At a glance:

- The Fundamental Computer Investigation Guide for Windows
- The Malware Removal Starter Kit
- Creating an investigation kit with Windows PE
- Preserving information for forensic analysis

A guide to basic computer forensics

Tom Cloward and Frank Simorjay

There are countless ways malicious people can use a computer to perform illegal activity – hacking into systems, leaking trade secrets, unleashing new viruses, using phishing messages to steal personal information, and so on. And we are constantly hearing about new exploits and techniques. What you don't hear about as often is all the ways computers can be used to investigate these sorts of activities.

While some investigations rely on highly trained professionals using expensive tools and complex techniques, there are easier, cheaper methods you can use for basic investigation and analysis. In this article, we will focus on computer forensic techniques that are readily accessible to you as a mainstream administrator.

Our discussion relies on two solution accelerators you can download for free: 'The Fundamental Computer Investigation Guide for Windows': *www.microsoft.com/uk/investigationguide* and The Malware Removal Starter Kit: *www.microsoft.com/uk/malware* In this article, we'll show you how you can combine these two solutions to build a bootable Windows® PE environment that will let you conduct an effective investigation and preserve your findings for reporting and analysis. Note that you can't use the method discussed here to investigate a hard drive that has been encrypted or that is part of a RAID volume. And if the hard drive is damaged, you'll need to perform additional steps ahead of time to restore its state.

Though our solution details an easy way to collect evidence from a Windows-based computer, it is nonetheless a basic, ad hoc approach. There are several more sophisticated solutions available commercially that can execute the work outlined here in a much more effective way.

Also keep in mind that the technique we discuss here is neither a guaranteed prescriptive solution nor certified by The International Society of Forensic Computer Examiners. Before beginning an investigation, you should consider whether evidence on the hard drive may potentially become part of a legal proceeding. If that possibility exists, a professionally certified computer examiner should be engaged to conduct the investigation. Depending on the nature of any potential legal proceedings, you must also consider whether to hand off the investigation directly to law enforcement officials. There is more information on this topic in 'The Fundamental Computer Investigation Guide for Windows'.

About the solution accelerators

'The Fundamental Computer Investigation Guide for Windows' discusses processes and tools you can use in an internal computer investigation. The guide outlines the four phases of the computer investigation model: assess, acquire, analyse and report. This is a handy model that can help IT professionals conduct investigations in a manner that preserves important findings.

This guide also covers when it's necessary to involve law enforcement officials – you should include your legal advisers when making this decision. You'll find information about managing computer-related crimes, how to contact the appropriate law enforcement agencies, and the Windows Sysinternals tools and other Windows tools that are useful in conducting investigations.

The other solution accelerator we reference in this article, The Malware Removal Starter Kit, provides guidance on how to build and use a bootable Windows PE CD-ROM to remove malware from a computer. This guide includes a list of threats and some of the mitigations that can help reduce their potential impact on an organisation. It also stresses the importance of developing an incident response plan that can be followed in case a malware outbreak is suspected. The Malware Removal Starter Kit also includes a four stage approach to help an IT professional determine the nature of the malware involved, limit its spread, remove it if possible, verify the removal and proceed with any next steps that may be required.

The Windows PE CD-ROM

There are two prerequisites for running an investigation of this sort: a Windows PE CD-ROM and an external storage device, such as a USB flash drive.

You've probably watched enough television to know that police officers should leave a crime scene unaltered. Well, for the same reason, you want to preserve the data on the hard drive being investigated. Unlike the Malware Removal Starter Kit disc, the bootable Windows PE disc we are building will only run tools in a manner that won't alter the hard drive data in any manner.

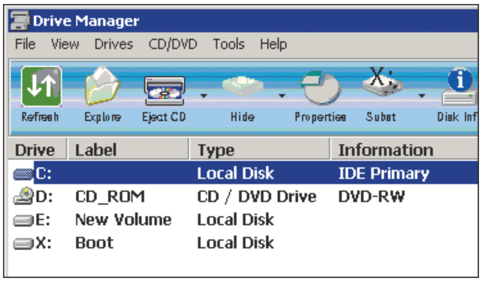
The Windows PE disc will boot the system into a limited Windows environment. When you create this bootable CD, you can include tools (such as in the Malware Removal Starter Kit) that are configured up-front for a special purpose. Note that the computer must have at least 512MB of RAM – this is a Windows PE requirement.

