



ISMAEL VALENZUELA

My ERP Got Hacked – An Introduction to Computer Forensics, Part II

Difficulty



In Part I of this article we introduced the scenario described in the Third Forensic Challenge organised by the UNAM-CERT (Mexico) back in 2006.

After describing how to set up a forensic lab and how to best perform the initial response, part II of this article will continue illustrating in practice the methods, techniques and tools used to investigate and analyse the digital evidence found during the course of a computer forensic investigation. Now we are finally getting closer to know if there was any unauthorised access to the Web-based *Enterprise Resource Planning* (ERP) server, how it happened and what was the extent of the damage...

Investigation and Analysis

At the end of Part I we described how to use *Regripper* and the *rip.pl* tool to parse key Windows Registry files such as *SYSTEM*, *SOFTWARE*, *SECURITY* and *SAM*. However, there is still a file that is part of the registry that we have not analysed yet, *NTUSER.DAT*.

Initial Reconnaissance

Each of the users extracted from the *SAM* registry hive (listed in part I), will have their own section of the registry contained in that particular file, stored under the *Documents and Settings\USERNAME* folder. Thus, we can use the *rip.pl* tool to enumerate the most recently used files, last files the user had searched for on the drive, last typed URLs, last saved files and even last commands executed on the system.

Here is the command used to retrieve all this information from *ver0k* home user folder, and an excerpt of the report (see Listing 1).

Looking at the details in the Listing 1, a forensic examiner can gain a better understanding of what types of files or applications have been accessed on the system. In this case, we can see the activity of the suspect *ver0k* account a little while after the account was created on the system. Some of these activities include:

- Typed the following URL on the browser (MSN home page) at 20:47: `http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome`.
- Ran the *MySQL Administrator* at 20:48.
- Browsed the Administrator home folder, executing many *.exe* files from 21:28 to 21:39.
- Ran *MSN Messenger* at 21:59.

It is also interesting to notice the information stored under the registry key *ComDlg32\OpenSaveMRU*. The *ComDlg32* control is used in many applications and saves its own set of history information separate from other Windows history. Every time a file is saved to the system, it keeps a record of this activity. Looking at the values in our report, we can see that both *c:\users.txt* and *c:\clients.txt* were the last files saved to the system around 21:06. Note that all the times found on these files are set to GMT and must be translated to PST (GMT-8).

Other files such as *config.php* and *accountgroups.php* were also accessed by the *ver0k* account.

WHAT YOU SHOULD KNOW...

Windows and Linux System Administration

Intrusion and hacker techniques

NTFS file system essentials

WHAT YOU WILL LEARN...

