
<td>BartPE</td>
<td>214-128-4 C:/WINDOWS/WindowsUpdate.log</td>
</tr>
<tr>
<td>BartPE</td>
<td>222-128-3 C:/WINDOWS/Fonts/dosapp.fon</td>
</tr>
<tr>
<td>BartPE</td>
<td>224-128-3 C:/WINDOWS/Fonts/ega40woa.fon</td>
</tr>
<tr>
<td>BartPE</td>
<td>225-128-3 C:/WINDOWS/Fonts/cgaoem.fon</td>
</tr>
<tr>
<td>BartPE</td>
<td>226-128-3 C:/WINDOWS/Fonts/cga80woa.fon</td>
</tr>
<tr>
<td>BartPE</td>
<td>230-144-5 C:/WINDOWS/Prefetch</td>
</tr>
<tr>
<td>BartPE</td>
<td>240-128-3 C:/WINDOWS/Fonts/sserife.fon</td>
</tr>
<tr>
<td>BartPE</td>
<td>256-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP</td>
</tr>
<tr>
<td>BartPE</td>
<td>257-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP</td>
</tr>
<tr>
<td>BartPE</td>
<td>257-128-3 C:/Program Files/Outlook Express/wabfind.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>2576-128-3 C:/Program Files/Outlook Express/setup50.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>258-128-1 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING.VER</td>
</tr>
<tr>
<td>BartPE</td>
<td>2614-144-1 C:/Program Files/VMware</td>
</tr>
<tr>
<td>BartPE</td>
<td>26-144-2 C:/$Extend/$Reparse:$R</td>
</tr>
<tr>
<td>BartPE</td>
<td>2621-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf</td>
</tr>
<tr>
<td>BartPE</td>
<td>2622-128-4 C:/WINDOWS/Prefetch/NU2MENU.EXE-0BF39A50.pf</td>
</tr>
<tr>
<td>BartPE</td>
<td>2623-128-4 C:/WINDOWS/Prefetch/NC.EXE-13FC38B.pf</td>
</tr>
<tr>
<td>BartPE</td>
<td>2625-128-3 C:/WINDOWS/system32/CatRoot2/tmp.edb</td>
</tr>
<tr>
<td>BartPE</td>
<td>2626-128-1 C:/WINDOWS/system32/wbem/Logs/wbemprox.log</td>
</tr>
<tr>
<td>BartPE</td>
<td>2628-128-4 C:/WINDOWS/Prefetch/PSINFO.EXE-2865B84E.pf</td>
</tr>
<tr>
<td>BartPE</td>
<td>2629-128-4 C:/WINDOWS/Prefetch/WMIAPSRV.EXE-1E2270A5.pf</td>
</tr>
<tr>
<td>BartPE</td>
<td>2630-144-1 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache</td>
</tr>
<tr>
<td>BartPE</td>
<td>2633-144-1 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache/MetaData</td>
</tr>
<tr>
<td>BartPE</td>
<td>2635-144-1 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache/Content</td>
</tr>
<tr>
<td>BartPE</td>
<td>2637-128-5 C:/Documents and Settings/test/Application Data/Microsoft/CryptnetUrlCache/Content</td>
</tr>
</tbody>
</table>

---

Ricky D. Smith
## Live CDs in Incident Handling and Forensic

### Pros and Cons of Using Linux and Windows

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>Data/Microsoft/CryptnetUrlCache/MetaData/3C83474D61E624A4F9844DF935AFE217</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/AUTORUNSC.EXE-0B526252.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/IPCONFIG.EXE-319C45AD.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/TASKLIST.EXE-1EDF9DC5.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/PSLIST.EXE-24B5729E.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/PULIST.EXE-2C9B24D0.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/PSTAT.EXE-03795CAD.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/NET1.EXE-254DD783.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/NET.EXE-1E6CB345.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/NBTSTAT.EXE-322DB66D.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/ATTRIB.EXE-3786FA3B.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/Program Files/NetMeeting/nmwb.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/drivers/etc/hosts</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/Program Files/NetMeeting/conf.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/FPORTEX.E-XE-047242F3.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/CatRoot2/edb.log</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/CatRoot2/edb.chk</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/PCHealth/HelpCtr/Binaries/msinfo.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/Prefetch/CMDLINE.EXE-13480A5C.pdf</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/netmsg.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/ntbackup.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/Logs</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/config</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/stdole2.tlb</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/DataStore.db</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/drivers</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/accwiz.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/cabview.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/Program Files/VMware/VMware Tools/hook.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/cabinet.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/browseui.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/ras</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/repair/setup.log</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/Documents and Settings/test</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/boot.ini</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/Documents and Settings</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/Documents and Settings/All Users</td>
</tr>
<tr>
<td>BartPE</td>
<td>C:/WINDOWS/system32/CatRoot2</td>
</tr>
</tbody>
</table>

