

BAN CƠ YẾU CHÍNH PHỦ  
**HỌC VIỆN KỸ THUẬT MẬT MÃ**  
-----



BÀI TẬP LỚN

**Windows Forensic Analysis – Chapter 5**

*Giảng viên:* **Lại Minh Tuấn**

*Sinh viên thực hiện:*

**Nguyễn Thanh Dung**

**Nguyễn Thị Dung**

**Phạm Thị Tâm**

Hà Nội, 12/2019

## MỤC LỤC

MỤC LỤC .....	0
DANH MỤC HÌNH ẢNH .....	3
DANH MỤC BẢNG BIỂU .....	4
5.1. Giới thiệu .....	5
5.2. Tập tin nhật ký .....	5
Nhật ký sự kiện .....	5
Hiểu biết về sự kiện .....	6
Định dạng tập tin nhật ký sự kiện .....	12
Tiêu đề nhật ký sự kiện.....	13
Cấu trúc bản ghi sự kiện .....	14
Nhật ký sự kiện vista.....	22
Nhật ký IIS.....	24
Trình phân tích cú pháp (Log Parser) .....	30
Lịch sử trình duyệt web.....	31
Các tập tin nhật ký khác.....	33
Setuplog.txt.....	33
Setupact.log .....	35
Setupapi.log .....	35
Netsetup.log .....	36
Task Scheduler Log (Nhật ký lập lịch tác vụ).....	37
XP Firewall Logs.....	39
Mrt.log .....	41
Dr.Watson Logs .....	42
Cbs.log.....	44
Creash Dump Files (Tập tin kết xuất sự cố).....	44
Recycle Bin (Thùng rác) .....	44
Vista Recycle Bin (Thùng rác Vista) .....	47
XP System Restore Points (Điểm khôi phục hệ thống XP) .....	48
Rp.log Files .....	48
Change.log.x Files .....	49
Vista Volume Shadow Copy Service .....	50
Prefetch Files (Tập tin tìm nạp trước).....	51
Vista SuperFetch .....	53

Shortcut Files .....	54
5.3. File Metadata (tệp tin siêu dữ liệu) .....	55
Word Documents.....	57
PDF Documents (Tài liệu PDF) .....	63
Image Files (tệp hình ảnh).....	66
File Signature Analysis (Phân tích chữ ký tệp tin) .....	66
NTFS Alternate Data Streams (Luồng dữ liệu thay thế NTFS) .....	68
Creating ADSes (Tạo ADSes) .....	69
Enumerating ADSes (Liệt kê ADSes) .....	70
Using ADSes (Sử dụng ADSes) .....	74
Removing ADSes (Loại bỏ ADSes).....	75
ADS Summary (Tóm lược ADS).....	76
5.4. Alternative Methods of Analysis (Phương pháp phân tích thay thế) .....	77
Mounting an Image (Gắn một hình ảnh) .....	79
Discovering Malware (Khám phá phần mềm độc hại).....	82
Timeline Analysis (Phân tích dòng thời gian) .....	87
5.5. Summary (Tóm lược) .....	89
5.6. Solutions Fast Track (Giải pháp theo dõi nhanh) .....	89
Log File.....	89
File Metadata .....	90
Alternative Methods of Analysis (Phương pháp phân tích thay thế).....	90
5.7. Frequently Asked Questions (Các câu hỏi thường gặp) .....	90

## DANH MỤC HÌNH ẢNH

Hình 5. 1. Bản ghi sự kiện Windows XP được xem trong Trình xem sự kiện.....	7
Hình 5. 2. Bản ghi sự kiện Windows 2003 show IP address .....	8
Hình 5. 3. Tiêu đề nhật ký sự kiện.....	13
Hình 5. 4. Cấu trúc bản ghi sự kiện mẫu .....	15
Hình 5. 5. Trình xem sự kiện Vista .....	23
Hình 5. 6. Cấu hình Windows XP Firewall Logging .....	39
Hình 5. 7. Ví dụ về thùng rác được xem qua ProDiscover.....	45
Hình 5. 8. Minh họa về đường dẫn tệp trong tệp .pf .....	53
Hình 5. 9. Thuộc tính tài liệu Idtheft.pdf.....	65
Hình 5. 10. Chữ ký tệp PDF .....	67
Hình 5. 11. Ví dụ về liệt kê ADS trên Vista.....	71
Hình 5. 12. Giao diện gián điệp ADS.....	73
Hình 5. 13. Hộp thoại được trả về khi bạn cố thực hiện một ADS trên Vista.....	74
Hình 5. 14. Menu ProDiscover hiển thị các công cụ mới .....	77
Hình 5. 15. Live view GUI.....	78
Hình 5. 16. Hình ảnh được gắn dưới dạng ổ đĩa thông qua Mount Image Pro v2.02 ..	79
Hình 5. 17. Gắn thông minh một tệp hình ảnh đã có .....	80
Hình 5. 18. Biểu tượng bảng điều khiển ImDisk.....	81
Hình 5. 19. Hộp thoại ImDisk .....	82
Hình 5. 20. WFPCheck đang chạy với tệp hình ảnh được gắn kết .....	85
Hình 5. 21. Đoạn trích của tệp .csv đầu ra WFPCheck .....	86

## **DANH MỤC BẢNG BIỂU**

Bảng 5. 1. Các loại đăng nhập sự kiện .....	8
Bảng 5. 2. Cấu trúc tiêu đề nhật ký sự kiện.....	13
Bảng 5. 3. Cấu trúc bản ghi sự kiện.....	15

# Chương 5: Phân tích tệp tin

Nội dung chương:

- Tệp tin nhật ký
- File Metadata
- Phương pháp phân tích thay thế

## 5.1. Giới thiệu

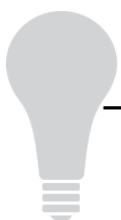
Các hệ thống Windows lưu trữ khá nhiều tệp tin hữu ích từ góc độ điều tra số. Trên thực tế, nhiều nhà điều tra có thể không nhận ra sự đa dạng của dữ liệu họ có thể tìm thấy trong một số tệp mà hệ thống Windows sử dụng để theo dõi các hoạt động và chức năng khác nhau. Biết nhiều địa điểm nơi thông tin được lưu trữ trong hệ thống cho phép điều tra viên chứng thực thông tin được tìm thấy ở các khu vực khác và giảm sự không chắc chắn trong phân tích của họ. Trong chương này, chúng tôi sẽ thảo luận về một số tệp tin khác nhau, bao gồm các tệp nhật ký, bạn có thể tìm thấy trên các hệ thống Windows cũng như thông tin về các tệp tin nói chung, cùng với các tệp cụ thể khác có giá trị cho một nhà điều tra. Chúng tôi sẽ thảo luận về một số khía cạnh khác nhau được gắn với nhau bởi thực tế là tất cả chúng đều nằm trong các tệp tin hoặc hệ thống tệp tin, cho dù ở định dạng ASCII có thể đọc được của con người hoặc ở định dạng nhị phân khó hiểu.

## 5.2. Tệp tin nhật ký

Các hệ thống Windows lưu trữ các tệp tin nhật ký cho một số sự kiện và hành động có thể liên quan đến nhà phân tích. Bên cạnh các tệp tin nhật ký ứng dụng, lưu trữ nhật ký các sự kiện liên quan đến các ứng dụng cụ thể, hệ điều hành Windows cũng lưu trữ một số nhật ký. Trong chương này, chúng tôi sẽ kiểm tra các tệp tin nhật ký có liên quan nhất để phân tích, trong đó đáng chú ý nhất có lẽ là Nhật ký sự kiện Windows.

### Event Log (Nhật ký sự kiện)

Nhật ký sự kiện có lẽ là nhật ký nổi tiếng nhất trên các hệ thống Windows, tương đương với syslog trên các hệ thống Linux. Nhật ký sự kiện ghi lại một loạt các sự kiện hàng ngày xảy ra trên các hệ thống Windows và có thể cấu hình (như được thảo luận trong Chương 4) để ghi lại một loạt các sự kiện bổ sung. Các sự kiện này được chia thành các danh mục được triển khai thông qua các nhật ký sự kiện khác nhau, chẳng hạn như nhật ký sự kiện bảo mật, hệ thống và ứng dụng. Nhật ký sự kiện có thể cung cấp rất nhiều thông tin hữu ích cho việc khắc phục sự cố cũng như hiểu các sự kiện trong quá trình phân tích điều tra số.



## Tip

Trên hầu hết các hệ thống Windows, bạn có thể sử dụng công cụ Resourcepol Audpol.exe để truy vấn và thiết lập chính sách kiểm toán. Trên Windows XP SP2 và 2003 SP1, audusr.exe cho phép các chính sách kiểm toán cho mỗi người dùng. Ví dụ: kiểm tra đăng nhập có thể được đặt cho tất cả người dùng, nhưng kiểm tra chi tiết hơn có thể được bật cho một người dùng cụ thể. Các thay đổi được thực hiện với audusr.exe sửa đổi khóa HKEY\_LOCAL\_MACHINE\System\CurrentControlset\Control\Lsa\Audit\PerUserAuditing\System Registry. Việc sử dụng công cụ này có thể cung cấp cho điều tra viên một chỉ dẫn về các loại sự kiện mà cô ấy sẽ thấy trong nhật ký sự kiện cũng như chỉ dẫn về mức độ kỹ năng kỹ thuật của người dùng hoặc quản trị viên.

---

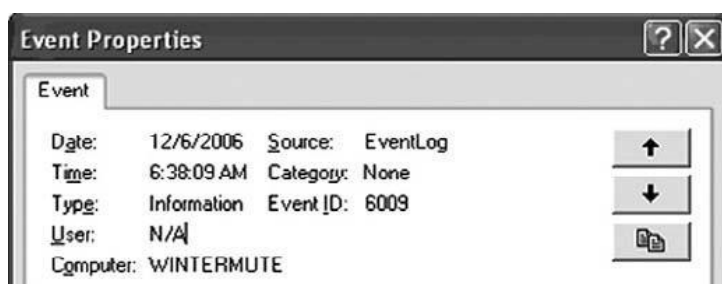
## Hiểu biết về sự kiện

Trên dòng hệ điều hành Windows NT, từ Windows 2000 đến XP và 2003, Nhật ký sự kiện bao gồm một cấu trúc nhị phân, với một tiêu đề và một loạt các bản ghi sự kiện được lưu trữ trong tệp. Dựa trên cách hệ điều hành được thiết kế, khi một số sự kiện nhất định, chẳng hạn như người dùng đăng nhập hoặc tắt xảy ra, một bản ghi về các sự kiện này được tạo ra. Một số sự kiện được ghi lại theo mặc định; các khía cạnh khác được ghi lại dựa trên cấu hình kiểm toán được duy trì trong khóa Đăng ký PolAdeEv, như đã thảo luận trong Chương 4. Các khía cạnh khác của cấu hình nhật ký sự kiện (kích thước tệp, thời gian lưu giữ hồ sơ, v.v.) được lưu trữ trong khóa Register sau:

*HKEY\_LOCAL\_MACHINE\System\CurrentControlset\Services\Eventlog\<Nhật ký sự kiện>*

Theo mặc định, Windows 2000, XP và 2003 đều có Nhật ký sự kiện ứng dụng, bảo mật và hệ thống. Các hệ thống được cấu hình làm bộ điều khiển miền cũng sẽ có Nhật ký sự kiện dịch vụ thư mục và sao chép tệp và các hệ thống được định cấu hình như máy chủ hệ thống tên miền (DNS) sẽ có Nhật ký sự kiện DNS. Các hệ thống khác cũng có thể có tệp Nhật ký Sự kiện dành riêng cho ứng dụng.

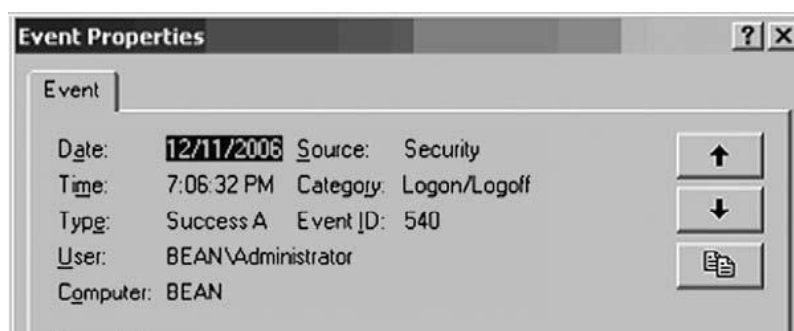
Quản trị viên quen thuộc nhất với việc tương tác với Nhật ký sự kiện thông qua Trình xem sự kiện, đây là trình quản lý giao diện người dùng đồ họa (GUI) cho Nhật ký sự kiện. Khi quản trị viên xem một bản ghi sự kiện trên Windows XP, anh ta sẽ thấy một cái gì đó tương tự như những gì xuất hiện trong Hình 5.1.



Hình 5. 1. Bản ghi sự kiện Windows XP được xem trong Trình xem sự kiện

Khi Trình xem sự kiện mở bản ghi sự kiện, nó sẽ điền vào trường Mô tả: bằng cách đọc các giá trị chuỗi từ bản ghi sự kiện, sau đó định vị tệp thông báo thích hợp (thư viện liên kết động hoặc DLL) trên hệ thống. Các tệp tin chứa các chuỗi thông báo được sử dụng để hỗ trợ quốc tế hóa trên các hệ điều hành Windows và các giá trị chuỗi từ các bản ghi sự kiện được chèn vào các vị trí thích hợp trong các chuỗi đó. Điều này cho phép quốc tế hóa Nhật ký sự kiện bằng cách cung cấp các chuỗi thông báo sự kiện bằng ngôn ngữ có nguồn gốc trong hệ thống (tiếng Anh, tiếng Đức, tiếng Pháp hoặc tương tự) và chỉ cần điền vào các khoảng trống thông tin cần thiết (tên hệ thống, ngày/dấu thời gian, v.v.). Điều này cho thấy mối tương quan chặt chẽ giữa Nhật ký sự kiện, Windows Registry và nhiều DLL trên hệ thống. Điều đó cũng có nghĩa là các ứng dụng của bên thứ ba ghi vào Nhật ký sự kiện sẽ cần bao gồm các tệp tin của riêng họ.

Trước Windows 2003, các sự kiện đăng nhập sẽ chỉ chứa tên NetBIOS của hệ thống mà đăng nhập bắt nguồn. Bắt đầu với Windows 2003, Nhật ký sự kiện bảo mật ghi lại cả tên máy trạm và địa chỉ Giao thức Internet (IP) của hệ thống, như Hình 5.2 minh họa.





Hình 5. 2. Bản ghi sự kiện Windows 2003 show IP address

Thông tin được hiển thị trong Hình 5.2 (như Địa chỉ mạng nguồn) có thể cực kỳ hữu ích trong quá trình điều tra, cụ thể nhất là vì địa chỉ IP của hệ thống từ xa có thể nhìn thấy trong bản ghi sự kiện. Thông tin này có thể được sử dụng để xác định nguồn đăng nhập và đăng xuất.

Ngay cả khi không có tệp tin DLL, không khó để biết các bản ghi sự kiện khác nhau có liên quan gì, bởi vì có thông tin nhận dạng khác trong bản ghi. Ví dụ, trong Hình 5.2, chúng ta thấy ID sự kiện, nguồn sự kiện và thông tin khác mà chúng ta có thể sử dụng để sắp xếp khi phân tích các bản ghi sự kiện. Ngoài ra còn có một dấu ngày/thời gian mà chúng ta có thể sử dụng để phân tích dòng thời gian; thực tế, có hai tem ngày/giờ trong một bản ghi sự kiện (như chúng ta sẽ thảo luận sau trong chương này). Microsoft cung cấp rất nhiều thông tin liên quan đến một số hồ sơ sự kiện mà bạn có thể thấy. Ví dụ: nếu bật tính năng kiểm tra và ghi nhật ký các sự kiện đăng nhập/đăng xuất (xem Chương 4 để biết cách xác định điều này từ một hình ảnh thu được), điều tra viên sẽ thấy ID sự kiện 528 (đăng nhập thành công) và 538 (đăng xuất) trong Nhật ký sự kiện bảo mật.

Nếu anh ta thấy một số bản ghi sự kiện tất cả có ID sự kiện 528, anh ta sẽ muốn kiểm tra loại đăng nhập, bởi vì có chín mã loại đăng nhập khác nhau. Bảng 5.1 liệt kê các mã loại đăng nhập bảo mật khác nhau để đăng nhập thành công và ý nghĩa của chúng.

Bảng 5. 1. Các loại đăng nhập sự kiện

Loại đăng nhập	Tiêu đề	Mô tả
----------------	---------	-------

2	Interactive	Kiểu đăng nhập này chỉ ra rằng người dùng đăng nhập tại bàn điều khiển
3	Network	Một người dùng/máy tính đã đăng nhập vào máy tính từ mạng, chẳng hạn như thông qua sử dụng mạng, truy cập vào một chia sẻ mạng, hoặc một lượt xem mạng thành công hướng vào một chia sẻ mạng. (Điều này đã được thay thế theo ID sự kiện 540)
4	Batch	Dành cho các ứng dụng chạy theo đợt
5	Service	Dịch vụ đăng nhập
6	Proxy	Không được hỗ trợ
7	Unlock	Người dùng đã mở khóa máy trạm
8	NetworkClearText	Một người dùng đã đăng nhập vào mạng và thông tin đăng nhập của người dùng đã được thông qua hình thức không được mã hóa
9	NewCredentials	Một tiến trình hoặc chuỗi nhân bản hiện tại của nó mã thông báo nhưng chỉ định thông tin đăng nhập mới cho các kết nối ra
10	RemoteInteractive	Đăng nhập bằng Terminal Services hoặc kết nối máy tính từ xa

11	CachedInteractive	Một người dùng đăng nhập vào máy tính với thông tin đã được lưu trữ cục bộ trên máy tính (tên miền bộ điều khiển có thể không có sẵn để xác minh thông tin đăng nhập)
12	CachedRemoteInteractive	Giống như Remote Interactive, được sử dụng nội bộ cho mục đích kiểm toán
13	CachedUnlock	Nỗ lực đăng nhập là để mở khóa một máy trạm

Từ góc nhìn tổng quát hơn, Microsoft cung cấp các bài viết trong Cơ sở kiến thức 299485 (<http://support.microsoft.com/kb/299475>) và 301677 liệt kê sự kiện bảo mật Windows 2000 mô tả. Các sự kiện bảo mật được liệt kê với một mô tả ngắn gọn cũng như giữ chỗ (% 1, % 2, v.v.) trong đó các chuỗi từ bản ghi sự kiện được chèn vào.

### Tip

ID sự kiện 540 (đăng nhập mạng) đã được giới thiệu trong Windows 2000 và có nghĩa tương tự như, và thay thế, ID sự kiện 528 loại 3 (đăng nhập thành công từ mạng). Người ứng phó sự cố hoạt động trong môi trường doanh nghiệp có thể gặp phải các bản ghi sự kiện đề cập đến Kerberos, chẳng hạn như ID sự kiện 672.

Bài viết Cơ sở tri thức Microsoft 301677 (<http://support.microsoft.com/kb/301677>) cung cấp thông tin về các ID sự kiện này cho Windows 2000 và bài viết Cơ sở tri thức 274176 (<http://support.microsoft.com/kb/274176>) mô tả cách liên kết sự kiện đăng nhập tài khoản với sự kiện tạo quy trình, chẳng hạn như khi dịch vụ được bắt đầu với tài khoản người dùng trên Windows XP. Bản ghi ID sự kiện 672 bao gồm địa chỉ IP của khách hàng, đây có thể là thông tin hữu ích trong quá trình kiểm tra.

Với Vista và Windows 2008, các sự kiện đăng nhập đã được thu gọn lại thành một ID sự kiện duy nhất (4624). Bài viết 947226 của Cơ sở tri thức Microsoft (<http://support.microsoft.com/kb/947226>) cung cấp danh sách ID sự kiện bảo mật

cho Vista và Windows 2008 và mô tả phương pháp lấy thông tin chi tiết hơn về các sự kiện thông qua việc sử dụng wevtutil. Exe.

---

Đối với các bản ghi sự kiện khác, nhiều trang web cung cấp thông tin chi tiết về chi tiết bản ghi sự kiện, tại sao các sự kiện được tạo, .... Để biết thông tin chi tiết về các mục cụ thể trong Nhật ký sự kiện ứng dụng, bạn có thể cần kiểm tra với nhà cung cấp. Một trong những trang web tốt nhất mà tôi đã tìm thấy để có được sự hiểu biết về những gì trong bản ghi sự kiện là EventID.net. Một số thông tin có sẵn từ trang EventID.net mà không cần đăng ký, nhưng nếu bạn đang dành nhiều thời gian để điều tra các hồ sơ sự kiện thuộc các loại khác nhau, thì đăng ký đó lệ phí rất xứng đáng với thông tin bổ sung và sự cố được lưu trong Google. Trong nhiều trường hợp, bạn chỉ cần cung cấp ID sự kiện được đề cập và bạn sẽ được cung cấp thông tin về sự kiện này, như được tạo bởi nhiều nguồn khác nhau, cũng như các liên kết đến tài liệu tham khảo. Ví dụ, nếu tôi tìm kiếm ID sự kiện 6009, tôi nhận được bốn nguồn sự kiện khác nhau. Từ đó, tôi có thể nhấp vào chi tiết cho cái tôi muốn (trong trường hợp này, nguồn sự kiện là EventLog) và tôi nhận được bình luận từ hai tác giả cũng như ba liên kết đến trang web Microsoft cung cấp thông tin chi tiết về ID sự kiện. Trong trường hợp này, theo thứ tự khá ngắn, tôi thấy rằng ID sự kiện được tạo khi hệ thống Windows được khởi động (vì vậy thời gian bản ghi sự kiện được tạo gần đúng với thời gian hệ thống được khởi động) và thông tin về hệ điều hành phiên bản được ghi vào trường Mô tả của sự kiện.



### Tip

---

Bản ghi ID sự kiện 6009 từ nguồn EventLog có thể được sử dụng để xác định hoặc xác minh hệ điều hành của hệ thống máy chủ cũng như tên hệ thống. mục Máy tính: sẽ chứa tên máy chủ và mô tả bản ghi sự kiện sẽ chứa một chuỗi xác định phiên bản của hệ điều hành Windows.

---

Bên cạnh EventID.net, một nguồn thông tin tuyệt vời về ghi nhật ký sự kiện của Windows là Nhật ký bảo mật Windows của Eric Fitzgerald, Nhật ký bảo mật Windows và blog Esoterica khác (<http://bloss.msdn.com/ericfitz/default.aspx>). Blog Eric chứa rất nhiều thông tin rất hữu ích liên quan đến Nhật ký sự kiện, bao gồm cả cách chúng có thể được sử dụng để đáp ứng các tiêu chuẩn tuân thủ thẻ thanh toán Visa công nghiệp (PCI), cũng như các mẹo và thủ thuật kiểm toán. Tôi đã tìm thấy rất nhiều thông tin trên blog của Eric, chẳng hạn như mô tả về loại đăng nhập 0, cũng như cách nhận thông tin sự kiện bảo mật chi tiết cho các sự kiện Windows Vista và Windows 2008 Security

Microsoft cũng có Trung tâm thông báo lỗi và sự kiện: Trang web tìm kiếm nâng cao ([www.microsoft.com/technet/support/ee/ee\\_advifed.aspx](http://www.microsoft.com/technet/support/ee/ee_advifed.aspx)) mà bạn có thể sử dụng để thu thập thông tin về các mục Nhật ký sự kiện khác nhau.



### Tip

Bạn còn nhớ thảo luận về tạo tác của thiết bị lưu trữ di động USB trong Chương 4? Trong Windows 2000, bất cứ khi nào thiết bị lưu trữ di động USB được kết nối với hệ thống, Dịch vụ lưu trữ di động đã tạo một bản ghi sự kiện với ID 134. Khi thiết bị bị xóa, nó tạo ra ID sự kiện là 135.

Những sự kiện này không còn hiển thị kể từ Windows XP, và bài viết Cơ sở tri thức 329463 (<http://support.microsoft.com/kb/329463/en-us>) cung cấp manh mối về lý do. Bài viết lưu ý rằng một khi hotfix được cài đặt:

Ấn các thông báo đến của thiết bị Plug and Play. Do đó, bạn không được thông báo về các thiết bị mới.

Vì vậy, bạn không nên thấy thông báo trong Nhật ký sự kiện rằng các thiết bị lưu trữ di động USB đã được chèn hoặc xóa.

---

Ngoài ra, bạn có thể tìm thêm tài liệu bằng cách truy cập vào trang của Randy Franklin UltimateWindowsSecurity.com; anh ta có các trang dành riêng cho Nhật ký sự kiện bảo mật của Windows, bao gồm bảng tham chiếu ID sự kiện và bách khoa toàn thư ([www.ultimatewindowsecurity.com/encyclopedia.aspx](http://www.ultimatewindowsecurity.com/encyclopedia.aspx)). Đối với Nhật ký sự kiện bảo mật, trang web này rất đáng để truy cập và đánh dấu trang.

## Định dạng tệp tin nhật ký sự kiện

Đôi khi trong quá trình điều tra, bạn có thể cần kiểm tra nội dung của tệp .evt Nhật ký Sự kiện theo định dạng dễ hiểu. (Định dạng Nhật ký sự kiện được thảo luận trong phần này liên quan đến các phiên bản của hệ điều hành Windows từ Windows 2000 đến 2003 và không bao gồm Vista.) Vì vậy, bạn trích xuất tệp .evt từ một hình ảnh thu được và bạn chỉ ra rằng bạn chỉ mở tệp trong Trình xem sự kiện. Hoặc bạn có thể thử sử dụng một công cụ như Trình ghi nhật ký sự kiện ([www.eventlogxp.com/](http://www.eventlogxp.com/)), thay vì trình xem sự kiện gốc. Tuy nhiên, khi bạn cố gắng làm như vậy, bạn sẽ nhận được thông báo lỗi cho bạn biết rằng Nhật ký sự kiện là “corrupt-”.

Trước đây, bạn có thể tìm kiếm thông qua các cụm chưa được phân bổ trong một hình ảnh, tìm kiếm một số thông tin có thể hữu ích cho trường hợp của bạn. Trong cả

hai trường hợp, việc biết chi tiết về cấu trúc của tệp Nhật ký sự kiện có thể cực kỳ có giá trị.

Nhật ký sự kiện Windows (dành cho Windows 2000, XP và 2003) là định dạng nhị phân với các tính năng riêng biệt, để nhận biết có thể hỗ trợ điều tra viên nhận biết và giải thích các tệp Nhật ký sự kiện hoặc đơn giản là các bản ghi sự kiện trên hệ thống, trong tệp hoặc nằm trong không gian chưa phân bổ. Mỗi Nhật ký sự kiện bao gồm một phần tiêu đề và một loạt các bản ghi sự kiện, cả hai chúng ta sẽ thảo luận chi tiết. Nhật ký sự kiện được duy trì dưới dạng bộ đệm tròn, do đó, khi các bản ghi sự kiện mới được thêm vào tệp, các bản ghi sự kiện cũ hơn sẽ được chuyển ra khỏi tệp.

## Tiêu đề nhật ký sự kiện

Tiêu đề Nhật ký sự kiện được chứa trong 48 byte đầu tiên của tệp Nhật ký sự kiện hợp lệ. Nếu tệp .evt không bị hỏng theo bất kỳ cách nào, tiêu đề sẽ xuất hiện tương tự như tiêu đề Nhật ký sự kiện mẫu trong Hình 5.3.

```
00000000h: 30 00 00 00 4C 66 4C 65 01 00 00 00 01 00 00 00 ; 0...LfLe.....
00000010h: 30 00 00 00 F0 A9 00 00 AD 00 00 00 01 00 00 00 ; 0...ð@..-.....
00000020h: 00 00 01 00 09 00 00 00 80 3A 09 00 30 00 00 00 ; .....€:..0...
```

Hình 5. 3. Tiêu đề nhật ký sự kiện

Tiêu đề Nhật ký sự kiện bao gồm 12 giá trị DWORD riêng biệt. Bảng 5.2 liệt kê chín trong số các giá trị đó và cung cấp một mô tả ngắn gọn về từng giá trị.

Bảng 5. 2. Cấu trúc tiêu đề nhật ký sự kiện

Offset	Size	Description
0	4 bytes	Kích thước của hồ sơ; đối với tiêu đề tệp .evt, kích thước là 0x30 (48) byte. Kích thước bản ghi sự kiện là 56 byte
4	4 bytes	Magic number ( <i>LfLe</i> )
16	4 bytes	Phần bù trong tệp .evt của bản ghi sự kiện cũ nhất
20	4 bytes	Phần bù trong tệp .evt sang bản ghi sự kiện tiếp theo được viết
24	4 bytes	ID của bản ghi sự kiện tiếp theo
28	4 bytes	ID của bản ghi sự kiện cũ hơn

32	4 bytes	Kích thước tối đa của tệp tin .evt ( từ cơ quan đăng ký)
40	4 bytes	Thời gian lưu giữ hồ sơ sự kiện (từ cơ quan đăng ký)
44	4 bytes	Kích thước của bản ghi (lặp lại DWORD ở offset 0)

Giá trị của tầm quan trọng trong tiêu đề là số ma thuật của người Viking, xuất hiện dưới dạng LfLe bắt đầu ở byte thứ tư (DWORD thứ hai) trong tiêu đề. Giá trị này là duy nhất cho Nhật ký sự kiện Windows (cho Windows 2000, XP và 2003) và được liên kết với các bản ghi sự kiện. Microsoft gọi giá trị này là ELF\_LOG\_SIGNATURE. (Mô tả về cấu trúc bản ghi sự kiện tại trang web của Microsoft nói rằng đây là giá trị DWORD luôn được đặt thành ELF\_LOG\_SIGNATURE. Để lưu ý rằng kích thước của bản ghi (cho tiêu đề, 0x30, hoặc 48 byte) ngoặc cho tiêu đề, xuất hiện ở cả đầu và cuối của bản ghi tiêu đề. Điều này cho phép điều tra viên lập trình (sử dụng mã) hoặc thủ công (sử dụng trình soạn thảo hex) xác định vị trí tiêu đề (hoặc bản ghi sự kiện), cho dù đang xem tệp Nhật ký sự kiện, không gian chưa phân bổ hoặc tệp không xác định. Số ID cho bản ghi sự kiện tiếp theo được viết và bản ghi sự kiện cũ nhất có thể được sử dụng để xác định tổng số bản ghi sự kiện mà điều tra viên sẽ thấy.

## NOTE

Khi chúng tôi làm việc với các tệp, chúng tôi sử dụng thuật ngữ số ma thuật để chỉ một chuỗi byte cụ thể trong tệp duy nhất cho loại tệp hoặc loại tệp đó. Các số ma thuật này được sử dụng để thực hiện phân tích chữ ký tệp, một kỹ thuật được sử dụng để xác định xem một tệp có phần mở rộng tệp chính xác dựa trên số ma thuật của nó hay không. Trong trường hợp tệp Nhật ký sự kiện, số ma thuật là 0x654c664c hoặc như trong Hình 5.3, 4C 66 4C 65. Mặc dù chuỗi byte này dịch sang chuỗi LfLe khi đảo ngược thời gian, nó vẫn được gọi là a con số kỳ diệu.

Các giá trị cho kích thước tối đa của tệp Nhật ký sự kiện và thời gian lưu của các bản ghi sự kiện được lấy từ Sổ đăng ký của hệ thống nơi Nhật ký sự kiện được duy trì.

## Cấu trúc bản ghi sự kiện

Các bản ghi sự kiện có một số giá trị cấu trúc chung với tiêu đề Nhật ký sự kiện, nhưng các bản ghi sự kiện chứa nhiều thông tin hơn, như được minh họa trong Hình 5.4. Tuy nhiên, tiêu đề cơ bản cho bản ghi sự kiện có phần lớn hơn tiêu đề của chính

Nhật ký sự kiện (như được mô tả ở trên), nặng 56 byte. Mặc dù kích thước bản ghi được cung cấp trong bản ghi sự kiện (0xF4 hoặc 244 byte) lớn hơn 56 byte, 56 byte đầu tiên của bản ghi sự kiện tạo thành tiêu đề bản ghi sự kiện.

00000030h:	F4 00 00 00 4C 66 4C 65 01 00 00 00 3D E1 20 43 ;	ó...LfLe....=á C
00000040h:	3D E1 20 43 64 02 00 00 08 00 15 00 06 00 00 00 ;	=á Cd.....
00000050h:	00 00 00 00 72 00 00 00 1C 00 00 00 56 00 00 00 ;	....r.....V...
00000060h:	00 00 00 00 EE 00 00 00 53 00 65 00 63 00 75 00 ;	....i...S.e.c.u.