How to investigate security breaches and analyse data without modifying it

How to create event timelines and how to recover data from unallocated space

How to extract evidence from the registry and how to parse windows event logs

Listing 1a. Running Regripper on ver0k's NTUSER.DAT

```
# perl rip.pl -r /mnt/hack/hakin9_090101mnt/Documents\ and\  
                Settings\ver0k\NTUSER.DAT -f ntuser >  
                /images/hakin9_090101/ver0k-ntuser.txt
```

```
Logon User Name  
Software\Microsoft\Windows\CurrentVersion\Explorer  
LastWrite Time [Sun Feb 5 23:44:08 2006 (UTC)]  
Logon User Name = ver0k
```

```
-----  
ComDlg32 v.20080324  
ComDlg32\LastVisitedMRU  
**All values printed in MRUList order.  
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\  
    LastVisitedMRU  
LastWrite Time Sun Feb 5 21:05:56 2006 (UTC)  
    MRUList = a  
    a -> C:\msnmsgr.exe
```

```
ComDlg32\OpenSaveMRU  
**All values printed in MRUList order.  
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\  
    OpenSaveMRU  
LastWrite Time Sun Feb 5 21:05:56 2006 (UTC)  
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\  
    OpenSaveMRU has no values.
```

```
Subkey: *  
LastWrite Time Sun Feb 5 21:06:37 2006 (UTC)  
    MRUList = ba  
    b -> C:\users.txt  
    a -> C:\clientes.txt
```

```
Subkey: txt  
LastWrite Time Sun Feb 5 21:06:37 2006 (UTC)  
    MRUList = ba  
    b -> C:\users.txt  
    a -> C:\clientes.txt
```

```
-----  
RecentDocs - recentdocs  
**All values printed in MRUList\MRUListEx order.  
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs  
LastWrite Time Sun Feb 5 21:58:56 2006 (UTC)  
    18 = Administrator's Documents  
    37 = examen.gif  
    36 = Apache  
    35 = ABOUT_APACHE.TXT  
    34 = maick  
    33 = Sti_Trace.log  
    32 = RRGEPPortadas.doc  
    31 = RRGEPPNotas.doc  
    30 = Notas.doc  
    24 = Indice Pormenorizado.doc  
    29 = ÍNDICE DOCTORADO.doc  
    28 = formulario.doc  
    23 = 30SEP_bolecart-book.doc  
    26 = Israel Robledo Gonzáles's Documents  
    27 = concha.doc  
    25 = Boletin11.doc  
    19 = modelos  
    22 = nm06082003.jpeg  
    21 = nm06052003.jpeg  
    20 = nm06042003.jpeg  
    10 = nm06032003.jpeg  
    9 = a017.jpg  
    7 = imagenes  
    8 = overlay_por_2006020110007_20060201224249.jpg
```

```
6 = overlay_por_2006020107034_20060201190204.jpg  
17 = overlay_9_2006020110006.jpg  
16 = overlay_8_2006020110005.jpg  
15 = overlay_8.jpg  
14 = overlay_7_2006020110005.jpg  
13 = overlay_6_2006020110004.jpg  
12 = overlay_6_2005112211035.jpg  
11 = overlay_5_2006020110004.jpg  
4 = Local Disk (C:)  
5 = users.txt  
3 = clientes.txt  
1 = web-erp  
2 = config.php  
0 = AccountGroups.php  
4294967295 =  
TypedURLs  
Software\Microsoft\Internet Explorer\TypedURLs  
LastWrite Time Sun Feb 5 20:47:38 2006 (UTC)  
    url1 -> http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&a  
        r=msnhome  
UserAssist (Active Desktop)  
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\  
    {75048700-EF1F-11D0-9888-006097DEACF9}\Count  
LastWrite Time Sun Feb 5 21:59:52 2006 (UTC)  
Sun Feb 5 21:59:52 2006 (UTC)  
    UEME_RUNPIDL (5)  
    UEME_RUNPATH (45)  
    UEME_RUNPIDL:%csidl2%\MSN Messenger 7.5.lnk (2)  
    UEME_RUNPATH:C:\Program Files\MSN Messenger\msnmsgr.exe  
        (2)  
    UEME_RUNPATH:{5CCEE3CA-03EC-11DA-BFBD-00065BBD0B5} (2)  
Sun Feb 5 21:53:46 2006 (UTC)  
    UEME_RUNPATH:C:\WINDOWS\system32\NOTEPAD.EXE (4)  
Sun Feb 5 21:47:41 2006 (UTC)  
    UEME_RUNPATH:C:\Program Files\Windows NT\Accessories\  
        WORDPAD.EXE (12)  
Sun Feb 5 21:39:45 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\  
        My Documents\My Videos\cartoons\  
        unbaileparati.exe (1)  
Sun Feb 5 21:39:26 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My  
        Documents\My Videos\cartoons\tortuga2.exe (1)  
Sun Feb 5 21:39:07 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My  
        Documents\My Videos\cartoons\tortugal.exe (1)  
Sun Feb 5 21:35:18 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My  
        Documents\My Videos\cartoons\TestdeRavenH.exe  
        (1)  
Sun Feb 5 21:35:08 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\  
        My Documents\My Videos\cartoons\  
        tequieromasqueamis.exe (1)  
Sun Feb 5 21:34:22 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My  
        Documents\My Videos\cartoons\temoc.exe (1)  
Sun Feb 5 21:33:50 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My  
        Documents\My Videos\cartoons\Te quiero como a  
        mi huevo.exe (1)  
Sun Feb 5 21:33:31 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My  
        Documents\My Videos\cartoons\sarten.exe (1)  
Sun Feb 5 21:33:17 2006 (UTC)  
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My  
        Documents\My Videos\cartoons\saludosamama.exe  
        (1)
```

To complete our analysis of the registry, we will do the same with every single user on the ERP system, analysing carefully all the traces that could help us in our investigation.

Timeline Creation and Analysis

A good starting point in your investigation would be to find out when did the attack start. Once you obtain that information you could check file access, creation and modification times around that period to get some idea of the actions that took place on the system and the files the attackers touched. Furthermore, you can correlate that with other time stamped files like windows event logs and application logs to get a bigger picture. That timing of events, or timeline, usually becomes the centre of your investigation, although you must be aware that an attacker can easily modify file times.

To create a timeline, we will make use of the Sleuth Kit tools and Autopsy,

both installed in your Linux Forensic Workstation. Autopsy works as a Web-based front end to all of the Sleuth Kit tools and makes it easy to perform most of the common forensic related tasks like to create timelines, to examine a file system and to organize multiple forensics analyses into different cases, so you can reference them later.

To start Autopsy, open a web browser and type in `http://localhost:9999/autopsy` to view the default page and click *New Case* to start your investigation. Name your case, provide a description and fill out the investigators names before you click *New Case* again to let Autopsy create the directory and configuration files. Now click *Add Host* to create a host for this case. As before fill out the information about the host you are adding.

Note that an optional Time Zone value can be given. By default Autopsy will use

the time zone of your analysis system to build a timeline of events. Hence, if your local time zone is set to a time zone different than *Pacific Standard Time*, be sure you specify it in the *Time Zone* field, as seen in Figure 1. Using correctly synced time is particularly important when piecing together a chain of events from different sources, as we will demonstrate later.

Click on *Add Host* when you are done. Adding a host will create a directory in the case directory and subdirectories in the host for the images, output data, logs and reports.