---

**Ricky D. Smith**

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

Ricky D. Smith

GCIH Gold
## Pros and Cons of Using Linux and Windows

### Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>574-128-3 C:/WINDOWS/system32/adslpc.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>5846-128-3 C:/WINDOWS/system32/zipfl dr.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>61-144-6 C:/WINDOWS/system32/wbem</td>
</tr>
<tr>
<td>BartPE</td>
<td>653-128-3 C:/WINDOWS/system32/deskadp.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>654-128-3 C:/WINDOWS/system32/desmon.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>655-128-3 C:/WINDOWS/system32/deskperf.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>685-128-3 C:/WINDOWS/system32/diskcopy.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>711-128-3 C:/WINDOWS/system32/docprop.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>742-128-3 C:/WINDOWS/system32/dskquoui.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>860-128-3 C:/WINDOWS/explorer.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>895-128-3 C:/WINDOWS/inf/unregmp2.exe</td>
</tr>
<tr>
<td>BartPE</td>
<td>906-128-3 C:/WINDOWS/system32/icmui.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>9580-144-6 C:/System Volume Information</td>
</tr>
<tr>
<td>BartPE</td>
<td>9629-128-3 C:/WINDOWS/system32/clusapi.dll</td>
</tr>
<tr>
<td>BartPE</td>
<td>9636-144-5 C:/Documents and Settings/test/Start Menu/Programs</td>
</tr>
<tr>
<td>BartPE</td>
<td>9637-144-1 C:/Documents and Settings/test/Start Menu/Programs/Startup</td>
</tr>
<tr>
<td>BartPE</td>
<td>9646-144-6 C:/Documents and Settings/test/Local Settings</td>
</tr>
<tr>
<td>BartPE</td>
<td>9661-144-6 C:/Documents and Settings/test/Application Data/Microsoft</td>
</tr>
<tr>
<td>BartPE</td>
<td>9664-144-1 C:/Documents and Settings/test/Application Data/Microsoft/SystemCertificates/My/CTLs</td>
</tr>
<tr>
<td>BartPE</td>
<td>9665-144-1 C:/Documents and Settings/test/Application Data/Microsoft/SystemCertificates/My/CRLs</td>
</tr>
<tr>
<td>BartPE</td>
<td>9666-144-1 C:/Documents and Settings/test/Application Data/Microsoft/SystemCertificates/My/Certificates</td>
</tr>
<tr>
<td>BartPE</td>
<td>9681-128-3 C:/Documents and Settings/test/Start Menu/Programs/Startup/desktop.ini</td>
</tr>
<tr>
<td>BartPE</td>
<td>9683-128-3 C:/Documents and Settings/test/Start Menu/Programs/desktop.ini</td>
</tr>
<tr>
<td>BartPE</td>
<td>9697-128-3 C:/Documents and Settings/test/Start Menu/desktop.ini</td>
</tr>
<tr>
<td>BartPE</td>
<td>982-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP</td>
</tr>
<tr>
<td>FIRE</td>
<td>1076-128-4 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP</td>
</tr>
<tr>
<td>FIRE</td>
<td>1106-128-4 C:/WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf</td>
</tr>
<tr>
<td>FIRE</td>
<td>1329-128-3 C:/WINDOWS/Fonts/arialbd.ttf</td>
</tr>
<tr>
<td>FIRE</td>
<td>1383-128-3 C:/WINDOWS/system32/msls31.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys</td>
</tr>
<tr>
<td>FIRE</td>
<td>15474-128-3 C:/WINDOWS/system32/drivers/fastfat.sys</td>
</tr>
<tr>
<td>FIRE</td>
<td>15496-128-3 C:/WINDOWS/system32/drivers/acpi.sys</td>
</tr>
<tr>
<td>FIRE</td>
<td>15498-128-3 C:/WINDOWS/system32/winspool.drw</td>
</tr>
<tr>
<td>FIRE</td>
<td>15503-128-3 C:/WINDOWS/system32/ulib.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15517-128-3 C:/WINDOWS/system32/samlib.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15520-128-3 C:/WINDOWS/system32/rasman.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15523-128-3 C:/WINDOWS/system32/rasapi32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15525-128-3 C:/WINDOWS/system32/perfctrrs.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15533-128-3 C:/WINDOWS/system32/msvl_0.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15545-128-3 C:/WINDOWS/system32/dhcppcsvc.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15561-128-3 C:/WINDOWS/system32/wzcsvc.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15563-128-3 C:/WINDOWS/system32/wzcsapi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15564-128-3 C:/WINDOWS/system32/wzcdig.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15565-128-3 C:/WINDOWS/system32/mtsapi32.dll</td>
</tr>
</tbody>
</table>

---

Ricky D. Smith  

© SANS Institute 2007,  
As part of the Information Security Reading Room  
Author retains full rights.
## Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRE</td>
<td>15568-128-3 C:/WINDOWS/system32/wssock32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15571-128-3 C:/WINDOWS/system32/wshtcip.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15579-128-3 C:/WINDOWS/system32/ws2help.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15581-128-3 C:/WINDOWS/system32/ws2_32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15601-128-3 C:/WINDOWS/system32/wmi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15610-128-3 C:/WINDOWS/system32/wldap32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15615-128-3 C:/WINDOWS/system32/winsta.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15616-128-3 C:/WINDOWS/system32/winsrv.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15619-128-3 C:/WINDOWS/system32/winrnr.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15627-128-3 C:/WINDOWS/system32/wininet.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15669-128-3 C:/WINDOWS/system32/urlmon.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15677-128-3 C:/WINDOWS/system32/upnp.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15709-128-3 C:/WINDOWS/system32/tapi32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15754-128-3 C:/WINDOWS/system32/snmpapi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15777-128-3 C:/WINDOWS/system32/shfolder.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15780-128-3 C:/WINDOWS/system32/shdocvw.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15781-128-3 C:/WINDOWS/system32/shdoclc.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15784-128-3 C:/WINDOWS/system32/sfc_os.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15786-128-3 C:/WINDOWS/system32/sfc.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15798-128-3 C:/WINDOWS/system32/secur32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>1580-128-3 C:/WINDOWS/system32/wbem/wmiutils.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15821-128-3 C:/WINDOWS/system32/rtutils.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15833-128-3 C:/WINDOWS/system32/riched20.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15835-128-3 C:/WINDOWS/system32/resutils.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15866-128-3 C:/WINDOWS/system32/rasadhlp.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15869-128-3 C:/WINDOWS/system32/query.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15884-128-3 C:/WINDOWS/system32/psapi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15901-128-3 C:/WINDOWS/system32/perfproc.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15902-128-3 C:/WINDOWS/system32/perfosl.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15904-128-3 C:/WINDOWS/system32/perfdisk.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15948-128-3 C:/WINDOWS/system32/ntmarta.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15957-128-3 C:/WINDOWS/system32/ntdsapi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15970-128-3 C:/WINDOWS/system32/netshell.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15974-128-3 C:/WINDOWS/system32/nettrap.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15977-128-3 C:/WINDOWS/system32/netman.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15983-128-3 C:/WINDOWS/system32/netcfgx.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15985-128-3 C:/WINDOWS/system32/netapi32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15987-128-3 C:/WINDOWS/system32/net1.exe</td>
</tr>
<tr>
<td>FIRE</td>
<td>15994-128-3 C:/WINDOWS/system32/ncobjapi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>15999-128-3 C:/WINDOWS/system32/mtxxclu.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>16008-128-3 C:/WINDOWS/system32/mswsock.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>16020-128-3 C:/WINDOWS/system32/msvcp60.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>16024-128-3 C:/WINDOWS/system32/msvbxm60.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>16046-128-3 C:/WINDOWS/system32/mspatcha.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>16065-128-3 C:/WINDOWS/system32/msimg32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>16077-128-3 C:/WINDOWS/system32/mshtml.dll</td>
</tr>
</tbody>
</table>
### Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/msdtcuiu.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/msdtcprx.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/mpapi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/mpr.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/mlang.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/mfc42u.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/loadperf.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/licwmi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/wbem/wmiprvse.exe</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/wbem/wmiprov.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/tapi perf.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/tasklist.exe</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/cfgmgr32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/Fonts/vgaoem.fon</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/rsvpperf.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/drivers/etc/services</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/wbem/mofd.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/wbem/framedyn.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/wbem/fastprox.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/cfgmgr32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/wbem/cimwin32.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/tapi perf.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>C:/WINDOWS/system32/tasklist.exe</td>
</tr>
</tbody>
</table>