Hình 5. 4. Cấu trúc bản ghi sự kiện mẫu

Như bạn có thể thấy, số ma thuật Nhật ký sự kiện xuất hiện trong giá trị DWORD thứ hai của bản ghi sự kiện, giống như đối với tiêu đề. Bảng 5.3 cung cấp chi tiết về nội dung của 56 byte đầu tiên của bản ghi sự kiện

Bảng 5. 3. Cấu trúc bản ghi sự kiện

Offset	Size	Description
0	4 bytes	Độ dài của bản ghi sự kiện hoặc kích thước của bản ghi theo byte
4	4 bytes	Reserved; magic number
8	4 bytes	Số bản ghi (Record number)
12	4 bytes	Thời gian tạo ra; được đo bằng thời gian UNIX hoặc số của giây trôi qua kể từ 00:00:00 ngày 1 tháng 1 năm 1970, trong Universal Thời gian phối hợp (UTC)
16	4 bytes	Thời gian viết; được đo bằng thời gian UNIX, hoặc số lượng giây trôi qua kể từ 00:00:00 ngày 1 tháng 1 năm 1970, tại UTC
20	4 bytes	ID sự kiện, dành riêng cho nguồn sự kiện và duy nhất xác định sự kiện; ID sự kiện được sử dụng cùng với tên nguồn để xác định chuỗi mô tả thích hợp trong tệp tin cho nguồn sự kiện
24	2 bytes	Loại sự kiện (0x01 = Error; 0x10 = Failure; 0x08 = Success; 0x04 = Information; 0x02 = Warning)
26	2 bytes	Số chuỗi
28	2 bytes	Danh mục sự kiện



30	2 bytes	Cờ dự trữ
32	4 bytes	Số hồ sơ kết thúc
36	4 bytes	Chuỗi bù; bù vào chuỗi mô tả trong kỷ lục sự kiện này
40	4 bytes	Độ dài của Mã định danh bảo mật người dùng (SID); kích thước của SID người dùng tính theo byte (nếu 0, không có SID người dùng nào được cung cấp)
44	4 bytes	Bù đắp cho người dùng SID trong hồ sơ sự kiện này
48	4 bytes	Độ dài dữ liệu; độ dài của dữ liệu nhị phân liên quan đến kỷ lục sự kiện này
52	4 bytes	Bù đắp dữ liệu (offset to the data)

---

Bảng 5.3 minh họa 56 byte đầu tiên của bản ghi sự kiện. Hãy nhớ rằng độ dài thực tế của bản ghi được liệt kê trong DWORD đầu tiên và cuối cùng của bản ghi. (Kích thước của bản ghi khớp với bản ghi thực, giống như tiêu đề tệp.) Với thông tin này trong tay, đây là một quy trình tương đối đơn giản để phân tích nội dung của tệp Nhật ký sự kiện, trích xuất và hiển thị các bản ghi sự kiện.

Có định nghĩa cấu trúc bản ghi sự kiện cũng cho phép ghép lại các bản ghi sự kiện một phần được tìm thấy trong không gian chưa phân bổ. Sử dụng số ma thuật làm bài hướng dẫn, nhà phân tích có thể tìm kiếm trong không gian chưa phân bổ; Cô ấy nên xác định vị trí số ma thuật, tất cả những gì cô ấy phải làm là đọc DWORD trước cho kích thước của bản ghi sự kiện, sau đó trích xuất số byte đó cho bản ghi sự kiện đầy đủ. Ngay cả khi toàn bộ bản ghi sự kiện không có sẵn, 56 byte đầu tiên sẽ cung cấp bản đồ đường đi để xây dựng lại các phần của bản ghi sự kiện.

## Tools & Traps

---

### Đọc nhật ký sự kiện

Một lần, tôi đã giúp đỡ một trường hợp trong đó một nhà phân tích cực kỳ quen thuộc với Linux đã sử dụng PyFlag ([www.pyflag.net](http://www.pyflag.net)) làm công cụ phân tích điều tra số của anh ta. Anh ấy quyết định rằng anh ấy muốn tôi mở Nhật ký sự kiện và lấy các hồ sơ có sẵn; Anh ấy đã cố gắng làm như vậy, nhưng khi anh ấy sao chép các tệp .evt vào hệ thống máy tính để bàn Windows của mình và cố gắng mở các tệp bằng Trình xem sự kiện, anh ấy đã nhận được một thông báo rằng các tệp bị hỏng.

Tôi đã nghiên cứu về Nhật ký sự kiện và cấu trúc bản ghi sự kiện, vì vậy tôi đã điều chỉnh tập lệnh Perl của mình chỉ một chút và phân tích cú pháp qua các tệp Nhật ký sự kiện, truy xuất tất cả các bản ghi sự kiện mà không gặp vấn đề gì. Tuy nhiên, tôi đã tìm thấy sự khác biệt giữa thông tin tôi nhận được từ tiêu đề của một trong các Nhật ký sự kiện và những gì tôi đã thấy trong đầu ra của các bản ghi sự kiện; bất kể tôi đã tiếp cận tình huống như thế nào, tôi luôn có một bản ghi sự kiện hoàn chỉnh hơn thông tin tiêu đề đang nói với tôi rằng tôi nên có. Sau khi điều tra vấn đề này một thời gian, tôi xác định rằng theo giao diện chương trình ứng dụng (API), một phần của Nhật ký sự kiện ngay trước bản ghi đầu tiên là vùng đệm còn sót lại từ khi Nhật ký sự kiện bị xóa. Vùng đệm này không được API đọc và nếu hệ thống được phép tiếp tục bình thường, nó sẽ bị xóa khỏi bộ đệm tròn vì các bản ghi sự kiện mới được ghi vào tệp. Tuy nhiên, bộ đệm này chứa một bản ghi sự kiện hoàn chỉnh; bởi vì công cụ tôi đang sử dụng không sử dụng API để truy xuất các bản ghi sự kiện mà thay vào đó đọc qua tệp ở chế độ nhị phân, phân tích thông tin mà nó tìm thấy, công cụ đã không nhận ra vùng đệm này.

Mặc dù hồ sơ sự kiện bị mất không có tác động đáng kể đến vụ án, nhưng nó đã cho thấy sự hữu ích (liên quan đến phân tích điều tra số) về việc hiểu định dạng của các tệp nhật định trên các hệ thống Windows và khi có thể, phát triển các công cụ phân tích thông qua thông tin trong các tệp đó theo cách không phụ thuộc vào API Windows. Điều này không chỉ cung cấp cho điều tra viên khả năng phát hiện ra thông tin của Hidden, mà còn cho phép điều tra viên thực hiện phân tích trên các nền tảng khác ngoài Windows (đặc biệt là trên Linux); các nhà điều tra không bị hạn chế trong việc phân tích hình ảnh Windows trên nền tảng Windows

---

Thư mục ch5\code\EVT trên DVD đi kèm chứa một số tập lệnh Perl cho phép bạn thu thập thông tin từ các tệp Nhật ký Sự kiện từ các hệ thống Windows 2000, XP và 2003. Evtstats.pl hiển thị số liệu thống kê đơn giản được thu thập từ tệp .evt, như được hiển thị ở đây:

```
C:\Perl\forensics\evt2xls>evtstats.pl d:\cases\evt\secevent.evt
```

<i>Kích thước tối đa của tệp tin Nhật ký sự kiện</i>	<i>= 65536 bytes</i>
<i>Kích thước thực tế của tệp tin Nhật ký sự kiện</i>	<i>= 65536 bytes</i>
<i>Tổng số bản ghi của sự kiện (thông tin header)</i>	<i>= 172</i>
<i>Tổng số bản ghi của sự kiện (count thực tế)</i>	<i>= 260</i>
<i>Tổng số bản ghi của sự kiện (rec_nums)</i>	<i>= 260</i>
<i>Tổng số bản ghi của sự kiện (sources)</i>	<i>= 260</i>
<i>Tổng số bản ghi của sự kiện (types)</i>	<i>= 260</i>

*Tổng số bản ghi của sự kiện (IDs)*

*= 260*

Kịch bản phân tích cú pháp tiêu đề của tệp Nhật ký sự kiện và xác định số lượng bản ghi cần tồn tại, sau đó phân tích cú pháp thông qua nội dung của chính Nhật ký sự kiện và sử dụng các thẻ khác nhau từ trong mỗi bản ghi sự kiện, thực hiện số lượng thực tế của số lượng hồ sơ sự kiện được tìm thấy trong tệp Nhật ký sự kiện.



### Tip

Để cài đặt mã trong thư mục `ch5\code\EVT` trên hệ thống của bạn, chỉ cần sao chép tất cả các tệp trong thư mục vào hệ thống phân tích của bạn. Nếu bạn sẽ sử dụng các tập lệnh Perl, hãy chắc chắn đã cài đặt Perl và giữ mô-đun `ReadEvt.pm` Perl trong cùng thư mục với các tập lệnh. Ngoài ra, bạn có thể sử dụng các tệp thực thi, nhưng bạn sẽ cần giữ DLL trong cùng thư mục với các tệp EXE.

Tập lệnh `evtrpt.pl` Perl hiển thị số liệu thống kê bổ sung về tệp Nhật ký sự kiện:

```
C:\Perl\forensics\evt2xls>evtrpt.pl
```

```
d:\cases\evt\secevent.evt EVT file parsed:
```

```
d:\cases\evt\secevent.evt (65536 bytes)
```

*Tổng số bản ghi sự kiện đã đếm được: 260*

-----

#### *Event Source/ID Frequency*

<i>Source</i>	<i>Event ID</i>	<i>Count</i>
-----	-----	-----
<i>Security</i>	<i>513</i>	<i>4</i>
<i>Security</i>	<i>514</i>	<i>28</i>
<i>Security</i>	<i>515</i>	<i>34</i>
<i>Security</i>	<i>518</i>	<i>4</i>
<i>Security</i>	<i>520</i>	<i>3</i>
<i>Security</i>	<i>528,2</i>	<i>7</i>
<i>Security</i>	<i>528,5</i>	<i>35</i>
<i>Security</i>	<i>529,2</i>	<i>7</i>
<i>Security</i>	<i>538,2</i>	<i>5</i>
<i>Security</i>	<i>538,3</i>	<i>8</i>

<i>Security</i>	<i>540,3</i>	<i>12</i>
<i>Security</i>	<i>551</i>	<i>7</i>
<i>Security</i>	<i>576</i>	<i>42</i>
<i>Security</i>	<i>612</i>	<i>5</i>
<i>Security</i>	<i>615</i>	<i>5</i>
<i>Security</i>	<i>680</i>	<i>14</i>
<i>Security</i>	<i>806</i>	<i>4</i>
<i>Security</i>	<i>848</i>	<i>4</i>
<i>Security</i>	<i>849</i>	<i>4</i>
<i>Security</i>	<i>850</i>	<i>28</i>

*Total: 260*

-----

*Event*

*Type      Frequency*

*Type                      Count*

-----

*AUDIT\_SUCCESS      245*

*AUDIT\_FAILURE      15*

*Total: 260*

-----

*Date*

*Range      (UTC)*

*Fri Sep 9 01:11:25 2005 to Tue Sep 27 00:38:58 2005*

Tôi sử dụng evtrpt.pl khá thường xuyên khi tôi tiến hành phân tích Nhật ký sự kiện. Tôi thường bắt đầu bằng cách phân tích tệp hive bảo mật cho chính sách kiểm toán (xem Chương 4) để xem loại sự kiện nào tôi sẽ thấy trong Nhật ký sự kiện, cũng như xác định xem có phải kiểm toán không kích hoạt. Từ đó, tôi có xu hướng chạy evtrpt.pl đối với tệp Nhật ký sự kiện (được trích xuất từ hình ảnh thu được) để xác định tần suất của các ID và nguồn sự kiện khác nhau trong tệp Nhật ký sự kiện, cũng như xác định phạm vi ngày của các sự kiện trong Nhật ký sự kiện. Trường thời gian mà evtrpt.pl thu thập là thời gian mà sự kiện được tạo (trái ngược với khi nó được viết) và điều này sẽ cho tôi biết liệu có các bản ghi sự kiện trong tệp nhật ký nằm trong cửa sổ thời gian cho

sự cố trong câu hỏi. Điều này có thể rất lộ liễu đối với các Nhật ký sự kiện khác nhau, đặc biệt nếu Nhật ký sự kiện ứng dụng có chứa các sự kiện do ứng dụng chống vi-rút tạo ra.

Một tập lệnh Perl khác, lsevt.pl, sử dụng mô-đun Perl ReadEvt.pm để phân tích thông qua tệp Nhật ký sự kiện và hiển thị các bản ghi sự kiện theo định dạng liệt kê đơn giản, như được minh họa ở đây:

```
Record Number      : 251
Source             : Security
Computer Name      : PETER
Event ID           : 528
Event Type         : EVENTLOG_AUDIT_SUCCESS
Time Generated     : Mon Sep 26 23:37:51 2005
Time Written       : Mon Sep 26 23:37:51 2005
SID               : S-1-5-21-839522115-1801674531-2147200963-1003
Message Str        : Harlan PETER (0x0,0x141B9C) 2 User32    Negotiate PETER
                   {00000000-0000-0000-0000-000000000000}

Record Number      : 252
Source             : Security
Computer Name      : PETER
Event ID           : 576
Event Type         : EVENTLOG_AUDIT_SUCCESS
Time Generated     : Mon Sep 26 23:37:51 2005
Time Written       : Mon Sep 26 23:37:51 2005
SID               : S-1-5-21-839522115-1801674531-2147200963-1003
Message Str        : (0x0,0x141B9C) SeChangeNotifyPrivilege
                   SeBackupPrivilege
                   SeRestorePrivilege
                   SeDebugPrivilege
```

Lsevt.pl bao gồm phân tích cú pháp người dùng SID (nếu có) thành định dạng có thể đọc được và có thể tương quan với các dữ liệu khác (ví dụ: từ Đăng ký) trong quá trình phân tích.

Lsevt2.pl cung cấp sự linh hoạt hơn một chút so với lsevt.pl ở chỗ nó cho phép bạn chọn xuất định dạng dưới dạng các giá trị được phân tách bằng dấu phẩy (CSV). Bằng cách này, điều tra viên có thể chạy tập lệnh đối với tệp Nhật ký sự kiện Windows bằng dòng lệnh sau:

```
C:\Perl>lsevt2.pl -f d:\cases\appevent.evt -c > testevt.csv
```

Sau đó, cô ấy có thể mở tệp testevt.csv kết quả trong Excel để sắp xếp, tìm kiếm và phân tích. Hơn nữa, lsevt2.pl là một tập lệnh độc lập và không yêu cầu sử dụng mô-đun PerE ReadEvt.pm. Tuy nhiên, lsevt2.pl không dịch người dùng SID sang định dạng dễ nhận biết hơn.

Evt2xls.pl là tập lệnh Perl đọc qua tệp Nhật ký sự kiện, trích xuất tất cả các bản ghi sự kiện, phân tích cú pháp và ghi chúng vào định dạng bảng tính tương thích nhị phân với Microsoft Excel. Điều này cho phép bạn mở bảng tính và sắp xếp trên các trường khác nhau, chẳng hạn như nguồn sự kiện (ví dụ: để hiển thị tất cả các bản ghi sự kiện Popup ứng dụng) hoặc ID sự kiện. Để sử dụng evt2xls.pl, bạn cần chỉ định một số tùy chọn tại dòng lệnh; ví dụ:

```
C:\perl>evt2xls.pl -e d:\case\evt\secevent.evt -o d:\case\secevent.xls
```

Dòng lệnh trước sử dụng khóa chuyển đổi để xác định tệp Nhật ký sự kiện sẽ được đọc và khóa chuyển đổi xác định vị trí và tên của tệp bảng tính đầu ra. Chỉ cần gõ evt2xls.pl vào dòng lệnh, không có đối số, sẽ hiển thị thông tin sử dụng cú pháp. Ví dụ: khóa chuyển đổi sẽ cho phép bạn chỉ định vị trí của tệp báo cáo, tương tự như những gì được tạo bởi evtrpt.pl. Ngoài ra, khóa chuyển đổi xx cho phép bạn chỉ định danh sách ID sự kiện được phân tách bằng dấu phẩy mà bạn muốn bỏ qua hoặc xóa khỏi bảng tính kết quả. Điều này ban đầu được dành cho Nhật ký sự kiện lớn có hơn 65.535 mục, vì một số phiên bản Microsoft Excel bị giới hạn số lượng hàng trên mỗi trang tính. Tuy nhiên, Excel 2007 rõ ràng không chứa giới hạn này và các ứng dụng bảng tính khác, chẳng hạn như ứng dụng là một phần của OpenOffice ([www.openoffice.org/](http://www.openoffice.org/)), không gặp khó khăn khi mở tệp. Hơn nữa, evt2xls.pl sử dụng mô-đun Bảng tính :: WriteExcel Perl để tạo bảng tính và mô-đun Bảng tính :: Đọc hoặc Bảng tính :: ParseExcel có thể được sử dụng để trích xuất dữ liệu từ bảng tính đầu ra.



### Tip

---

Rob Faber đã viết một bài viết xuất sắc có tiêu đề Pháp lý nhật ký Windows Windows: bạn đã bao gồm các bài hát của mình chưa? .pdf).

Trong bài viết, Rob trình bày một số thông tin tuyệt vời có thể được sử dụng trong một loạt các kỳ thi. Nó rất đáng để in ấn vấn đề này của tạp chí INSECURE, nếu không phải cho toàn bộ tạp chí, thì chỉ dành cho bài viết của Rob lẻ.

---

Tất cả các tập lệnh Perl này phân tích cú pháp thông qua các tệp Nhật ký sự kiện ở chế độ nhị phân, bỏ qua hoàn toàn API Windows. Bằng cách này, không chỉ các tệp Nhật ký Sự kiện có thể được phân tích cú pháp trên một nền tảng khác ngoài Windows (Mac OS X, Linux, v.v.), mà một nhà điều tra vẫn có thể phân tích các tệp Nhật ký Sự kiện ngay cả khi Trình xem Sự kiện cung cấp cho anh ta thông báo lỗi rằng tập tin bị lỗi Một số tập lệnh yêu cầu sử dụng mô-đun Perl ReadEvt.pm cũng được bao gồm trong DVD đi kèm.

## Warning

Vào tháng 2 năm 2007, Andreas Schuster đã viết blog về một điều kiện đặc biệt liên quan đến các bản ghi Nhật ký Sự kiện, trong đó một bản ghi được ghi vào cuối tệp .evt nhưng bao quanh phần đầu của tệp để một phần của bản ghi tuân theo tiêu đề. Bản ghi này sẽ được đọc không chính xác bởi các công cụ (chẳng hạn như các tập lệnh Perl được liệt kê trong chương này) tìm kiếm số ma thuật của bản ghi sự kiện, bởi vì chỉ một phần của bản ghi sẽ được xác định. Andreas đã đủ tử tế để cung cấp một tệp .evt ví dụ để các trình phân tích cú pháp có thể được kiểm tra (và cải thiện) đối với điều kiện này (bạn có thể tìm thấy bài đăng trên blog và tệp kiểm tra mẫu tại:

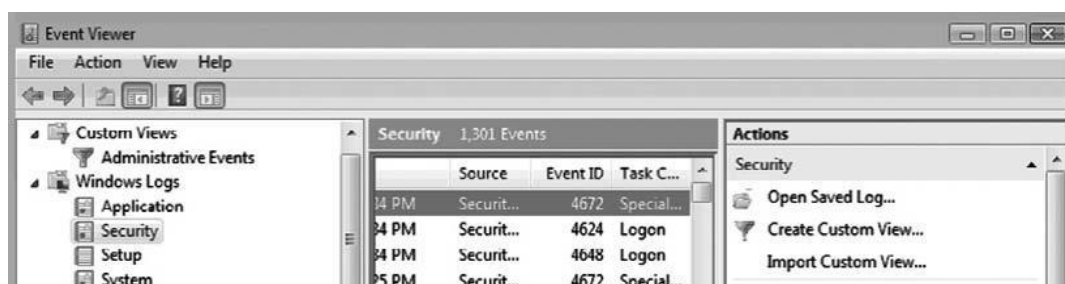
[http://computer.forensikblog.de/en/2007/02/a\\_common\\_misconception.html](http://computer.forensikblog.de/en/2007/02/a_common_misconception.html)).

---

## Nhật ký sự kiện vista

Rất nhiều điều về hệ điều hành Windows đã thay đổi với sự ra đời của Vista, bao gồm cả cấu trúc Nhật ký sự kiện được sử dụng bởi hệ điều hành. Ví dụ: dịch vụ này hiện được gọi là Nhật ký sự kiện Windows thay vì Nhật ký sự kiện và nó có một định dạng hoàn toàn mới cho các bản ghi sự kiện đã lưu. Vista sử dụng định dạng XML để lưu trữ các sự kiện và hiện hỗ trợ bộ sưu tập các bản ghi sự kiện trung tâm.

Các thay đổi khác bao gồm thực tế là mặc dù Vista vẫn duy trì ba loại nhật ký sự kiện chính (Ứng dụng, Bảo mật và Hệ thống), nhưng hiện tại nó có một loạt các danh mục theo đó các sự kiện khác nhau có thể được ghi lại, như Hình 5.5 minh họa.



### Hình 5. 5. Trình xem sự kiện Vista

Như Hình 5.5 minh họa, hiện có nhiều Nhật ký sự kiện, bao gồm một Nhật ký cho Internet Explorer cũng như Sự kiện phần cứng. (Cài đặt Internet Explorer phiên bản 7 mới cũng thêm Nhật ký sự kiện Internet Explorer vào Windows XP và 2003.) Mặc dù bộ chứa nhật ký được tạo nhưng nó không được kích hoạt và dường như chỉ được sử dụng để kiểm tra khả năng tương thích của ứng dụng (<http://msdn.microsoft.com/en-us/library/bb250493.aspx>); như vậy, dường như không có nhiều giá trị từ góc độ phân tích điều tra số.

Cũng lưu ý ở phía dưới bên phải của Hình 5.5, bên dưới hành động, mục có tên đánh kèm tác vụ với sự kiện này. Vì các công cụ được phát triển để phân tích cú pháp thông qua Nhật ký sự kiện Vista và khi người ứng phó sự cố và nhà phân tích điều tra số sử dụng các công cụ đó, mục này sẽ được quan tâm. Andreas Schuster và Eric Fitzgerald đã đăng một số thông tin trên blog tương ứng của họ về cấu trúc được sử dụng để lưu trữ các bản ghi sự kiện.

Andreas cũng cung cấp một bài đăng blog mô tả một số loại dữ liệu có sẵn trong nhật ký sự kiện mới, cũng như trình phân tích cú pháp để chuyển đổi Sự kiện Vista Đăng nhập vào văn bản thuần túy.

*[http://computer.forensikblog.de/en/2007/08/evtx\\_parser.html](http://computer.forensikblog.de/en/2007/08/evtx_parser.html).*

Trên hệ thống Vista trực tiếp, bạn có thể sử dụng lệnh `wevtutil.exe` để truy xuất thông tin về Nhật ký sự kiện Windows mà không dễ thấy thông qua giao diện người dùng Sự kiện. Ví dụ: lệnh sau sẽ hiển thị danh sách Nhật ký sự kiện có sẵn trên hệ thống:

*C:\>wevtutil el*



Từ đó, bạn có thể sử dụng lệnh tiếp theo để liệt kê thông tin cấu hình về Nhật ký sự kiện cụ thể, bao gồm tên và đường dẫn đến tệp:

C: \> wevtutil gl tên đăng nhập

Phần lớn thông tin được hiển thị bởi lệnh này cũng có sẵn trong phần sau

Khóa Register trên hệ thống Vista:

*HKEY\_LOCAL\_MACHINE \ System \ ControlSet00x \ Services \ EventLog \ tên nhật ký*

Đây sẽ là thông tin hữu ích cho những người ứng phó sự cố và các nhà phân tích điều tra số. Các công cụ và kỹ thuật cần được phát triển cho phép người ứng phó sự cố và nhà phân tích điều tra số trích xuất thông tin liên quan và thích hợp từ nhật ký sự kiện Windows trên các hệ thống Vista.

Để dễ phân tích khi kiểm tra Nhật ký sự kiện từ cả hai hệ thống XP và Vista, các tệp Nhật ký sự kiện (.evt) có thể được chuyển đổi sang định dạng Nhật ký sự kiện Windows (.evtx) bằng cách sử dụng bất kỳ tùy chọn nào được liệt kê trong blog trên trang web TechNet (<http://blog.Technet.com/askperf/archive/2007/10/12/windows-vista-and-exported-event-log-files.aspx>).

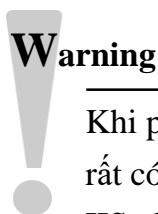
## **Nhật ký IIS**

Máy chủ thông tin Internet Microsoft (IIS) là một nền tảng máy chủ Web phổ biến với cả người dùng và kẻ tấn công. Các quản trị viên có thể dễ dàng cài đặt tình vi đến mức đôi khi họ không nhận ra rằng họ có một máy chủ Web đang chạy trên hệ thống của họ. Nó cũng là một mục tiêu rất phổ biến cho những kẻ tấn công, và với lý do chính đáng. Nhiều lần có các lỗ hổng cho máy chủ Web do các vấn đề về mã hóa hoặc cấu hình, khi không được giải quyết, không chỉ phần mềm máy chủ Web mà toàn bộ nền tảng mở để khai thác. Một trong những cách tốt nhất để khám phá các nỗ lực thỏa hiệp máy chủ Web IIS hoặc chi tiết khai thác thành công là kiểm tra nhật ký được tạo bởi máy chủ Web.

Nhật ký máy chủ Web IIS thường được lưu trữ trong %WinDir%\System32\LogFiles folder. Mỗi máy chủ ảo có thư mục con riêng cho các tệp nhật ký, được đặt tên cho chính máy chủ đó. Trong hầu hết các tình huống, chỉ một phiên bản của máy chủ Web có thể đang chạy, vì vậy thư mục con nhật ký sẽ là W3SVC1. Trong quá trình điều tra, bạn có thể tìm thấy nhiều thư mục con có tên W3SVCn, trong đó n là số lượng máy chủ ảo. Tuy nhiên, vị trí của các bản ghi có thể được cấu hình bởi quản trị viên và có thể được sửa đổi để trở đến bất kỳ vị trí nào, ngay cả một ổ đĩa chung. Theo mặc định, các tệp nhật ký là định dạng văn bản ASCII (đây cũng là cấu hình bởi quản trị viên), có nghĩa là chúng dễ dàng được mở và tìm kiếm. Trong nhiều trường hợp, các tệp nhật ký có thể khá lớn, đặc biệt đối với các trang web

cực kỳ hoạt động, do đó, việc mở và tìm kiếm tệp bằng tay sẽ không khả thi hoặc hiệu quả. Các tìm kiếm có thể được viết kịch bản bằng cách sử dụng tập lệnh Perl hoặc tìm kiếm grep hoặc nếu bạn đang tìm kiếm thứ gì đó cụ thể, khả năng tìm/tìm kiếm được tìm thấy trong bất kỳ trình soạn thảo nào bạn chọn sử dụng cũng có thể hoạt động.

Nói về các tìm kiếm, một trong những câu hỏi lớn nhất mà các nhà điều tra phải đối mặt là, làm thế nào để chúng ta loại bỏ các bản ghi máy chủ Web đồ sộ để tìm ra những gì có thể là kim châm ngôn trong một máy chủ có khối lượng lớn, các tệp nhật ký có thể khá lớn và việc tìm kiếm chúng để tìm dữ liệu liên quan có thể là một nhiệm vụ khó khăn. Đôi khi, sử dụng báo cáo sự cố của nạn nhân có thể giúp điều tra viên thu hẹp khung thời gian khi cuộc tấn công xảy ra, cho phép giảm bớt dữ liệu. Tuy nhiên, điều này không luôn luôn làm việc. Không có gì lạ khi một điều tra viên tìm thấy một hệ thống đã bị xâm phạm hàng tuần hoặc thậm chí vài tháng trước khi bất kỳ hoạt động bất thường nào được báo cáo. Vậy bạn làm gì?



## Warning

Khi phân tích tệp nhật ký IIS, một điều cần lưu ý là dấu thời gian cho các sự kiện rất có thể sẽ ở định dạng GMT (<http://support.microsoft.com/kb/194699>). Khi IIS ghi nhật ký ở định dạng tệp nhật ký mở rộng W3C, là mặc định, tem thời gian được ghi ở định dạng GMT, thay vì dựa trên định dạng múi giờ địa phương cho hệ thống. Do đó, nhật ký IIS sẽ được chuyển sang ngày hôm sau vào nửa đêm GMT (mỗi <http://support.microsoft.com/kb/944884>), cũng sẽ cần được tính đến khi thực hiện phân tích.

Ngoài ra, hãy lưu ý các trường có thể có trong nhật ký trên các phiên bản khác nhau của IIS. Ví dụ: IIS 6.0 và 7.0 bao gồm một trường thời gian sử dụng thời gian trực tuyến (<http://support.microsoft.com/kb/944884>) có thể hữu ích trong việc phân tích nhật ký.

Trong khi trở lại, một thời gian dài trong những năm qua Internet, từ năm 1997, Marcus Marcus Ranum đã phát triển một phác thảo cho cái mà ông gọi là sự thiếu hiểu biết nhân tạo của ED (AI). Ý tưởng cơ bản là nếu bạn loại bỏ tất cả các hoạt động hợp pháp khỏi nhật ký máy chủ Web, những gì bạn còn lại sẽ là bất thường.

## Tools & Traps

## Triển khai “AI”

Tôi đã sử dụng phương pháp “artificial ignorance” của người Viking để lọc các phần khác nhau và nó là một kỹ thuật rất hữu ích. Tôi đã viết một tập lệnh Perl sẽ liên hệ với doanh nghiệp cho tôi (tôi đang làm việc trong một công ty nhỏ có từ 300 đến 400 nhân viên) và thu thập nội dung của các khóa Đăng ký cụ thể từ tất cả các hệ thống đã đăng nhập vào miền. Tôi có thể chạy tập lệnh này trong bữa trưa và quay lại một tệp nhật ký đẹp, dễ phân tích và mở trong Excel. Tuy nhiên, nó khá lớn và tôi chỉ muốn nhìn thấy những thứ cần sự chú ý của tôi. Vì vậy, tôi bắt đầu kiểm tra một số mục tôi tìm thấy và khi tôi xác minh rằng mỗi mục đó là hợp pháp, tôi sẽ thêm nó vào một tệp của các mục nhập được biết đến của Good. Sau đó, tôi sẽ thu thập nội dung của các khóa Registry và chỉ ghi lại những nội dung không xuất hiện trong tệp đã biết. Trong một thời gian ngắn, tôi đã đi từ một vài trang mục đến ít hơn nửa trang mục tôi cần điều tra.

---

Với nhật ký máy chủ Web, đây là một quy trình khá đơn giản để thực hiện loại AI này. Ví dụ: giả sử rằng bạn đang điều tra một trường hợp máy chủ Web có thể đã bị xâm nhập và có một số lượng rất nhỏ tệp trên máy chủ đó là tệp index.html và có lẽ là một nửa tá tệp HTML khác có hỗ trợ thông tin cho trang web chính (about.html, contact.html, links.html, v.v.).

Nhật ký máy chủ IIS Web được lưu ở định dạng ASCII (mặc định) có định dạng khá đơn giản, do đó, việc sử dụng ngôn ngữ kịch bản yêu thích của bạn để mở tệp, đọc trong mỗi mục nhật ký, một dòng tại một mục là một nhiệm vụ khá dễ dàng. thời gian, và thực hiện xử lý. Nhật ký IIS thường sẽ có các tiêu đề cột nằm ở đầu tệp hoặc thông tin đó có thể ở một nơi khác trong tệp nếu máy chủ Web được khởi động lại. Sử dụng các tiêu đề cột làm khóa, sau đó bạn có thể phân tích từng mục để biết thông tin liên quan, chẳng hạn như động từ yêu cầu (GET, HEAD hoặc POST), trang được yêu cầu và trạng thái hoặc mã phản hồi (bạn có thể tìm thấy danh sách IIS Mã trạng thái 5.0 và 6.0 tại <http://support.microsoft.com/kb/318380>) đã được trả lại. Nếu bạn tìm thấy một trang được yêu cầu không có trong danh sách các trang đã biết, bạn có thể đăng nhập tên tệp, ngày/giờ của yêu cầu, địa chỉ IP nguồn của yêu cầu và muốn một tệp riêng để phân tích.

### Warning

Tôi không cung cấp mã cho kỹ thuật này, đơn giản vì không phải tất cả các bản ghi Web IIS đều có cùng định dạng. Thông tin được ghi lại có thể được cấu hình bởi quản trị viên máy chủ Web, vì vậy tôi thực sự không thể cung cấp một kịch thước một kịch thước phù hợp với tất cả các giải pháp. Hơn nữa, các thông số kỹ

thuật chính xác của một tìm kiếm có thể khác nhau giữa các trường hợp. Ví dụ: trong một trường hợp, bạn có thể quan tâm đến tất cả các trang được yêu cầu không phải là một phần của máy chủ Web; trong trường hợp khác, bạn có thể chỉ quan tâm đến các yêu cầu được phát ra từ một địa chỉ IP hoặc dải địa chỉ cụ thể. Trong một trường hợp khác, bạn có thể chỉ quan tâm đến các yêu cầu tạo mã phản hồi cụ thể.