The process of building the Windows PE CD-ROM, which is detailed in The Malware Removal Starter Kit, is fairly straightforward. Before you build this bootable disc, you'll need to install the Windows Automated Installation Kit (AIK), the Sysinternals Suite, available at: *www.microsoft.com/uk/internalsuite* place the Sysinternals tools in your tool list as outlined in Task 2 of The Malware Removal Starter Kit, and install any other malware-scanning tools and utilities. For detailed instructions on creating the disc, use the steps outlined in The Malware Removal Starter Kit document.

The external USB drive

Since this process will not alter the drive being investigated, you'll also need a USB

Before beginning an investigation, consider whether evidence on the hard drive may potentially become part of a legal proceeding



Drive	Label	Type	Information
C:		Local Disk	IDE Primary
D:	CD_ROM	CD / DVD Drive	DVD-RW
E:	New Volume	Local Disk	
X:	Boot	Local Disk	

Figure 1 **Viewing disk information with Drive Manager**

thumb drive or some other kind of external hard drive so you can store the output files that will be generated. (A USB thumb drive is the recommended media since Windows PE can mount USB devices automatically.) You may also want to use an external hard drive to store an image of the original hard drive. With all of these requirements and options, it's quite important that you plan ahead to take into account the total disk space the investigation will require.

Because you want to ensure that the kit is clean when you start an investigation, all previous data needs to be completely removed from the external disk drive you are going to use to save the investigation files. This can easily be done with a disk wiping utility that overwrites the entire writeable drive surface. The external disk can then be formatted and labelled as necessary for use in the investigation. This precaution ensures that the device will contain no files that could possibly contaminate the evidence you gather during the investigation.

You should also include a chain-of-custody form so there will be official documentation regarding who has handled the computer throughout the investigation. 'The Fundamental Computer Investigation Guide for Windows' provides a sample chain-of-custody form. After you've finished packaging the kit (with the necessary bootable Windows PE disc, external storage device and a chain-of-custody form) you are ready to proceed.

Running an investigation

Now you're ready to perform an investigation. First, boot the suspect system using the Windows PE disc, making sure that the computer's boot order identifies the CD-ROM drive as the primary boot device. When prompted, press any key to complete the boot from CD-ROM. This will provide access to the tools you installed on the disc.

We will use our kit on a sample machine to demonstrate how you can collect information from a computer (which we will call Testbox1). The CD drive assignment on Testbox1 is X:\ and the default location provided for the tools from the Malware Removal Starter Kit is X:\tools. To access the tools in the kit, we simply type: cd \tools.

There are several tools that can identify the target drives mounted on a computer. Bginfo.exe, which is located in the Sysinternals tool directory, can provide this information and place it in a background window on the desktop for easy reference. Drive Manager can also identify all the drives on the computer, including the target hard disk drives and the external USB device. **Figure 1** shows the disk information for Testbox1. The boot drive is X:\, the target hard drive is C:\, and our external USB drive is F:\.

Checking for malware

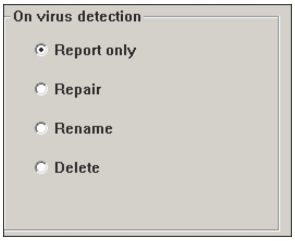
It is important to run anti-malware tools before you begin an investigation to ensure that the investigation isn't tainted by a virus or other malicious code. The report that the anti-malware tool generates can be used as evidence, if needed. But not checking a computer for malware can jeopardise the investigation, as well as the examiner's credibility for thoroughness and accuracy. We recommend that you run the provided anti-malware tools in a read-only or reporting mode.

The Malware Removal Starter Kit discusses a number of recommended tools, including the Malicious Software Removal Tool and McAfee AVERT Stinger. When you run the Malicious Software Removal Tool be sure to include the command-line option /N to instruct the tool to only report on malware and not try to remove it:

```
x:\tools\windows-KB890830-v1.29.exe /N
```

The resulting report file will be located in %windir%\debug\mrt.log.