Next, the image we previously acquired should be added to the host. Click *Add Image* to see the Host Manager screen. Select *Add Image File* and type the full file path to the image file in the location field. The Type field lets you inform Autopsy of the type of image you created. Our dd image doesn't

Listing 1b. Running Regripper on ver0k's NTUSER.DAT (continuation)

```
Sun Feb  5 21:32:28 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\Poetas Huevos 2a Edicion.exe (1)
Sun Feb  5 21:32:19 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\Perdonam.exe (1)
Sun Feb  5 21:32:05 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\no muerdo.exe (1)
Sun Feb  5 21:31:53 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\no existieras.exe (1)
Sun Feb  5 21:30:21 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\Muchos Huevos.exe (1)
Sun Feb  5 21:30:05 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\mordida.exe (2)
Sun Feb  5 21:29:36 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\mi vecina.exe (1)
Sun Feb  5 21:29:15 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\amigas de huevos.exe (1)
Sun Feb  5 21:28:54 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\el df.exe (1)
Sun Feb  5 21:28:37 2006 (UTC)
    UEME_RUNPATH:C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\fiesta en el antro.exe (1)
Sun Feb  5 21:11:00 2006 (UTC)
    UEME_UISCUT (2)
    UEME_RUNPATH:::{645FF040-5081-101B-9F08-00AA002F954E} (2)
Sun Feb  5 20:49:43 2006 (UTC)
    UEME_RUNPATH:C:\WINDOWS\system32\rundll32.exe (1)
Sun Feb  5 20:49:04 2006 (UTC)
    UEME_RUNPATH:C:\WINDOWS\explorer.exe (1)
    UEME_RUNPIDL:%csidl2%\Accessories\Windows Explorer.lnk (1)
Sun Feb  5 20:48:17 2006 (UTC)
    UEME_RUNPIDL:%csidl2%\MySQL\MySQL Administrator.lnk (1)
    UEME_RUNPIDL:%csidl2%\MySQL (1)
    UEME_RUNPATH:C:\Program Files\MySQL\MySQL Administrator 1.1\MySQLAdministrator.exe (1)
Sun Feb  5 20:46:04 2006 (UTC)
    UEME_RUNPIDL:%csidl2%\Accessories\Notepad.lnk (14)
```

contain a full disk but rather an individual partition, so we select *Partition*. Then select *Symlink* for Autopsy to create in its evidence locker a symbolic link to the image file and avoid unnecessary duplication. After that the next window will show you the file system for the partition to be imported and will allow you to specify or calculate an MD5 hash for the image file.

Now that you have created the case, added a host and selected the NTFS partition image, you are ready to create a

timeline and start the analysis. Creating a timeline in Autopsy takes two major steps:

- Extract the file metadata from the file system image and save it to a data file usually referred as *body* file.
- Parse the *body* file and create an ASCII timeline of file activity between two given dates.

To create a timeline from our acquired image, click *File Activity Timelines* from the Host Manager screen. Then click *Create*

Data File from the top menu, select the Windows 2003 image and choose what type of files you want to extract the metadata from. Two types are available:

- Allocated files: Those that can be seen while browsing the file system. In other words, those that have an allocated file name structure.
- Unallocated files: Those that have been deleted, but that Sleuth Kit can still access, such as orphan files. Orphan files are files that no longer have a name but whose metadata still exists.

Select both types of files and check the *Generate MD5 Value* before you click OK. When Autopsy completes the Sleuth Kit command *fls -r -m* on the image, a *body* file will be created in the output directory and an entry added to the host config file.

The next screen will allow you sort the newly created *body* file into a timeline. We will continue with the default settings, without specifying a particular starting or ending date. The resulting *timeline.txt* file will be created in the output directory, using the time zone set for this host (*Pacific Standard Time* in our case).

As you can see now a timeline has many columns, the most relevant being the following:

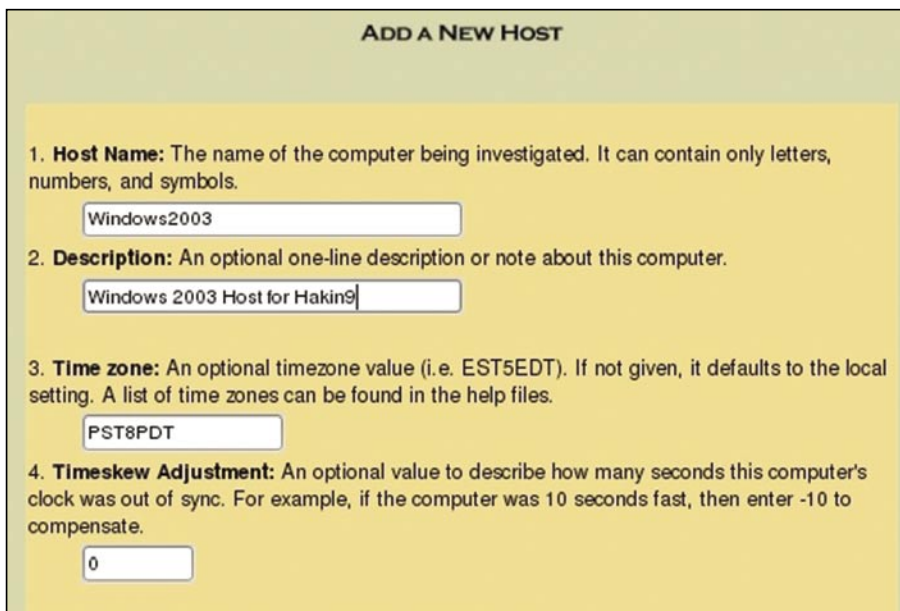


Figure 1. Add new host screenshot. Time zone must be set to PST8PDT

Date	Time	Size	Permissions	Mode	UID	GID	Path
Sun Feb 05 2006	12:47:22	804	...b	r/rwxrwxrwx	0	0	C:/Documents and Settings/ver0k/Start Menu/Programs/Accessories/Entertainment/Windows Media Player.lnk
		56	...b	d/drwxrwxrwx	0	0	C:/Documents and Settings/ver0k
		786432	...b	r/r-r-xr-x	0	0	C:/Documents and Settings/ver0k/NTUSER.DAT
		48	...b	d/dr-xr-xr-x	0	0	C:/Documents and Settings/ver0k/Templates
		256	...b	d/d-wx-wx-wx	0	0	C:/Documents and Settings/ver0k/Start Menu
		56	...b	d/d-wx-wx-wx	0	0	C:/Documents and Settings/ver0k/Start Menu/Programs
		152	...b	d/d-wx-wx-wx	0	0	C:/Documents and Settings/ver0k/Start Menu/Programs/Startup
		56	...b	d/d-wx-wx-wx	0	0	C:/Documents and Settings/ver0k/Start Menu/Programs/Accessories
		400	...b	d/d-wx-wx-wx	0	0	C:/Documents and Settings/ver0k/Start Menu/Programs/Accessories/Entertainment
		56	...b	d/d-wx-wx-wx	0	0	C:/Documents and Settings/ver0k/Start Menu/Programs/Accessories/Accessibility
		56	...b	d/d--x--x--x	0	0	C:/Documents and Settings/ver0k/SendTo
		328	...b	d/d--x--x--x	0	0	C:/Documents and Settings/ver0k/Recent
		48	...b	d/dr-xr-xr-x	0	0	C:/Documents and Settings/ver0k/PrintHood
		48	...b	d/dr-xr-xr-x	0	0	C:/Documents and Settings/ver0k/NetHood
		56	...b	d/d-wx-wx-wx	0	0	C:/Documents and Settings/ver0k/My Documents
		56	...b	d/dr-xr-xr-x	0	0	C:/Documents and Settings/ver0k/Local Settings
		256	...b	d/drwxrwxrwx	0	0	C:/Documents and Settings/ver0k/Local Settings/Temporary Internet Files
		672	...b	d/drwxrwxrwx	0	0	C:/Documents and Settings/ver0k/Local Settings/Temporary Internet Files/Content.IE5
		56	...b	d/drwxrwxrwx	0	0	C:/Documents and Settings/ver0k/Local Settings/Temporary Internet Files/Content.IE5/NDT7RLDC
		56	...b	d/drwxrwxrwx	0	0	C:/Documents and Settings/ver0k/Local Settings/Temporary Internet Files/Content.IE5/K1MJW92V

Figure 2. The timeline shows what files were modified, accessed and born at the time of the creation of account ver0k

- *Date and time of the activity.* If no date is given, then the activity occurred at the same time as the previous entry with a time.
- *Entry Type.* The *m*, *a*, *c*, and *b* letters identify which of the activity types this entry corresponds to. *m* is for modified times, *a* is for access times, *c* is for change times, and *b* is for created (or born) times.
- *Meta Data Address.* The inode or MFT entry address for the associated file.
- *File Name.* The name of the file and the destination of a symbolic link. Deleted entries will have *(deleted)* at the end and deleted entries that point to an allocated meta data structure will have *(realloc)*.

To focus our analysis of the timeline we will review the activity that took place on the

5th of Feb 2006, the date when the `ver0k` account was created. Too see a sample of this activity check Figure 2.

A search for the first occurrence of `ver0k` reveals that the user profile directory was created under the *Documents and Settings* folder on the 5th of Feb at 12:47, as Figure 2 shows. It's interesting to notice that only 3 minutes before, user Jonathan had some *.tiff* and *.htm* files created under the Internet Explorer temporary files directory, which indicates some Internet browsing activity. Some of these files appear as *deleted* but they still can be retrieved from the unallocated space.

It also catches our attention that between Jonathan's Internet activity and the creation of account `ver0k`, the files `net.exe`, `reg.exe`, `rdpwsx.dll` and `rdpwd.sys`,

all found in `c:\windows\system32` directory, were accessed. Remember that some of the uses of `net.exe` and `reg.exe` include creating user accounts and making changes to the windows registry.

Last, at 12:47, the executable `c:\windows\system32\rdpclip.exe` is accessed along with the `c:\windows\media\windows\startup.wav` file and a good number of *.lnk* files within the `ver0k` home directory, a clear indication of a user logon.

Do you have a clearer picture now?

File and Directory Analysis

We have a good amount of information at this point. So what should you look for next? Well, the following is a brief list of things you should be looking for when browsing the offline file system:

Listing 2. Excerpt of `config.php` located under `C:\apache\apache\htdocs\web-erp`

```
/* $Revision: 1.64 $ */

/*-----\
|           | config.php |
|-----|
| Web-ERP - http://web-erp.sourceforge.net |
| by Logic Works Ltd |
|-----|
| |
|-----*/

// User configurable variables
//-----

//DefaultLanguage to use for the login screen and the setup of new users - the users language selection will override
$DefaultLanguage = 'en_GB';

// Whether to display the demo login and password or not on the login screen
$allow_demo_mode = False;

// webERP version

$Version = '3.04';
...
// Connection information for the database
// $host is the computer ip address or name where the database is located
// assuming that the web server is also the sql server
$host = 'localhost';

//The type of db server being used - currently only postgres or mysql
$dbType = 'mysql';
//$dbType = 'postgres';
//$dbType = 'mysql';

$DatabaseName='weberp';

// sql user & password
$dbuser = 'weberp_us';
$dbpassword = '';
```

- Relevant files (*pagefile.sys*, *index.dat*, etc...).
- Windows event logs.
- Application configuration files and logs.
- Evidence of malware, rootkits, etc...