---

“Artificial ignorance” là một cách tiếp cận khi tìm kiếm nhật ký máy chủ Web; công nghệ này rất linh hoạt và có thể được thực hiện trên một loạt các bản ghi và tệp. Một kỹ thuật khác bạn có thể sử dụng là tìm kiếm các cổ vật cụ thể bị bỏ lại bởi các cuộc tấn công cụ thể. Kỹ thuật này có thể rất hữu ích trong trường hợp có nhiều thông tin về cơ sở hạ tầng, mức độ truy cập mà kẻ tấn công thu được và các chi tiết cụ thể khác được biết đến. Ngoài ra, nếu dường như có một lỗ hổng đặc biệt được phát hành vào thời điểm bị xâm nhập hoặc có sự gia tăng các nỗ lực được báo cáo chống lại một khai thác cụ thể, tìm kiếm các tạo tác cụ thể có thể là một kỹ thuật hiệu quả.

## Warning

---

Tôi đã từng ngạc nhiên khi thấy một số cuộc tấn công trở nên phổ biến và tôi đoán rằng nó phải làm với sự thành công của chính cuộc tấn công. Trong một số trường hợp, rất nhiều thông tin rất chi tiết và chính xác về kỹ thuật có sẵn về các cuộc tấn công. Ví dụ: một bảng cheat SQL giải quyết một số biến thể của các cuộc tấn công SQL có sẵn từ <http://ferruh.mavituna.com/sql-injection-chcoeeee-oku/>. Từ thông tin trong bảng cheat này, một điều rất thú vị mà bạn có thể tìm thấy trong các bản ghi do một cuộc tấn công SQL là việc sử dụng từ khóa `sp_password`. Từ khóa này là thường được sử dụng để thay đổi mật khẩu và yêu cầu Microsoft SQL Server không ghi nhật ký lệnh. Đối với kẻ tấn công, đây chỉ là vấn đề nếu đăng nhập được bật trên máy chủ SQL; cuộc tấn công vẫn xuất hiện trong nhật ký máy chủ Web. Tuy nhiên, nó là loại lén lút!

---

Ví dụ: nếu máy chủ Web IIS sử dụng máy chủ cơ sở dữ liệu Microsoft SQL làm nơi lưu trữ dữ liệu, thì một cuộc tấn công cần tìm là SQL injection. Kẻ tấn công có thể sử dụng các truy vấn được gửi đến máy chủ Web để được xử lý bởi máy chủ cơ sở dữ liệu phía sau để trích xuất thông tin, tải tệp lên máy chủ hoặc mở rộng phạm vi tiếp cận của chúng vào cơ sở hạ tầng mạng. Một dấu hiệu nhận biết về một cuộc tấn công tiêm nhiễm SQL là sự tồn tại của `xp_cmdshell` trong các mục nhập tệp nhật ký. `xp_cmdshell` là một thủ tục được lưu trữ mở rộng, là một phần của máy chủ Microsoft SQL có thể

cho phép kẻ tấn công chạy các lệnh trên máy chủ cơ sở dữ liệu có cùng đặc quyền như chính máy chủ (thường là đặc quyền cấp hệ thống). Vào giữa đến cuối năm 2007, chúng tôi đã thấy một số các cuộc tấn công này về cơ bản là các cuộc tấn công văn bản đơn giản, trong đó một lần chỉ ra việc tiêm SQL được tìm thấy trong các tệp nhật ký máy chủ Web IIS (thường là bằng cách tìm kiếm từ khóa cho `xp_cmdshell`), nhà phân tích có thể thấy rõ các hoạt động của kẻ tấn công. Trong nhiều trường hợp, kẻ tấn công sẽ thực hiện trình sát mạng bằng cách sử dụng các công cụ có trong hệ thống Microsoft SQL Server, chẳng hạn như `ipconfig/all`, `nbtstat`, `netstat`, các biến thể của các lệnh `net` để vạch ra các hệ thống khác trên mạng hoặc để thêm tài khoản người dùng vào hệ thống, cũng như sử dụng `ping.exe` hoặc các công cụ khác để xác định kết nối mạng từ hệ thống. Khi điều này được thực hiện, kẻ tấn công sẽ tải các công cụ xuống máy chủ SQL bằng `tftp.exe` hoặc `ftp.exe` (sau khi sử dụng các lệnh `echo` để tạo tệp tập lệnh giao thức truyền tệp [FTP]). Trong một trường hợp cụ thể, kẻ tấn công đã chia một tệp thực thi thành các đoạn 512 byte, sau đó ghi từng đoạn vào bảng cơ sở dữ liệu. Khi tất cả các khối đã được tải vào cơ sở dữ liệu, kẻ tấn công đã nói với cơ sở dữ liệu (một lần nữa, tất cả việc này được thực hiện từ xa thông qua máy chủ Web) để trích xuất các đoạn, lắp lại chúng vào một tệp duy nhất và sau đó khởi chạy tệp đó. Thật hấp dẫn, nó đã làm việc!

#### Tip

Điều quan trọng cần lưu ý là trong một cuộc tấn công SQL, bản thân máy chủ Web không thực sự bị xâm phạm và truy cập trực tiếp bởi kẻ tấn công. Kẻ tấn công đưa ra các truy vấn được xây dựng cụ thể cho máy chủ Web, sau đó chuyển tiếp các truy vấn đó đến cơ sở dữ liệu để xử lý. Một yếu tố quan trọng khác mà nhà phân tích cần lưu ý khi kiểm tra tệp nhật ký máy chủ Web là trạng thái máy chủ Web hoặc mã phản hồi không cho biết mã tiêm SQL có thành công hay không.

Khi năm mới bắt đầu vào mùa xuân năm 2008, các phương tiện truyền thông đã xuất bản một số bài viết mô tả việc sử dụng SQL để lật đổ các máy chủ Web bằng cách tiêm các tệp JavaScript độc hại vào các trang máy chủ Web. Mặc dù điều này nhấn mạnh vấn đề tiêm SQL, nhưng chắc chắn nó đã bỏ qua các cuộc tấn công độc hại được cho là tiếp tục dẫn đến lật đổ hoàn toàn cơ sở hạ tầng mạng nạn nhân. Các nhà phân tích bắt đầu thấy ngày càng nhiều các cuộc tấn công phổ biến, nhưng cũng có sự gia tăng rõ rệt về độ tinh vi của các kỹ thuật tấn công tiêm SQL được sử dụng, vì chúng không còn sử dụng các lệnh ASCII văn bản đơn giản. Các tìm kiếm từ khóa không tìm thấy bất kỳ lượt truy cập nào trên `xp_cmdshell`, ngay cả khi rõ ràng rằng một số hình thức truy cập tương tự như những gì có thể đạt được thông qua SQL đã đạt được. Nhìn kỹ hơn cho

thấy những kẻ tấn công hiện đang sử dụng các câu lệnh DECLARE và CAST để mã hóa các lệnh của chúng theo chuỗi thập lục phân hoặc theo chuỗi các bộ ký tự (ví dụ: ký tự %20 tương đương với một khoảng trắng). Các thuật ngữ độc đáo khác, chẳng hạn như nvarchar, cũng được sử dụng trong các câu lệnh SQL. Để biết ví dụ về mục nhập tệp nhật ký như vậy, hãy xem bài đăng trên blog “tạo khai thác tiêm nhiễm vào SQL” (<http://dominoyesmaybe.blogspot.com/2008/05/create-of-sql-injection-exploits.html>). Do kết quả của những thích ứng mới với cuộc tấn công, các kỹ thuật phân tích và phát hiện mới cần được phát triển.

Theo mặc định, máy chủ Web IIS sẽ ghi lại nhật ký của nó ở định dạng dựa trên văn bản. Định dạng này bao gồm một số trường, chuỗi sẽ xuất hiện trong dòng #Fields: ở đầu tệp nhật ký. Một phương tiện phân tích có thể được sử dụng để phát hiện các cuộc tấn công SQL injection bất kể mã hóa là phân tích cú pháp thông qua nhật ký, trích xuất trường cs-uri-query, là trang Web đích, chẳng hạn như default.asp hoặc jobs.asp. Sau đó, đối với mỗi trường cs-uri-query duy nhất, hãy theo dõi độ dài của các trường truy vấn cs-uri, hiển thị truy vấn thực tế được nhập cho trang Web đích. Vì các lệnh tiêm SQL thường rất dài hơn nhiều so với các truy vấn thông thường được gửi đến các trang đó trong hoạt động thường xuyên, bạn có thể dễ dàng theo dõi các mục nhật ký quan tâm. Trường gốc cs-uri cũng có thể được sử dụng để xác định trang web nào dễ bị tấn công SQL SQL, chỉ dựa trên nội dung của nhật ký.

Bạn có thể tìm kiếm một số vấn đề khác dựa trên các từ khóa hoặc cụm từ khác nhau. Ví dụ: sự tồn tại của vti\_auth\Author.dll trong nhật ký máy chủ Web có thể chỉ ra sự cố (<http://xforce.iss.net/xforce/xfdb/3682>) với các quyền trên tiện ích mở rộng FrontPage có thể dẫn đến các lỗi của trang Web. Các chữ ký khác mà tôi đã sử dụng trong quá khứ để tìm sâu Nimda ([www.cert.org/advisories/CA-2001-26.html](http://www.cert.org/advisories/CA-2001-26.html)) (xem phần dấu chân hệ thống của nhà cung cấp trong tư vấn CERT) bao gồm các nỗ lực để thực thi cmd.exe và tftp.exe thông qua các URL được gửi tới trình duyệt Web.

## **Ghi chú từ Field**

---

### **Nhật ký máy chủ web**

Một số cam kết có liên quan đến phân tích nhật ký máy chủ Web và trong một số trường hợp, tôi đã thấy các dấu hiệu rõ ràng về việc sử dụng các ứng dụng quét máy chủ Web tự động dựa trên dấu chân của ứng dụng trong các nhật ký. Khi tôi tìm thấy các mục này, tôi muốn hỏi người quản trị máy chủ Web xem tổ chức có chịu quét hay không dựa trên các yêu cầu tuân thủ quy định. Đôi khi, phản hồi là có, vâng, ngày và địa chỉ IP của

các lần quét có thể được gắn trực tiếp với hoạt động được ủy quyền, nhưng điều này không phải lúc nào cũng đúng.

---

Phân tích nhật ký IIS (và máy chủ Web khác) có thể là một chủ đề mở rộng, một chủ đề phù hợp cho toàn bộ một chương. Tuy nhiên, như với hầu hết các tệp nhật ký, các nguyên tắc giảm dữ liệu vẫn giống nhau: Xóa tất cả các mục mà bạn biết nên có ở đó, kể toán cho hoạt động hợp pháp. Hoặc, nếu bạn biết hoặc ít nhất có ý tưởng về những gì bạn đang tìm kiếm, bạn có thể sử dụng chữ ký để tìm kiếm các chỉ dẫn về hoạt động cụ thể.

## **Ghi chú từ Field**

---

### **Nhật ký FTP**

Tôi đã hỗ trợ một cuộc điều tra trong đó ai đó có quyền truy cập vào hệ thống Windows thông qua tiện ích quản lý từ xa (như WinVNC hoặc pcAnywhere) và sử dụng máy chủ Microsoft FTP đã cài đặt để truyền tệp đến và từ hệ thống. Tương tự như máy chủ Web IIS, máy chủ FTP duy trì nhật ký của nó trong thư mục LogFiles, bên dưới thư mục con MSFTPSVCx. Không có dấu hiệu nào cho thấy cá nhân đó đã làm bất cứ điều gì để cố gắng che giấu hoặc làm xáo trộn sự hiện diện của anh ta trên hệ thống và chúng tôi có thể phát triển dòng thời gian hoạt động bằng cách sử dụng nhật ký FTP làm tài liệu tham khảo ban đầu. Nhờ định dạng nhật ký FTP mặc định, chúng tôi không chỉ có dấu ngày/thời gian truy cập của anh ấy và tên người dùng anh ấy đã sử dụng mà còn cả địa chỉ FTP mà các kết nối của anh ấy bắt nguồn. Chúng tôi đã tương quan thông tin đó với tem ngày/giờ từ hoạt động trong Cơ quan đăng ký (ví dụ: khóa UserAssist, v.v.) và Nhật ký sự kiện (một số mục ID 10 sự kiện cho biết kết nối FTP đã hết thời gian do không hoạt động) để phát triển hình ảnh rõ ràng hơn hoạt động của cá nhân này trên hệ thống

---

### **Trình phân tích cú pháp (Log Parser)**

Bây giờ chúng ta đã thảo luận về Nhật ký sự kiện Windows và Nhật ký máy chủ Web IIS, đây là thời điểm tốt để đề cập đến một công cụ mà Microsoft sản xuất cực kỳ hữu ích cho các nhà phân tích (mặc dù nó không nhận được sự chú ý lớn từ nhà cung cấp). Công cụ đó là Log Parser (URL khá dài và có thể thay đổi, do đó, đủ để nói rằng cách tốt nhất để xác định liên kết đến công cụ là Google cho trình phân tích cú pháp log), một công cụ mạnh mẽ cho phép bạn sử dụng SQL để tìm kiếm một số tệp dựa trên

văn bản hoặc XML, cũng như các tệp nhị phân như Nhật ký sự kiện và Register và xuất dữ liệu thành văn bản, SQL hoặc thậm chí định dạng nhật ký hệ thống.

Để làm cho công cụ dễ sử dụng hơn, GUI Visual Pars Parser có sẵn từ [www.codeplex.com/visuallogparser](http://www.codeplex.com/visuallogparser).

Log Parser là một công cụ mạnh mẽ nhưng được đánh giá thấp đến mức mà Gabriele Giuseppini và Mark Burnett đã viết Microsoft Log Parser Toolkit, có sẵn từ Syngress Publishing (cũng như trên Amazon và tại các nhà sách). Ngoài ra, một số tài nguyên có sẵn cung cấp các ví dụ về việc sử dụng Log Parser ở các mức độ phức tạp khác nhau, chẳng hạn như Trung tâm Dev của Windows:

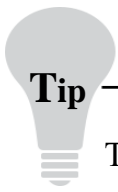
[www.windowsdevcenter.com/pub/a/windows/2005/07/12/logparser.html](http://www.windowsdevcenter.com/pub/a/windows/2005/07/12/logparser.html)

Tôi đã nghe nói về các nhà phân tích sử dụng Log Parser như một vấn đề tất nhiên, cũng như những người sử dụng nó cho các nhiệm vụ cụ thể, chẳng hạn như phân tích cú pháp thông qua số lượng đáng kể Nhật ký sự kiện từ nhiều hệ thống.

## **Lịch sử trình duyệt web**

Đối xứng với nhật ký máy chủ Web là lịch sử duyệt web của Internet Explorer. Internet Explorer được cài đặt theo mặc định trên các hệ thống Windows và là trình duyệt mặc định cho nhiều người dùng. Trong một số trường hợp, như với người dùng doanh nghiệp, một số trang web mạng nội bộ của công ty (để gửi thông tin về thời gian hoặc chi phí đi lại) có thể được thiết kế riêng để sử dụng với Internet Explorer; các trình duyệt khác (như Firefox và Opera) không được hỗ trợ. Khi Internet Explorer được sử dụng để duyệt Web, nó sẽ lưu lại lịch sử hoạt động của nó mà nhà đầu tư có thể sử dụng để phát triển sự hiểu biết về hoạt động của người dùng cũng như thu thập bằng chứng. Các tệp lịch sử trình duyệt Internet Explorer được lưu trong thư mục hồ sơ người dùng, bên dưới thư mục con Cài đặt cục bộ\Tệp Internet tạm thời\Content.IE5. Bên dưới đường dẫn thư mục này, điều tra viên có thể tìm thấy một số thư mục con có tên chứa tám ký tự ngẫu nhiên. Cấu trúc và nội dung của các thư mục này, bao gồm cấu trúc của các tệp index.dat trong mỗi thư mục này, đã được bảo vệ rất dài thông qua các tài nguyên khác, vì vậy chúng tôi đã giành được thông tin đó ở đây. Đối với các hệ thống trực tiếp, các nhà điều tra có thể sử dụng công cụ Lịch sử web (Phiên bản 1.3 có sẵn từ Mandiant.com tại thời điểm viết bài này) để phân tích lịch sử trình duyệt Internet. Khi kiểm tra một hình ảnh, điều tra viên có thể sử dụng các công cụ như ProDiscover, Internet Internet Viewer để hợp nhất thông tin lịch sử trình duyệt thành một thứ dễ xem và dễ hiểu. Có thể xem tệp index.dat từ mỗi thư mục con (từ hệ thống trực tiếp hoặc khi được trích xuất từ hình ảnh) bằng các công cụ như Index Dat Spy và Bộ phân tích Index.dat ([www.systemance.com/indexdat.php](http://www.systemance.com/indexdat.php)).





### Tip

Thông thường khi bạn tiến hành điều tra, có những nơi bạn có thể tìm kiếm thông tin về những gì bạn sẽ thấy. Ví dụ: nếu kiểm toán trên hệ thống được thiết lập để ghi lại các lần đăng nhập thành công và bạn có thể thấy từ Cơ quan đăng ký khi nhiều người dùng khác đăng nhập lần cuối, bạn sẽ thấy các bản ghi sự kiện đăng nhập thành công trong Nhật ký sự kiện bảo mật. Liên quan đến lịch sử duyệt Internet, Internet Explorer có cài đặt cho số ngày nó sẽ giữ lịch sử của các URL đã truy cập. Bạn có thể tìm thấy cài đặt đó trong hive người dùng (tệp ntuser.dat hoặc HKEY\_CURRENT\_USER nếu người dùng đã đăng nhập), trong KEY\Software\Microsoft\Windows\CurrentVersion\Internet Settings\URLHistory. Giá trị trong câu hỏi là DaysToKeep và cài đặt mặc định là 0x014 hoặc 20 trong ký hiệu thập phân. Nếu dữ liệu được liên kết với giá trị không phải là cài đặt mặc định, bạn có thể giả sử rằng giá trị đã được thay đổi, rất có thể bằng cách chọn Công cụ từ thanh menu Internet Explorer và chọn Tùy chọn Internet, sau đó tìm trong phần Lịch sử của tab Chung. Thời gian LastWrite cho khóa Registry sẽ cho bạn biết khi nào giá trị được thay đổi.

Nhiều nhà điều tra đã quen với việc sử dụng lịch sử duyệt Internet như một cách ghi lại các hoạt động của người dùng. Ví dụ: bạn có thể tìm thấy các tham chiếu đến các trang web mà từ đó các công cụ phần mềm độc hại có thể được tải xuống, MySpace.com hoặc các trang web khác mà người dùng không nên duyệt như với hầu hết các khía cạnh của các đồ tạo tác điều tra số trên một hệ thống, những gì bạn tìm kiếm như là bằng chứng của hồi giáo thực sự phụ thuộc vào bản chất của vụ án của bạn. Tuy nhiên, không có gì nên bỏ qua; một chút thông tin có thể cung cấp manh mối hoặc bối cảnh cho bằng chứng của bạn hoặc trường hợp như một toàn thể. Tuy nhiên, không phải tất cả người dùng đều sử dụng trình duyệt Internet Explorer và một số trình duyệt khác có sẵn, cụ thể là, Mozilla, Firefox, Opera và trình duyệt Google Chrome. Các công cụ tự do có sẵn từ NirSoft ([www.nirsoft.net/utils/](http://www.nirsoft.net/utils/)) cho phép bạn xem lưu trữ lịch sử, bộ nhớ cache và cookie cho một số trình duyệt, cũng như (trong một số trường hợp) truy xuất mật khẩu do chính trình duyệt duy trì. Tất cả các công cụ này có thể cung cấp thông tin cực kỳ có giá trị trong một kỳ thi.

Các công cụ khác có sẵn để phân tích điều tra số các trình duyệt bao gồm điều tra số Firefox (F3) và điều tra số Google Chrome, cả hai đều có sẵn (có tính phí) từ Machor Software ([www.machor-software.com/home](http://www.machor-software.com/home)) và Nhà sử học từ Gaijin (miễn phí, bằng tiếng Đức, từ [www.gaijin.at/dlhistorian.php](http://www.gaijin.at/dlhistorian.php)). Một số bài viết đề cập đến điều tra số trình duyệt Web cũng có sẵn, chẳng hạn như bài đăng trên blog điều tra số của

John McCash, Sans trên điều tra số Safari, cũng như một loạt bài viết gồm hai phần về điều tra số trình duyệt Web từ Keith Jones và Rohyt Belani tại trang web SecurityFocus (phần 1 có tại [www.securityfocus.com/infofocus/1827](http://www.securityfocus.com/infofocus/1827)). Tìm kiếm Google cho điều tra số trình duyệt cho thấy rất nhiều thông tin, mặc dù một số không chi tiết như các bài viết mà tôi đã đề cập. Tuy nhiên, rất nhiều công việc đang được thực hiện và ghi lại trong lĩnh vực này, vì vậy hãy theo dõi.

Link bài viết Sans trên điều tra số Safari là:

(<http://sansforensics.wordpress.com/2008/10/22/safari-browser-forensics/>)

## Các tệp nhật ký khác

Các hệ thống Windows duy trì một số tệp nhật ký khác ít được biết đến hơn trong suốt quá trình cài đặt ban đầu của hệ điều hành và các hoạt động hàng ngày. Một số tệp nhật ký này nhằm ghi lại các hành động và lỗi xảy ra trong quá trình thiết lập. Các tệp nhật ký khác được tạo hoặc gắn vào chỉ khi một số sự kiện nhất định xảy ra. Các tệp nhật ký này có thể cực kỳ có giá trị đối với một nhà điều tra, người không chỉ hiểu rằng họ tồn tại mà còn những hoạt động nào gây ra sự mở rộng hoặc mở rộng của họ và cách phân tích và hiểu thông tin họ chứa. Trong phần này, chúng tôi sẽ xem xét một vài tệp nhật ký này.

## Setuplog.txt

Tệp setuplog.txt, nằm trong thư mục Windows, được sử dụng để ghi thông tin trong quá trình thiết lập, khi Windows được cài đặt. Có lẽ điều quan trọng nhất đối với một nhà điều tra về tệp tin này là nó duy trì dấu thời gian trên tất cả các hành động được ghi lại, cho bạn biết ngày và thời gian hệ thống được cài đặt. Thông tin này có thể giúp bạn thiết lập dòng thời gian hoạt động trên hệ thống.

An excerpt of a setuplog.txt file from a Windows XP SP2 system is shown here:

08/07/2006

16:14:22.921,d:\xpsprtm\base\ntsetup\syssetup\syssetup.c,6434,  
BEGIN\_SECTION,Installing Windows NT

08/07/2006

16:14:24.921,d:\xpsprtm\base\ntsetup\syssetup\wizard.c,1568,,  
SETUP: Calculating registry size

08/07/2006

16:14:24.921,d:\xpsprtm\base\ntsetup\syssetup\wizard.c,1599,,  
SETUP: Calculated time for Win9x migration = 120 seconds

08/07/2006

16:14:24.937,d:\xpsprtm\base\ntsetup\syssetup\syssetup.c,6465,  
BEGIN\_SECTION,Initialization

08/07/2006

16:14:24.984,d:\xpsprtm\base\ntsetup\syssetup\syssetup.c,6585,  
BEGIN\_SECTION,Common Initialiazation

08/07/2006

16:14:25.000,d:\xpsprtm\base\ntsetup\syssetup\syssetup.c,1674,  
BEGIN\_SECTION,Initializing action log

08/07/2006 16:14:25.046,d:\xpsprtm\base\ntsetup\syssetup\log.c,133,,GUI  
mode Setup has started.

08/07/2006

16:14:25.078,d:\xpsprtm\base\ntsetup\syssetup\syssetup.c,1679,  
END\_SECTION,Initializing action log

08/07/2006

16:14:25.093,d:\xpsprtm\base\ntsetup\syssetup\syssetup.c,1764,  
BEGIN\_SECTION,Creating setup background window

## Warning

---

Trong khi viết cuốn sách này, tôi chắc chắn để có một cái nhìn tại các phiên bản khác nhau của Windows liên quan đến các tập tin setuplog.txt. Trên Windows 2000, tệp có dấu thời gian, nhưng không có ngày nào được đưa vào. Trên Windows XP và 2003, các nội dung của tập tin là tương tự ở chỗ mỗi mục có một tem thời gian với một ngày. Tôi không tìm thấy tệp setuplog.txt trên Vista.

---

Như bạn có thể thấy trong đoạn trích của tệp setuplog.txt từ hệ thống XP, dấu ngày và thời gian được bao gồm trong mỗi mục.

## Warning

Nếu bạn đang phân tích hình ảnh từ một hệ thống và dấu thời gian mà bạn thấy trong tệp setuplog.txt dường như không có ý nghĩa (ví dụ: dòng thời gian không tương ứng với thông tin khác bạn đã thu thập), hệ thống có thể đã được cài đặt thông qua một hình ảnh ma hoặc được khôi phục từ bản sao lưu. Hãy nhớ rằng tệp setuplog.txt ghi lại hoạt động trong khi cài đặt, vì vậy hệ thống thao tác phải được cài đặt trên hệ thống để tệp cung cấp thông tin hữu ích.

## Setupact.log

Tệp tin setupact.log, nằm trong thư mục của Windows, lưu trữ một danh sách hành động xảy ra trong phần đồ họa của quá trình thiết lập. Trong windows 2000, XP, và 2003, tệp tin này không có dấu thời gian liên quan đến các hành động khác nhau được ghi lại, nhưng ngày mà tệp được tạo ra và sửa đổi lần cuối cùng sẽ cung cấp cho điều tra viên một manh mối về việc khi hệ điều hành được cài đặt. Trên Vista, tệp này chứa các mục bao gồm dấu thời gian và ngày trên nhiều hành động được ghi lại.

## Setupapi.log

Tệp tin setupapi.log (nằm trong thư mục của Windows), chứa một bản ghi của thiết bị, gói dịch vụ, cài đặt hotfix trên hệ thống Windows. Tệp nhật ký trong Windows XP và những version sau của Windows có kích thước lớn hơn so với các phiên bản trước và mặc dù Microsoft sử dụng tệp này chủ yếu cho mục đích khắc phục sự cố, thông tin trong tệp này có thể cực kỳ hữu ích cho một nhà điều tra.

Microsoft lưu trữ một tài liệu được gọi là “cài đặt thiết bị khắc phục sự cố với tệp tin nhật ký SetupAPI” cung cấp rất nhiều thông tin cực kỳ hữu ích về tệp setupapi.log. Ví dụ, tệp setupapi.log liệt kê phiên bản hệ điều hành cùng với các thông tin khác. Nếu tệp setupapi.log bị xóa với bất kỳ lý do gì, hệ điều hành tạo một tệp tin mới và chèn một tiêu đề cài đặt Windows mới.

Cài đặt thiết bị cũng được ghi lại trong tệp tin này, cùng với tem thời gian mà một điều tra viên có thể sử dụng để theo dõi loại hoạt động này trên hệ thống. Trong Chương 4, bạn đã thấy rằng khi thiết bị lưu trữ di động USB (ổ USB, iPod hoặc tương tự) được gắn vào hệ thống Windows, các thay đổi sẽ được ghi lại trong Register). Khi một loại thiết bị cụ thể được gắn vào hệ thống lần đầu tiên, trình điều khiển phải được định vị và tải để hỗ trợ thiết bị. Trong trường hợp có nhiều bản sao của cùng loại thiết bị được gắn vào hệ thống Windows, chỉ có thiết bị đầu tiên được đính kèm sẽ khiến trình điều khiển được định vị. Tất cả các thiết bị tiếp theo cùng loại được kết nối với hệ thống sẽ thực hiện cập nhật trong Register. Hãy xem đoạn trích này từ tệp setupapi.log:

```
[2006/10/18 14:11:53 1040.8 Driver Install] #-019 Searching for hardware ID(s):  
usbstor\disksony____sony_  
dsc_____5.00,usbstor\disksony____sony_dsc_____,usbstor\disksony____,usbs
```

```

tor\
sony____sony_dsc_____5,sony____sony_dsc_____5,usbstor\gendisk,gendisk
#-018 Searching for compatible ID(s): usbstor\disk,usbstor\raw #-198 Command line
processed: C:\WINDOWS\system32\services.exe #I022 Found "GenDisk" in
C:\WINDOWS\inf\disk.inf; Device: "Disk drive"; Driver: "Disk drive"; Provider:
"Microsoft"; Mfg: "(Standard disk drives)"; Section name: "disk_install". #I023 Actual
install section: [disk_install.NT]. Rank: 0x00000006. Effective driver date: 07/01/2001.
#-166 Device install function: DIF_SELECTBESTCOMPATDRV.
#I063 Selected driver installs from section [disk_install] in "c:\windows\ inf\disk.inf".
#I320 Class GUID of device remains: {4D36E967-E325-11CE-BFC1-
08002BE10318}.
#I060 Set selected driver. #I058 Selected best compatible driver.
#-166 Device install function: DIF_INSTALLDEVICEFILES.
#I124 Doing copy-only install of "USBSTOR\DISK&VEN_SONY&PROD_SONY_
DSC&REV_5.00\6&1655167&0".

```

Từ trích đoạn tệp nhật ký này, chúng ta có thể thấy rằng một thiết bị lưu trữ di động USB do Sony sản xuất đã được kết nối lần đầu tiên với hệ thống vào ngày 18 tháng 10 năm 2006. Dựa trên những gì chúng tôi trình bày trong Chương 4, chúng tôi có thể thấy từ mục nhật ký cuối cùng trong đoạn trích thiết bị không có số sê-ri. Tuy nhiên, dấu ngày và thời gian từ phần cài đặt trình điều khiển của MSN cho chúng tôi biết ngày thiết bị được cắm vào hệ thống lần đầu tiên, chúng tôi có thể sử dụng cùng với thời gian sửa đổi cuối cùng của khóa Register thích hợp để xác định thời gian khi thiết bị đã được sử dụng trên hệ thống.

## Netsetup.log

Tệp tin netsetup.log được tạo trong thời gian cài đặt hệ thống; trong Windows XP bạn có thể tìm nó trong thư mục Windows\Debug. Tệp tin ghi lại thông tin về thành viên nhóm làm việc và miền cho hệ thống, lưu dấu thời gian trong tất cả tin nhắn nó ghi lại. Các tem thời gian bên trong tệp tin netsetup.log xảy ra trong khung thời gian tương tự như thời gian trong các tệp tin setuplog.txt. Các mục bổ sung sẽ được thêm vào tệp nếu nhóm làm việc hoặc miền của hệ thống bị thay đổi. Ví dụ: tôi đã cài đặt hệ điều hành Windows XP cho máy tính xách tay cá nhân của mình vào ngày 7 tháng 8 năm 2006, bằng chứng là dấu thời gian trong các tệp Netsetup.log và setuplog.txt. Vào ngày 19 tháng 11 năm 2006, tôi đã sửa đổi tư cách thành viên nhóm làm việc (tôi đã chuyển từ nhóm làm việc Workgroup sang nhóm làm việc Trang chủ) của hệ thống bằng cách cho phép chia sẻ tệp. Thông tin này đã được ghi lại trong tệp Netsetup.log, cùng với

dấu thời gian thích hợp. Các mục nhật ký cũng sẽ được thêm vào tệp nếu hệ thống được thêm vào hoặc xóa khỏi miền.

## Task Scheduler Log (Nhật ký lập lịch tác vụ)

Dịch vụ lập lịch tác vụ trên các hệ thống Windows có thể được truy cập thông qua `at.exe` hoặc trình hướng dẫn tác vụ theo lịch trình trong bảng điều khiển. Dịch vụ này cho phép người dùng có đặc quyền quản trị viên lên lịch để thực hiện một tác vụ tại một số thời điểm trong tương lai hoặc được chạy liên tục vào các thời điểm cụ thể mỗi ngày, tuần hoặc tháng. Điều này rất có lợi cho việc quản trị và quản lý một hệ thống hoặc toàn bộ mạng. Tính năng tương tự này rất hữu ích cho những kẻ xâm nhập muốn tạo ra một phần mềm độc hại chạy liên tục trên hệ thống bị xâm nhập; thực tế, một số ví dụ về phần mềm độc hại (ví dụ: Conficker/Downadup) sử dụng chính phương pháp này như một phương tiện duy trì liên tục trên một hệ thống bị nhiễm. May mắn thay, trong một tệp có tên là `calendarlg.txt`, dịch vụ này sẽ ghi nhật ký các tác vụ đã được chạy. Tệp nhật ký này thực sự là tên mặc định được liên kết với giá trị `LogFile` nằm trong khóa Register sau:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SchedulingAgent*

Trong Windows XP, nhật ký `calendarlg.txt` được đặt trong thư mục Windows theo mặc định (`C:\Windows`), trong khi trên Windows 2003 và Vista, tệp `calendarlg.txt` được đặt (theo mặc định) trong thư mục Tasks (`C:\Windows\Tasks`).