Ricky D. Smith

GCIH Gold
## Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>FIRE</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>1993-128-3</td>
<td>C:/WINDOWS/system32/utilidll.dll</td>
</tr>
<tr>
<td>214-128-4</td>
<td>C:/WINDOWS/WindowsUpdate.log</td>
</tr>
<tr>
<td>222-128-3</td>
<td>C:/WINDOWS/Fonts/dosapp.fon</td>
</tr>
<tr>
<td>224-128-3</td>
<td>C:/WINDOWS/Fonts/ega40woa.fon</td>
</tr>
<tr>
<td>225-128-3</td>
<td>C:/WINDOWS/Fonts/cga80woa.fon</td>
</tr>
<tr>
<td>226-128-3</td>
<td>C:/WINDOWS/Fonts/cga40woa.fon</td>
</tr>
<tr>
<td>230-144-5</td>
<td>C:/WINDOWS/Prefetch</td>
</tr>
<tr>
<td>240-128-3</td>
<td>C:/WINDOWS/Fonts/sserife.fon</td>
</tr>
<tr>
<td>256-128-3</td>
<td>C:/WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP</td>
</tr>
<tr>
<td>257-128-3</td>
<td>C:/WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP</td>
</tr>
<tr>
<td>258-128-1</td>
<td>C:/WINDOWS/system32/wbem/Repository/FS/MAPPING.VER</td>
</tr>
<tr>
<td>2621-128-3</td>
<td>C:/Documents and Settings/test/Local Settings/Temp/-DF375.tmp</td>
</tr>
<tr>
<td>2622-128-4</td>
<td>C:/WINDOWS/Prefetch/FIRE.EXE-28F7DF6F.pdf</td>
</tr>
<tr>
<td>2623-128-4</td>
<td>C:/WINDOWS/Prefetch/CMD.EXE-339B0F65.pdf</td>
</tr>
<tr>
<td>2625-128-4</td>
<td>C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pdf</td>
</tr>
<tr>
<td>2626-128-4</td>
<td>C:/WINDOWS/Prefetch/NC.EXE-27A8D0F4.pdf</td>
</tr>
<tr>
<td>2628-128-4</td>
<td>C:/WINDOWS/Prefetch/IPCONFIG.EXE-28418EC3.pdf</td>
</tr>
<tr>
<td>2629-128-4</td>
<td>C:/WINDOWS/Prefetch/PSINFO.EXE-21A4D93B.pdf</td>
</tr>
<tr>
<td>2630-128-4</td>
<td>C:/WINDOWS/Prefetch/WMIAPSRV.EXE-1E2270A5.pdf</td>
</tr>
<tr>
<td>2633-128-4</td>
<td>C:/WINDOWS/Prefetch/TASKLIST.EXE-10D94B23.pdf</td>
</tr>
<tr>
<td>2635-128-4</td>
<td>C:/WINDOWS/Prefetch/PSLIST.EXE-25551EEB.pdf</td>
</tr>
<tr>
<td>2637-128-4</td>
<td>C:/WINDOWS/Prefetch/NET1.EXE-029B9DB4.pdf</td>
</tr>
<tr>
<td>2639-128-4</td>
<td>C:/WINDOWS/Prefetch/NET.EXE-338CD3B1.pdf</td>
</tr>
<tr>
<td>2640-128-4</td>
<td>C:/WINDOWS/Prefetch/NBTSTAT.EXE-1CFCA700.pdf</td>
</tr>
<tr>
<td>2641-128-4</td>
<td>C:/WINDOWS/Prefetch/ATTRIB.EXE-39EABF02.pdf</td>
</tr>
<tr>
<td>2651-128-4</td>
<td>C:/WINDOWS/Prefetch/AT.EXE-2770DD18.pdf</td>
</tr>
<tr>
<td>2654-128-4</td>
<td>C:/WINDOWS/Prefetch/NETSTAT.EXE-3B985F66.pdf</td>
</tr>
<tr>
<td>2664-128-4</td>
<td>C:/WINDOWS/Prefetch/FPORT.EXE-23BFDE24.pdf</td>
</tr>
<tr>
<td>272-128-3</td>
<td>C:/WINDOWS/system32/drivers/etc/hosts</td>
</tr>
<tr>
<td>282-128-3</td>
<td>C:/WINDOWS/system32/netmsg.dll</td>
</tr>
<tr>
<td>289-128-4</td>
<td>C:/WINDOWS/Prefetch/WMIPRVSE.EXE-28F301A9.pdf</td>
</tr>
<tr>
<td>292-128-3</td>
<td>C:/WINDOWS/system32/wpa.db1</td>
</tr>
<tr>
<td>298-144-1</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore</td>
</tr>
<tr>
<td>299-144-1</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/Logs</td>
</tr>
<tr>
<td>300-128-3</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log</td>
</tr>
<tr>
<td>30-144-5</td>
<td>C:/WINDOWS/system32/config</td>
</tr>
<tr>
<td>307-128-3</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk</td>
</tr>
<tr>
<td>308-128-4</td>
<td>C:/WINDOWS/SoftwareDistribution/DataStore/DataStore.edb</td>
</tr>
<tr>
<td>31-144-6</td>
<td>C:/WINDOWS/system32/drivers</td>
</tr>
<tr>
<td>3170-128-3</td>
<td>C:/Program Files/VMware/VMware Tools/hook.dll</td>
</tr>
<tr>
<td>317-128-3</td>
<td>C:/WINDOWS/system32/cabinet.dll</td>
</tr>
<tr>
<td>3325-128-3</td>
<td>C:/WINDOWS/repair/setup.log</td>
</tr>
<tr>
<td>3326-144-5</td>
<td>C:/Documents and Settings/test</td>
</tr>
<tr>
<td>3339-128-10</td>
<td>C:/boot.ini</td>
</tr>
<tr>
<td>342-128-3</td>
<td>C:/WINDOWS/system32/perfo009.dat</td>
</tr>
<tr>
<td>343-128-3</td>
<td>C:/WINDOWS/system32/perfh009.dat</td>
</tr>
</tbody>
</table>