Considering that we know we have a WAMP (Windows + Apache + MySQL + PHP) environment, the next thing we will review is the configuration files for these applications that form the basis of the Web-based ERP system.

A quick look at the apache installation directory reveals a couple of interesting things. First, the `httpd.conf` confirms that the server was indeed listening on port 80. Second, installed under `C:\apache\apache\htdocs\` we find a folder named *web-erp*, an open-source ERP created by Logic Works Ltd and available on www.weberp.org. Soon we realise that MySQL is the database of choice that supports this web-based ERP, so the postgres database can be ignored in our analysis.

Listing 2 is an excerpt from the content of `config.php`, the file that holds the web-erp configuration located under the `C:\apache\apache\htdocs\web-erp` directory.

Notice that the database for the Web based ERP was accessible with user `weberp_us` and `blank` password!

We can also find the Apache logs under `C:\apache\apache\logs` while MySQL logs are found under `C:\apache\`

`apache\mysql\data`. It's interesting that we can connect directly to those logs using the MySQL Administrator console on the bootable image, as we know there is no password (yes, no password!) to connect to the database. This gives us a hint of what the attacker could have possibly done.

A further analysis correlating the timestamped files `access.log` and `error.log` from Apache and `counters.log` from MySQL reveals that on Feb 5 at 13:57, a new account called *admin* was created on the Web-based ERP System from the IP address 70.107.249.150.

Parsing Windows Event Logs

A great source of information is the Windows Event Logs. They can provide a good amount of information that's useful for understanding events during a forensic analysis. These logs record a variety of daily events that take place on your Windows system and can also be configured to record a range of additional events. These events are categorised as Security, System and Application Event Logs. These are stored in binary files under the `Windows/system32/config` with the extension `*.evt`.

Alternatively, the presence of a file called `dnsevent.evt` in our system, confirms that it was configured as a DNS server. While administrators are most familiar with interacting with the Event Logs through

the built-in Event Viewer, we will make use of more powerful and flexible tool in our forensic analysis: Microsoft's LogParser.

LogParser is a command-line tool that provides a SQL interface to a variety of log files, XML files and CSV files, including key data sources such as the Event Log, the Registry, the file system, and Active Directory. The latest version of this versatile tool can be downloaded from <http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en>.

To start digging into the actual log files we will use a simple SELECT ALL query. Then, we change to the LogParser directory and type the following command to parse the Security Event Log:

```
LogParser "SELECT * FROM 'X:\hakin9_090101mnt\WINDOWS\system32\config\SecEvent.evt'" -i: EVT -o:CSV > security.csv
```

This command assumes that you have mounted your offline system on the X: drive of your windows workstation. The `-i:EVT` is the input engine argument telling log parser that the format is coming from the Windows Event Log format, while the `-o:csv` is the output engine argument telling log parser to format the output into the CSV or comma separated value file. A file in a csv format can be easily imported into a

Time	ID	Category	Source	Details
05/02/2006 21:44	592	Detailed Tracking	Security	3376 C:\WINDOWS\system32\cmd.exe 884 Johnatan COUNTERS (0x0,0x3DF69A)
05/02/2006 21:45	592	Detailed Tracking	Security	2832 C:\Program Files\PostgreSQL\8.1\bin\postgres.exe 2664 postgres COUNTERS (0x0,0x288206)
05/02/2006 21:45	593	Detailed Tracking	Security	2832 C:\Program Files\PostgreSQL\8.1\bin\postgres.exe postgres COUNTERS (0x0,0x288206)
05/02/2006 21:45	592	Detailed Tracking	Security	2988 C:\WINDOWS\system32\net.exe 3376 Johnatan COUNTERS (0x0,0x3DF69A)
05/02/2006 21:45	592	Detailed Tracking	Security	3700 C:\WINDOWS\system32\net1.exe 2988 Johnatan COUNTERS (0x0,0x3DF69A)
05/02/2006 21:45	560	Object Access	Security	Security Account
05/02/2006 21:45	632	Account Management	Security	- (S-1-5-21-2780117151-1340924567-2512508698-1024) None COUNTERS (S-1-5-21-2780117151-1340924567-2512508698-513) Jo
05/02/2006 21:45	624	Account Management	Security	ver0k COUNTERS (S-1-5-21-2780117151-1340924567-2512508698-1024) Johnatan COUNTERS (0x0,0x3DF69A) - ver0k 1793 -
05/02/2006 21:45	626	Account Management	Security	ver0k COUNTERS (S-1-5-21-2780117151-1340924567-2512508698-1024) Johnatan COUNTERS (0x0,0x3DF69A) - ver0k 1793 -
05/02/2006 21:45	642	Account Management	Security	- ver0k COUNTERS (S-1-5-21-2780117151-1340924567-2512508698-1024) Johnatan COUNTERS (0x0,0x3DF69A) - ver0k 1793 -
05/02/2006 21:45	628	Account Management	Security	ver0k COUNTERS (S-1-5-21-2780117151-1340924567-2512508698-1024) Johnatan COUNTERS (0x0,0x3DF69A) - ver0k 1793 -
05/02/2006 21:45	562	Object Access	Security	Security Account Manager 767616 468 C:\WINDOWS\system32\lsass.exe
05/02/2006 21:45	560	Object Access	Security	Security Account
05/02/2006 21:45	560	Object Access	Security	Security Account
05/02/2006 21:45	636	Account Management	Security	- (S-1-5-21-2780117151-1340924567-2512508698-1024) Users Bulltin (S-1-5-32-545) Johnatan COUNTERS (0x0,0x3DF69A) -
05/02/2006 21:45	562	Object Access	Security	Security Account Manager 770584 468 C:\WINDOWS\system32\lsass.exe
05/02/2006 21:45	562	Object Access	Security	Security Account Manager 770160 468 C:\WINDOWS\system32\lsass.exe
05/02/2006 21:45	593	Detailed Tracking	Security	3700 C:\WINDOWS\system32\net1.exe Johnatan COUNTERS (0x0,0x3DF69A)
05/02/2006 21:45	593	Detailed Tracking	Security	2988 C:\WINDOWS\system32\net.exe Johnatan COUNTERS (0x0,0x3DF69A)
05/02/2006 21:45	592	Detailed Tracking	Security	2744 C:\WINDOWS\system32\net.exe 3376 Johnatan COUNTERS (0x0,0x3DF69A)
05/02/2006 21:45	592	Detailed Tracking	Security	2576 C:\WINDOWS\system32\net1.exe 2744 Johnatan COUNTERS (0x0,0x3DF69A)