---

Microsoft lưu rất nhiều thông tin trong các bài viết kiến thức cơ bản. Một điều đặc biệt liên quan đến tác vụ được lên lịch là thông tin về cách giới hạn kích thước của tệp nhật ký tác vụ lên lịch, trong bài viết cơ sở kiến thức 169443 (<http://support.microsoft.com/kb/169443>).

Chú ý rằng cần có đặc quyền cấp quản trị viên để tạo các tác vụ được lập lịch; thông thường, các hệ thống lây nhiễm phần mềm độc hại và sử dụng cơ chế tồn tại này (và khác) là thành công vì người dùng thông thường có các đặc quyền cấp quản trị viên.

---

Nếu trình lập lịch tác vụ không được sử dụng bởi quản trị viên, điều tra viên sẽ thấy các mục ghi rằng dịch vụ lập lịch tác vụ bắt đầu và kết thúc vào các ngày và giờ cụ thể. Vì dịch vụ lập lịch tác vụ thường được thiết lập để khởi động cùng với hệ thống, thông tin này có thể cung cấp cho người điều tra một cái nhìn về thời điểm hệ thống được khởi động và tắt.

Nếu một nhiệm vụ được lập lịch và thực hiện, bạn sẽ thấy các mục đó trong tệp tin schedlgu.txt như ví dụ bên dưới (trích từ một tệp tin schedlgu.txt của Windows XP):

"At1.job" (regedit.exe)

*Started 9/26/2006 4:35:00 PM*

"At1.job" (regedit.exe)

*Finished 9/26/2006 4:35:04 PM*

*Result: The task completed with an exit code of (0).*

"Pinball.job" (PINBALL.EXE)

*Started 9/26/2006 4:36:00 PM*

"Pinball.job" (PINBALL.EXE)

*Finished 9/26/2006 4:36:07 PM*

*Result: The task completed with an exit code of (0).*

Công việc đầu tiên được thiết lập thông qua at.exe và công việc thứ hai (pinball.job) được thiết lập thông qua trình hướng dẫn tác vụ theo lịch trình. Các tệp .job này được giữ trong thư mục Windows\Tasks.

## Notes from the Underground....

### Ẩn các tác vụ theo lịch trình

Có một phương pháp hiệu quả để ẩn các tác vụ theo lịch trình. Tạo một tác vụ theo lịch trình thông qua at.exe hoặc trình hướng dẫn tác vụ theo lịch trình. Truy cập vào Control Panel và mở Scheduled Tasks applet và thấy tác vụ bạn vừa tạo được liệt kê. Bây giờ đóng applet, mở command prompt, điều hướng đến thư mục Windows\Tasks và sử dụng attrib.exe để đặt bit ẩn trong tệp .job. Khi bạn hoàn thành việc này, trở lại Scheduled Tasks applet và bạn không thấy tác vụ được liệt kê nữa. Tất nhiên, các cảnh báo thông thường cho command prompt (bạn phải sử dụng chuyển đổi đúng với lệnh dir) và Windows Explorer (Theo mặc định, nó sẽ không hiển thị tệp tin với bộ thuộc tính ẩn). Tuy nhiên, tác vụ sẽ chạy khi bạn lập lịch cho nó chạy.

Tôi thực sự bắt gặp điều này trong khi viết cuốn sách đầu tiên của tôi. Tôi đã viết một số bài trong khi đi nghỉ và thực hiện các thủ tục trước đó với card trò chơi Solitaire. Tuy nhiên, tôi không xóa các tệp tin, vì vậy khi tôi về nhà, tôi đã đi làm vào một ngày cuối tuần và nghỉ ngơi. Khi tôi trở lại văn phòng của mình, Solitaire đã mở trên máy tính để bàn của tôi và lúc đầu tôi nghĩ ai đó đã ở trong văn phòng của tôi! Sau đó, nó làm tôi ngạc nhiên về những gì đã xảy ra và tôi đã xóa tệp .job.

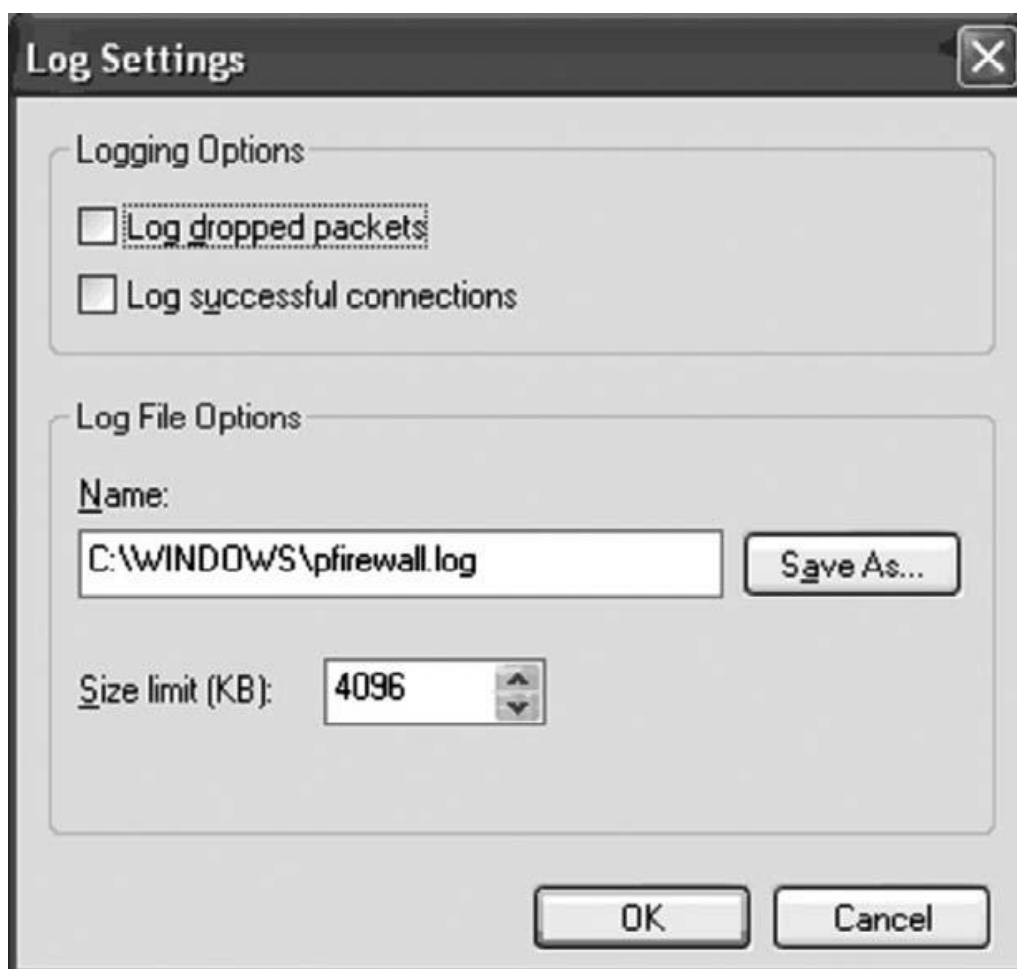
Thật không may, đường dẫn đầy đủ để chạy thực thi bởi tác vụ không được ghi lại trong tệp nhật ký, nhưng một dấu hiệu cho biết khi nào một chương trình được chạy thông qua dịch vụ lập lịch tác vụ được cung cấp.

## XP Firewall Logs

Hầu hết chúng ta đều quen thuộc với các thành phần tường lửa được cung cấp cùng với Windows XP, có lẽ từ các phương tiện truyền thông tin tức và các vấn đề đã được giải quyết trong bản phát hành Windows XP SP2. Hầu hết người dùng thậm chí không nhìn thấy hoặc tương tác với tường lửa XP và nó được bật theo mặc định.

Tường lửa có thể bị vô hiệu hóa (một vài phần mềm độc hại cố gắng làm điều này) và đây có thể là một phần của sơ đồ cấu hình lập thành để dễ dàng quản lý các hệ thống đó. Tường lửa cũng có thể được cấu hình thủ công để cho phép các ứng dụng cụ thể có quyền truy cập mạng.

Tường lửa Windows XP có một tệp tin nhật ký ghi lại hoạt động khác nhau xảy ra, nhưng theo mặc định, không có việc ghi nhật ký (logging) xảy ra. Hình 5.6 minh họa các cài đặt mặc định thông qua hộp thoại cài đặt nhật ký cho tường lửa.



Hình 5. 6. Cấu hình Windows XP Firewall Logging

Như bạn có thể nhìn thấy, các tùy chọn ghi nhật ký khá hạn chế. Ghi nhật ký không được bật theo mặc định, nên bạn không thể tìm nhật ký tường lửa pfirewall.log trong



hầu hết các hệ thống. Sự thiếu sót của một tệp tin nhật ký không có nghĩa là tường lửa không được bật. Tuy nhiên, nếu bạn tìm thấy một tệp nhật ký trên hệ thống, định dạng nhật ký tường lửa rất đơn giản và dễ hiểu. Một đoạn trích từ nhật ký tường lửa mẫu xuất hiện như sau:

```
#Version: 1.0
#Software: Microsoft Internet Connection Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn
tcpack tcpwin icmptype icmpcode info
2003-10-10 10:21:11 DROP ICMP 131.107.0.2 131.107.0.1 - - 60 - - - - 8 0 -
2003-10-10 10:21:16 DROP ICMP 131.107.0.2 131.107.0.1 - - 60 - - - - 8 0 -
2003-10-10 10:21:21 DROP ICMP 131.107.0.2 131.107.0.1 - - 60 - - - - 8 0 2003-10-
10 10:21:26 DROP ICMP 131.107.0.2 131.107.0.1 - - 60 - - - - 8 0 2003-10-10 10:21:34
DROP TCP 131.107.0.2 131.107.0.1 1045 21 48 S 1226886480 0 16384 - - 2003-10-
10 10:21:37 DROP TCP 131.107.0.2 131.107.0.1 1045 21 48 S 1226886480 0 16384
- - 2003-10-10 10:21:43 DROP TCP 131.107.0.2 131.107.0.1 1045 21 48 S
1226886480 0 16384 - -
```

Những trường tag trong phần đầu nhật ký tường lửa cho chúng ta biết các phần khác nhau của nhật ký đề cập đến và cách diễn giải thông tin trong tệp nhật ký. Chúng ta có thể xem từ danh sách các mục trong đoạn trích từ pfilewall.log rằng một số gói giao thức thông báo điều khiển Internet (ICMP) (có lẽ từ ứng dụng ping.exe) đã bị hủy, cũng như một số lần thử kết nối với máy tính trên cổng 21, là cổng mặc định cho máy chủ FTP.



#### WARNING

Thường rất khó để hiểu hoạt động trong một tệp tin pfilewall.log nếu không có thêm hiểu biết chi tiết về hệ thống và môi trường của nó. Ví dụ, khi xem một nhật ký khác của hoạt động dựa trên mạng, như nhật ký tường lửa hoặc hệ thống phát hiện xâm nhập (IDS) của công ty, tôi đã bị hỏi bởi quản trị viên về hoạt động đại diện. Trong trường hợp một hệ thống đơn giản, cố gắng truy cập một cổng phổ biến như cổng 80 (Web server) hoặc 21 (FTP server) không cần thiết chỉ ra cái gì đó đang chạy trong hệ thống đó, mà là ai đó có thể đang cố gắng để xác định xem cái gì đang chạy trong cổng này. Hoạt động điều tra có thể là quét cổng. Nếu nhật ký hiển thị rằng hoạt động tương tự được hướng vào một số hệ thống, trong cùng một khoảng thời gian, điều này chỉ ra việc quét cổng rộng rãi. Vấn đề là chỉ vì một mục nhật ký hiển thị hoạt động được hướng vào một cổng cụ thể, điều đó không nhất

---

thiết có nghĩa là cổng đã mở (rằng một dịch vụ đang lắng nghe trên cổng đó) trên hệ thống. Đây là một hiện tượng hay bị hiểu lầm, đặc biệt phổ biến khi nó đến từ các hoạt động quét rộng rãi trực tiếp từ cổng sử dụng ứng dụng backdoor Trojan.

---

Để dễ xem, một số tiện ích có sẵn miễn phí sẽ phân tích tệp này và giúp dễ hiểu hơn, thậm chí đến mức mã hóa màu nhất định các mục nhất định. Bạn có thể google cho các kết hợp khác nhau của XP và tường lửa và xem để xác định vị trí đáp ứng nhu cầu của bạn.



---

DVD đi kèm bao gồm một thư mục con trong thư mục Chương 5 được gọi là các mẫu. Thư mục con này chứa một tệp có tên nmap\_xp\_scan.txt, chứa dòng lệnh được sử dụng để khởi chạy quét Nmap đối với hệ thống Windows XP SP2 (đã bật tường lửa), cũng như kết quả quét được gửi đến STDOUT. Một tệp khác có tên pfirewall\_nmap\_scan.txt chứa một phần các gói đã ghi được gửi đến hệ thống đích. Để dễ xem, quét Nmap được khởi chạy từ 192.168.1.28 và hệ thống đích là 192.168.1.6.

---

## Mrt.log

Ngoài phần mềm bảo vệ như tường lửa, Microsoft cũng triển khai giải pháp để giải quyết vấn đề với phần mềm độc hại, một trong số đó là công cụ loại bỏ phần mềm độc hại (<http://support.microsoft.com/kb/890830>) hoặc MRT. Giống như công cụ Stringer từ McAfee (<http://vil.nai.com/vil/stringer/>), MRT không được thiết kế phát hiện và bảo vệ chống lại tất cả các mối đe dọa phần mềm độc hại; thay vào đó, MRT được thiết kế để quét và xử lý các mối đe dọa rất cụ thể, được liệt kê trong bài viết 890830. Bạn nên lưu ý rằng mỗi tháng hoặc lâu hơn, công cụ được cập nhật để giải quyết một hoặc hai mối đe dọa khác mặc dù vào tháng 6/2018 phiên bản 1.42 của công cụ giải quyết tổng cộng tám mối đe dọa.

Tệp nhật ký cho MRT, mrt.log, nằm trong thư mục %WinDir%\Debug. Tệp nhật ký này chứa thông tin về phiên bản của công cụ, khi nó được cài đặt và kết quả quét, như được minh họa dưới đây:

*Microsoft Windows Malicious Software Removal Tool v2.5, December 2008 Started On  
Fri Dec 12 06:55:23 2008*

*Results Summary:*

-----  
*No infection found.*

*Return code: 0*

*Microsoft Windows Malicious Software Removal Tool Finished On*

*Fri Dec 12 06:56:52 2008*

Thông tin này có thể hữu ích cho người kiểm tra, giúp cô ấy cảm nhận được trong khi tìm kiếm phần mềm độc hại về những gì hệ thống có thể dễ bị ảnh hưởng và những mối đe dọa nào có thể được bảo vệ chống lại.

Bạn cũng có thể tìm một tệp tin tên mrteng.log trong cùng một thư mục chứa thông tin tương tự, mặc dù không có kết quả quét.

## **Dr.Watson Logs**

Công cụ Dr. Watson (<http://support.microsoft.com/kb/308538/>) đã phát hành với các phiên bản Windows trong một thời gian khá dài, nhưng nói chung, nó không xuất hiện trong cuộc trò chuyện ngày nay. Khi xảy ra lỗi chương trình trên hệ thống, công cụ Dr. Watson thu thập thông tin về hệ thống và lỗi chương trình trong tệp nhật ký văn bản có thể được gửi tới nhân viên hỗ trợ để khắc phục sự cố và giải quyết chương trình. Thông tin này cũng có thể hữu ích khi bạn đang điều tra một vấn đề trên hệ thống.

Tệp nhật ký văn bản được tạo bởi Dr. Watson có tên là drwtsn32.log và được lưu trữ trong thư mục sau:

*C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson*

Thông tin cấu hình cho công cụ Dr. Watson được lưu trong khóa Register sau:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\DrWatson*

Khóa Register này chứa một số giá trị hiển thị trong giao diện Dr. Watson, có thể nhìn thấy khi bạn bấm Start|Run và gõ drwtsn32. Theo mặc định, tệp nhật ký sẽ lưu trữ thông tin từ 10 trường hợp ngoại lệ của chương trình. Các giá trị này sẽ chỉ ra cho điều tra viên những gì cô ấy sẽ thấy nếu có bất kỳ trường hợp ngoại lệ nào xảy ra trên hệ thống.

Khi xảy ra lỗi, thông tin được lưu bởi công cụ Dr. Watson sẽ được thêm vào tệp drwtsn32.log. Đầu tiên Dr. Watson viết một phần bắt đầu bằng ngoại lệ ứng dụng xảy ra: to the file. Phần này chứa thông tin về chương trình gây ra lỗi, cùng với ngày và thời gian xảy ra lỗi:

*App: C:\Perl\bin\perl.exe (pid=4040)*

*When: 8/21/2006 @ 10:17:35.859*

Lưu ý rằng tên của chương trình gây ra lỗi có thể bao gồm đường dẫn đầy đủ đến hình ảnh thực thi cùng với dấu ngày/thời gian. Như chúng ta đã thấy trong các chương

trước, thông tin này có thể hữu ích cho một nhà điều tra, đặc biệt trong các trường hợp chương trình đang nghi vấn là phần mềm độc hại hoặc thứ gì đó được đặt trên hệ thống do bị xâm nhập hoặc sử dụng sai. Dr.Watson sau đó viết một số thông tin hệ thống, danh sách các quy trình đang chạy, danh sách các mô-đun (DLL) được chương trình tải và xếp dumps vào tệp nhật ký có thể được sử dụng để khắc phục ngoại lệ của chương trình. Một điều tra viên có thể sử dụng thông tin này để chứng minh người dùng đã đăng nhập vào hệ thống vào một ngày nhất định, quá trình là gì đang chạy (có thể hiển thị các ứng dụng đã được cài đặt) và chương trình DLL nào được chương trình gây ra ngoại lệ (có thể hiển thị các đối tượng trợ giúp trình duyệt [BHOs] được cài đặt qua Internet Explorer, bất kỳ DLL nào được đưa vào quy trình để lật đổ quá trình đó ...).

#### NOTE

Nhật ký của Dr.Watson có thể cực kỳ có lợi trong việc chứng minh hoặc chứng thực một dòng thời gian hoạt động trên một hệ thống. Trong một trường hợp, một cá nhân đã truy cập một hệ thống đã tải các công cụ lên hệ thống đó và khi cố gắng chạy một số công cụ đó, đã tạo ra các ngoại lệ ứng dụng. Chúng tôi đã tìm thấy nhật ký quyền truy cập của anh ấy vào hệ thống, nhật ký hiển thị khi anh ấy tải lên các công cụ (bao gồm địa chỉ IP mà kết nối của anh ấy bắt nguồn), các mục nhật ký sự kiện hiển thị thông báo bật lên ngoại lệ của ứng dụng và nhật ký của Dr.Watson cho thấy các ứng dụng đã bị lỗi. Ngoài thông tin này, chúng tôi cũng có bối cảnh người dùng cho ứng dụng khi nó bị sập cũng như một danh sách các ứng dụng khác đang chạy tại thời điểm xảy ra sự cố. Tất cả thông tin này đã giúp củng cố quan điểm của chúng tôi về những ứng dụng đã có trước khi người này truy cập hệ thống, ứng dụng nào anh ta đã thêm vào hệ thống và khi anh ta sử dụng chúng.

Dr.Watson cũng tạo ra một tệp kết xuất sự cố (user.dmp) nằm trong cùng thư mục với tệp nhật ký dựa trên văn bản. Tệp kết xuất này chứa các trang riêng được sử dụng bởi quy trình tại thời điểm ngoại lệ và không chứa các trang mã từ các tệp thực thi (EXE, DLL hoặc tương tự). Tệp user.dmp có thể được mở trong công cụ WinDbg, một phần của công cụ gỡ lỗi của Microsoft. Tuy nhiên, tệp user.dmp bị ghi đè với mỗi ngoại lệ, vì vậy bạn sẽ chỉ thấy tệp user.dmp chứa ngoại lệ cuối cùng. Tuy nhiên, tệp user.dmp có sẵn có thể chứa thông tin cực kỳ hữu ích, chẳng hạn như mật khẩu, văn bản thuần túy hoặc dữ liệu không được mã hóa hoặc chỉ dẫn về hoạt động của người dùng.

## Cbs.log

Các hệ thống Windows Vista và 2008 bao gồm ứng dụng trình quản lý gói được sử dụng để cài đặt và gỡ cài đặt các gói khác nhau trên các hệ điều hành. Trình quản lý gói lưu nhật ký của nó trong tệp % WinDir%\Logs\Cbs\cbs.log. Microsoft cung cấp một số thông tin hữu ích giải thích cách phân tích các mục trong tệp này (<http://support.microsoft.com/kb/928228>) và nhà phân tích có thể tìm thấy nội dung hữu ích trong tệp để giúp giải thích vấn đề. Ví dụ: Trình kiểm tra tài nguyên Windows (sfc.exe) ghi nhật ký các mục vào tệp này, xác minh trong quá trình quét mà các tệp hệ thống không thể định cấu hình không thay đổi. Bài viết 928228 của cơ sở tri thức Microsoft cung cấp một ví dụ về quá trình quét xóa sạch, cũng như một ví dụ về sự cố với tệp bị hỏng được tìm thấy và xử lý. Thông tin trong nhật ký này có khả năng là nguồn thông tin tốt cho nhà phân tích, minh họa hoặc loại trừ các vấn đề với các tệp bị hỏng. Theo bài viết 954402 của Cơ sở tri thức Microsoft (<http://support.microsoft.com/kb/954402>), bạn cũng có thể tìm thấy trong tệp cbs.log trên các hệ thống Windows 2008 mà một số tệp không được sửa chữa, mặc dù quá trình quét được báo cáo là hoàn tất thành công.

## Creash Dump Files (Tệp tin kết xuất sự cố)

Chúng tôi đã thảo luận về các tệp kết xuất sự cố trong Chương 3. Tôi nghĩ rằng cũng nên tham khảo chúng trong chương này, vì mục đích hoàn chỉnh. Trong chương 3, chúng tôi đã thảo luận về cách để định cấu hình và tạo ra các tệp kết xuất sự cố, nhưng trong hầu hết các trường hợp, tôi đã thấy rằng các hệ thống không thể tự thực hiện tất cả sửa đổi. Trong một số sự cố hoặc điều tra, nếu bạn tìm thấy một tệp kết xuất sự cố, có thể là một ý tưởng tốt để xem những gì nó giữ. Bạn có thể sử dụng các công cụ như dumpchk.exe (đối với Windows 2000/2003, xem <http://support.micososf.com/kb/156280>; đối với Xp, xem <http://support.micososf.com/kb/315271>) để xác minh tệp kết xuất và đảm bảo rằng nó là hợp lệ. Sau đó, bạn có thể tải tệp vào một công cụ gỡ lỗi (chẳng hạn như WinDbg) và sử dụng các lệnh như *! Process 0 0* để xem danh sách các tiến trình đang chạy tại thời điểm xảy ra sự cố hoặc *lm kv* để xem danh sách các trình điều khiển chế độ kernel đã tải. Hơn nữa, bạn có thể sử dụng các công cụ như biểu thức String.exe, bintext.exe và grep để xác định thông tin cụ thể.

## Recycle Bin (Thùng rác)

Hầu hết các nhà điều tra số đều biết rằng khi một tập tin bị xóa, nó thực sự đã biến mất. Điều này thậm chí còn đúng hơn với sự ra đời của thùng rác trên máy tính để bàn Windows. Thùng rác tồn tại như một phép ẩn dụ để ném các tập tin đi, như thể bạn đang vò nát chúng và ném chúng vào thùng rác. Thùng rác cũng cho phép chúng tôi truy xuất và khôi phục các tệp mà chúng tôi đã vô tình ném đi. Chúng tôi có thể mở

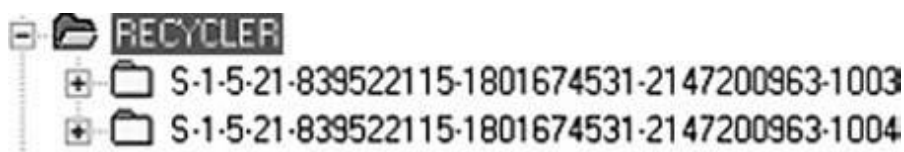
Thùng rác, chọn các tệp mà chúng tôi đã vứt trước đó và khôi phục chúng về vị trí trước đó.

Vì vậy, khi một cái gì đó bị xóa thông qua shell, đó là khi người dùng chọn một tệp trên máy tính để bàn hoặc thông qua Windows Explorer và xóa nó, nó thực sự đã biến mất. Tệp chỉ đơn giản được chuyển đến Thùng rác, xuất hiện theo mặc định trong cấu trúc tệp dưới dạng thư mục Recycler ở thư mục gốc của mỗi ổ đĩa. Trong nhiều trường hợp, thư mục này có thể cung cấp một lượng thông tin đáng kể liên quan đến một cuộc điều tra.

Để hiểu rõ hơn về cách thông tin trong thư mục này có thể được sử dụng làm bằng chứng, hãy xem xét những gì xảy ra khi người dùng xóa một tệp qua shell. Khi mỗi người dùng trên một hệ thống bắt đầu xóa các tệp thông qua shell (trái ngược với việc sử dụng lệnh *del* hoặc *erase* tại command line), thư mục con được tạo cho người dùng đó trong thư mục Recycler; thư mục con đó được đặt tên với SID của người dùng. Ví dụ: từ command prompt, thư mục con sẽ trông giống như thế này:

```
C:\RECYCLER\S-1-5-21-1454471165-630328440-725345543-1003>
```

Khi bạn mở Thùng rác từ máy tính để bàn, thư mục con của người dùng sẽ tự động được mở để xem. Vì vậy, nếu bạn sử dụng máy tính xách tay của người dùng có tài khoản của người dùng đã đăng nhập và bạn đã mở Thùng rác để xem nội dung, bạn sẽ thấy các tệp mà người dùng đã xóa. Nếu bạn chuyển đổi tài khoản và lặp lại quá trình, bạn sẽ tự động thấy các tệp bị xóa trong tài khoản người dùng đang hoạt động. Khi xem thư mục Recycler qua một hình ảnh, bạn sẽ thấy một thư mục con cho mỗi người dùng đang hoạt động trên hệ thống đã xóa các tệp qua shell, như Hình 5.7 minh họa.



Hình 5. 7. Ví dụ về thùng rác được xem qua ProDiscover

Trong mỗi thư mục con, bạn có thể thấy một số tệp, tùy thuộc vào hoạt động của người dùng và mức độ thường xuyên mà người dùng đã dọn sạch thùng rác. Các tệp được gửi đến thùng rác được duy trì theo một quy ước đặt tên cụ thể (<http://support.microsoft.com/kb/136517>), khi bạn hiểu quy ước đó, việc xác định các loại tệp nhất định và loại tệp nào tương đối dễ dàng có được quan tâm. Khi tệp được chuyển đến thùng rác, nó được đổi tên theo quy ước sau:

```
D<original drive letter of file><#>.<original extension>
```

Tên tệp bắt đầu bằng chữ D và theo sau là chữ cái của ổ đĩa gốc mà tệp đã bị xóa, sau đó chỉ mục dựa trên số không cho số tệp (nghĩa là tệp thứ năm bị xóa sẽ có số 4). Các tập tin duy trì phần mở rộng ban đầu. Hơn nữa, một bản ghi được thêm vào tệp INFO2 trong thư mục, đây là tệp nhật ký của tất cả các tệp hiện có trong thùng rác. Số chỉ mục của tệp bị xóa đóng vai trò tham chiếu đến tên tệp gốc (và đường dẫn) được duy trì trong tệp INFO2.

May mắn thay, Keith Jones (trước đây của Foundstone và Mandiant) đã có thể ghi lại định dạng của tệp INFO2 để thông tin này sẽ hữu ích hơn cho các nhà phân tích điều tra số. Tệp INFO2 chứa các bản ghi tương ứng với từng tệp đã xóa trong thùng rác; mỗi bản ghi chứa số bản ghi, chỉ định ổ đĩa, dấu thời gian khi tệp được chuyển đến thùng rác, kích thước tệp và tệp tên gốc và đường dẫn đầy đủ, trong cả ASCII và Unicode.

Tệp INFO2 bắt đầu bằng tiêu đề 16 byte, trong đó giá trị DWORD cuối cùng là kích thước của mỗi bản ghi. Giá trị này là 0x320 (endian nhỏ), có nghĩa là 800 byte. Bản ghi đầu tiên bắt đầu ngay sau tiêu đề và có tổng chiều dài 800 byte.

DWORD đầu tiên (bốn byte) của bản ghi có thể bị bỏ qua. Tên và đường dẫn đầy đủ ban đầu của tệp tin, ở định dạng ASCII, là một chuỗi kết thúc null bắt đầu sau DWORD đầu tiên và chiếm 260 byte đầu tiên của bản ghi. Mở tệp INFO2, bạn sẽ thấy rằng hầu hết không gian được sử dụng bởi định dạng ASCII của tên tệp là số không. Những số không này có thể được loại bỏ để chỉ lấy tên tệp. Phần còn lại của các mục trong hồ sơ xuất hiện như sau:

- Số bản ghi là DWORD nằm ở offset 264 trong bản ghi.
- Trình chỉ định ổ đĩa là DWORD nằm ở offset 268 trong bản ghi. Trình chỉ định ổ đĩa được sử dụng để xác định ổ đĩa đã bị xóa khỏi ổ đĩa; 2 = C: \, 3 = D: \, v.v.
- Dấu thời gian khi tệp tin bị chuyển vào thùng rác là đối tượng 64 bit FILETIME lưu ở offset 272 trong hồ sơ.
- Kích thước của tệp tin bị xóa (theo giá số của kích thước cụm) là DWORD nằm ở độ lệch 280 trong bản ghi.

Tên tệp gốc ở định dạng Unicode sẽ chiếm phần còn lại của bản ghi, từ offset 284 trong bản ghi đến hết (516 byte). Chỉ cần tước bỏ các byte rỗng sẽ cung cấp cho bạn đường dẫn và tên của tệp ở định dạng tiếng Anh ASCII. (Định dạng Unicode rộng hai byte và việc loại bỏ các byte rỗng khỏi nửa sau của định dạng Unicode sẽ khiến bạn chỉ còn định dạng ASCII, bằng tiếng Anh.)

Tập lệnh Perbin.pl Perl nằm trên DVD đi kèm sẽ lấy các phần tử khác nhau từ mỗi bản ghi, hiển thị số bản ghi, dấu thời gian cho biết khi tệp được chuyển đến thùng rác (ở định dạng UTC; cài đặt múi giờ cho hệ thống không được đưa vào tài khoản) và

tên gốc và đường dẫn của tệp. Tập lệnh lấy đường dẫn đến tệp INFO2 làm đối số duy nhất của nó và đầu ra có thể được thao tác dễ dàng để cung cấp bất kỳ cấu trúc và định dạng nào mà nhà điều tra yêu cầu.

Keith Jones cũng đã cung cấp một công cụ có tên Rifiuti (tên có nghĩa là rác trong tiếng Ý) để phân tích nội dung của tệp INFO2. Rifiuti.exe có sẵn miễn phí từ Foundstone.com và sẽ phân tích tệp INFO2 theo định dạng dễ dàng mở để xem ở định dạng bảng tính.

## Note from the underground...

### Hãy nhìn kỹ trong thùng rác

Các nhà điều tra cũng nên đề phòng các tệp đã được thêm vào thư mục Recycler nhưng không được lưu trữ trong một trong các thư mục con SID của người dùng, cũng như các tệp không đáp ứng quy ước đặt tên cho các tệp được chuyển vào thùng rác. Điều này có thể chỉ ra hoạt động độc hại của người dùng hoặc phần mềm độc hại, có ý định cố tình che giấu một tệp. Các nhà điều tra cũng cần lưu ý rằng các ứng dụng như Norton AntiVirus có thể sử dụng thùng rác, Norton's Recycle Bin Protector sẽ đặt một tệp có tên nprotect.log trong thư mục. Datalifter, một công ty sản xuất các công cụ phân tích điều tra số, có NProtect Viewer

([www.dirthifter.com/tutorial/bt/NProtect\\_Using\\_NProtect.htm](http://www.dirthifter.com/tutorial/bt/NProtect_Using_NProtect.htm)) sẽ phân tích nội dung của tệp nprotect.log. Nprotect Viewer là một phần của gói Datalifter .Net Bonus Tools.

Một trong những điều tôi làm khi đào sâu vào một hình ảnh là kiểm tra thời gian sửa đổi lần cuối trên tệp INFO2. Điều này sẽ cho tôi biết khi bản ghi cuối cùng được thêm vào tệp INFO2, gần đúng với thời gian tệp được đề cập đã được chuyển đến thùng rác. Nếu thư mục con của người dùng trong thư mục Recycler chỉ chứa các tệp desktop.ini và INFO2 và tệp INFO2 nhỏ, thời gian sửa đổi cuối cùng đề cập đến thời gian mà người dùng đã xóa thùng rác (nghĩa là nhấp chuột phải vào thùng rác và đã chọn thùng rác rỗng từ context menu).