Ricky D. Smith

© SANS Institute 2007, as part of the Information Security Reading Room. Author retains full rights.
## Pros and Cons of Using Linux and Windows

**Live CDs in Incident Handling and Forensic**

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRE</td>
<td>3787-144-6 C:/Program Files</td>
</tr>
<tr>
<td>FIRE</td>
<td>398-128-3 C:/WINDOWS/system32/actives.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>43-144-1 C:/WINDOWS/system32/drivers/etc</td>
</tr>
<tr>
<td>FIRE</td>
<td>459-128-3 C:/WINDOWS/system32/at1.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>466-128-3 C:/WINDOWS/system32/attrib.exe</td>
</tr>
<tr>
<td>FIRE</td>
<td>471-128-3 C:/WINDOWS/system32/at.exe</td>
</tr>
<tr>
<td>FIRE</td>
<td>477-128-3 C:/WINDOWS/system32/asycfilt.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>5224-144-5 C:/WINDOWS/system32/wbem/Logs</td>
</tr>
<tr>
<td>FIRE</td>
<td>5225-128-1 C:/WINDOWS/system32/wbem/Logs/FrameWork.log</td>
</tr>
<tr>
<td>FIRE</td>
<td>5231-128-3 C:/WINDOWS/system32/wbem/Logs/wmiprov.log</td>
</tr>
<tr>
<td>FIRE</td>
<td>5234-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.DATA</td>
</tr>
<tr>
<td>FIRE</td>
<td>5235-128-3 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.BTR</td>
</tr>
<tr>
<td>FIRE</td>
<td>5244-144-6 C:/Program Files/Internet Explorer</td>
</tr>
<tr>
<td>FIRE</td>
<td>533-128-3 C:/WINDOWS/system32/apphelp.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>546-128-3 C:/WINDOWS/system32/advpack.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>574-128-3 C:/WINDOWS/system32/adsldpc.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>61-144-6 C:/WINDOWS/system32/wbem</td>
</tr>
<tr>
<td>FIRE</td>
<td>9629-128-3 C:/WINDOWS/system32/clusapi.dll</td>
</tr>
<tr>
<td>FIRE</td>
<td>9647-144-1 C:/Documents and Settings/test/Local Settings/Temporary Internet Files</td>
</tr>
<tr>
<td>FIRE</td>
<td>9648-144-1 C:/Documents and Settings/test/Local Settings/Temporary Internet Files/Content.IE5</td>
</tr>
<tr>
<td>FIRE</td>
<td>9653-144-5 C:/Documents and Settings/test/Local Settings/Temp</td>
</tr>
<tr>
<td>FIRE</td>
<td>9654-144-1 C:/Documents and Settings/test/Local Settings/History</td>
</tr>
<tr>
<td>FIRE</td>
<td>9655-144-1 C:/Documents and Settings/test/Local Settings/History/History.IE5</td>
</tr>
<tr>
<td>FIRE</td>
<td>9659-144-1 C:/Documents and Settings/test/Cookies</td>
</tr>
<tr>
<td>FIRE</td>
<td>9706-128-4 C:/Documents and Settings/test/Local Settings/Temporary Internet Files/Content.IE5/index.dat</td>
</tr>
<tr>
<td>FIRE</td>
<td>9708-128-4 C:/Documents and Settings/test/Local Settings/History/History.IE5/index.dat</td>
</tr>
<tr>
<td>FIRE</td>
<td>9713-128-4 C:/Documents and Settings/test/Cookies/index.dat</td>
</tr>
<tr>
<td>FIRE</td>
<td>982-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP</td>
</tr>
<tr>
<td>Helix</td>
<td>1076-128-4 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP</td>
</tr>
<tr>
<td>Helix</td>
<td>1106-128-4 C:/WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>1329-128-3 C:/WINDOWS/Fonts/arialbd.ttf</td>
</tr>
<tr>
<td>Helix</td>
<td>15464-128-3 C:/WINDOWS/system32/drivers/ipnat.sys</td>
</tr>
<tr>
<td>Helix</td>
<td>15496-128-3 C:/WINDOWS/system32/drivers/acpi.sys</td>
</tr>
<tr>
<td>Helix</td>
<td>15498-128-3 C:/WINDOWS/system32/winspool drv</td>
</tr>
<tr>
<td>Helix</td>
<td>15503-128-3 C:/WINDOWS/system32/ulib.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15517-128-3 C:/WINDOWS/system32/samlib.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15520-128-3 C:/WINDOWS/system32/rasman.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15523-128-3 C:/WINDOWS/system32/rasapi32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15525-128-3 C:/WINDOWS/system32/perfctrs.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15533-128-3 C:/WINDOWS/system32/msvl_0.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15545-128-3 C:/WINDOWS/system32/dhcppsvc.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15561-128-3 C:/WINDOWS/system32/wzcsvc.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15563-128-3 C:/WINDOWS/system32/wzcsapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15564-128-3 C:/WINDOWS/system32/wzcdlg.dll</td>
</tr>
</tbody>
</table>

---

**Ricky D. Smith**

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
## Live CDs in Incident Handling and Forensic Analysis