Likewise, when you run McAfee AVERT Stinger, change the preference to Report only, as shown in **Figure 2**, so that it will scan the computer but not make any changes to the hard drive. And be sure to save a report from the tool when the scan is complete.



On virus detection

● Report only

○ Repair

○ Rename

○ Delete

Figure 2 **Use Report only mode in McAfee AVERT Stinger**

Figure 3 **Tools to locate files and data of interest**

Application	Description
AccessChk	Displays access to files, registry keys and Windows services by the user or group you specify.
AccessEnum	Displays who has access to which directories, files and registry keys on a computer. You can use this to find places where permissions aren't properly applied.
Du	Displays disk usage by directory.
PsInfo	Displays information about a computer.
Strings	Searches for ANSI and UNICODE strings in binary images.

Saving critical files

If the entire disk was not backed up before you began the investigation, you should at least back up key user files. Configuration information can be used for future review if needed. Begin by collecting the registry files and settings, which contain all relevant information about how the computer has been used and what software is installed on the system.

To save the registry hive for Testbox1, we first create a folder on the removable F:\ drive and then record the date and time when the investigation started by using the following commands:

```
f:
Mkdir f:\evidence_files
Date /t >> f:\evidence_files\Evidence_start.txt
Time /t >> f:\evidence_files\Evidence_start.txt
```

Now we save the registry hive using the xcopy command to copy the entire configuration directory and its contents. The registry files you'll be interested in are located in %windows%\system32\config. In our case, we run the following:

```
xcopy c:\windows\system32\config\*.* f:\registrybkup
/s /e /k /v
```

This command copies all the configuration information located in the config folder. Textbox1 contains approximately 95MB of information in the config folder.

Next, focus on user data, which can be located anywhere on the hard disk. For our sample, we are copying only data from a directory called c:\HR. To ensure the data is collected completely, we copy all the data in the directory and its sub-directories using the following xcopy command:

```
Mkdir f:\evidence_files\HR_Evidence
Mkdir f:\evidence_files\documents_and_settings
Mkdir f:\evidence_files\users
xcopy c:\HR\*.* f:\evidence_files\HR_Evidence /s /e
/k /v
```

Now you can focus on personal folder information. Again, we want to copy all the data from these directories and their sub-directories. To do this, we use the following commands:

```
Xcopy c:\documents and settings\*.* f:\evidence_files\
documents_and_settings /s /e /k /v

Xcopy c:\users\*.* f:\evidence_files\users /s /e /k /v
```

This sample collected about 500MB of data, which we can now analyse if necessary. As you can see, the amount of data you are collecting can be enormous – especially if you encounter audio files, videos and photos. Still, it is important to preserve as much original data as possible because an investigation may require not only the evidence you physically collect, but also the assurance that this information has not been altered during the collection process. Ideally, you should do a full disk image for your investigation, but this can be difficult due to size constraints. Needless to say, you can see why it's important to scope out ahead of time just how much storage space your investigation is likely to require.

Gathering additional information

System files can also be a useful asset in the evidence collection, but gathering this data may require some exploration of the target computer since these files may not always be located in the same place. Still, certain types of files are worth looking for because they can provide useful insight. Swap files, for instance, contain information about what files have been accessed by memory. Furthermore, swap files can even provide detailed usage activity. Similarly, Web browser data and cookies offer information about browsing behaviour and patterns.

Finding this data may require some detective work, especially if a user has changed his configuration to store data somewhere other than in the default locations. There are several Sysinternals tools that can help you find critical files. **Figure 3** lists five useful applications and describes how they can help your investigation. ■

Tom Cloward, *CCE, CISSP, is Program Manager at Microsoft, focused on delivering security and compliance solution accelerators for IT professionals. He has worked in the software and IT industries for over 15 years and has a passion for IT security, forensics and compliance.*

Frank Simorjay, *CISSP, CET, is a Technical Program Manager and security subject matter expert for the Microsoft Solution Accelerator – Security and Compliance group. He designs security solutions for Microsoft customers. His most recent work is the Malware Removal Starter Kit, available on Microsoft TechNet.*