## Vista Recycle Bin (Thùng rác Vista)

Một khía cạnh khác của hệ điều hành Windows đã thay đổi với sự ra đời của Vista là kiến trúc cơ bản về cách thức thùng rác được triển khai. Mặc dù điều này là minh bạch đối với người dùng, nhưng sự thay đổi này cung cấp một nguồn tài nguyên rất hữu ích cho nhà phân tích điều tra số, như Mitchell Machor đã đề cập trong bài báo



của mình, phân tích điều tra số của Microsoft Windows Vista Recycle Bin ([www.forensicfocus.com/downloads/forensic-analysis-vista-recycle-bin.pdf](http://www.forensicfocus.com/downloads/forensic-analysis-vista-recycle-bin.pdf)). Cũng như các phiên bản trước của Windows, các tệp bị xóa bởi người dùng vẫn được liên kết với SID của người dùng nhưng hiện được tìm thấy trong thư mục C:\\$ Recycl.Bin. Trường hợp Vista tiếp tục xử lý các tệp bị xóa khác nhau là một tệp bị xóa được đổi tên thành "\$R", sau đó là một loạt sáu ký tự ngẫu nhiên, và sau đó là phần mở rộng tệp gốc. Sau đó, một tập tin thứ hai có cùng tên, với "\$I" thay vì "\$R", được tạo ra có chứa thông tin tương tự với những gì được tìm thấy trong tập tin INFO2. Tuy nhiên, tập tin chỉ mục này trong tập tin thùng rác trong thùng rác Vista chỉ chứa tên tệp gốc, tập tin kích thước gốc của tập tin và ngày và thời gian tập tin bị xóa.

## **XP System Restore Points (Điểm khôi phục hệ thống XP)**

Chúng tôi đã thảo luận về các tệp Registry được duy trì trong Điểm khôi phục hệ thống Windows XP trong Chương 4. Trong chương này, chúng tôi sẽ giải quyết các tệp nhật ký khác được lưu trữ trong các điểm khôi phục đó.

### **Rp.log Files**

Rp.log là tệp nhật ký điểm khôi phục nằm trong thư mục điểm khôi phục (RPxx). Nhật ký điểm khôi phục này chứa một giá trị cho biết loại điểm khôi phục, tên mô tả cho sự kiện tạo điểm khôi phục (nghĩa là cài đặt trình điều khiển ứng dụng hoặc thiết bị, gỡ cài đặt ứng dụng hoặc tương tự) và đối tượng FILETIME 64 bit cho biết khi nào điểm khôi phục đã được tạo. Loại điểm khôi phục là giá trị 4 byte (DWORD) bắt đầu từ byte thứ tư của tệp. Mô tả về điểm khôi phục là chuỗi Unicode kết thúc null bắt đầu ở offset 16 (0x10) trong tệp và ngày/giờ tạo là giá trị 8 byte (QWORD) nằm ở offset 528 (0x210) trong tệp. Bạn có thể chạy tập lệnh Perl sr.pl (nằm trên phương tiện đi kèm; đây là tập lệnh sr.pl Perl mà chúng ta đã thảo luận trong Chương 4) trên hệ thống trực tiếp để thu thập thông tin về các điểm khôi phục. Tập lệnh triển khai lớp SystemRestore Windows Management instrumentation (WMI) để truy cập các giá trị loại điểm khôi phục (RestorePointType), mô tả (Description) và thời gian tạo (CreationTime) cho mỗi điểm khôi phục và hiển thị chúng cho người dùng.

Tập lệnh sysrestore.pl Perl (nằm trên DVD đi kèm) là một ProScript mà bạn có thể sử dụng với ProDiscover để lấy thông tin từ các tệp rp.log nằm trong thư mục điểm khôi phục của hình ảnh của hệ thống Windows XP (được mở trong ProDiscover). Tập lệnh mở tệp rp.log trong mỗi thư mục và lấy mô tả về điểm khôi phục và ngày mà điểm khôi phục được tạo.

Mô tả về điểm khôi phục có thể hữu ích cho nhà điều tra, đặc biệt nếu anh ấy tìm kiếm thông tin liên quan đến việc cài đặt hoặc gỡ bỏ một ứng dụng. Điểm khôi phục hệ thống sẽ được tạo khi các ứng dụng và trình điều khiển không dấu được cài đặt, khi cài

đặt Windows AutoUpdate được thực hiện và khi thao tác khôi phục được thực hiện. Điểm khôi phục cũng có thể được tạo bằng tay.

Khi một điểm khôi phục được tạo, một mô tả về sự kiện gây ra việc tạo điểm khôi phục được ghi vào tệp rp.log. Trong nhiều thời điểm, bạn sẽ thấy mô tả điểm kiểm tra hệ thống, là điểm khôi phục được tạo bởi Windows XP cứ sau 24 giờ (cài đặt mặc định). Mô tả dịch vụ phân phối phần mềm đề cập đến các cập nhật Windows đang được cài đặt. Tôi cũng đã thấy các mô tả như đã cài đặt QuickTime, đã xóa ProDiscover 4.8a và Windows Media Player 11 đã cài đặt trên các hệ thống. Mô tả có thể cho người điều tra biết ngày mà một ứng dụng cụ thể đã được cài đặt hoặc gỡ bỏ.

Ngày tạo của điểm khôi phục cũng có thể hữu ích cho nhà điều tra theo những cách khác. Nó không chỉ thêm thông tin vào dòng thời gian hoạt động trên hệ thống, mà điều tra viên còn có thể sử dụng ngày tạo để xác định xem các thay đổi có được thực hiện theo thời gian của hệ thống hay không. Nếu các điểm khôi phục liên tiếp (liên tiếp dựa trên số điểm khôi phục, chẳng hạn như RP80, RP81, RP82, v.v.) có ngày tạo không tuần tự, thì có thể chỉ ra rằng ai đó đã sửa đổi thời gian hệ thống.

## **Change.log.x Files**

Khi điểm khôi phục đã được tạo, các tệp ứng dụng và hệ thống chính tiếp tục được theo dõi để hệ thống có thể được khôi phục về trạng thái cụ thể. Thay đổi tệp được ghi lại và nếu cần, toàn bộ tệp được bảo toàn để hệ thống có thể được khôi phục. Những thay đổi này được ghi lại trong tệp change.log, được đặt trong thư mục điểm khôi phục. Vì các thay đổi đối với các tệp được giám sát được phát hiện bởi trình điều khiển hệ thống tệp điểm khôi phục, tên tệp gốc được nhập vào tệp change.log cùng với số thứ tự và các thông tin cần thiết khác, chẳng hạn như loại thay đổi đã xảy ra (xóa tệp, thay đổi thuộc tính tệp hoặc thay đổi nội dung). Nếu tệp được giám sát cần được bảo tồn (như với thao tác xóa tệp), tệp sẽ được sao chép vào thư mục điểm khôi phục và được đổi tên thành định dạng Axxxxxxx.ext, trong đó x đại diện cho số thứ tự và .ext là phần mở rộng ban đầu của tệp.

Khi hệ thống được khởi động lại, tệp Change.log đầu tiên được gắn thêm số thứ tự (tên của tệp Change.log được thay đổi thành Change.log.1) và tệp Change.log mới được tạo. Tuy nhiên, bạn sẽ không tìm được một tập tin có tên là Change.log trong các thư mục điểm khôi phục; thay vào đó, bạn sẽ tìm thấy một số tệp có tên là Change.log.x, trong đó x là số lượng của tệp Change.log.

Mỗi tệp change.log.x bao gồm một số bản ghi nhật ký thay đổi. Tôi đã có thể định vị một trang web có chứa thông tin chi tiết về định dạng nhị phân của các bản ghi này (bao gồm số ma thuật 0xABCDEF12, để xác định các bản ghi nhật ký thay đổi trong không gian chưa phân bổ). Sử dụng thông tin trên trang web này, tôi có thể tạo

tập lệnh Perl để phân tích và giải thích nội dung của các tệp `change.log.x`. Tập lệnh Perl `lscl.pl` (cho Nhật ký thay đổi LiSt) nằm trên DVD đi kèm.



`Fifo.log` là một tệp khác được duy trì bởi (và nằm trong thư mục gốc của) khôi phục hệ thống (System Restore). Khi khôi phục hệ thống đạt 90% dung lượng, nó sẽ xóa các điểm khôi phục trên cơ sở nhập trước, xuất trước (FIFO), giảm dung lượng xuống 75 phần trăm kích thước tối đa (giá trị mặc định hoặc do người dùng xác định). Tệp `fifo.log` duy trì một danh sách các điểm khôi phục trước đây đã bị xóa hoặc xóa khỏi ổ đĩa được giám sát, cũng như ngày và giờ chúng bị xóa. Điểm khôi phục cũng sẽ là mười lăm năm trước khi họ 90 tuổi.

## Vista Volume Shadow Copy Service

Windows Vista sử dụng chức năng tương tự Điểm khôi phục hệ thống XP để lưu trữ các bản sao của các tệp quan trọng; chức năng này được gọi là Volume Shadow Copy (<http://technet.microsoft.com/en-us/Library/cc785914.aspx>). Giống như các điểm khôi phục XP, các volume shadow copy được lưu trữ trong thư mục System Volume Information và được bật theo mặc định trên Vista. Thông thường, volume shadow copy được tạo khi khởi động hệ thống, nhưng chúng cũng có thể được tạo vào thời điểm khác. Cũng như các điểm khôi phục XP, các Vista Volume Shadow Copy có thể chứa nhiều thông tin có giá trị cho các nhà phân tích điều tra số. Tuy nhiên, không giống như các điểm khôi phục XP, các Volume Shadow Copy rõ ràng chỉ có thể truy cập trực tiếp trên hệ thống Vista, thông qua `vssadmin.exe`. Để biết thông tin về việc khởi động một hình ảnh thu được từ hệ thống Windows, vui lòng xem phần phương pháp phân tích thay thế của chương này.



Christopher Hargreaves và Howard Chivers là tác giả của một bài báo có tựa đề tác động tiềm năng của Windows Vista trên điều tra kỹ thuật số ([www.forensictfocus.com/download/potential-impact-windows-vista.pdf](http://www.forensictfocus.com/download/potential-impact-windows-vista.pdf)), một phiên bản mở rộng có sẵn trên tạp chí điều tra kỹ thuật số. Trong bài viết, họ mô tả một phương pháp tương tự để có được quyền truy cập vào thông tin được lưu trữ trong Volume Shadow Copy như được mô tả trong phần này. Ngoài phương pháp được mô tả trong phần này, ShadowExplorer ([www.shadowexplorer.com/](http://www.shadowexplorer.com/)) cũng có thể được sử dụng để truy cập thông tin

---

cũng như các tệp và thư mục trong Volume Shadow Copy trên hệ thống Vista trực tiếp (và trên Windows 2003, nếu khả năng truy cập được kích hoạt).

---

Sử dụng `vssadmin.exe` trên một hệ thống Vista live, bạn có thể sử dụng câu lệnh dưới đây để liệt kê các Volume Shadow Copy sẵn có:

```
C:\>vssadmin list shadows /for=c: \
```

Khi các Volume Shadow Copy được liệt kê, bạn có thể tạo một liên kết đến bất kỳ chúng sử dụng `mklink.exe` như hướng dẫn (trong đó `n` là số Volume Shadow Copy được xác định) để tạo liên kết tượng trưng đến Volume Shadow Copy:

```
C:\>mklink /d C:\Voln\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyn
```

Tại thời điểm này, các tệp Volume Shadow Copy có thể truy cập được thông qua `C:\Voln` (ví dụ: `C:\Vol3` sẽ là một liên kết tượng trưng đến `HarddiskVolumeShadowCopy3`). Ngoài quy trình này, Rob Lee đã đề cập trong blog *Forensic Sans* (<http://sansforensics.wordpress.com/2008/10/10/Shadow-forensics/>) rằng `dd.exe` có thể được sử dụng để thu được hình ảnh cụ thể. Rob tuyên bố trong bài đăng trên blog của mình rằng lệnh sau, chạy từ ổ USB, có thể được sử dụng để thu được hình ảnh của Volume Shadow Copy:

```
F:\>dd.exe if=\\.\HarddiskVolumeShadowCopy4 of=f:\snapshot4.img --localwrt
```

Bạn có thể tìm `dd.exe` tại <http://gmgsystemsinc.com/fau/>.

Do thực tế là bạn dường như chỉ có thể truy cập các Volume Shadow Copy trên hệ thống Vista trực tiếp, bạn phải cẩn thận để đảm bảo rằng người trả lời biết về thực tế này để có thể thực hiện các bước thích hợp để bảo toàn dữ liệu. Điều này có thể bao gồm việc có được hình ảnh của các Volum Shadow Copy từ các hệ thống trực tiếp hoặc có thể bao gồm lấy tên người dùng và mật khẩu để truy cập hình ảnh thu được đã được khởi động để truy cập vào Volume Shadow Copy.

## **Prefetch Files (Tệp tin tìm nạp trước)**

Bắt đầu với Windows XP, các hệ điều hành của Microsoft đã bắt đầu sử dụng một cái gì đó gọi là “prefetching” để cải thiện hiệu năng hệ thống. XP, Windows 2003 và Vista thực hiện boot prefetching theo mặc định và XP và Vista cũng thực hiện tìm nạp trước ứng dụng theo mặc định.

Để boot prefetching, trình quản lý bộ đệm giám sát các lỗi trang cứng (yêu cầu dữ liệu được đọc từ đĩa) và lỗi trang mềm (yêu cầu dữ liệu trong bộ nhớ được thêm vào bộ làm việc của quy trình) trong bất kỳ trường hợp nào xảy ra trước trong hai phút đầu tiên của quá trình khởi động xử lý, phút đầu tiên sau khi tất cả các dịch vụ Windows đã bắt đầu hoặc 30 giây đầu tiên sau khi bắt đầu shell của người dùng. Dữ liệu lỗi được xử

lý cùng với các tham chiếu đến các tệp và thư mục được truy cập, cuối cùng cho phép tất cả dữ liệu này được truy cập từ một tệp duy nhất thay vì yêu cầu dữ liệu được lấy từ các tệp và thư mục khác nhau nằm rải rác trên ổ cứng. Điều này, làm giảm lượng thời gian cần thiết để khởi động hệ thống.

Trong quá trình tìm nạp trước ứng dụng, trình quản lý bộ đệm sẽ theo dõi 10 giây đầu tiên sau khi quá trình được bắt đầu. Khi dữ liệu này được xử lý, nó được ghi vào tệp .pf trong thư mục Windows\Prefetch. Tên tệp tin này được tạo bằng cách sử dụng tên ứng dụng theo sau là dấu gạch ngang và sau đó là biểu diễn thập lục phân của hàm băm của đường dẫn đến ứng dụng. Do đó, cùng một chương trình chạy từ các vị trí khác nhau sẽ tạo các tệp .pf khác nhau. Ví dụ: trên hệ thống Windows XP, hai tệp .pf khác nhau sẽ được tạo khi Notepad chạy từ thư mục C:\Windows và từ thư mục C:\Windows\system32. (Vì một số lý do, Windows XP có một bản sao của Notepad trong mỗi thư mục.)

Việc tìm nạp trước (prefetching) được kiểm soát bởi khóa Registry sau:

*HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet00x\Control\Session  
Manager\Memory Management\ PrefetchParameters*

Trong khóa này là một giá trị có tên là EnablePrefetcher. Dữ liệu được liên kết với giá trị này sẽ cho bạn biết hình thức tìm nạp trước hệ thống sử dụng:

- 0: Prefetching bị vô hiệu hóa.
- 1: Ứng dụng prefetching được cấp quyền.
- 2: Boot prefetching được cấp quyền.
- 3. Cả ứng dụng và boot prefetching được cấp quyền.

Trong Windows XP và Vista, giá trị mặc định cho EnablePrefetcher là 3; nó là 2 trong Windows 2003. Một trong những điều thú vị về ứng dụng prefetching là Windows Xp chỉ chứa giới hạn 128 tệp tin .pf.

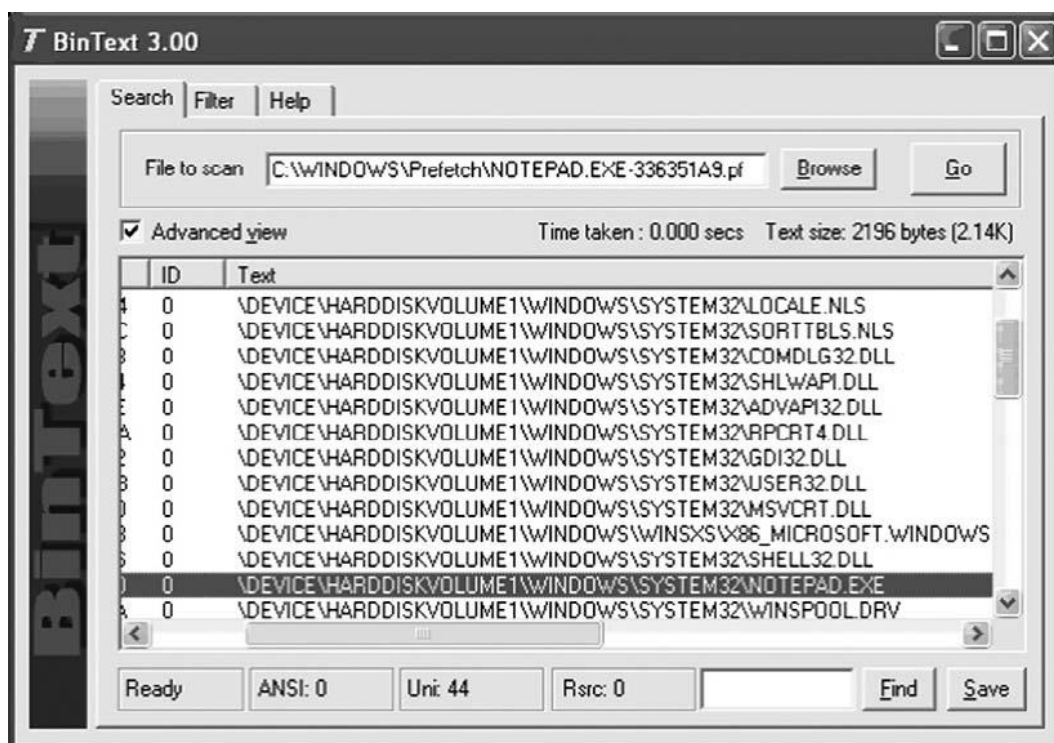
Một số thông tin trong các tệp .pf trong thư mục Prefetch có thể cực kỳ hữu ích cho một nhà điều tra. Ở offset 144 trong tệp là giá trị DWORD (4 byte) tương ứng với số lần ứng dụng được khởi chạy. Ở offset 120 trong tệp là một giá trị 64 bit là đối tượng FILETIME tương ứng với lần cuối cùng ứng dụng được chạy.

Giá trị này được lưu trữ ở định dạng UTC, tương tự như giờ GMT. Tập lệnh prefetch.pl Perl trên DVD đi kèm là một ProScript sẽ phân tích thư mục Prefetch cho các tệp .pf và sau đó trích xuất số lần chạy và thời gian chạy cuối cùng từ các tệp .pf. Tập lệnh pref.pl Perl (phiên bản tập lệnh thực thi được biên dịch của tập tin cũng có sẵn trên DVD đi kèm) sẽ chạy qua thư mục Prefetch trên hệ thống trực tiếp và truy xuất thời gian MAC (nhiều hơn về thời gian MAC trong phần tiếp theo) và thời gian chạy cuối



cùng từ các tệp .pf, gửi đầu ra của nó tới bàn điều khiển ở định dạng được phân cách bằng dấu phẩy (thích hợp để mở trong bảng tính Excel).

Đường dẫn đến ứng dụng đã chạy được lưu trong một chuỗi Unicode trong tệp .pf (cùng với một loạt các chuỗi khác), như Hình 5.8 minh họa.



Hình 5. 8. Minh họa về đường dẫn tệp trong tệp .pf

Bạn có thể tương quan các thông tin khác nhau từ trong tệp .pf với thông tin từ Register (tham khảo Chương 4) hoặc nhật ký sự kiện để xác định ai đã đăng nhập vào hệ thống, ai đang chạy ứng dụng nào... Một trong những lợi ích của mối tương quan này là nếu người dùng cài đặt một ứng dụng, chạy nó và sau đó xóa ứng dụng đó, dấu vết của ứng dụng đó có thể được để lại trong thư mục Prefetch. Khi tôi nói chuyện với các viên chức thuộc cơ quan thực thi pháp luật về các vấn đề như các ứng dụng steganography được sử dụng trong tội phạm trực tuyến, tất cả trong số họ đã nói rằng họ không thường tìm kiếm steganography trừ khi một cái gì đó chỉ ra rằng một ứng dụng như vậy đã được sử dụng. Sự tồn tại của tệp .pf với tên của một ứng dụng cụ thể có thể là dấu hiệu đó.

## Vista SuperFetch

Windows Vista kết hợp một phiên bản tìm nạp trước có tên SuperFetch và tạo các tệp về bản chất tương tự như tìm nạp trước ứng dụng Windows XP. Tuy nhiên, phần bù trong tệp là hơi khác nhau đối với các siêu dữ liệu khác nhau so với các siêu dữ liệu cho các tệp tìm nạp trước của ứng dụng XP. Các tệp lệnh vista\_pref.pl Perl (và các tệp

tin thực thi được biên dịch trên nền tảng tổng hợp, có sẵn trên phương tiện truyền thông kèm theo cuốn sách này) sẽ trích xuất ngày chạy cuối cùng từ tệp tìm nạp trước Vista.

## Shortcut Files

Các tập tin phím tắt có thể chứng minh hữu ích trong quá trình điều tra. Hãy nghĩ về các phím tắt (tập tin với phần mở rộng .lnk) được tạo và truy cập trong sử dụng hàng ngày. Người dùng truy cập tài liệu trên ổ cứng, thiết bị lưu trữ di động hoặc chia sẻ mạng và lối tắt là được tạo trên hệ thống trong thư mục Recent (thư mục Recent là thư mục ẩn trong người dùng thư mục hồ sơ cá nhân). Các phím tắt có thể cung cấp thông tin về các tệp (hoặc chia sẻ mạng) người dùng đã truy cập cũng như các thiết bị mà người dùng có thể đã gắn với hệ thống tại một điểm. Một số công cụ phân tích điều tra số thương mại, chẳng hạn như Bộ công cụ điều tra số AccessData (FTK) và EnCase từ phần mềm hướng dẫn, cung cấp khả năng phân tích nội dung của các tệp .lnk để tiết lộ thông tin được nhúng trong tệp. Ngoài ra, trình phân tích tệp Windows (WFA) từ MiTeC là một công cụ phần mềm miễn phí sẽ phân tích thông tin từ trong tệp .lnk. Cách đây không lâu, Jesse Hager đã xuất bản một tờ giấy trắng, định dạng Windows Shortcut File Format, trong mà ông đã ghi lại các độ lệch và kích thước của các thành phần khác nhau của một tệp phím tắt. Nathan Weilbacher đã viết một bài báo ([www.forensicfocus.com/link-file-evidenterator-value](http://www.forensicfocus.com/link-file-evidenterator-value)) cho trang ForensicFocus.com đã tham chiếu giấy Jesse, và nêu chi tiết giá trị bằng chứng của các tập tin phím tắt Windows.

Tập lệnh Perl lslnk.pl (được tìm thấy trên DVD đi kèm) thực hiện phần lớn giấy trắng Jesse và cho phép điều tra viên xem nội bộ của các tệp phím tắt Windows, hiển thị thông tin như thời gian MAC của tệp đích, cờ và thuộc tính khác nhau cài đặt và thông tin âm lượng cục bộ, một ví dụ được hiển thị ở đây:

Tệp tin shortcut được lưu trữ trong ổ đĩa địa phương.

*Tên ổ đĩa = C-DISK*

*Loại ổ đĩa = Fixed*

*SN ổ đĩa = 0x303d30de*

Nếu tệp đích nằm trên chia sẻ mạng, lslnk.pl sẽ trích xuất đường dẫn đến chia sẻ, như minh họa ở đây:

Tệp tin trong một chia sẻ mạng máy tính.

*Tên chia sẻ mạng máy tính: = \\192.168.1.22\c\$ Z:*

Tập lệnh lslnk.pl mở tệp lối tắt ở chế độ nhị phân, phân tích cú pháp nội dung mà không cần sử dụng API Windows. Bạn có thể sử dụng tập lệnh Perl trên bất kỳ hệ thống nào hỗ trợ Perl. Jake Cunningham đã viết một tập lệnh Perl tương tự có tên lnk-parse.pl và có sẵn trên trang web của JAFAT của anh ấy:

### 5.3. File Metadata (tệp tin siêu dữ liệu)

Thuật ngữ siêu dữ liệu đề cập đến dữ liệu về dữ liệu. Siêu dữ liệu phổ biến nhất được biết về các tệp trên hệ thống Windows là tệp thời gian MAC; trong trường hợp này, MAC là viết tắt của sửa đổi, truy cập, và được tạo ra. Thời gian MAC là dấu thời gian đề cập đến thời gian tệp được sửa đổi lần cuối theo cách nào đó (dữ liệu được thêm vào tệp hoặc bị xóa khỏi tệp), truy cập lần cuối (khi tệp được mở lần cuối) và được tạo ban đầu. Hệ điều hành quản lý như thế nào những lần này phụ thuộc vào hệ thống tệp tin được sử dụng. Ví dụ: trên hệ thống tệp FAT, thời gian là được lưu trữ dựa trên thời gian cục bộ của hệ thống máy tính, trong khi hệ thống tệp NTFS lưu trữ thời gian MAC ở định dạng UTC, tương tự như GMT. Khi các ứng dụng như Windows Explorer hiển thị cài đặt thời gian MAC, múi giờ và thời gian tiết kiệm ánh sáng ban ngày được đưa vào tài khoản. Hơn nữa, độ phân giải thời gian MAC cho hệ thống tệp FAT là 10 mili giây cho thời gian tạo, hai giây cho thời gian sửa đổi và một ngày cho lần cuối cùng thời gian truy cập (ngày, thực sự, đó là hạt nhỏ khủng khiếp). Đối với hệ thống tệp NTFS, cuối cùng thời gian truy cập có độ phân giải một giờ.



#### WARNING

Trên các hệ thống Windows, giá trị đăng ký NtfsDisableLastAccessUpdate (nằm trong HKEY\_LOCAL\_MACHINE\System\CurrentControlset\Control\FileSystem key) sẽ cho phép bạn vô hiệu hóa việc cập nhật lần truy cập cuối cùng trong hệ điều hành (giá trị DWORD là 1 sẽ vô hiệu hóa chức năng). Mặc dù đây là một cài đặt được đề xuất cho các máy chủ tệp có khối lượng lớn (để tối ưu hóa hiệu suất và tăng thời gian phản hồi tổng thể), nó có thể gây khó khăn cho phân tích điều tra số, đặc biệt khi xác định thời gian truy cập tệp. Bạn có thể đặt giá trị này thông qua lệnh fsutil trên Windows XP và 2003 và được thiết lập (nghĩa là, cập nhật lần truy cập cuối bị tắt) theo mặc định trên Vista. Điều này có nghĩa là các nhà phân tích forensic sẽ cần phải phát triển phân tích bổ sung kỹ thuật và phương pháp và dựa vào các nguồn bằng chứng khác.

Một khía cạnh khác của thời gian tệp và thư mục MAC mà một điều tra viên có thể quan tâm theo cách mà tem thời gian được hiển thị



(<http://support.microsoft.com/?kbid=299648>) dựa trên các hành động di chuyển và sao chép khác nhau. Đối với hệ thống tệp FAT16:

- Sao chép myfile.txt từ C:\ đến C:\subdir Myfile.txt giữ cùng ngày chỉnh sửa, những ngày tạo sẽ được cập nhật theo ngày và giờ hiện tại.
- Chuyển myfile.txt từ C:\ đến C:\subdir Myfiel.txt sẽ giữ cùng ngày chỉnh sửa và ngày tạo.
- Sao chép myfile.txt từ phân vùng FAT16 sang phân vùng NTFS Myfile.txt giữ cùng ngày sửa đổi, nhưng ngày tạo được cập nhật thành ngày và giờ hiện tại.
- Di chuyển myfile.txt từ phân vùng FAT16 sang phân vùng NTFS Myfile.txt giữ cùng ngày sửa đổi và ngày tạo.

Tóm lại, bất kể hệ thống tệp đang sử dụng là gì, nếu tệp được sao chép, ngày tạo cho các tập tin được cập nhật đến ngày giờ hiện tại; nếu tệp được di chuyển, ngày tạo vẫn giống nhau. Ngày sửa đổi được cập nhật khi thay đổi được thực hiện cho tệp.

## Note from the Underground...

### Sửa đổi thời gian MAC

Thông tin hữu ích như thời gian MAC của tệp có thể được điều tra, bạn cần lưu ý rằng có những người ngoài kia có thể đang tích cực cố gắng che giấu dữ liệu trên một hệ thống bằng cách sửa đổi thời gian MAC của các tập tin. Tôi đã chứng minh việc sử dụng các công cụ đó cho phép người dùng sửa đổi thời gian MAC trên một tệp tại các hội nghị, sử dụng tập lệnh Perl để truy cập các API Windows cần thiết (và được ghi chép kỹ lưỡng) để trước tiên tạo tệp, sau đó thay đổi ngày tạo thành sáu năm trong tương lai và thực hiện sửa đổi ngày hai năm trong quá khứ. Điều đó có thể khiến một cuộc điều tra bị hủy bỏ, và khi nào bạn thấy một cái gì đó như thế, làm thế nào để bạn tin tưởng bất kỳ lần MAC nào? Nhưng đó không phải là tất cả. Dự án Metasploit có Dự án Chống điều tra số ([www.metasploit.org/research/projects/antiforensics/](http://www.metasploit.org/research/projects/antiforensics/)) bao gồm một công cụ gọi là timestomp.exe cho phép kẻ tấn công sửa đổi không chỉ thời gian MAC của tệp mà cả mục nhập đã được sửa đổi, dấu ngày/thời gian của Nhật Bản, cho biết thời điểm các thuộc tính tệp được sửa đổi. Tuy nhiên, hy vọng đến lúc bạn đạt được điểm này trong cuốn sách, bạn đã có nhận ra rằng các công cụ chống nhiễu trùng nhằm mục đích lật đổ nhà phân tích, thay vì một ứng dụng phân tích forensic cụ thể.

Phần còn lại của phần này đề cập đến siêu dữ liệu được nhúng trong các định dạng tệp khác nhau

## Word Documents

Siêu dữ liệu có trong các tài liệu Word từ lâu đã là một vấn đề. Tài liệu Word là tài liệu hỗn hợp, dựa trên công nghệ liên kết và nhúng đối tượng (OLE) định nghĩa một cấu trúc tập tin trong một tập tin. Bên cạnh định dạng của thông tin, tài liệu Word có thể chứa khá nhiều thông tin bổ sung mà người dùng không nhìn thấy, tùy thuộc vào chế độ xem người dùng của tài liệu. Ví dụ: tài liệu Word có thể lưu trữ không chỉ các bản sửa đổi trong quá khứ mà còn có một danh sách tối đa 10 tác giả cuối cùng để chỉnh sửa một tệp. Điều này đã đặt ra một thông tin rủi ro tiết lộ cho các cá nhân và tổ chức. Có lẽ một trong những điều dễ thấy nhất đã được thực hiện công khai vào giữa năm 2003 bởi Richard M. Smith, liên quan đến một tài liệu được phát hành bởi British Prime Minister Tony Blair ([www.computerbytesman.com/privacy/blair.htm](http://www.computerbytesman.com/privacy/blair.htm)). Chính phủ Blair đã phát hành một hồ sơ của các tổ chức tình báo và an ninh Iraq như một tài liệu Word về Web vào tháng 2 năm 2003. Một giảng viên chính trị tại Đại học Cambridge đã công nhận các phần về nội dung của tài liệu này như ban đầu được viết bởi một nhà nghiên cứu Hoa Kỳ ở Iraq. Điều này khiến khá nhiều người nhìn kỹ hơn vào tài liệu. Trong thảo luận của anh ấy về vấn đề công bố thông tin, giảng viên minh họa thông tin ông có thể dễ trích xuất từ tài liệu Word, bao gồm danh sách 10 tác giả cuối cùng cần sửa đổi tài liệu. Thông tin này khá lúng túng đối với nhân viên của Prime Minister Blair.