Figure 3. A CSV file showing the output of LogParser on the Security Event Log

ATTACK

spreadsheet, something we will find very valuable soon.

We do the same with the System and Application Event Logs, so we finally have 3 different csv files, one for each kind of event log. However, it would be best if we could combine those three files into a single one, one that we could sort by time/date and create a timeline of events. To do so, we will use the handy yet simple copy command:

```
Copy *.csv combined.csv
```

After tidying up a bit the resulting combined csv file, we obtain a spreadsheet that can be easily analysed as shown in Figure 3.

After a detailed analysis we realise that the user Jonathan uses the Administrator account interchangeably on several occasions. To visualise this, create a filter on the column *EventCategoryName* to see all the Logon/Logoff events. Based on this evidence we can suppose that it was the user Jonathan; who was actually a system administrator for that box.

There are other interesting events we can find on our combined spreadsheet. For example, the System Event Log shows that the system time zone was initially set to Alaskan Standard Time on January 25, when the system was installed. Then, it was changed to Pacific Standard Time on the 2nd of Feb. The Security Event Log also contains several entries related to the execution of Internet Explorer.

However, the most interesting event is the one that took place on Feb 05 2006 at 12:45:30 p.m.

```
User Account Created: New Account
Name: verok New Domain: COUNTERS
New Account ID: %[S-1-5-21-2780117151-
1340924567-2512508698-1024] Caller
User Name: Jonathan Caller
```

The entry shown above evidences that it was the user Jonathan who called the process that resulted in the creation of the account *verok*. The event log shows further activity from the *verok* user from that time on. Again, some of this activity includes the use of the Internet Explorer browser, so let's analyse that next.

Analysing the Internet Explorer Browsing History File

Internet Explorer keeps a history of its activity that a forensic investigator can use to get a clearer picture of the user's activity. This information is stored in a file named *INDEX.dat* that is kept at multiple locations. *INDEX.dat* provides useful information on URL access, use of cookies, etc, along with their corresponding date-time stamps. Again, these are in a binary structure but we will use *pasco*, a free tool from <http://www.foundstone.com>, to parse this file.

Given that most of our evidence points to two users, Jonathan and *verok*, we will start analysing the Internet Browsing History for them. To examine Jonathan's activity we change to *\Documents and Settings\Johnathn\Local Settings\History\History.IE5* and run the following command:

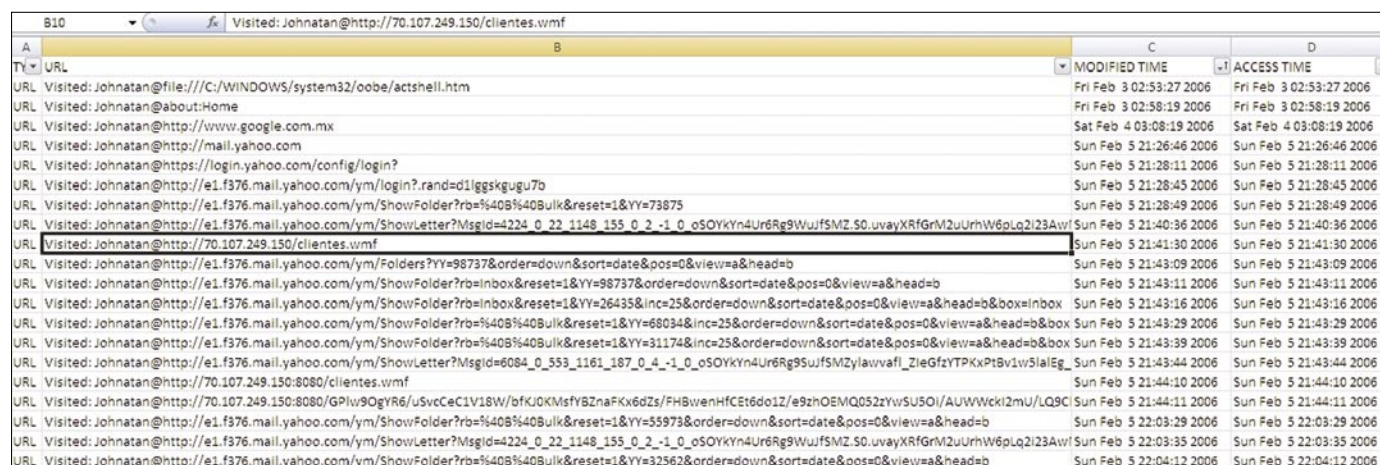
```
# pasco index.dat > /images/hakin9_
090101/Jonathan-
ie.csv
```

Pasco will output the results in a field-delimited format so you can open it as a TAB delimited file in your favourite spreadsheet program to further sort and filter the results. Figure 4 shows an excerpt of that file.