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helix</td>
<td>15565-128-3 C:/WINDOWS/system32/wtsapi32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15568-128-3 C:/WINDOWS/system32/wssock32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15571-128-3 C:/WINDOWS/system32/wshtcpip.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15579-128-3 C:/WINDOWS/system32/ws2help.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15581-128-3 C:/WINDOWS/system32/ws2_32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15601-128-3 C:/WINDOWS/system32/wmi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15610-128-3 C:/WINDOWS/system32/wldap32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15615-128-3 C:/WINDOWS/system32/winsta.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15616-128-3 C:/WINDOWS/system32/winsrv.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15619-128-3 C:/WINDOWS/system32/winrnr.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15627-128-3 C:/WINDOWS/system32/wininet.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15643-128-3 C:/WINDOWS/system32/wdmaud drv</td>
</tr>
<tr>
<td>Helix</td>
<td>15669-128-3 C:/WINDOWS/system32/urlmon.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15677-128-3 C:/WINDOWS/system32/upnp.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15709-128-3 C:/WINDOWS/system32/tapi32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15754-128-3 C:/WINDOWS/system32/snmpapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15777-128-3 C:/WINDOWS/system32/shfolder.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15784-128-3 C:/WINDOWS/system32/sfc_os.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15786-128-3 C:/WINDOWS/system32/sfc.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15798-128-3 C:/WINDOWS/system32/secur32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1580-128-3 C:/WINDOWS/system32/wbem/wmiutils.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15821-128-3 C:/WINDOWS/system32/rututils.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15835-128-3 C:/WINDOWS/system32/resutils.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15866-128-3 C:/WINDOWS/system32/rasadhlp.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15869-128-3 C:/WINDOWS/system32/query.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15884-128-3 C:/WINDOWS/system32/psapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15901-128-3 C:/WINDOWS/system32/perfproc.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15902-128-3 C:/WINDOWS/system32/perfos.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15904-128-3 C:/WINDOWS/system32/perfdisk.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15911-128-3 C:/WINDOWS/system32/olepro32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1593-128-3 C:/WINDOWS/system32/oledlg.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15948-128-3 C:/WINDOWS/system32/ntmarta.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15957-128-3 C:/WINDOWS/system32/ntdsapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15970-128-3 C:/WINDOWS/system32/netshell.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15974-128-3 C:/WINDOWS/system32/nettrap.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15977-128-3 C:/WINDOWS/system32/netman.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15983-128-3 C:/WINDOWS/system32/ntcfgx.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15985-128-3 C:/WINDOWS/system32/netapi32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15987-128-3 C:/WINDOWS/system32/net1.exe</td>
</tr>
<tr>
<td>Helix</td>
<td>15994-128-3 C:/WINDOWS/system32/ncobjapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>15999-128-3 C:/WINDOWS/system32/mtxclu.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16008-128-3 C:/WINDOWS/system32/mswsock.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16020-128-3 C:/WINDOWS/system32/msvcp60.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16046-128-3 C:/WINDOWS/system32/mspatcha.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16065-128-3 C:/WINDOWS/system32/msimg32.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16086-128-3 C:/WINDOWS/system32/msdtcui.dll</td>
</tr>
</tbody>
</table>