Trên trang web của mình, giảng viên đề cập đến một tiện ích mà ông đã viết để trích xuất thông tin này từ các tài liệu Word, nhưng tiện ích này không được cung cấp cho người khác sử dụng. Tôi đã viết một tập lệnh Perl được gọi là `wmd.pl`, được bao gồm trong DVD đi kèm, phân tích cú pháp thông qua tiêu đề nhị phân của tài liệu Word để trích xuất một số thông tin. Tập lệnh sử dụng các mô-đun Perl (tập lệnh không sử dụng Microsoft Word API, vì vậy bạn có thể chạy tập lệnh Perl trên bất kỳ hệ thống nào hỗ trợ Perl và có các mô-đun cần thiết, như được liệt kê trong các pragma sử dụng cho tập lệnh, cài đặt) để lấy thông tin bổ sung. Đầu ra của tập lệnh chạy với tài liệu Blair xuất hiện như sau:

```
C:\Perl>wmd.pl g:\book2\ch5\blair.doc
```

```
-----  
Statistics
```

```
-----  
File = g:\book2\ch5\blair.doc
```

```
Size = 65024 bytes
```

```
Magic = 0xa5ec (Word 8.0)
```

*Version = 193*

*LangID = English (US)*

*Document was created on Windows.*

*Magic Created : MS Word 97*

*Magic Revised : MS Word 97*

-----

*Last Author(s) Info*

-----

*1 : cic22 : C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd*

*2 : cic22 : C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd*

*3 : cic22 : C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd*

*4 : JPratt : C:\TEMP\Iraq - security.doc*

*5 : JPratt : A:\Iraq - security.doc*

*6 : ablackshaw : C:\ABlackshaw\Iraq - security.doc*

*7 : ablackshaw : C:\ABlackshaw\A;Iraq - security.doc*

*8 : ablackshaw : A:\Iraq - security.doc*

*9 : MKhan : C:\TEMP\Iraq - security.doc*

*10 : MKhan : C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc*

-----

*Summary Information*

-----

*Title : Iraq- ITS INFRASTRUCTURE OF CONCEALMENT, DECEPTION AND INTIMIDAT*

*Subject :*

*Authress : default*

*LastAuth : MKhan*

*RevNum : 4*

*AppName : Microsoft Word 8.0*  
*e*

*Created : 03.02.2003, 09:31:00*

*Last : 03.02.2003, 11:18:00*  
*Saved*

-----  
*Document Summary Information*  
-----

*Organization : default*

Như bạn có thể thấy, một số thông tin mà ẩn giấu trong các tài liệu Word có bị tiết lộ và bị lúng túng. Ngoài 10 tác giả cuối cùng, tập lệnh sẽ tiết lộ nền tảng (Windows hoặc Mac) mà tài liệu đã được tạo trên đó, cũng như phiên bản Word đã được sử dụng để tạo và sau đó sửa lại tài liệu. Tập lệnh cũng trích thông tin tóm tắt từ tài liệu (được thảo luận thêm trong luồng dữ liệu thay thế NTFS của chương này).

Tôi cũng đã bao gồm một tiện ích nhỏ khác trên DVD đi kèm, được gọi là oledmp.pl. Tiện ích này sử dụng các mô-đun Perl giống như wmd.pl nhưng thực hiện một chức năng hơi khác. Oledmp.pl sẽ liệt kê các luồng OLE và thùng rác được nhúng trong tài liệu Word cũng như thông tin tóm tắt tương tự mà wmd.pl trích xuất, như được minh họa trong mẫu sau đây:

*C:\Perl>oledmp.pl blair.doc*

*ListStreams*

*Stream : \*CompObj*

*Stream : WordDocument*

*Stream : \*DocumentSummaryInformation*

*Stream : ObjectPool*

*Stream : ITable*

*Stream : \*SummaryInformation*

*Trash Bin Size*

*BigBlocks 0*

*SystemSpace 940*

*SmallBlocks 0*

*FileEndSpace 1450*

*Summary Information*

*subject*

*lastauth MKhan*

*lastprinted 30.01.2003, 21:33:00*

*appname Microsoft Word 8.0*

*created 03.02.2003, 09:31:00*

*lastsaved 03.02.2003, 11:18:00*

*revnum 4*

*title*                *Iraq- ITS INFRASTRUCTURE OF CONCEALMENT, DECEPTION AND*  
*authress*        *INTIMIDATION*  
*default*

*1Table*

*1 cic22 C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd*

*2 cic22 C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd*

*3 cic22 C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd*

*4 JPratt C:\TEMP\Iraq - security.doc*

*5 JPratt A:\Iraq - security.doc*

*6 ablackshaw C:\ABlackshaw\Iraq - security.doc*

*7 ablackshaw C:\ABlackshaw\A;Iraq - security.doc*

*8 ablackshaw A:\Iraq - security.doc*

*9 MKhan C:\TEMP\Iraq - security.doc*

*10 MKhan C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc*

Thông tin ListStreams hiển thị tên của các luồng OLE khác nhau tạo nên tài liệu Word. Microsoft gọi OLE là một hệ thống tệp trong tệp tin, và các luồng này tên tham chiếu đến “các tệp tin” trong tài liệu.



Đôi khi có thể khá sốc khi có bao nhiêu thông tin được tiết lộ trong tài liệu siêu dữ liệu Word. Hãy thử một thử nghiệm nhỏ: Nhìn xung quanh một máy chủ tệp tại nơi làm việc (với sự cho phép, tất nhiên) và tìm một số tài liệu Word, chẳng hạn như một cái gì đó có thể đã được gửi cho khách hàng, và xem những gì siêu dữ liệu ẩn nói về các tài liệu. Tôi đã thử một cái gì đó tương tự, chỉ có tôi sử dụng Google thay vì một máy chủ tệp tin công ty. Do số lượng phản hồi tôi đã nhận được, tôi đã giới hạn các tìm kiếm của mình ở các tên miền .mil và .gov, nhưng tôi vẫn tìm thấy nhiều tài liệu hơn cái tôi cần tìm.

Thật thú vị, khi tôi đang viết cuốn sách đầu tiên của mình, một trong người đánh giá kỹ thuật không muốn tôi biết tên anh ấy và đặc biệt yêu cầu nhà xuất bản không chia sẻ bất kỳ thông tin nào của người đánh giá với tôi. Thêm một bước nữa người đánh giá này sẽ hoàn thành các mẫu đánh giá trong tài liệu

---

Word nhưng lưu nội dung dưới dạng tài liệu văn bản ASCII thẳng, xóa tất cả siêu dữ liệu. Tôi đoán anh ấy thực sự đã không muốn tôi biết anh ấy là ai!

---

Siêu dữ liệu này không chỉ có thể gây rủi ro tiết lộ thông tin cho một cá nhân hoặc tổ chức, nhưng nó cũng có thể hữu ích cho một nhà điều tra đang tìm kiếm thông tin cụ thể liên quan đến các tài liệu. Điều này có thể đặc biệt quan trọng trong các trường hợp khám phá điện tử, đặc biệt là nếu tìm kiếm từ khóa hoặc cụm từ được giới hạn trong văn bản hiển thị của tài liệu.

Để hoàn thiện chủ đề này, tôi cần nói thêm một vài điều trước khi chuyển sang chủ đề tiếp theo. Đầu tiên, Microsoft cung cấp thông tin cho người dùng về siêu dữ liệu các tài liệu Word và các cách để giảm thiểu siêu dữ liệu có sẵn. Thứ hai, tài liệu Word không phải là các tệp Office duy nhất có vấn đề với siêu dữ liệu. Để giải quyết cả hai mục, Microsoft cung cấp các bài viết cơ sở Kiến thức sau:

- 223790: WD97: “How to Minimize Metadata in Microsoft Word Documents”
- 223396: OFF: “How to Minimize Metadata in Microsoft Office Documents”
- 223789: XL: “How to Minimize Metadata in Microsoft Excel Workbooks”
- 223793: PPT97: “How to Minimize Metadata in Microsoft PowerPoint Presentations”
- 290945: “How to Minimize Metadata in Word 2002”
- 290945: “How to Minimize Metadata in Word 2002”

Ngoài các bài viết trong cơ sở kiến thức này, Microsoft cũng cung cấp công cụ xóa dữ liệu ẩn (<http://support.microsoft.com/kb/834427>) dưới dạng bổ trợ cho Office 2003 và XP. Tác giả có thể sử dụng công cụ này để loại bỏ rất nhiều siêu dữ liệu khỏi tài liệu.

Đây là một công cụ tuyệt vời để đảm bảo rằng số lượng siêu dữ liệu có sẵn được giảm thiểu, thậm chí nếu quá trình biên soạn của bạn bao gồm lưu tệp theo định dạng khác, chẳng hạn như PDF.

## **Note from the Underground**

---

### **Tiện ích hợp nhất luồng**

Một tiện ích có tên Merge Streams ([www.ntkernel.com/w&p.php?id=23](http://www.ntkernel.com/w&p.php?id=23)), có sẵn từ NT Kernel Resources, thực hiện một khía cạnh thú vị của các tài liệu Office OLE. Tóm lại, nó cho phép bạn hợp nhất một bảng tính Excel vào một tài liệu Word. Tiện ích có một giao diện đơn giản cho phép bạn chọn tài liệu Word và bảng tính Excel và hợp nhất hai cái lại với nhau. Giả sử bạn có mỗi tài liệu trong một thư mục. Nếu bạn chạy tiện ích và hợp nhất hai tài liệu, bạn sẽ được một tài liệu Word lớn hơn tài liệu

---

---

Word gốc cũng như lớn hơn tài liệu gốc Excel. Tuy nhiên, nếu bạn đã xóa bảng tính Excel, hãy thay đổi phần mở rộng tệp của tài liệu Word thành .xls, sau đó bấm đúp vào tệp, bạn sẽ xem bảng tính Excel được mở trên màn hình nền, không có bằng chứng về tài liệu Word hoặc nội dung của gốc nó. Thay đổi phần mở rộng tệp tin trở lại .doc cho phép bạn mở tài liệu Word mà không có bằng chứng rõ ràng về bảng tính Excel.

Khi trình bày về chủ đề này tại các hội nghị, tôi thường bao gồm một trình diễn về công cụ. Thông thường tôi chứng minh điều đó từ khía cạnh của một người dùng doanh nghiệp đang cố gắng làm lậu bảng tính dự báo tài chính hoặc thông tin hợp đồng thích hợp với một giá thầu quan trọng trong một tổ chức. Tất cả người dùng phải làm là hợp nhất bảng tính Excel vào tài liệu Word (một cái gì đó vô hại, chẳng hạn như một chữ cái) và sau đó sao chép tài liệu Word vào USB. Nếu có ai ngăn người dùng trên đường ra cửa trước và kiểm tra nội dung của USB, tất cả những gì anh ta sẽ thấy là tài liệu Word.

Tuy nhiên, khi nói chuyện với các nhân viên thực thi pháp luật, tôi có một tiếp cận khác biệt nhẹ. Giả sử một nhân viên công ty có một số hình ảnh bất hợp pháp mà anh ấy muốn chia sẻ với bạn bè của mình. Anh ta sao chép các hình ảnh vào một tài liệu Word, sau đó định vị một bảng tính Excel trên máy chủ tệp mà tất cả mọi người đều có quyền truy cập (cũng như hợp pháp cần truy cập) và hợp nhất chúng. Sau đó, anh ta đổi tên tài liệu Word thành tên gốc và phần mở rộng của bảng tính và cho bạn bè của anh ấy biết những gì anh ấy đã làm. Cách này, anh ta có thể phân phối các hình ảnh mà không để lại bất kỳ dấu vết. Phát hiện việc sử dụng một tiện ích như Merge Streams không nhất thiết phải nhiệm vụ quá mức khó khăn. Sử dụng các tập lệnh bao gồm chức năng tương tự như oledmp.pl, như đã đề cập trước đây trong chương này, bạn có thể liệt kê các luồng OLE tạo nên tài liệu Word. Nếu bạn thấy bất kỳ tên luồng nào (sổ làm việc, bảng tính hoặc tương tự) mà sẽ chỉ ra sự hiện diện của bảng tính Excel, tài liệu Word chắc chắn là đáng để kiểm tra.



Tập lệnh Perl của oledmp.pl cực kỳ hữu ích trong các kỳ thi liên quan đến bảng tính Excel và thuyết trình PowerPoint. Trong một trường hợp, tôi đã thực hiện kiểm tra một hệ thống mà từ đó khách hàng nghi ngờ rằng ai đó đã thực hiện gian lận, sử dụng số tài khoản nhân viên có quyền truy cập như một phần trách nhiệm hàng ngày của mình. Sử dụng một danh sách từ khóa được tạo với sự giúp đỡ của khách hàng, tôi tìm một bảng tính Excel trên hệ

---

thông, trích xuất nó từ hình ảnh và cung cấp cho khách hàng để xem xét. Như một phần của báo cáo của tôi, tôi đã có thể bao gồm thông tin về nơi tập tin đã đến (theo vị trí của tập tin, nó đã là một tệp đính kèm Outlook), khi người dùng đã truy cập tệp (dựa trên dữ liệu được tìm thấy trong Registry), cũng như thực tế là người dùng đã có chỉnh sửa và sau đó in bảng tính. Hai bit cuối cùng của thông tin đã được truy xuất từ siêu dữ liệu bảng tính bằng cách sử dụng oledmp.pl.

---

Cory Althiede gần đây đã chỉ ra cho tôi một phương tiện khác để trích xuất thông tin hữu ích từ các tài liệu Microsoft Word (và các OLE khác). Khi viết bản thảo cho cuốn sách này, tôi sẽ đánh dấu / chọn văn bản từ một tập tin, sao chép nó vào Clipboard, dán văn bản đó vào tài liệu tôi đang làm việc và sau đó đảm bảo rằng nó đúng định dạng cho mục đích của nó. Tuy nhiên, khi ai đó kéo và thả văn bản vào tài liệu Microsoft Word, nó trở thành một tập tin đính kèm. Nếu bạn có nhu cầu giải nén những tài liệu đính kèm OLE đó, Cory đã chỉ ra một công cụ tuyệt vời để sử dụng, được gọi là b2xtranslator (<http://b2xtranslator.sourceforge.net/>). Theo phần giới thiệu của trang web, mục đích của công cụ này là cho phép người dùng chuyển từ định dạng tài liệu nhị phân sang định dạng XML / zip mới được sử dụng trong các phiên bản sau của Microsoft Office (ví dụ: di chuyển từ định dạng .doc sang định dạng .docx). Trang tài liệu được liên kết từ trang Web chính cung cấp một số minh họa rất tốt về cách thức hoạt động của công cụ và cho thấy cách thức các đối tượng OLE khác nhau được nhúng trong tài liệu Word hoặc bảng tính Excel có thể truy cập. Nếu bạn cần làm nhiều hơn là chỉ xem lại tác giả cuối cùng hoặc ngày mà OLE tài liệu đã được in, bạn có thể xem xét xem công cụ này.

## **PDF Documents (Tài liệu PDF)**

Các tệp định dạng tài liệu di động (PDF – Portable Document Format) cũng có thể chứa siêu dữ liệu như tên của người tạo, ngày tệp được tạo và ứng dụng được sử dụng để tạo tệp PDF. Thông thường siêu dữ liệu có thể cho ta thấy rằng tệp PDF đã được tạo trên máy Mac hoặc tệp PDF được tạo bằng cách chuyển đổi tài liệu Word sang định dạng PDF. Cũng như các tài liệu Word, siêu dữ liệu này có thể gây rủi ro tiết lộ thông tin. Tuy nhiên, tùy thuộc vào tình huống, thông tin này cũng có thể hữu ích cho người điều tra viên, có thể hỗ trợ việc tìm hiểu hoặc cho thấy rằng một ứng dụng cụ thể đã được cài đặt trên hệ thống người dùng. Trên DVD đi kèm, tôi đã kèm hai tập lệnh Perl (pdfmeta.pl và pdfdmp.pl) mà tôi đã sử dụng để trích xuất siêu dữ liệu từ các tệp PDF. Sự khác biệt duy nhất giữa hai tập lệnh là chúng sử dụng các mô-đun Perl khác nhau để tương tác với các tệp PDF. Thành thật mà nói, tôi đã có được nhiều thành công



với các tập lệnh; trong một số trường hợp, cả hai tập lệnh sẽ truy xuất thành công siêu dữ liệu từ tệp PDF, trong khi đó trong các trường hợp khác, một hoặc các tập lệnh khác sẽ thất bại vì một số lý do. Để thử nghiệm, tôi đã sử dụng Google để tìm kiếm một số tệp PDF mẫu và tìm thấy hai tệp, một từ FTC và một từ IRS. Tệp PDF từ FTC được gọi là idtheft.pdf và pdfmeta.pl trả về thông tin sau:

```
C:\Perl>pdfmeta.pl d:\pdf\idtheft.pdf
```

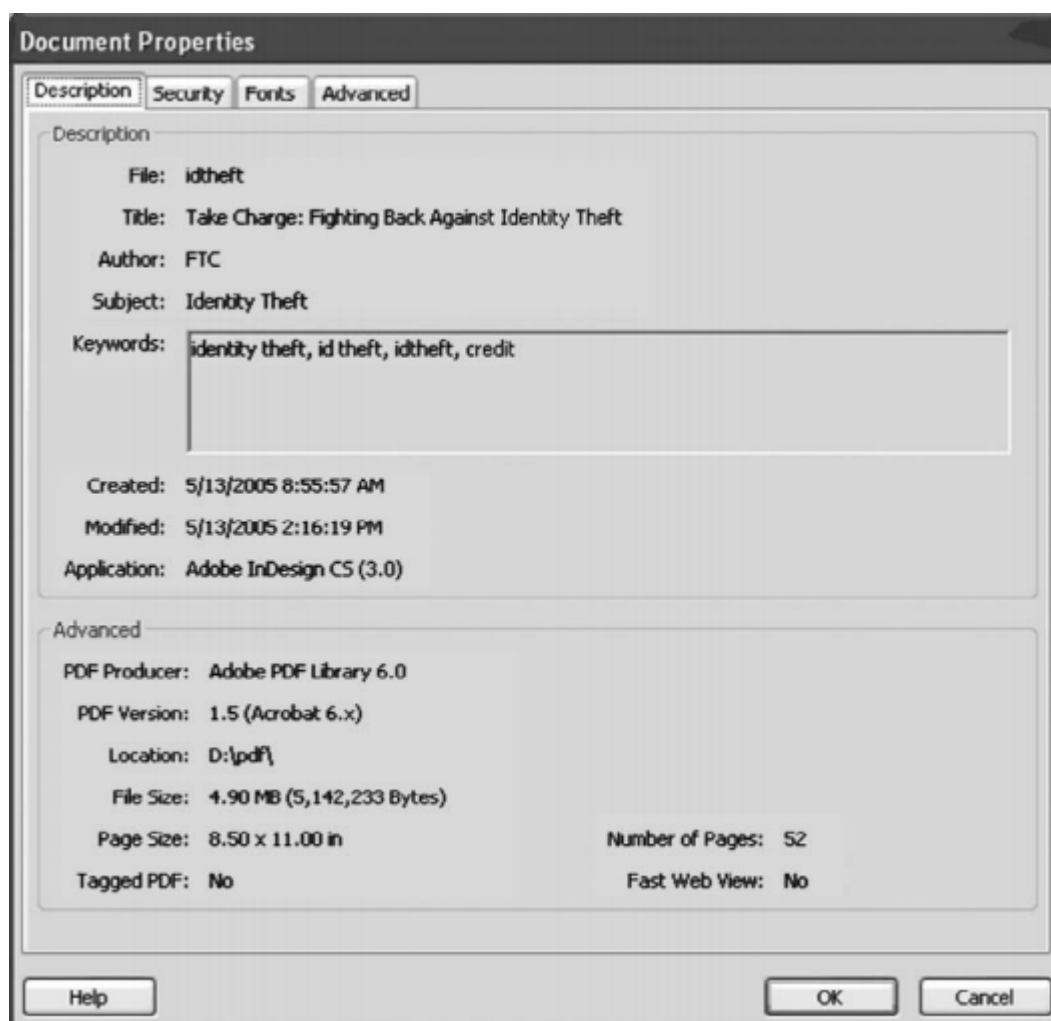
```
Author          FTC
CreationDate     D:20050513135557Z
Creator          Adobe InDesign CS (3.0)
Keywords         identity theft, id theft, idtheft, credit
ModDate          D:20050513151619-04'00'
Producer         Adobe PDF Library 6.0
Subject          Identity Theft
Title            Take Charge: Fighting Back Against Identity Theft
```

Tệp PDF được tải xuống từ trang IRS là bản sao của Mẫu W-4 năm 2006, được gọi là fw4.pdf. Pdfmeta.pl đã trả lại thông tin sau:

```
C:\Perl>pdfmeta.pl d:\pdf\fw4.pdf
```

```
Author          SE:W:CAR:MP
CreationDate     D:20051208083254-05'00'
Creator          OneForm Designer Plus
Keywords         Fillable
ModDate          D:20060721144654-04'00'
Producer         APJavaScript 2.2.1 Windows SPDF_1112 Oct 3 2005
Subject          Employee's Withholding Allowance Certificate
Title            2006 Form W-4
```

Cả hai ví dụ này đều khá chung chung, nhưng dễ dàng để xem cách siêu dữ liệu trong các tệp PDF được sử dụng trong khám phá điện tử (đề cập đến khám phá trong các thủ tục tố tụng như tố tụng, điều tra của chính phủ hoặc yêu cầu Luật Tự do Thông tin, trong đó thông tin tìm kiếm ở định dạng điện tử (thường được gọi là thông tin được lưu trữ điện tử hoặc ESI). hoặc ít nhất nên được xem xét trong tìm kiếm từ khóa. Nếu bạn gặp sự cố khi truy xuất siêu dữ liệu với một trong hai tập lệnh Perl được cung cấp trong cuốn sách này, thì phương án dự phòng là mở tệp trong Adobe Reader (có sẵn miễn phí từ Adobe.com) và nhấp vào File | Document Properties. Tab Mô tả của hộp thoại Document Properties chứa tất cả các siêu dữ liệu có sẵn. Hình 5.9 minh họa các thuộc tính tài liệu cho idtheft.pdf.



Hình 5. 9. Thuộc tính tài liệu Idtheft.pdf

Vào mùa thu năm 2008, Didier Stevens đã phát triển một công cụ dựa trên Python có tên pdf-Parser.py (có sẵn từ <http://blog.didierstevens.com/programs/pdf-tools/#pdf-parser>; trang web cũng bao gồm một liên kết đến Screencast (Screencast là một bản ghi kỹ thuật số của đầu ra màn hình máy tính, còn được gọi là chụp màn hình video, thường chứa lời tường thuật âm thanh) hiển thị hoạt động của công cụ). Theo Didier, tập lệnh Python này “sẽ phân tích tài liệu PDF để xác định các yếu tố cơ bản được sử dụng trong tệp được phân tích. Nó sẽ không hiển thị tài liệu dạng PDF”.



---

Bạn có thể tải xuống trình thông dịch Python miễn phí từ ActiveState.com, cùng một trang web cung cấp trình thông dịch Perl miễn phí.

---

Pdf-Parser.py trích xuất các siêu dữ liệu và nội dung khác nhau từ tài liệu PDF, bao gồm các đối tượng và mã JavaScript được nhúng trong tài liệu. Ví dụ: Didier đã đăng một blog (<http://blog.didierstevens.com/2008/11/10/shoulder-surfing-a-malicy->

pdf-author/) trong đó ông mô tả việc phân tích thông tin từ tài liệu PDF độc hại chứa mã khai thác lỗ hổng cho hàm JavaScript.printf (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-2992>).

Didier cũng cung cấp tập lệnh Python, ExtractScripts (<http://blog.didierstevens.com/programs/extucescripts/>), trích xuất các tập lệnh độc hại tiềm ẩn được nhúng trong các tệp HTML vào các tệp riêng biệt.

## **Image Files (tệp hình ảnh)**

Các tệp xử lý văn bản không phải là các tệp duy nhất duy trì siêu dữ liệu nội bộ. Vào tháng 2 năm 2006, một bài viết về một người chăn nuôi bot (tin tặc cài đặt vào các hệ thống để bị tấn công chương trình bot và sau đó quản lý và thậm chí thuê các mạng đó) trên Tạp chí Washington Post đã đưa hình ảnh JPEG vào phiên bản trực tuyến của câu chuyện. Mặc dù tác giả của câu chuyện đã phải cố gắng rất nhiều để giữ bí mật về danh tính của người chăn nuôi bot, nhưng hình ảnh JPEG bao gồm các ghi chú từ nhiếp ảnh gia đã chỉ ra địa điểm (thành phố và tiểu bang) nơi bức ảnh được chụp.

Siêu dữ liệu có sẵn trong hình ảnh JPEG phụ thuộc phần lớn vào ứng dụng đã tạo hoặc sửa đổi nó. Ví dụ: máy ảnh kỹ thuật số nhúng thông tin định dạng tệp hình ảnh có thể thay đổi (EXIF) trong hình ảnh, có thể bao gồm kiểu máy và nhà sản xuất máy ảnh (không may, dường như không có số sê-ri nào được sử dụng hoặc lưu trữ) và thậm chí có thể lưu trữ hình ảnh thu nhỏ hoặc thông tin âm thanh (EXIF sử dụng định dạng thư mục tệp hình ảnh TIFF). Các ứng dụng như Photoshop của Adobe có bộ siêu dữ liệu riêng mà họ thêm vào tệp JPEG.

Các công cụ như Exifer ([www.friedemann-schmidt.com/software/exifer/](http://www.friedemann-schmidt.com/software/exifer/)), IrfanView ([www.irfanview.com](http://www.irfanview.com)) và mô-đun Image :: Metadata :: JPEG Perl cho phép bạn xem, truy xuất và trong một số trường hợp sửa đổi siêu dữ liệu được nhúng trong các tệp hình ảnh JPEG. Chris Brown (của Technology Pathways) cung cấp một tờ giấy trắng ([http://toorcon.techpathways.com/cs/forums/st Storage / 8/11 / EXIF. Pdf](http://toorcon.techpathways.com/cs/forums/st%20Storage%20-%208/11/EXIF.Pdf)) mô tả dữ liệu EXIF và, ở một mức độ nhỏ, định dạng của một tệp JPEG.

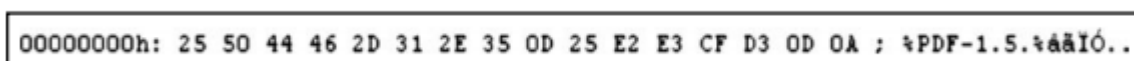
## **File Signature Analysis (Phân tích chữ ký tệp tin)**

Trong quá trình nghiên cứu, bạn có thể bắt gặp các tệp có phần mở rộng bất thường hoặc tệp có phần mở rộng quen thuộc ở vị trí bất thường. Trong những trường hợp như vậy, bạn có thể sử dụng phân tích chữ ký tệp để xác định bản chất của các tệp cũng như hiểu rõ hơn về khả năng kỹ thuật của kẻ tấn công. Một cách để xác định bản chất thực sự của các tệp, không kể đến phần mở rộng của chúng là thông qua phân tích chữ ký tệp.

Phân tích chữ ký tệp liên quan đến việc thu thập thông tin từ 20 byte đầu tiên của tệp và tìm kiếm một chữ ký cụ thể hoặc “số ma thuật” sẽ cho bạn biết loại và chức năng của tệp. Các loại tệp khác nhau có chữ ký khác nhau và các chữ ký này độc lập với phần mở rộng tệp. Trên thực tế, thường thì kẻ xấu sẽ thay đổi phần mở rộng của tệp để khi xem nó trong Windows Explorer, tệp sẽ xuất hiện với một biểu tượng che dấu thật hiệu quả nội dung và mục đích của tập tin. Một lần, cách đây rất lâu, trên một hệ thống ở xa, rất xa, tôi đã phân tích một IRCbot mà tôi đặt tên là bot russiantopz ([www.securityfocus.com/infocenter/showthread.php?p=1618](http://www.securityfocus.com/infocenter/showthread.php?p=1618)). IRCbot này đã gửi một số tệp trên hệ thống bị nhiễm bệnh và cung cấp các tệp .dvr và phần mở rộng .dll. Vì vậy, khi quản trị viên xem các tệp đó, chúng sẽ xuất hiện như những tệp bất thường mà hầu hết các quản trị viên không mở được. Xét cho cùng, trong hầu hết các trường hợp khi quản trị viên mở một tệp có một trong các phần mở rộng đó trong trình soạn thảo hex, tất cả những gì anh ta thấy là một loạt các công cụ nhị phân. Trong khi phân tích, tôi thực sự đã mở các tệp đó và có thể thấy rằng chúng chứa thông tin văn bản, thông tin cấu hình cụ thể và các hành động mà bot sẽ thực hiện khi gửi lệnh.

Các công cụ phân tích điều tra số như ProDiscover cho phép điều tra viên dễ dàng thực hiện phân tích chữ ký tệp và dễ dàng xem kết quả. Khi các công cụ đó thực hiện phân tích, họ nhận được phần mở rộng của tập tin và so sánh chữ ký được liên kết với phần mở rộng đó với thông tin có trong 20 byte đầu tiên của tệp. Ví dụ: các tệp thực thi di động (PE) của Windows sẽ bắt đầu bằng các chữ cái MZ (tham chiếu đến Mark Zbikowski [[http://en.wikipedia.org/wiki/Mark\\_Zbikowski](http://en.wikipedia.org/wiki/Mark_Zbikowski)], một kiến trúc sư của Microsoft), được đặt ở hai byte đầu tiên của tệp PE. Các tệp có thể thực thi có thể có các phần mở rộng tệp .exe, .dll, .Sys, .ocx, hoặc .drv (kể tên một số phần mở rộng tệp), như đã thấy trong tệp headersig.txt được ProDiscover sử dụng làm cơ sở dữ liệu của phần mở rộng tệp và các chữ ký. Nói tóm lại, nếu một tệp có phần mở rộng thực thi, bạn sẽ thấy chữ ký thực thi hợp lệ. Các tệp không có chữ ký hợp lệ phù hợp với tiện ích mở rộng của chúng được gắn cờ để điều tra thêm.

Các tệp hình ảnh như tệp JPEG và GIF cũng có chữ ký riêng. Chữ ký cho tệp JPEG là JFIF và chữ ký cho tệp GIF là GIF87a hoặc GIF89a. Hình 5.10 minh họa chữ ký cho tài liệu PDF, hoặc % PDF-, theo sau là phiên bản định dạng Tài liệu Di động cho tệp.



Hình 5. 10. Chữ ký tệp PDF

Tập lệnh sigs.pl Perl nằm trên DVD đi kèm sẽ cho phép bạn thực hiện phân tích chữ ký tệp trên các hệ thống trực tiếp. Tập lệnh sẽ kiểm tra một tệp, một thư mục tệp, hoặc tất cả các tệp trong cấu trúc thư mục để xác định xem chữ ký tệp có khớp với phần mở rộng tệp không. Tập lệnh sử dụng tệp headersig.txt từ Technology Pathways làm cơ sở dữ liệu mặc định của chữ ký tệp; Tuy nhiên, các danh sách khác có cùng định dạng có thể được sử dụng. Khi tập lệnh phân tích cú pháp thông qua các tệp, nó sẽ xác định liệu chữ ký tệp có khớp với phần mở rộng không, nhưng nó cũng sẽ cảnh báo cho điều tra viên nếu không tìm thấy phần mở rộng tệp tin trong cơ sở dữ liệu của họ. Nếu đây là trường hợp, tập lệnh sẽ cung cấp phần mở rộng và chữ ký để điều tra viên có thể cập nhật cơ sở dữ liệu của cô ấy, nếu cô ấy thấy cần phải làm như vậy. Theo mặc định, tập lệnh gửi đầu ra của nó tới bàn điều khiển ở định dạng giá trị được phân tách bằng dấu phẩy (.csv) để có thể chuyển hướng đến một tệp và mở trong Excel để dễ dàng phân tích.

## **NTFS Alternate Data Streams (Luồng dữ liệu thay thế NTFS)**

Luồng dữ liệu thay thế NTFS (ADS) là một tính năng của hệ thống tệp NTFS không được biết đến cũng như không được hiểu rõ giữa các thành viên của cộng đồng quản trị hệ thống. Rốt cuộc, tại sao nó lại như vậy? Nhìn bề ngoài, các ADS được sử dụng ngoài lề trong một số ứng dụng của Microsoft, vì vậy chúng có thể rất tệ, phải không?

Hãy để tôi xem xét nó theo một cách khác. Điều gì sẽ xảy ra nếu tôi nói với bạn rằng có một cách để tạo các tệp hợp pháp trên hệ thống Windows, các tệp có thể chứa dữ liệu cũng như tập lệnh hoặc mã thực thi và các tệp này có thể được tạo hoặc khởi chạy nhưng không có công cụ gốc trong phân phối hệ điều hành sẽ cho phép bạn phát hiện sự hiện diện của các tệp tùy ý. Hệ điều hành Windows có tất cả các công cụ gốc để tạo, sửa đổi và thao tác với các ADS, nhưng không có công cụ gốc nào có sẵn để xem sự tồn tại của các ADS tùy ý. Chà, điều đó không hoàn toàn đúng, bởi vì bắt đầu với Vista, lệnh dir bây giờ có một công tắc để cho phép bạn xem ADSes. Chúng tôi sẽ giải quyết vấn đề này ngay lập tức.