We find several things in this file. For example, we can see that between 12:26 PST and 13:06 PST on Feb 5 2006, the user Jonathan used the Yahoo mail service as we find several hits to <http://e1.f376.mail.yahoo.com>, and that at 12:41 PST he visited <http://70.107.249.150/clientes.wmf>, then at 12:44 PST <http://70.107.249.150:8080/clientes.wmf> and right after [This activity looks really suspicious given that the IP 70.107.249.150 was already found to be the address from where the *admin* account was created on the ERP system. Furthermore, the account *verok* was created at 12:45 PST on the same day, just a minute after the user Jonathan clicked on that link.](http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJOKMsfYBZnaFKx6dZs/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU5Oi/AUWWckl2mU/LQ9ClubsIAJKla2jdYtSFExez4sRyL.tiff</p></div><div data-bbox=)

The analysis of the Internet activity for the user *verok* confirms that the MSN service was accessed along with other web-erp configuration files such as *config.php* and *accountgroups.php*, both, as we already found when doing the *NTUSER.dat* registry analysis.

To complement this information we will run a keyword search using Autopsy's built-in capabilities.



A	B	C	D
URL	MODIFIED TIME	ACCESS TIME	
URL Visited: Johnatan@http://70.107.249.150/clientes.wmf	Fri Feb 3 02:53:27 2006	Fri Feb 3 02:53:27 2006	
URL Visited: Johnatan@http://www.google.com.mx	Fri Feb 3 02:58:19 2006	Fri Feb 3 02:58:19 2006	
URL Visited: Johnatan@http://mail.yahoo.com	Sat Feb 4 03:08:19 2006	Sat Feb 4 03:08:19 2006	
URL Visited: Johnatan@https://login.yahoo.com/config/login?	Sun Feb 5 21:26:46 2006	Sun Feb 5 21:26:46 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/login?.rand=d1ggskgugu7b	Sun Feb 5 21:28:45 2006	Sun Feb 5 21:28:45 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=inbox&reset=1&YY=26435&inc=25&order=down&sort=date&pos=0&view=a&head=b	Sun Feb 5 21:28:49 2006	Sun Feb 5 21:28:49 2006	
URL Visited: Johnatan@http://70.107.249.150/clientes.wmf	Sun Feb 5 21:40:36 2006	Sun Feb 5 21:40:36 2006	
URL Visited: Johnatan@http://70.107.249.150:8080/clientes.wmf	Sun Feb 5 21:41:30 2006	Sun Feb 5 21:41:30 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/Folders?YY=98737&order=down&sort=date&pos=0&view=a&head=b	Sun Feb 5 21:43:09 2006	Sun Feb 5 21:43:09 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=inbox&reset=1&YY=98737&order=down&sort=date&pos=0&view=a&head=b	Sun Feb 5 21:43:11 2006	Sun Feb 5 21:43:11 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=inbox&reset=1&YY=26435&inc=25&order=down&sort=date&pos=0&view=a&head=b&box=inbox	Sun Feb 5 21:43:16 2006	Sun Feb 5 21:43:16 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=%40B%40B%40B&reset=1&YY=68034&inc=25&order=down&sort=date&pos=0&view=a&head=b&box	Sun Feb 5 21:43:29 2006	Sun Feb 5 21:43:29 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=%40B%40B%40B&reset=1&YY=31174&inc=25&order=down&sort=date&pos=0&view=a&head=b&box	Sun Feb 5 21:43:39 2006	Sun Feb 5 21:43:39 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowLetter?MsgId=6084_0_553_1161_187_0_4_-1_0_o5OYKyn4Ur6Rg9WuJfSMZ.S0.uvayXRfGrM2UUrHw6pLq2I23Awf	Sun Feb 5 21:43:44 2006	Sun Feb 5 21:43:44 2006	
URL Visited: Johnatan@http://70.107.249.150:8080/clientes.wmf	Sun Feb 5 21:44:10 2006	Sun Feb 5 21:44:10 2006	
URL Visited: Johnatan@http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJOKMsfYBZnaFKx6dZs/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU5Oi/AUWWckl2mU/LQ9ClubsIAJKla2jdYtSFExez4sRyL.tiff	Sun Feb 5 21:44:11 2006	Sun Feb 5 21:44:11 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=%40B%40B%40B&reset=1&YY=55973&order=down&sort=date&pos=0&view=a&head=b	Sun Feb 5 22:03:29 2006	Sun Feb 5 22:03:29 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowLetter?MsgId=4224_0_22_1148_155_0_2_-1_0_o5OYKyn4Ur6Rg9WuJfSMZ.S0.uvayXRfGrM2UUrHw6pLq2I23Awf	Sun Feb 5 22:03:35 2006	Sun Feb 5 22:03:35 2006	
URL Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=%40B%40B%40B&reset=1&YY=32562&order=down&sort=date&pos=0&view=a&head=b	Sun Feb 5 22:04:12 2006	Sun Feb 5 22:04:12 2006	

Figure 4. Pasco can dump the contents of *INDEX.DAT* into a TAB delimited file, showing the URLs that Jonathan visited on the 5th of Feb 2006

Keyword Search

It's time now to use one of the most powerful features of Autopsy, the Keyword Search Mode. This functionality can automatically extract the strings from a particular image and use that for subsequent keyword searches. At this point in our investigation we have several clues we can search for within the image, like usernames, IP addresses, etc...