Ricky D. Smith
<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helix</td>
<td>16088-128-3 C:/WINDOWS/system32/msdtcprx.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16109-128-3 C:/WINDOWS/system32/mprapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16132-128-3 C:/WINDOWS/system32/midimap.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16136-128-3 C:/WINDOWS/system32/mfc42u.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16156-128-3 C:/WINDOWS/system32/loadperf.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1616-128-3 C:/WINDOWS/system32/wbem/wmiprovse.exe</td>
</tr>
<tr>
<td>Helix</td>
<td>16190-128-3 C:/WINDOWS/system32/iphlpapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16202-128-3 C:/WINDOWS/system32/inetmib1.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1622-128-3 C:/WINDOWS/system32/wbem/wmiprov.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16235-128-3 C:/WINDOWS/system32/hnetcfg.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1624-128-3 C:/WINDOWS/system32/perfsets.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16263-128-3 C:/WINDOWS/system32/esent.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1628-128-3 C:/WINDOWS/system32/perfcts.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16290-128-3 C:/WINDOWS/system32/dsound.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16318-128-3 C:/WINDOWS/system32/dnsapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16357-128-3 C:/WINDOWS/system32/dbghelp.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16385-128-3 C:/WINDOWS/system32/credui.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1668-128-3 C:/WINDOWS/system32/wbem/wmiapsrv.exe</td>
</tr>
<tr>
<td>Helix</td>
<td>16758-128-3 C:/WINDOWS/system32/wups.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16762-128-3 C:/WINDOWS/system32/wuaueng.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16763-128-3 C:/WINDOWS/system32/wuauclrt.cpl</td>
</tr>
<tr>
<td>Helix</td>
<td>16765-128-3 C:/WINDOWS/system32/wuauclt.exe</td>
</tr>
<tr>
<td>Helix</td>
<td>16780-128-3 C:/WINDOWS/system32/winhttp.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1682-128-3 C:/WINDOWS/system32/wbem/wmiaprpl.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1683-128-3 C:/WINDOWS/system32/wbemwmiapres.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>16897-128-3 C:/WINDOWS/system32/drivers/mssmbios.sys</td>
</tr>
<tr>
<td>Helix</td>
<td>16900-128-3 C:/WINDOWS/system32/drivers/intelppm.sys</td>
</tr>
<tr>
<td>Helix</td>
<td>16901-128-3 C:/WINDOWS/system32/drivers/http.sys</td>
</tr>
<tr>
<td>Helix</td>
<td>1691-128-3 C:/WINDOWS/system32/rasctrs.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1696-128-3 C:/WINDOWS/system32/wbemsvc.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1703-128-3 C:/WINDOWS/system32/bemprox.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1735-128-3 C:/WINDOWS/system32/wbemcomm.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>175-128-3 C:/WINDOWS/Fonts/vgaoem.fon</td>
</tr>
<tr>
<td>Helix</td>
<td>1765-128-3 C:/WINDOWS/system32/rsvpperf.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1813-128-3 C:/WINDOWS/system32/drivers/etc/services</td>
</tr>
<tr>
<td>Helix</td>
<td>1816-128-3 C:/WINDOWS/system32/wbem/mofd.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1833-128-3 C:/WINDOWS/system32/wbem/fastprox.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1924-128-3 C:/WINDOWS/system32/tapiperf.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>1993-128-3 C:/WINDOWS/system32/utildll.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>2141-128-3 C:/WINDOWS/Fonts/Windows XP Ding.wav</td>
</tr>
<tr>
<td>Helix</td>
<td>214-128-4 C:/WINDOWS/WindowsUpdate.log</td>
</tr>
<tr>
<td>Helix</td>
<td>222-128-3 C:/WINDOWS/Fonts/dosapp.fon</td>
</tr>
<tr>
<td>Helix</td>
<td>224-128-3 C:/WINDOWS/Fonts/ega40woa.fon</td>
</tr>
<tr>
<td>Helix</td>
<td>225-128-3 C:/WINDOWS/Fonts/cga80woa.fon</td>
</tr>
<tr>
<td>Helix</td>
<td>226-128-3 C:/WINDOWS/Fonts/cga40woa.fon</td>
</tr>
<tr>
<td>Helix</td>
<td>230-144-5 C:/WINDOWS/Prefetch</td>
</tr>
</tbody>
</table>
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helix</td>
<td>240-128-3 C:/WINDOWS/Fonts/sserife.fon</td>
</tr>
<tr>
<td>Helix</td>
<td>256-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP</td>
</tr>
<tr>
<td>Helix</td>
<td>257-128-3 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP</td>
</tr>
<tr>
<td>Helix</td>
<td>258-128-1 C:/WINDOWS/system32/wbem/Repository/FS/MAPPING.VER</td>
</tr>
<tr>
<td>Helix</td>
<td>2621-144-1 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1</td>
</tr>
<tr>
<td>Helix</td>
<td>2622-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/arial_1.TTF</td>
</tr>
<tr>
<td>Helix</td>
<td>2623-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/arial_1.FON</td>
</tr>
<tr>
<td>Helix</td>
<td>2625-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/ARIAL_1.TTF</td>
</tr>
<tr>
<td>Helix</td>
<td>2626-128-3 C:/Documents and Settings/test/Local Settings/Temp/_ir_tmpfnt_1/ARIAL_1.FON</td>
</tr>
<tr>
<td>Helix</td>
<td>2628-128-4 C:/WINDOWS/Prefetch/HELIX.EXE-2AC0706C.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2629-128-4 C:/WINDOWS/Prefetch/LS.EXE-0EACACF4.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2630-128-4 C:/WINDOWS/Prefetch/CMD.EXE-31FFA378.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2633-128-4 C:/WINDOWS/Prefetch/HORE.EXE-1CE4AB20.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2635-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2637-128-4 C:/WINDOWS/Prefetch/NC.EXE-22B21017.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2639-128-1 C:/WINDOWS/system32/wbem/Logs/wbemprox.log</td>
</tr>
<tr>
<td>Helix</td>
<td>2640-128-4 C:/WINDOWS/Prefetch/PSINFO.EXE-3ADEAEEF.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2641-128-4 C:/WINDOWS/Prefetch/WMIAPSERV.EXE-1E2270A5.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2651-128-4 C:/WINDOWS/Prefetch/IPCONFIG.EXE-2A403659.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2654-128-4 C:/WINDOWS/Prefetch/PSSLIST.EXE-372E93F.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2664-128-4 C:/WINDOWS/Prefetch/NET1.EXE-029B9DB4.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2665-128-4 C:/WINDOWS/Prefetch/NET.EXE-02C522BD.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2667-128-4 C:/WINDOWS/Prefetch/NBTSTAT.EXE-1F49A3E4.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2674-128-4 C:/WINDOWS/Prefetch/ATTRIB.EXE-2DD00289.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2681-128-4 C:/WINDOWS/Prefetch/AT.EXE-0432F398.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2688-128-4 C:/WINDOWS/Prefetch/NETSTAT.EXE-10EBC1A8.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>272-128-3 C:/WINDOWS/system32/drivers/etc/hosts</td>
</tr>
<tr>
<td>Helix</td>
<td>2738-128-4 C:/WINDOWS/Prefetch/FFPORT.EXE-287E45A5.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2739-128-4 C:/WINDOWS/Prefetch/CMDLINE.EXE-1D2AD11F.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>277-128-3 C:/WINDOWS/system32/msacm32.drv</td>
</tr>
<tr>
<td>Helix</td>
<td>282-128-3 C:/WINDOWS/system32/netmsg.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>289-128-4 C:/WINDOWS/Prefetch/WMIPRVSE.EXE-28F301A9.pf</td>
</tr>
<tr>
<td>Helix</td>
<td>2935-128-3 C:/WINDOWS/system32/ksuser.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>298-144-1 C:/WINDOWS/SoftwareDistribution/DataStore</td>
</tr>
<tr>
<td>Helix</td>
<td>299-144-1 C:/WINDOWS/SoftwareDistribution/DataStore/Logs</td>
</tr>
<tr>
<td>Helix</td>
<td>300-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log</td>
</tr>
<tr>
<td>Helix</td>
<td>30-144-5 C:/WINDOWS/system32/config</td>
</tr>
<tr>
<td>Helix</td>
<td>307-128-3 C:/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk</td>
</tr>
<tr>
<td>Helix</td>
<td>308-128-4 C:/WINDOWS/SoftwareDistribution/DataStore/DataStore.edb</td>
</tr>
<tr>
<td>Helix</td>
<td>31-144-6 C:/WINDOWS/system32/drivers</td>
</tr>
<tr>
<td>Helix</td>
<td>3170-128-3 C:/Program Files/VMware/VMware Tools/hook.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>317-128-3 C:/WINDOWS/system32/cabinet.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>33-144-1 C:/WINDOWS/system32/ras</td>
</tr>
<tr>
<td>Helix</td>
<td>3326-144-5 C:/Documents and Settings/test</td>
</tr>
</tbody>
</table>
## Live CDs in Incident Handling and Forensic Analysis