Vậy, các luồng dữ liệu thay thế là gì, chúng đến từ đâu và chúng được sử dụng như thế nào? ADSes là một tính năng của hệ thống tệp NTFS được giới thiệu bắt đầu với Windows NT 3.1. Các ADS đã được thêm vào hệ thống tệp để hỗ trợ Hệ thống tệp tin phân cấp (HFS) được Macintosh sử dụng. HFS sử dụng các nhánh tài nguyên để hệ thống tệp có thể duy trì siêu dữ liệu về tệp, chẳng hạn như biểu tượng, menu hoặc hộp thoại. Chức năng này được tích hợp vào hệ thống tệp NTFS nhưng chưa bao giờ được thảo luận rộng rãi. Trên thực tế, trong thời gian dài nhất, có rất ít thảo luận về ADSes và rất ít thông tin có sẵn về chủ đề này, ngay cả từ Microsoft. Mặc dù các ứng dụng và

chức năng của Microsoft cho phép tạo ra các ADS cụ thể, nhưng thực tế vẫn còn rất ít hoạt động cho các ADS. Kẻ xấu đã nhận ra điều này và đã sử dụng ADSes để ẩn các công cụ, thậm chí là một phần của rootkits. Đây là một cách tiếp cận hiệu quả vì một số tiện ích chống vi-rút không quét ADSes hoặc không làm theo mặc định. Do đó, phần mềm độc hại được thả vào hệ thống trong ADS có thể không bị phát hiện hoặc xóa/cách ly bởi ứng dụng chống vi-rút.

## Note from the Underground

---

### Sử dụng ADSes

Vào cuối những năm 1990, với tư cách là một nhà tư vấn, tôi đã tham gia vào một số bài kiểm tra thâm nhập và đánh giá lỗ hổng. Trong quá trình kiểm tra thâm nhập, nếu chúng tôi có quyền truy cập vào hệ thống Windows và được cho phép làm như vậy, chúng tôi sẽ để lại một ADS trên hệ thống. Điều này không có tác động gì ngoài việc tiêu tốn một vài byte, bởi vì chúng tôi chỉ để lại một tin nhắn văn bản.

Tuy nhiên, đây là cách chúng tôi nói với quản trị viên hệ thống “Thẻ Tag, là nó!” và để cung cấp bằng chứng rằng chúng tôi đã nhận được theo như chúng tôi đã nói. Tôi đã nói chuyện với những người Pentest (đánh giá độ an toàn bằng cách tấn công vào hệ thống, là quá trình xem xét lại các dịch vụ và hệ thống để tìm ra các vấn đề an ninh tiềm tàng hoặc dò tìm các dấu vết khi hệ thống bị tổn thương) khác, những người sẽ sao chép tất cả các công cụ của họ sang một hệ thống bị xâm nhập vào ADSes.

---

## Creating ADSes (Tạo ADSes)

Tạo một ADS tương đối đơn giản; một số ứng dụng Microsoft làm điều đó tự động. Bất kỳ người dùng nào cũng có thể làm điều đó, miễn là người dùng có khả năng tạo tệp. Ví dụ, cách đơn giản nhất để tạo ADS là nhập lệnh sau:

```
D:\ads>notepad myfile.txt:ads.txt
```

Ban đầu, bạn sẽ thấy một hộp thoại hỏi bạn có muốn tạo một tệp mới không. Bấm Yes, thêm một số văn bản vào cửa sổ, lưu tệp và sau đó đóng cửa sổ Notepad. Tại thời điểm này, nếu bạn nhập dir, bạn sẽ thấy rằng tệp myfile.txt có kích thước bằng 0 byte, mặc dù bạn chỉ cần gõ một loạt văn bản vào Notepad. Một cách khác để tạo ADS là sử dụng lệnh echo:

```
D:\ads>echo "This is another ADS test file" > myfile.txt:ads2.txt
```

Được rồi, do đó, bạn đã tạo ra hai ADS và cho dù bạn nhập dir hoặc xem nội dung của thư mục trong Windows Explorer, bạn sẽ thấy một tệp duy nhất trong thư mục và tệp đó sẽ có kích thước bằng 0 byte.

Tuy nhiên, một cách khác để tạo ADS là sử dụng lệnh type để sao chép tệp khác vào ADS:

```
D:\ads>type c:\windows\system32\sol.exe > myfile.txt:ads3.exe
```

Vì vậy, bây giờ những gì bạn đã thực hiện được sao chép nội dung tệp có tên sol.exe (là trò chơi thẻ Solitaire trên Windows 2000, XP và 2003) vào một ADS. Bạn có thể chạy các lệnh tương tự trên Vista để tạo ADSes, mặc dù đối với một số ứng dụng (như trò chơi Solitaire), các đường dẫn đến tệp thực thi có thể khác.

Bạn cũng có thể thêm ADSes vào danh sách thư mục, sử dụng cú pháp sau:

```
D:\ads>echo "This is an ADS attached to a directory" > :ads.txt
```

Lưu ý rằng không có tên tệp cụ thể được cung cấp. Điều này làm cho ADS được gắn vào danh sách thư mục; trong trường hợp này, D:\ads

ADSes cũng được tạo theo những cách khác, thường xuyên mà bạn không bao giờ nhận thức được về nó. Khi bạn nhấp chuột phải vào một tệp và chọn Properties, một trong các tab bạn thấy được gọi là Summary (đủ thú vị, tab này không có vẻ như có sẵn trên Vista). Bạn có thể nhập bất cứ thứ gì vào các trường văn bản khác nhau và khi bạn lưu thông tin bằng cách bấm OK, thông tin sẽ được lưu trong ADS (trừ khi bạn làm việc với tài liệu Office, trong trường hợp đó thông tin bạn đã nhập được lưu trong bộ lưu trữ có cấu trúc hoặc chính tài liệu OLE).

Hơn nữa, Trình quản lý tệp đính kèm (<http://support.microsoft.com/kb/883260>) là một phần của Windows XP SP2 sẽ thêm ADS vào các tệp được tải xuống từ Internet hoặc truy xuất dưới dạng tệp đính kèm từ email (qua Internet Explorer và Outlook). Khi bạn tải xuống một tệp qua Internet Explorer, tệp sẽ được ghi vào bất kỳ vị trí nào bạn chọn và một ADS có tên là Zone.Identifier sẽ được thêm vào tệp (giả sử rằng hệ thống tệp là NTFS, nếu không, theo bài viết của Cơ sở Kiến thức 883260, Trình quản lý tệp đính kèm sẽ thất bại). ADS được thêm vào tệp để khi người dùng cố gắng thực thi hoặc mở tệp, họ sẽ thấy một hộp thoại cảnh báo thông báo rằng tệp có thể không an toàn để mở.

## **Enumerating ADSes (Liệt kê ADSes)**

Bây giờ bạn đã tạo ra một số ADS, làm thế nào để bạn phát hiện ra chúng? Như tôi đã đề cập trước đây, không có công cụ nào dành riêng cho các hệ thống Windows cho phép bạn liệt kê các ADSes tùy ý. Bạn không thể nhìn thấy chúng thông qua Windows Explorer, và lệnh dir cũng vô dụng. Chà, câu nói cuối cùng đó không đúng lắm; Vista có một công tắc cho phép bạn liệt kê các ADSes với dir bằng cách sử dụng công tắc /r, như hình 5.11 minh họa.

```
C:\ads>dir /r
Volume in drive C has no label.
Volume Serial Number is 98A5-80D5

Directory of C:\ads

11/20/2006  07:17 PM    <DIR>          .
11/20/2006  07:17 PM    <DIR>          ..
11/20/2006  07:33 PM                0 myfile.txt
                23 myfile.txt:ads.txt:$DATA
                34 myfile.txt:ads2.txt:$DATA
            982,528 myfile.txt:ads3.exe:$DATA
      1 File(s)                0 bytes
      2 Dir(s)  14,823,571,456 bytes free
```

Hình 5. 11. Ví dụ về liệt kê ADS trên Vista

Hình 5.11 cho thấy kết quả của việc chạy lệnh `dir/r` trên Vista sau khi tạo một số ADSes theo cách tương tự như chúng ta đã làm trong phần “Tạo ADSes” (trong phần đó, chúng tôi đã tạo ADSes trên XP).

Với các hệ điều hành Windows khác (2000, XP và 2003), bạn cần trợ giúp từ bên ngoài để liệt kê các ADSes. Sở thích của tôi là `lads.exe` ([www.heysoft.de/Frames/f\\_sw\\_la\\_en.htm](http://www.heysoft.de/Frames/f_sw_la_en.htm)), được viết bởi Frank Heyne. `Lads.exe` là một công cụ giao diện dòng lệnh (CLI) mà bạn có thể chạy với bất kỳ thư mục nào ngay lập tức.

```
D:\tools>lads d:\ads
```

*LADS - Freeware version 4.00*

*(C) Copyright 1998-2004 Frank Heyne Software (<http://www.heysoft.de>)*

*This program lists files with alternate data streams (ADS)*

*Use LADS on your own risk!*

*Scanning directory d:\ads\*

*size ADS in file*

-----  
*0 d:\ads\myfile.txt:ads.txt*

*34 d:\ads\myfile.txt:ads2.txt*

*1032192 d:\ads\myfile.txt:ads3.exe*

*1032226 bytes in 3 ADS listed*

`Lads.exe` chỉ là một trong những công cụ có sẵn cho phép bạn liệt kê các ADSes trên Windows. Có những công cụ khác cũng là công cụ CLI, có công cụ GUI và thậm chí có một số công cụ cài đặt dưới dạng trình cắm shell để bạn có thể liệt kê các ADS thông qua giao diện người dùng Windows Explorer.

Các ADSes được thêm vào một tệp bằng cách thêm thông tin tóm tắt vào tệp (được đề cập trong phần trước) có vẻ hơi khác so với các ADSes mà chúng tôi đã thêm.



Ví dụ, nếu chúng tôi thêm thông tin tóm lược vào myfile.txt và sau đó chạy lại lads.exe, chúng tôi sẽ thấy:

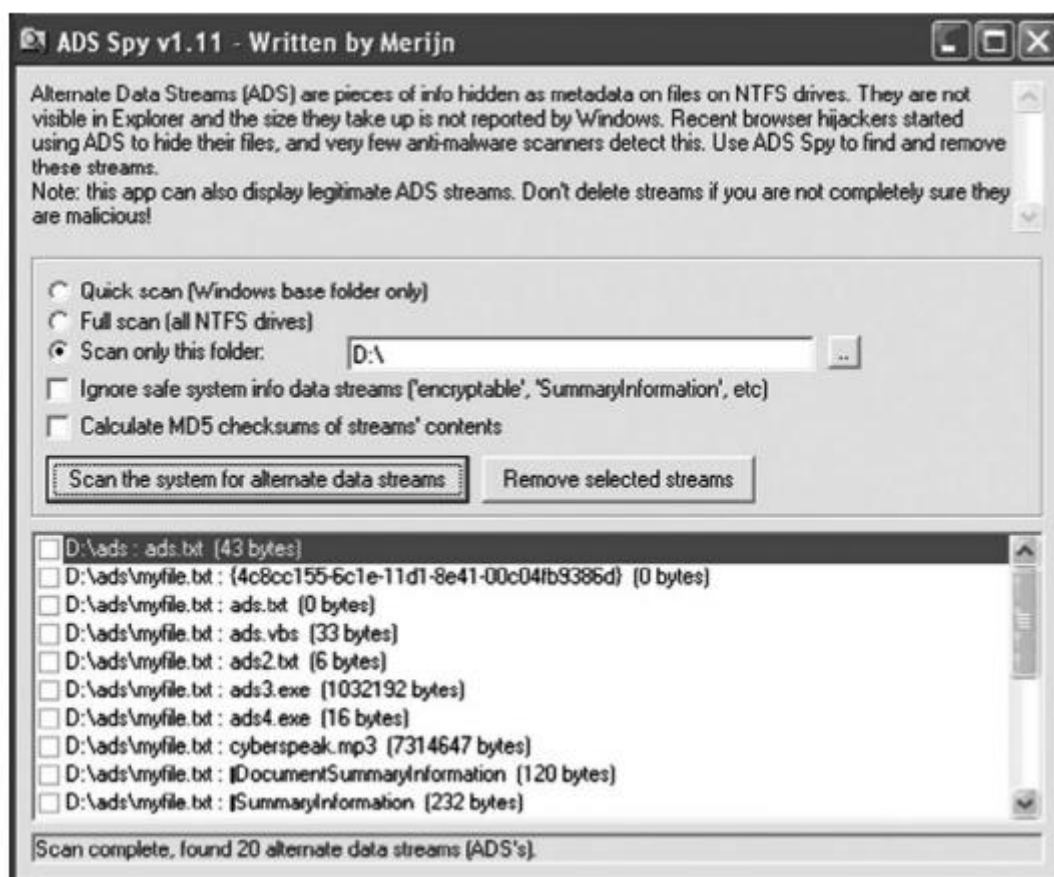
*size ADS in file*

```
-----  
120 d:\ads\myfile.txt: *DocumentSummaryInformation  
232 d:\ads\myfile.txt: *SummaryInformation  
0 d:\ads\myfile.txt:ads.txt  
34 d:\ads\myfile.txt:ads2.txt  
1032192 d:\ads\myfile.txt:ads3.exe  
0 d:\ads\myfile.txt:{4c8cc155-6c1e-11d1-8e41-00c04fb9386d}
```

Từ đầu ra của lads.exe, chúng ta có thể thấy rằng ba ADS bổ sung đã được thêm vào myfile.txt: một cái xuất hiện dưới dạng định danh duy nhất toàn cầu hoặc GUID (và có kích thước 0 byte) và hai cái khác bắt đầu bằng \*. Hai cái cuối cùng này là nơi thông tin được nhập vào Properties | Tab Summary được lưu.

Đôi khi bạn có thể thấy một ADS có tên AFP\_AfpInfo hoặc AFP\_Resource. Nếu bạn thấy một ADS có tên theo cách này, bạn nên kiểm tra xem liệu Dịch vụ tệp (File Services) cho dịch vụ Macintosh có được cài đặt và bật trên hệ thống của bạn không. Nếu vậy, luồng không tên có thể đã được sao chép từ hệ thống Macintosh thông qua giao thức AppleTalk. Khi điều này xảy ra, nhánh dữ liệu cho tệp được lưu vào tên tệp, chẳng hạn như myfile.txt. Nhánh tài nguyên sau đó được lưu vào myfile. txt: AFP\_Resource và thông tin về công cụ tìm hoặc thuộc tính được lưu vào myfile.txt: AFP\_AfpInfo.

Như đã đề cập trước đây, các công cụ khác tồn tại để liệt kê các ADS. Streams.exe (một công cụ Sysinternals có sẵn từ Microsoft), lns.exe (từ Arne Vidstrom, tại NTSecurity.nu) và sfind.exe (một phần của Bộ công cụ pháp lý có sẵn từ Foundstone.com) là các công cụ CLI tương tự lads.exe. Trình phát hiện ADS là trình cắm shell (tức là Windows Explorer) từ CodeProject.com, cho phép “xem trực quan thời gian thực của một tập tin không được mã hóa thay thế các luồng dữ liệu”. Cuối cùng, CrucialADS (từ CrucialSecurity.com) và ADS Spy (từ SpyWareInfo.com) là các công cụ dựa trên GUI để liệt kê các ADSes. ADS Spy, được minh họa trong Hình 5.12, cũng cho phép người dùng xóa các ADSes đã chọn.



Hình 5. 12. Giao diện gián điệp ADS

Khi bạn đã tìm thấy một ADS, bạn có thể xem nội dung của tệp bằng cách mở nó trong Notepad hoặc bằng cách sử dụng tiện ích cat (một tiện ích Unix tiêu chuẩn đọc các tệp tuần tự, ghi chúng vào đầu ra tiêu chuẩn), một phần của gói UnxUtils trên SourceForge.net. Bạn có thể sử dụng cat để xem nội dung của một ADS tại bàn điều khiển (tức là, STDOUT) hoặc bằng cách chuyển hướng đầu ra của lệnh sang một tệp riêng.

#### WARNING

Năm 2000, Benny và Ratter, sau đó thuộc nhóm virus-writing (Virus này xóa tất cả nội dung của một ổ đĩa) được gọi là 29A đã phát hành một loại virus có tên W2K. Luồng đã sử dụng ADSes. Virus lây nhiễm một tệp, thay thế nó, và sau đó sao chép tệp gốc vào ADS. Ví dụ: nếu virus bị nhiễm notepad.exe, nó sẽ thay thế tệp thực thi và sao chép Notepad gốc vào Notepad.exe: STR. Điều này chỉ hoạt động trên các hệ thống định dạng NTFS. Nếu hệ thống tệp được định dạng là hệ thống tệp FAT, thì không có ADS và tất cả những gì bạn còn lại là tệp bị truyền nhiễm.

Vào tháng 6 năm 2006, blog của công ty chống vi-rút F-Secure có chứa một mục mô tả trình điều khiển rootkit chế độ kernel Mailbot.AZ (còn gọi là

---

Rustock.A) (nói thêm về rootkit trong Chương 7) khiến việc phát hiện đặc biệt khó khăn bằng cách ẩn mình trong ADS. Hơn nữa, ADS được báo cáo là không thể được làm rõ bởi các công cụ phát hiện ADSes, bởi vì nó bị ẩn bởi rootkit. Rất khôn ngoan!

---

## Using ADSes (Sử dụng ADSes)

Vì vậy, bạn có thể tự hỏi, ADSes có thể được sử dụng để làm gì ngoài việc ẩn dữ liệu? Hóa ra, chúng có thể được sử dụng cho một số thứ. Ví dụ, bạn có thể đặt một tệp thực thi vào ADS và chạy nó từ đó. Sử dụng lệnh type, giống như chúng ta đã làm trước đây, để đặt một tệp thực thi trong một ADS, như vậy:

```
D:\ads>type c:\windows\system32\sol.exe > myfile.txt:ads4.exe
```

Trong trường hợp này, chúng tôi đã đặt trò chơi Solitaire trong một ADS. Đây là một ví dụ tốt để sử dụng vì khi chạy, nó dẫn đến một GUI tốt cho phép chúng ta thấy mọi thứ đang hoạt động tốt. Để thực hiện chương trình, gõ lệnh sau:

```
D:\ads>start .\myfile.txt:ads4.exe
```

Như bạn có thể thấy, chúng tôi đã trình bày với Solitaire GUI. Và điều này không bị hạn chế đối với các tệp thực thi, bởi vì các tập lệnh (Windows Scripting Host [WSH], Perl, v.v.) có thể được ẩn trong ADSes và khởi chạy một cách dễ dàng. Các công cụ WSH (cscript.exe, wscript.exe) sẽ chạy các tập lệnh ẩn trong ADSes mà không gặp vấn đề, cũng như Perl; ngay cả máy chủ Web IIS cũng sẽ cung cấp các tệp HTML và tập lệnh ẩn trong ADSes (đây là một cách tuyệt vời để bình phẩm sự kiện “Bắt cò”).

Cố gắng thực thi một ADS trên Vista trả về một kết quả khác, như Hình 5.13 minh họa



Hình 5. 13. Hộp thoại được trả về khi bạn cố thực hiện một ADS trên Vista

Các nỗ lực để khởi chạy ADS (myfile.txt: ads3.exe chứa phiên bản Solitaire của Vista) đã được đáp ứng với cùng một kết quả, bao gồm các biến thể của lệnh Start cũng như sử dụng Start|Run. Tuy nhiên, việc khởi chạy các tập lệnh WSH từ bên trong một ADS đã hoạt động mà không gặp sự cố nào trên Vista.

Một cách sử dụng thú vị khác cho ADSes là trong việc ẩn phương tiện. Phim và podcast có thể được ẩn trong ADSes, và sau đó Windows Media Player có thể được khởi chạy từ dòng lệnh để mở phương tiện:

```
wmplayer d:\ads\myfile.txt:cyberspeak.mp3
```

Tôi đã nghe một phiên bản podcast của CyberSpeak theo cách này. Thật thú vị, mặc dù podcast được khởi chạy từ dòng lệnh, tên tệp đã xuất hiện trong khóa Registry sau:

```
HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player\RecentFile  
List
```

Mục nhập được liệt kê trong dữ liệu được liên kết với giá trị File0, chỉ ra rằng bất cứ khi nào một tệp mới được thêm vào danh sách này, tên tệp sẽ được thêm vào đầu danh sách và tên tệp cũ hơn được đẩy xuống danh sách; số tập tin càng nhỏ, tập tin càng gần đây. Như bạn đã học trong Chương 4, LastWriteTime từ khóa Registry sẽ cho bạn biết khi nào tệp đó được truy cập thông qua Windows Media Player.

#### WARNING

Khi xem xét một trường hợp mẫu trong ProDiscover, tôi nhận thấy rằng có một số ADS trong Thùng rác (Recycle bin). ProDiscover hiển thị các ADS với phông chữ màu đỏ để chúng nổi bật và rõ ràng. Tôi đã xóa một số tệp mà tôi đã làm việc cùng, một trong số đó tôi đã tải xuống từ Internet. Tôi nhận thấy rằng ADS của Zone.Identifier hiển thị cho tệp (tôi đã tải xuống tệp qua Internet Explorer) nhưng số lượng bản ghi cho tổng số tệp qua tệp INFO2 không phản ánh sự tồn tại của ADS.

## Removing ADSes (Loại bỏ ADSes)

Bây giờ bạn đã thấy cách ADSes có thể được tạo và sử dụng, bạn có thể làm gì để loại bỏ chúng? Có một số cách để giải quyết vấn đề này và cách bạn chọn tùy thuộc vào nhu cầu và sở thích của bạn.

Một cách để loại bỏ một ADS là chỉ cần xóa tệp mà ADS được đính kèm. Tuy nhiên, kết quả rõ ràng là nếu tệp gốc quan trọng đối với bạn (tài liệu, bảng tính, tệp hình ảnh), bạn sẽ mất dữ liệu đó.

Để lưu dữ liệu gốc của bạn, bạn có thể muốn sử dụng lệnh type để sao chép nội dung của luồng không tên ban đầu (trong ví dụ của chúng tôi, myfile.txt) sang tên tệp khác và sau đó xóa tệp gốc. Một tùy chọn khác là sao chép tệp vào phương tiện không phải là NTFS. Hãy nhớ rằng, ADS là một tính năng NTFS, vì vậy sao chép tệp vào đĩa mềm, Ổ đĩa USB hoặc một phân vùng khác được định dạng trong FAT, FAT32 hoặc

một số hệ thống tệp khác (tệp FTP sang hệ thống Linux được định dạng ext2 và sau đó quay lại lần nữa) sẽ loại bỏ ADS một cách hiệu quả.

Nhưng điều gì sẽ xảy ra nếu ADS mà bạn đã phát hiện được dính kèm vào danh sách thư mục, chẳng hạn như C:\ hoặc C:\windows\system32? Bạn có thể chỉ cần xóa thư mục và sao chép nó từ một hệ thống tệp khác, nhưng khá khó khăn. Vậy bạn làm gì? Sử dụng lệnh echo, bạn có thể làm ADS thành tệp văn bản vô hại, bất kể nội dung của nó. Từ ví dụ trước đây của chúng tôi về việc sao chép trò chơi Solitaire vào ADS, chúng tôi có thể chạy lads.exe và nhận thông tin về ADS đó:

```
56832 d:\ads\myfile.txt:ads4.exe
```

Được rồi, vì vậy chúng tôi có một ADS có kích thước 56.832 byte và chúng tôi đã biết đây là một tệp thực thi. Vì vậy, gõ lệnh sau:

```
D:\ads>echo "deleted ADS" > myfile.txt:ads4.exe
```

Chạy lại lads.exe, chúng tôi thấy rằng kích thước tệp đã thay đổi:

```
16 d:\ads\myfile.txt:ads4.exe
```

Vì vậy, chúng tôi đã “chăm sóc” một cách hiệu quả ADS; mặc dù chúng tôi đã không xóa nó, nhưng chúng tôi đã làm cho nó trở nên vô hại. Bạn thậm chí có thể viết một tin nhắn cho ADS nêu rõ bản chất của ADS bạn đặt, tên của bạn và khi bạn xóa nó. Cuối cùng, một tùy chọn khác là sử dụng ứng dụng ADS Spy GUI đã đề cập trước đó.

## **ADS Summary (Tóm lược ADS)**

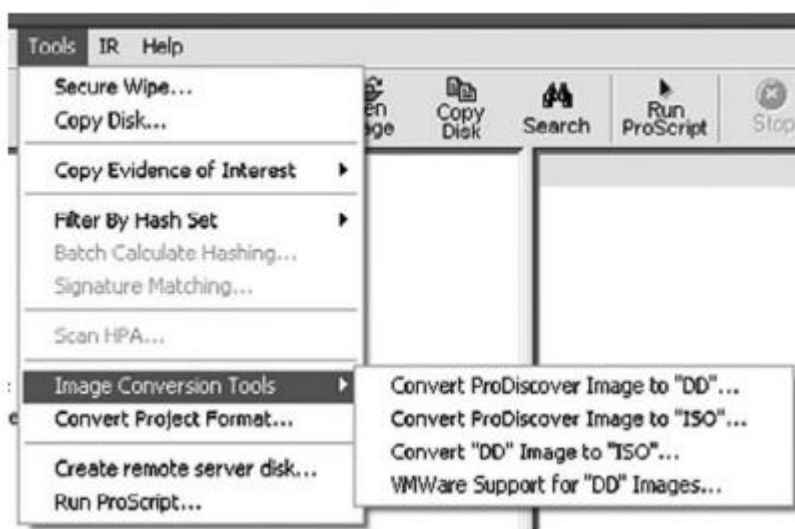
Tại thời điểm này, chúng tôi đã đưa ra rất nhiều thông tin về ADS, thảo luận về cách chúng được tạo ra và cách chúng có thể được sử dụng và loại bỏ. Thông tin này rất quan trọng để ghi nhớ khi bạn thực hiện phản ứng sự cố hoặc hoạt động pháp y trên máy tính. ADSes đủ bất thường để các công cụ phân tích điều tra số thương mại như ProDiscover hiển thị ADSes màu đỏ. Tuy nhiên, không phải tất cả các ADS đều có bản chất độc hại; bạn đã thấy một số ứng dụng sử dụng ADS như thế nào chỉ là một phần trong cách chúng hoạt động.

Một điều mà các nhà điều tra nên ghi nhớ là xem nội dung của một ADS. Chỉ bởi vì một ADS được đặt tên bằng cách sử dụng một trong các chương trình đặt tên trong các ứng dụng đã được biết đến, các ứng dụng hợp pháp không có nghĩa là những gì trong ADS không phải là độc hại. Đó là để nói, không chỉ đơn giản viết tắt ADS là tốt vì nó có tên là AFP\_AfpInfo. Kẻ xấu thích che giấu phần mềm độc hại bằng cách đặt cho nó một cái tên mà quản trị viên hoặc nhà phân tích pháp y rất có thể sẽ bỏ qua.

## 5.4. Alternative Methods of Analysis (Phương pháp phân tích thay thế)

Đôi khi, khi bạn đang tiến hành phân tích điều tra số máy tính sau khi chết (sau khi bạn đã lấy được một hình ảnh), bạn có thể cần phải thực hiện việc phân tích đơn giản khó khăn hơn khi bạn làm việc với một hình ảnh. Ví dụ, bạn có thể quyết định rằng bạn muốn quét hệ thống để tìm phần mềm độc hại, chẳng hạn như Trojans, backdoor hoặc phần mềm gián điệp. Khi bạn đang làm việc với một hình ảnh của hệ thống, bạn đã có sẵn cho một tệp duy nhất (hoặc, như thường lệ, nhiều tệp có kích thước tương đương với ổ cứng ban đầu) và bạn cần một cách để quét các tập tin trong hình ảnh. Vì vậy, thay vì kéo tất cả các tệp ra khỏi hình ảnh, có một số công cụ mà bạn có thể sử dụng để chuyển đổi hình ảnh thành định dạng phù hợp để quét.

Một công cụ như vậy có sẵn thông qua ProDiscover. Bắt đầu với Phiên bản 4.85 của ProDiscover, công cụ có khả năng chuyển đổi hình ảnh từ định dạng ProDiscover ban đầu hoặc định dạng dd sang định dạng ISO. ProDiscover cũng có khả năng tạo các tệp cần thiết để khởi động hình ảnh trong VMware. Hình 5.14 minh họa các tùy chọn mới này.



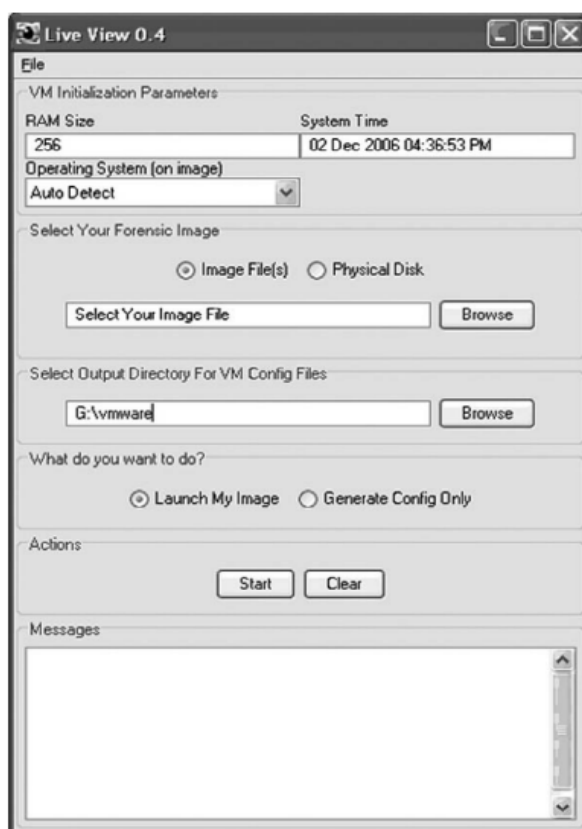
Hình 5. 14. Menu ProDiscover hiển thị các công cụ mới

Như bạn có thể thấy trong Hình 5.14, bạn có thể sử dụng ProDiscover để chuyển đổi từ định dạng tệp ProDiscover .eve ban đầu sang định dạng dd hoặc từ hình ảnh ProDiscover hoặc dd sang hình ảnh thông số kỹ thuật ISO 9660 Joliet. Bạn cũng có thể sử dụng ProDiscover để tạo các tệp cần thiết để khởi động hình ảnh trong VMware, tương tự như công cụ phụ tá VMware P2V (viết tắt của công cụ Trợ lý vật lý-ảo) cho phép bạn làm. Sử dụng các công cụ như thế này, bạn có thể khởi động hệ thống để thực hiện phân tích bổ sung, chẳng hạn như quét phần mềm chống vi-rút và phần mềm chống

gián điệp hoặc để xem hệ thống trông như thế nào khi vận hành. Đôi khi, điều này có thể rất hữu ích khi bạn điều tra một trường hợp, bởi vì rất khó xác định bản chất của một hệ thống đang chạy (do các tương tác giữa các cài đặt cấu hình khác nhau, phần mềm được cài đặt, v.v.) trong quá trình phân tích hậu kết thúc.

Một Webnir kỹ thuật có sẵn tại trang web của Trung tâm tài nguyên đường dẫn công nghệ ([www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14](http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14)) hướng dẫn bạn chi tiết về cách sử dụng các công cụ ProDiscover để khởi động hình ảnh trong VMware. Webnir yêu cầu phần mềm máy khách phù hợp từ WebEx.com.

Một công cụ khác miễn phí và cực kỳ dễ sử dụng để khởi động một hình ảnh thu được trong VMware là Live View (<http://liveview.sourceforge.net>), có sẵn từ CERT. Live View sử dụng GUI dễ hiểu (như minh họa trong Hình 5.15) để hướng dẫn bạn qua nhiều tùy chọn cấu hình cần thiết để định cấu hình hình ảnh được khởi động trong VMware và nó tự động tạo ra các tệp cần thiết.



Hình 5. 15. Live view GUI

Chạy Live View là một quá trình đơn giản và trực quan. Live View hỗ trợ hầu hết các phiên bản Windows và có hỗ trợ hạn chế cho Linux. Tôi đã sử dụng công cụ này thành công nhiều lần để khởi động và đăng nhập vào hình ảnh thu được.