In the Keyword Search mode tab, Autopsy allows to perform very unique searches. In fact, Autopsy can extract the unallocated data of the image and generate the strings file for that, so you can perform string searches on both the unallocated image and the full image. This is obviously useful when trying to recover deleted data.

Searching the string `ver0k` in the entire file system produces more than 1400 results, so we will need to use a different keyword to reduce these results to a manageable amount.

However, a search on the IP address '70.107.249.150' returns 7 hits. One of those includes the following email recovered from a deleted file on Jonathan's Internet Explorer cache, under the *Temporary Internet Files* folder (see Listing 3).

The recovered file also contains the mail header that shows that it was sent on 5 Feb 2006 at 14:42:47 (CST), the same date when the system user `ver0k` and the WebERP *admin* user were created.

Putting it all together

Search for the *wmf* and *vulnerability* keywords on Google and you will find plenty of information related to MS06-001, a security bulletin issued by Microsoft in January 2006 that could result in remote code execution. We can easily check that the KB912919 patch that Microsoft issued to address this vulnerability was never installed on this machine, just by looking at the *KB*.log* files stored under the *C: \WINDOWS* folder.

Our Google search also reveals that there is a working exploit imported into Metasploit that allows an attacker to set up a webserver on port 8080 on the attacker host, to inject a specially crafted *.tiff* file to exploit the vulnerability and finally return a command shell to the attacker gaining the same user rights as the logged on user. As we know, in this case those were full admin rights.

Conclusion

This article has introduced some of the techniques that can be used during the course of a computer forensic investigation using many tools and resources that are freely available on the Internet. However, as stated in Part I of this article, it's necessary to reiterate that forensic investigations need to be conducted only if *authorized* and by qualified personnel. Therefore make sure you have the proper approval before initiating any real investigation and that the appropriate personnel (e.g. human resources, legal and even law enforcement, if necessary) are notified as soon as possible, and if in doubt, ask for professional help, as that may save both you and your employer from some serious trouble.

Also there are still many other techniques and topics that a computer forensic investigator need to master and that were not analysed in this article. Those include live memory analysis and network forensics just to mention a few. For upcoming articles on Computer Forensics stay tuned to future Hakin9 issues!

Listing 3. Email recovered from a deleted file on Jonathan's Internet explorer cache

```
Asunto: Urgente!! (correccion)
Contenido:
Johnny:
Esta es la liga correcta,

Por favor baja el catalogo que esta en
<a href="http://70.107.249.150:8080/clientes.wmf" target=_blank onclick="return
ShowLinkWarning()" >http://70.107.249.150:8080/clientes.wmf</
a>

Alberto Lopez
Director General
Electronica y Computacion S.A. de C.V.
```

On The 'Net

- UNAM-CERT Forensic challenge: <http://www.seguridad.unam.mx/eventos/reto/>
- SANS Forensic Blog: <http://sansforensics.wordpress.com/>
- RegRipper: <http://www.regripper.net/>
- Windows Incident Response (Harlan Carvey's blog): <http://windowsir.blogspot.com/>
- The Sleuth Kit and Autopsy Browser: <http://www.sleuthkit.org/>
- LogParser 2.2: <http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en>
- Forensic Log Parsing with Microsoft LogParser, by Mark Burnett <http://www.securityfocus.com/infocus/1712>
- Pasco analysis tool: http://sourceforge.net/project/shownotes.php?group_id=78332&release_id=237810
- Computer Forensics eStore: <http://www.insectraforensics.com>
- Other forensic challenges: <http://www.jessland.net/JISK/Forensics/Challenges.php> and <http://dfws.org/2009/challenge/index.shtml>
- Computer forensic links and whitepapers: <http://www.forensics.nl/links>

Ismael Valenzuela

Ismael Valenzuela, CISSP, CISM, GCFA, GCIA, GPEN, IRCA 27001 LA, ITIL Certified
Since he founded G2 Security, one of the first IT Security consultancies in Spain, Ismael Valenzuela has participated as a security professional in international projects across UK, Europe, India and Australia. He holds a Bachelor in Computer Science, is certified in Business Administration and also holds the following security related certifications: GIAC Certified Forensic Analyst, GIAC Certified Intrusion Analyst, GIAC Certified Penetration Tester, ITIL, CISM, CISSP and IRCA ISO 27001 Lead Auditor by Bureau Veritas UK. He is also a member of the SANS GIAC Advisory Board and international BSI Instructor for ISO 27001, ISO 20000 and BS 25999 courses.
He currently works as Global ICT Security Manager at iSOFT and can be contacted through his *blog* at <http://blog.ismaelvalenzuela.com>