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helix</td>
<td>3345-144-6 C:/Documents and Settings</td>
</tr>
<tr>
<td>Helix</td>
<td>3347-144-6 C:/Documents and Settings/All Users</td>
</tr>
<tr>
<td>Helix</td>
<td>342-128-3 C:/WINDOWS/system32/perfc009.dat</td>
</tr>
<tr>
<td>Helix</td>
<td>343-128-3 C:/WINDOWS/system32/perfh009.dat</td>
</tr>
<tr>
<td>Helix</td>
<td>380-128-3 C:/WINDOWS/Fonts/verdanab.ttf</td>
</tr>
<tr>
<td>Helix</td>
<td>398-128-3 C:/WINDOWS/system32/activeds.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>43-144-1 C:/WINDOWS/system32/drivers/etc</td>
</tr>
<tr>
<td>Helix</td>
<td>4466-128-3 C:/WINDOWS/system32/drivers/es1371mp.sys</td>
</tr>
<tr>
<td>Helix</td>
<td>4491-144-1 C:/Documents and Settings/All Users/Application Data/Microsoft/Network/Connections/Pbk</td>
</tr>
<tr>
<td>Helix</td>
<td>459-128-3 C:/WINDOWS/system32/atl.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>463-128-3 C:/WINDOWS/system32/atmfd.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>5224-144-5 C:/WINDOWS/system32/wbem/Logs</td>
</tr>
<tr>
<td>Helix</td>
<td>5224-144-5 C:/WINDOWS/system32/wbem/Logs</td>
</tr>
<tr>
<td>Helix</td>
<td>5231-128-3 C:/WINDOWS/system32/wbem/Logs/wmiprov.log</td>
</tr>
<tr>
<td>Helix</td>
<td>5234-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.DATA</td>
</tr>
<tr>
<td>Helix</td>
<td>5235-128-3 C:/WINDOWS/system32/wbem/Repository/FS/INDEX.BTR</td>
</tr>
<tr>
<td>Helix</td>
<td>533-128-3 C:/WINDOWS/system32/apphelp.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>546-128-3 C:/WINDOWS/system32/advpack.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>574-128-3 C:/WINDOWS/system32/adsldpc.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>61-144-6 C:/WINDOWS/system32/wbem</td>
</tr>
<tr>
<td>Helix</td>
<td>9629-128-3 C:/WINDOWS/system32/clusapi.dll</td>
</tr>
<tr>
<td>Helix</td>
<td>9653-144-5 C:/Documents and Settings/test/Local Settings/Temp</td>
</tr>
<tr>
<td>Helix</td>
<td>982-128-4 C:/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP</td>
</tr>
</tbody>
</table>

**INSERT**

- 1298-128-3 C:/WINDOWS/Fonts/times.ttf
- 1383-128-3 C:/WINDOWS/system32/msls31.dll
- 15616-128-3 C:/WINDOWS/system32/winsrv.dll
- 15627-128-3 C:/WINDOWS/system32/wininet.dll
- 15669-128-3 C:/WINDOWS/system32/urlmon.dll
- 15671-128-3 C:/WINDOWS/system32/url.dll
- 15717-128-3 C:/WINDOWS/system32/sxs.dll
- 15780-128-3 C:/WINDOWS/system32/shdocvw.dll
- 15781-128-3 C:/WINDOWS/system32/shdoclic.dll
- 15798-128-3 C:/WINDOWS/system32/security.dll
- 15833-128-3 C:/WINDOWS/system32/ rigged20.dll
- 16063-128-3 C:/WINDOWS/system32/msimt.dll
- 16073-128-3 C:/WINDOWS/system32/msi.dll
- 16077-128-3 C:/WINDOWS/system32/mshlink.dll
- 16077-128-3 C:/WINDOWS/system32/mshlink.dll
- 16095-128-3 C:/WINDOWS/system32/msctf.dll
- 16130-128-3 C:/WINDOWS/system32/mlang.dll
- 16206-128-3 C:/WINDOWS/system32/imm32.dll
- 16369-128-3 C:/WINDOWS/system32/cscui.dll
- 16372-128-3 C:/WINDOWS/system32/cscdll.dll
- 17131-128-3 C:/Program Files/Messenger/mmsmsgs.exe
- 175-128-3 C:/WINDOWS/Fonts/vgaoem.fon
- 222-128-3 C:/WINDOWS/Fonts/dosapp.fon

---

Ricky D. Smith
Pros and Cons of Using Linux and Windows  
Live CDs in Incident Handling and Forensic  

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

*Ricky D. Smith*  

56
## Pros and Cons of Using Linux and Windows

### Live CDs in Incident Handling and Forensic

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator 15774-128-3</td>
<td>C:/WINDOWS/system32/shimgvw.dll</td>
</tr>
<tr>
<td>Operator 15884-128-3</td>
<td>C:/WINDOWS/system32/psapi.dll</td>
</tr>
<tr>
<td>Operator 2621</td>
<td>&lt;Operator_WXP_data.img-2cg8crtk.TMP-dead-2621&gt;</td>
</tr>
<tr>
<td>Operator 325-128-3</td>
<td>C:/WINDOWS/system32/browselc.dll</td>
</tr>
<tr>
<td>Operator 325-128-3</td>
<td>C:/WINDOWS/system32/SET483.tmp (deleted-realloc)</td>
</tr>
</tbody>
</table>
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

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

9 Linux Virtual Machine

/bin/bash
/bin/cut
/bin/egrep
/bin/grep
/bin/mount
/bin/sh -> bash
/bin/stty
/dev/cdrom -> /dev/scd0
/etc/.nsswitch.conf.swx (deleted-realloc)
/etc/bashrc
/etc/DIR.COLORS.xterm
/etc/fonts/fonts.conf
/etc/fstab
/etc/fstab.NEW (deleted-realloc)
/etc/gnome-vfs-2.0/modules/default-modules.conf
/etc/gnome-vfs-2.0/modules/extra-modules.conf
/etc/gnome-vfs-2.0/modules/font-method.conf
/etc/gnome-vfs-2.0/modules/help-methods.conf
/etc/gnome-vfs-2.0/modules/mapping-modules.conf
/etc/gnome-vfs-2.0/modules/mapping-modules.conf;40012009 (deleted-realloc)
/etc/gnome-vfs-2.0/modules/ssl-modules.conf
/etc/group
/etc/gtk-2.0/gdk-pixbuf.loaders
/etc/gtk-2.0/gtk.immodules
/etc/gtk-2.0/gtkrc
/etc/gtk-2.0/gtkrc;40012009 (deleted-realloc)
/etc/host.conf
/etc/hosts
/etc/inputrc
/etc/ld.so.cache
/etc/modules.conf
/etc/mtab
/etc/mtab- (deleted-realloc)
/etc/nsswitch.conf
/etc/pango/pango.modules
/etc/passwd
/etc/profile.d
/etc/profile.d/atrmps.sh
/etc/profile.d/colorls.sh
/etc/profile.d/colorls.sh;43cc0503 (deleted-realloc)
/etc/profile.d/glib2.sh
/etc/profile.d/gnome-ssh-askpass.sh
/etc/profile.d/gnome-ssh-askpass.sh;43cc0503 (deleted-realloc)

Ricky D. Smith

58
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

Ricky D. Smith
Pros and Cons of Using Linux and Windows
Live CDs in Incident Handling and Forensic

GCIH Gold

Ricky D. Smith

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
Pros and Cons of Using Linux and Windows

Live CDs in Incident Handling and Forensic

/GCIH Gold

/Ricky D. Smith

62
Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensic

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.

<table>
<thead>
<tr>
<th>Live CD</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>BartPE</td>
<td>/2/bin/ls</td>
</tr>
<tr>
<td>BartPE</td>
<td>/2/etc/localtime</td>
</tr>
<tr>
<td>BartPE</td>
<td>/2/tmp/orbit-root/linc-96f-0-1aa79962a5c27</td>
</tr>
<tr>
<td>BartPE</td>
<td>/2/usr/lib/perl5/5.8.0/CGI/Carp.pm.newcgi (deleted-realloc)</td>
</tr>
<tr>
<td>BartPE</td>
<td>/2/usr/share/icons/Bluecurve/cursors/top_side</td>
</tr>
<tr>
<td>BartPE</td>
<td>/2/var/log/wtmp</td>
</tr>
<tr>
<td>BartPE</td>
<td>/2/var/run/utmp</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/bin/basename</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/bin/basename;43cc0503 (deleted-realloc)</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/bin/sed</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/bin/sleep</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/bin/uname</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/cron.hourly</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/cups/certs</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/cups/certs/0</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/localtime</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/rc.d/init.d/functions</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/services</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/sysconfig/init</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/sysconfig/network</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/sysconfig/networking/ifcfg-lo</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/sysconfig/network-scripts/ifcfg-eth0</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/sysconfig/network-scripts/ifcfg-lo -&gt; ../networking/ifcfg-lo</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/etc/sysconfig/network-scripts/network-functions</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/lib/libc.so.6 -&gt; libc-2.3.2.so</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/lib/libc-2.3.2.so</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/lib/modules/2.4.20-31.9/kernel/fs/nls/nls.iso8859-1.o</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/mnt</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/root/.gconfd</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/root/.gconfd/saved_state.orig (deleted)</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/sbin/dhclient-script</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/sbin/ifconfig</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/tmp/orbit-root/linc-96f-0-41d7400fa0924</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/usr</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/usr/bin</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/usr/bin/expr</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/usr/bin/nc</td>
</tr>
<tr>
<td>FIRE</td>
<td>/2/usr/bin/run-parts</td>
</tr>
</tbody>
</table>

Ricky D. Smith
Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensic

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

Ricky D. Smith

© SANS Institute 2007, as part of the Information Security Reading Room. Author retains full rights.
Pros and Cons of Using Linux and Windows Live CDs in Incident Handling and Forensic

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

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Madrid March 2020</td>
<td>Madrid, Spain</td>
<td>Mar 23, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Secure Canberra 2020</td>
<td>Canberra, Australia</td>
<td>Mar 23, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Oslo March 2020</td>
<td>Oslo, Norway</td>
<td>Mar 23, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Seattle Spring 2020</td>
<td>Seattle, WA</td>
<td>Mar 23, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Frankfurt March 2020</td>
<td>Frankfurt, Germany</td>
<td>Mar 30, 2020 - Apr 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Philadelphia 2020</td>
<td>Philadelphia, PA</td>
<td>Mar 30, 2020 - Apr 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Bethesda 2020</td>
<td>Bethesda, MD</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Minneapolis 2020</td>
<td>Minneapolis, MN</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Boston Spring 2020</td>
<td>Boston, MA</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>CS-Cybersecure Catalyst New Career Academy SEC504</td>
<td>Brampton, ON</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Brussels April 2020</td>
<td>Brussels, Belgium</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>CS-Cybersecure Catalyst New Canadians Academy SEC504</td>
<td>Brampton, ON</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS London April 2020</td>
<td>London, United Kingdom</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>CS Cybersecure Catalyst Women Academy SEC504</td>
<td>Brampton, ON</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2020</td>
<td>Austin, TX</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2020</td>
<td>Baltimore, MD</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Community SANS Nashville SEC542</td>
<td>Nashville, TN</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 06, 2020 - May 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam May 2020</td>
<td>Amsterdam, Netherlands</td>
<td>May 11, 2020 - May 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Hong Kong 2020</td>
<td>Hong Kong, Hong Kong</td>
<td>May 11, 2020 - May 16, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio 2020</td>
<td>San Antonio, TX</td>
<td>May 17, 2020 - May 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Northern Virginia- Alexandria 2020</td>
<td>Alexandria, VA</td>
<td>May 17, 2020 - May 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Autumn Sydney 2020</td>
<td>Sydney, Australia</td>
<td>May 18, 2020 - May 23, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Atlanta Spring 2020</td>
<td>Atlanta, GA</td>
<td>May 26, 2020 - May 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2020</td>
<td>CyberCast,</td>
<td>May 27, 2020 - Jun 03, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Rocky Mountain HackFest Summit &amp; Training 2020</td>
<td>Denver, CO</td>
<td>Jun 01, 2020 - Jun 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, IL</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Charlotte SEC504</td>
<td>Charlotte, NC</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Community SANS</td>
</tr>
</tbody>
</table>