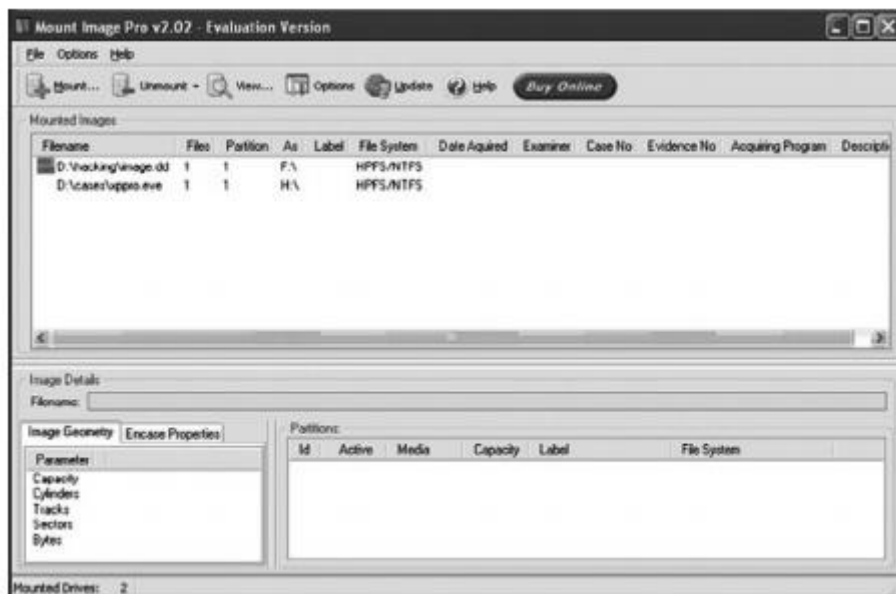
**NOTE**

Một khi bạn có được hình ảnh để khởi động, bạn có thể làm nhiều thứ khác nhau. Nếu bạn sử dụng sản phẩm VMware Workstation và cấu hình như một mạng cầu nối, bạn có thể kích hoạt giao diện mạng cho hình ảnh mới khởi động của mình và quét nó giống như khi bạn thực hiện quét cổng từ xa và /hoặc quét lỗ hổng. Bạn cũng có thể muốn đăng nhập vào hệ thống đang chạy, vì vậy trừ khi quản trị viên hoặc mật khẩu người dùng trống, bạn sẽ cần phải có sự hợp tác của bộ phận người dùng hoặc bộ phận công nghệ thông tin (IT) để lấy mật khẩu hoặc đoán mật khẩu sử dụng các công cụ mạnh mẽ hoặc mật khẩu thu được từ việc kiểm tra điều tra số của hệ thống.

Khởi động hình ảnh qua Live View là điều mà một nhà phân tích có thể đưa vào như một phần trong phân tích của họ để “xem những gì người dùng đã thấy”. Một cách khác để sử dụng các công cụ như Live View là gắn hình ảnh dưới dạng hệ thống tệp chỉ đọc.

## Mounting an Image (Gắn một hình ảnh)

Một công cụ tuyệt vời khác (mặc dù không miễn phí) là Mount Image Pro (MIP, có sẵn từ [www.mountimage.com](http://www.mountimage.com)). MIP là một công cụ tuyệt vời cho phép bạn gắn hình ảnh dưới dạng ổ đĩa chỉ đọc trên hệ thống hiện tại của bạn. Hình 5.16 minh họa hai hình ảnh được gắn dưới dạng ổ đĩa F:\ và H:\ thông qua phiên bản đánh giá 30 ngày của Mount Image Pro.



Hình 5. 16. Hình ảnh được gắn dưới dạng ổ đĩa thông qua Mount Image Pro v2.02

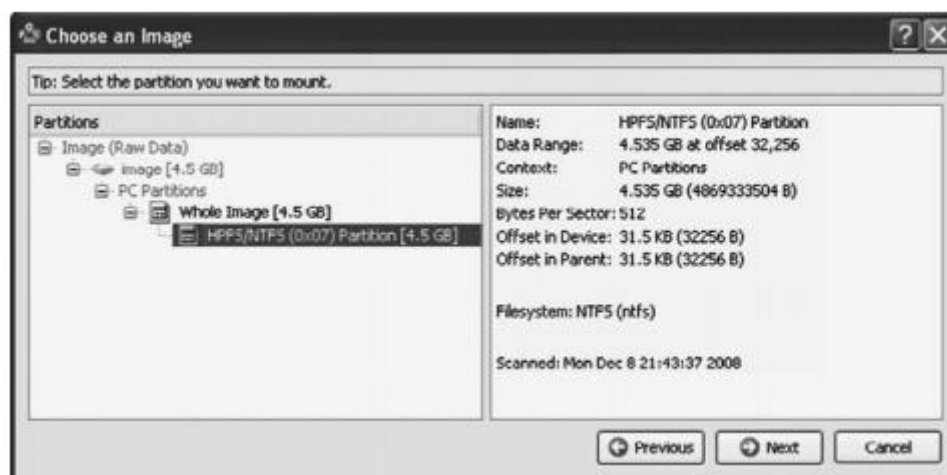
MIP không khởi động hình ảnh và cho phép bạn truy cập hình ảnh khi hệ thống đang chạy; bạn sẽ không thể trích xuất các quy trình đang chạy cho hệ thống đó từ bộ



nhớ vật lý. Thay vào đó, nó gắn hình ảnh dưới dạng ký tự ổ đĩa để bạn có thể truy cập các tệp trong hình ảnh giống như bất kỳ ký tự ổ đĩa nào khác và nó làm như vậy trong chế độ chỉ đọc để không có thay đổi nào được thực hiện đối với hình ảnh. Để xác minh điều này, tôi đã sử dụng md5deep.exe để tính toán hàm băm mật mã cho hình ảnh của một hệ thống thu được có trong một tệp duy nhất. Sau đó, tôi đã sử dụng MIP để gắn hình ảnh dưới dạng ký tự ổ đĩa và tôi đã truy cập một số tệp và sao chép một số tệp từ ổ đĩa được gắn sang phân vùng khác trên hệ thống của mình. Khi tôi đã hoàn thành một số hành động, bao gồm chạy một số tập lệnh Perl đối với các tệp trong ổ đĩa được gắn, tôi đã gỡ bỏ ký tự ổ đĩa và tắt hoàn toàn ứng dụng MIP. Sau đó, tôi chạy lại md5deep.exe đối với tệp hình ảnh và hàm băm được trả về giống hệt với hàm băm đầu tiên mà tôi đã tính toán, xác minh rằng hình ảnh được gắn ở chế độ chỉ đọc. Tạo và xác minh băm mật mã bằng thuật toán đã biết và được chấp nhận sẽ là một phần của quy trình vận hành tiêu chuẩn nếu bạn sử dụng các công cụ như Mount Image Pro. (Một số công cụ có sẵn miễn phí như MD5, SHA-1 và SHA-256 thực hiện nhiều thuật toán được chấp nhận).

Một công cụ rất mạnh khác sử dụng để gắn hình ảnh thu được dưới dạng hệ thống tệp chỉ đọc là Smart Mount từ ASR Data ([www.asrdata.com/SmartMount/](http://www.asrdata.com/SmartMount/)). Theo ASR Data, Andy Rosen, tác giả của công cụ, Smart Mount cung cấp đáng kể nhiều chức năng hơn (ví dụ: nó chạy trên Windows và Linux, sẽ gắn các tệp .E01 được bảo vệ bằng mật khẩu mà không cần mật khẩu, v.v.) so với MIP, và mặc dù đây cũng là một sản phẩm thương mại phải mua, phiên bản đánh giá cũng có sẵn.

Smart Mount sẽ gắn một loạt các tệp hình ảnh, bao gồm các tệp VMware.vmdk và các tệp Định dạng nhân chứng chuyên gia EnCase (EWF), cũng như các tệp hình ảnh chưa qua xử lý. Hình 5.17 minh họa một phần của quá trình sử dụng Smart Mount để gắn tệp hình ảnh thu được dưới dạng hệ thống tệp chỉ đọc (lưu ý rằng hình ảnh thu được có sẵn từ [www.cfreds.nist.gov/Hacking\\_Case.html](http://www.cfreds.nist.gov/Hacking_Case.html)).



Hình 5. 17. Gắn thông minh một tệp hình ảnh đã có

Bạn cũng có thể sử dụng các công cụ có sẵn miễn phí để gắn hình ảnh thu được dưới dạng hệ thống tệp, mặc dù với các mức độ dễ sử dụng và chức năng khác nhau. Hai công cụ như vậy là VDK (<http://chitchat.at.infoseek.co.jp/vmware/vdk.html>) và ImDisk ([www.ltr-data.se/opencode.html](http://www.ltr-data.se/opencode.html)). VDK cài đặt dưới dạng tệp thực thi CLI (vdk.exe) và dưới dạng trình điều khiển (vdk.sys). Nhập lệnh VDK trợ giúp vào dòng lệnh sẽ hiển thị cho bạn các tùy chọn khác nhau có sẵn với VDK hoặc bạn có thể tải xuống và cài đặt GUI VDKWin (<http://petruska.stardock.net/Software/VMware.html>), hiện có sẵn như Phiên bản 1.1.1 và cho phép bạn gắn các tệp hình ảnh dưới dạng các ổ đĩa ảo, chỉ đọc. VDK cho phép bạn gắn kết cả đĩa ảo VMware (tệp .vmdk) cũng như hình ảnh chưa qua xử lý dưới dạng hệ thống tệp chỉ đọc. Bạn cũng có thể sử dụng vdk.exe để thực hiện nhiều chức năng khác nhau; ví dụ: để lấy thông tin về tệp hình ảnh thu được, chẳng hạn như các phân vùng trong tệp hình ảnh, sử dụng lệnh view:

```
D:\vdk\vdk view D:\hacking\image.dd
```

*Đầu ra của lệnh này trông giống như sau:*

*Image Name : image*

*Disk Capacity : 9514260 sectors (4645MB)*

*Number Of Files : 1*

*Type Size Path*

```
-----
FLAT 9514260 d:\hacking\image.dd
```

*Partitions :*

*# Start Sector Length in sectors Type*

```
-----
0 0 9514260 (4645MB) <disk>
```

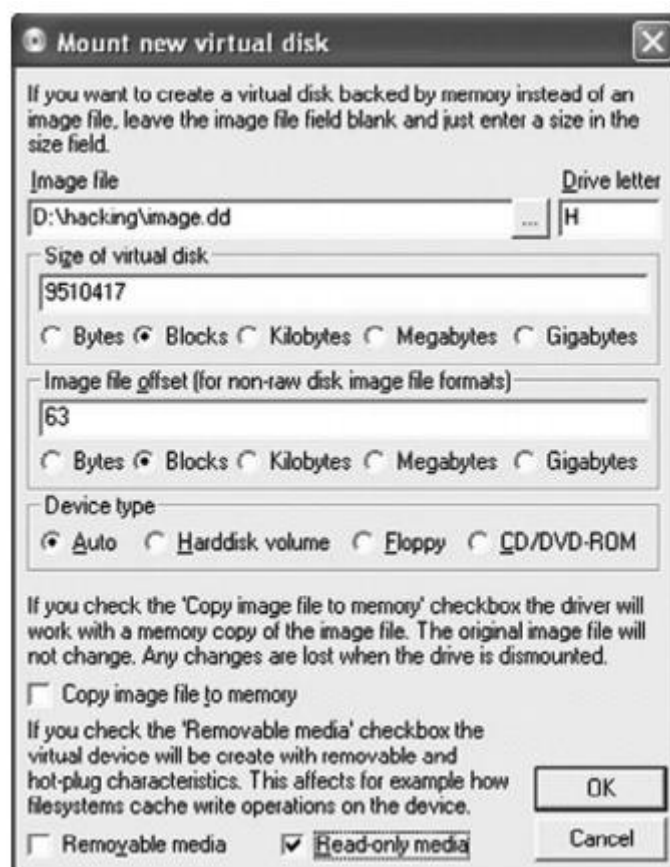
```
1 63 9510417 (4643MB) 07h:HPFS/NTFS
```

ImDisk cài đặt như một ứng dụng bảng điều khiển và một applet Control Panel (như Hình 5.18 minh họa) và cung cấp chức năng tương tự như VDK.



Hình 5. 18. Biểu tượng bảng điều khiển ImDisk

Hình 5.19 minh họa hộp thoại ImDisk sau khi tệp hình ảnh được chọn. Bước tiếp theo trong quy trình sẽ gắn tệp hình ảnh đã chọn dưới dạng đĩa ảo chỉ đọc với ký tự ổ đĩa H:\



Hình 5. 19. Hộp thoại ImDisk

Gắn hình ảnh dưới dạng ký tự ổ đĩa chỉ đọc có rất nhiều lợi thế, đặc biệt là trong các lĩnh vực giám và phân tích dữ liệu. Ví dụ: bạn có thể chạy bất kỳ số lượng công cụ nào, chẳng hạn như trình phát hiện phần mềm chống vi-rút và phần mềm gián điệp, phân tích chữ ký tệp và các công cụ để liệt kê NTFS ADSes, chống lại hình ảnh theo kiểu tự động. Thay vì liệt kê thông qua một hình ảnh và sau đó phải sao chép các tệp yêu thích ra khỏi hình ảnh để phân tích chi tiết hơn, bạn có thể tự động hóa nhiều phương pháp này thông qua các tập lệnh Perl.

## Discovering Malware (Khám phá phần mềm độc hại)

Một nhiệm vụ phân tích tốn nhiều công sức mà nhiều nhà phân tích gặp phải là định vị phần mềm độc hại trên hệ thống hoặc trong một hình ảnh thu được. Trong một trường hợp, tôi đã kiểm tra hình ảnh của một hệ thống mà người dùng đã báo cáo các sự kiện đáng ngờ. Cuối cùng tôi đã tìm ra phần mềm độc hại chịu trách nhiệm cho những sự kiện đó, nhưng sử dụng một công cụ để gắn hình ảnh thu được dưới dạng hệ thống tệp chỉ đọc sẽ không chỉ cho phép tôi xác định phần mềm độc hại cụ thể nhanh hơn cách quét nó bằng ứng dụng quét chống vi-rút, nhưng cũng cho phép tôi tự động quét qua một số hình ảnh để xác định phần mềm độc hại đó hoặc sử dụng nhiều công cụ để quét phần mềm độc hại hoặc phần mềm gián điệp. Điều này sẽ có lợi cho tôi trong

một trường hợp cụ thể khi sự lây nhiễm ban đầu vào hệ thống xảy ra hai năm trước khi hình ảnh được thu nhận. Có khả năng quét các tệp từ một hình ảnh thu được giống như chúng là các tệp trên hệ thống trực tiếp của bạn, nhưng không sửa đổi chúng theo bất kỳ cách nào, có thể cực kỳ có giá trị đối với người kiểm tra.

---

Khi cố gắng xác định xem một hình ảnh thu được có chứa phần mềm độc hại hay không, một tài nguyên tuyệt vời là các tệp nhật ký từ ứng dụng chống vi-rút được cài đặt, nếu có. Ví dụ, tệp mrt.log được đề cập trước đó trong chương này có thể cung cấp cho bạn một số dấu hiệu về những gì hệ thống đã được bảo vệ chống lại. Các ứng dụng chống vi-rút khác duy trì các tệp nhật ký ở các vị trí khác trong hệ thống tệp, một số tùy thuộc vào phiên bản của ứng dụng. McAfee VirusScan Enterprise Phiên bản 8.0i duy trì các tệp nhật ký của nó trong thư mục C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan, trong khi một phiên bản khác của ứng dụng duy trì tệp onaccessscanlog.txt của nó trong C:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection. Ngoài ra hãy chắc chắn kiểm tra Nhật ký sự kiện ứng dụng cho các mục được viết bởi các ứng dụng chống vi-rút.

---

Khi bạn đã gắn hình ảnh thu được (tất nhiên là chỉ đọc), bạn sẵn sàng quét nó bằng ứng dụng quét chống vi-rút mà bạn chọn. Một số giải pháp chống vi-rút thương mại và phần mềm miễn phí có sẵn, và ý kiến hay là nên sử dụng nhiều hơn một ứng dụng quét chống vi-rút. Claus Valca có một số ứng dụng quét chống vi-rút di động được liệt kê trong blog Grand Stream Dreams của anh ấy (<http://grandstreamdreams.blogspot.com/2008/11/portable-anti-virusmalware-security.html>). Khi sử dụng bất kỳ công cụ quét phần mềm chống vi-rút hoặc phần mềm gián điệp nào (có quá nhiều tùy chọn để liệt kê ở đây), hãy đảm bảo định cấu hình các công cụ để không xóa hoặc cách ly hoặc sửa đổi bất kỳ tệp nào được phát hiện. Nhiều công cụ quét đi kèm với một tùy chọn chỉ cảnh báo và không có hành động nào khác, vì vậy hãy chắc chắn kiểm tra các tùy chọn đó.

Vì việc gắn hình ảnh thu được có thể cung cấp quyền truy cập chỉ đọc vào các tệp trong một hình ảnh, bạn có thể truy cập các tệp đó giống như các tệp thông thường trên hệ thống mà không thay đổi nội dung của các tệp. Như vậy, các ngôn ngữ script như Perl sẽ trả về các tệp xử lý khi bạn mở tệp và thư mục, làm cho điểm khôi phục và phân tích thư mục prefetch (cơ chế tìm nạp ngầm) trở thành một quy trình đơn giản. Các tập lệnh Perl được sử dụng trên các hệ thống trực tiếp để thực hiện các chức năng

này chỉ cần được “chỉ vào” các vị trí thích hợp. RegRipper, được thảo luận ở độ dài trong Chương 4, là một công cụ hoạt động như thế; nhà phân tích có thể gắn tệp hình ảnh thu được dưới dạng hệ thống tệp chỉ đọc, và sau đó trỏ RegRipper vào tệp hive Registry thích hợp. Trong các ví dụ được sử dụng trong phần “Gắn kết hình ảnh”, một nhà phân tích sẽ hướng RegRipper về phía H:\Windows\system32\config, trong đó các tệp trung tâm của Registry nằm trong hình ảnh được gắn. Sử dụng các công cụ như RegRipper theo cách này sẽ cho phép bạn kiểm tra các vị trí tự khởi động trong Sổ đăng ký (bạn có thể sử dụng các công cụ khác để kiểm tra các vị trí tự khởi động trong hệ thống tệp) để biết các dấu hiệu có thể có của phần mềm độc hại.

---

Vị trí tự khởi động là các vị trí trong các hệ thống Windows cho phép các ứng dụng được khởi động với ít tương tác hoặc không có tương tác người dùng. Như bạn đã thấy trong Chương 4, Windows Registry chứa nhiều vị trí như vậy, cũng như hệ thống tệp. Trong Chương 1, bạn đã thấy rằng bạn có thể sử dụng ứng dụng Autorun có sẵn từ Microsoft (từ trang Sysinternals) hoặc anh em CLI của nó, autorunsc.exe, để nhanh chóng kiểm tra các vị trí tự khởi động trên hệ thống trực tiếp.

---

Một ví dụ khác là về một công cụ mà tôi viết có tên WFPCheck (WFPCheck không có sẵn trên phương tiện đi kèm). Tại Hội nghị điều tra số Sans vào tháng 10 năm 2008, các chuyên gia tư vấn từ Mandiant đã đề cập đến phần mềm độc hại có thể lây nhiễm các tệp được bảo vệ bởi Windows File Protection (WFP) và các tệp đó sẽ vẫn bị lây nhiễm. Tôi đã đọc các báo cáo về phần mềm độc hại tương tự trước đây và đã nghiên cứu về vấn đề này. Tôi thấy rằng có một cuộc gọi API không có giấy tờ được gọi là SfcFileException ([www.bitsum.com/aboutwfp.asp](http://www.bitsum.com/aboutwfp.asp)) sẽ bị đình chỉ WFP trong một phút. WFP “lắng nghe” các thay đổi tập tin và “thức dậy” khi sự kiện thay đổi tập tin xảy ra đối với một trong các tệp được bảo vệ và không thăm dò các tệp được bảo vệ một cách thường xuyên để xác định xem có bị sửa đổi theo cách nào không. Tạm dừng WFP trong một phút là quá đủ thời gian để lây nhiễm tệp và một khi WFP hoạt động trở lại, không có cách nào để phát hiện ra rằng tệp được bảo vệ đã bị sửa đổi.

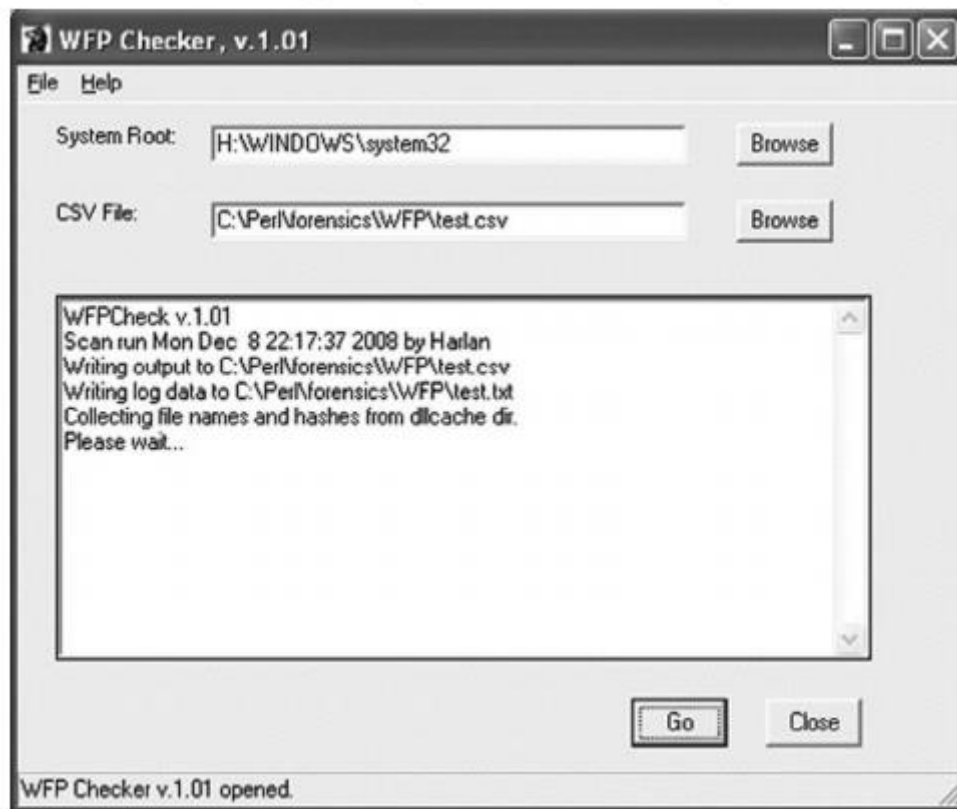


---

API SfcFileException được gọi bởi công cụ trình diễn, WfpDeprotect ([www.bitsum.com/wfpdeprotect.php](http://www.bitsum.com/wfpdeprotect.php)).

---

Như kết quả của vấn đề này, tôi đã quyết định viết WFPCheck (wfpchk.pl). WFPCheck hoạt động bằng cách trước tiên đọc danh sách các tệp từ thư mục system32 \ dllcache và tạo băm MD5 cho mỗi tệp. Sau đó WFPCheck sẽ tìm kiếm từng tệp, đầu tiên trong thư mục system32 và sau đó trong toàn bộ phân vùng (bỏ qua các thư mục system32 và system32\dllcache). Là một tệp có cùng tên với một trong các tệp được bảo vệ, WFPCheck tạo ra hàm băm MD5 cho tệp đó và so sánh nó với hàm băm mà nó đã có. WFPCheck đưa kết quả của nó vào tệp giá trị được phân tách bằng dấu phẩy (.csv) và ghi việc tính toán dựa trên văn bản của các hoạt động của nó vào cùng thư mục với tệp .csv. Hình 5.20 minh họa WFPCheck đang chạy với tệp hình ảnh được gắn kết.



Hình 5. 20. WFPCheck đang chạy với tệp hình ảnh được gắn kết

Tệp .csv từ WFPCheck bao gồm ba cột: tên tệp từ thư mục system32\dllcache, đường dẫn đầy đủ đến nơi tìm thấy tệp (bên ngoài thư mục dllcache) và kết quả so sánh. Nếu WFPCheck thấy rằng các giá trị băm được tạo ra khớp với nhau, kết quả sẽ là “phù hợp” (được minh họa trong hình 5.21). Nếu các giá trị băm không khớp, kết quả sẽ là “không phù hợp”, theo sau là hai bộ giá trị được phân tách bằng dấu hai chấm; kích thước tệp tương ứng theo sau băm tương ứng của chúng. Hai bộ số này được phân tách bằng dấu gạch ngang.

File	Full Path	Result
12520437.cpx	H:\WINDOWS\system32\12520437.cpx	Match
12520850.cpx	H:\WINDOWS\system32\12520850.cpx	Match
6to4svc.dll	H:\WINDOWS\system32\6to4svc.dll	Match
aaaamon.dll	H:\WINDOWS\system32\aaaamon.dll	Match
access.cpl	H:\WINDOWS\system32\access.cpl	Match
acctres.dll	H:\WINDOWS\system32\acctres.dll	Match
accwiz.exe	H:\WINDOWS\system32\accwiz.exe	Match

Hình 5. 21. Đoạn trích của tệp .csv đầu ra WFPCheck

## WARNING

Trên các hệ thống được cập nhật nhưng không xóa các tệp cũ hơn, WFPCheck có thể tạo ra một số kết quả “không phù hợp”. Điều này là do các tệp được thay thế khi hệ thống cập nhật, và nếu các phiên bản cũ của các tệp từ các bản cập nhật trước đó bị bỏ lại quanh hệ thống tệp, WFPCheck có thể sẽ thấy rằng một tệp được bảo vệ khớp với dllcache mate của nó, nhưng sẽ xác định các tệp cũ hơn của cùng tên không khớp với nhau. Khi sử dụng WFPCheck, bạn phải kiểm tra chặt chẽ các kết quả, vì có thể có kết quả dương tính giả (lỗi báo cáo dữ liệu trong đó kết quả xét nghiệm không đúng cho thấy sự hiện diện của một tình trạng, như bệnh xuất hiện). Để hỗ trợ giảm dương tính giả, tôi đã viết một phiên bản khác của WFPCheck có tên WFPCheckf, trích xuất thông tin phiên bản tệp từ phần tài nguyên của tệp, là nơi thích hợp (xem Chương 6 để biết giải thích về các phần khác nhau của tệp thực thi).

Tuy nhiên, một phương tiện khác dùng để kiểm tra phần mềm độc hại tiềm ẩn trong hình ảnh thu được được gắn dưới dạng hệ thống tệp chỉ đọc là sử dụng sigcheck.exe từ Microsoft (<http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx>). Sigcheck.exe kiểm tra xem một tập tin có được ký điện tử hay không, cũng như loại bỏ thông tin phiên bản của tập tin, nếu có. Ví dụ: lệnh sau sẽ kiểm tra nội dung của thư mục Windows \ system32 được gắn kết tệp hình ảnh (được gắn dưới dạng ổ H: \) cho tất cả các tệp thực thi chưa được ký:

```
D:\tools>sigcheck -u -e H:\Windows\system32
```

Mặc dù nó không dứt khoát, bạn có thể sử dụng kỹ thuật này như một trong một số kỹ thuật được sử dụng để cung cấp phân tích toàn diện các tệp trong hình ảnh thu được trong khi tìm kiếm phần mềm độc hại.



## Timeline Analysis (Phân tích dòng thời gian)

Phân tích dòng thời gian là một phương tiện để xác định hoặc liên kết một chuỗi các sự kiện theo cách dễ dàng cho những người như người ứng phó sự cố để hình dung và hiểu. Rất nhiều thứ chúng tôi làm như các nhà phân tích được liên kết với thời gian theo một cách nào đó; ví dụ: một trong những điều tôi theo dõi khi nhận được cuộc gọi hỗ trợ là thời gian tôi nhận được cuộc gọi đó. Trong quá trình xử lý, tôi cố gắng xác định khi nào người gọi lần đầu tiên nhận được dấu hiệu của sự cố, chẳng hạn như khi anh ta lần đầu tiên nhận thấy điều gì đó bất thường hoặc nhận được thông báo từ nguồn bên ngoài. Thông tin này thường xuyên giúp tôi thu hẹp những gì tôi tìm kiếm trong quá trình phản hồi cũng như trong quá trình phân tích và trong dữ liệu thu được (hình ảnh, bãi chứa bộ nhớ, nhật ký, v.v.) tôi tìm kiếm. Tất cả những điều này có liên quan đến việc dữ liệu có một loại giá trị thời gian nào đó được liên kết với nó, hoặc là một “dấu ấn thời gian” theo cách nào đó.

Khi một người phản hồi bắt đầu tham gia vào một sự cố, đột nhiên cánh cửa mở ra một lượng dữ liệu đáng kể theo thời gian. Các tệp trong một hình ảnh thu được có thời gian MAC được liên kết với chúng, cho biết khi nào chúng được sửa đổi hoặc truy cập lần cuối. Nhật ký tệp trên hệ thống (Nhật ký sự kiện Windows, Nhật ký máy chủ Web IIS, Nhật ký dịch vụ FTP, tệp nhật ký ứng dụng chống vi-rút, v.v.) chứa các mục có thời gian liên quan đến các sự kiện cụ thể. Như bạn đã thấy trong Chương 4, không chỉ các khóa Registry có dấu thời gian ở dạng LastWrite, mà trong các danh sách được sử dụng gần đây nhất (MRU), sự kiện gần đây nhất được liên kết với thời gian khóa LastWrite đó. Thêm vào đó là các giá trị Registry khác nhau chứa giá trị thời gian trong dữ liệu của họ và có khá nhiều dữ liệu được đóng dấu thời gian có sẵn cho người phản hồi để không chỉ biết được khi nào sự cố có thể xảy ra, mà còn có thể xác định các sự việc do con người gây ra bổ sung của sự việc.

Thông thường, các nhà phân tích đã bắt đầu phát triển dòng thời gian bằng cách thu thập dữ liệu được đóng dấu thời gian và thêm nó vào bảng tính. Một trong những lợi ích của loại phát triển dòng thời gian này là việc thêm các sự kiện mới khi chúng được phát hiện là tương đối đơn giản và khi dữ liệu mới được thêm vào, các mục nhập có thể được sắp xếp để đưa tất cả các mục vào trình tự phù hợp trên dòng thời gian. Quá trình này cũng hữu ích cho việc giảm dữ liệu (vì nhà phân tích chỉ thêm các giá trị họ quan tâm), nhưng nó có thể tốn thời gian và gây cản trở. Ngoài ra, quá trình này không đặc biệt có khả năng mở rộng, vì với các hệ điều hành hiện đại và các nguồn dữ liệu khác trong khi kiểm tra, nhà phân tích có thể nhanh chóng bị choáng ngợp bởi số lượng sự kiện có thể có hoặc không có bất kỳ tác động nào đối với việc kiểm tra.



Một phương tiện tự động để thu thập thông tin có dấu thời gian từ hình ảnh thu được là sử dụng công cụ fls có sẵn với Bộ công cụ Sleuth (TSK, bạn có thể tìm thấy tại [www.sleuthkit.org/](http://www.sleuthkit.org/)), được viết bởi Brian Carrier. Công cụ fls được chạy với một tệp hình ảnh thu được để liệt kê các tệp và thư mục trong ảnh, cũng như các tệp đã bị xóa gần đây, gửi đầu ra của nó tới tệp được gọi là “tập tin cơ thể” ([http://wiki.sleuthkit.org/index.php?title=Body\\_file](http://wiki.sleuthkit.org/index.php?title=Body_file)). Tập tin cơ thể sau đó có thể được phân tích cú pháp bởi tập lệnh mactime.pl Perl để chuyển đổi tập tin cơ thể thành dòng thời gian theo định dạng dựa trên văn bản dễ hiểu hơn. Trang Timelines tại trang web Sleuth Kit (<http://wiki.sleuthkit.org/index.php?title=Timelines>) cung cấp thêm thông tin về quy trình này.

Hiển thị dữ liệu tệp được đóng dấu thời gian từ một hình ảnh thu được bằng fls.exe tương đối đơn giản. Sử dụng lệnh sau, đầu ra từ công cụ được hiển thị trong bảng điều khiển (tức là, STDOUT) ở định dạng tệp mactime hoặc body:

```
D:\tools\tsk>fls -m C: -i raw -f ntfs -l -r d:\cases\xp\xp.001
```

Lưu ý rằng để hiển thị chỉ có các mục đã bị xóa khỏi hình ảnh thu được, hãy thêm khóa chuyển đổi. Để biết thêm chi tiết về việc sử dụng fls, hãy tham khảo trang hướng dẫn cho công cụ mà bạn có thể tìm thấy tại [www.sleuthkit.org/sleuthkit/man/fls.html](http://www.sleuthkit.org/sleuthkit/man/fls.html). Đầu ra của fls được phân tách bằng đường ống (và dễ dàng phân tích cú pháp) và có thể được chuyển hướng đến một tệp để lưu trữ và phân tích sau này. Một đoạn trích của đầu ra của fls xuất hiện như sau:

```
0/C:/Program Files/Internet Explorer/Connection Wizard/inetwiz.exe/5091-128-3/r/
rrwxrwxrwx/0/0/20480/1201700419/1057579200/1201700199/1201700199
0/C:/Program Files/Internet Explorer/Connection Wizard/isignup.exe/5092-128-3/r/
rrwxrwxrwx/0/0/16384/1201700420/1057579200/1201700199/1201700199
0/C:/Program Files/Internet Explorer/Connection Wizard/msicw.isp/5107-128-1/r/
rrwxrwxrwx/0/0/158/1201700200/1057579200/1201700200/1201700200
0/C:/Program Files/Internet Explorer/Connection Wizard/msn.isp/5108-128-1/r/
rrwxrwxrwx/0/0/197/1201700200/1057579200/1201700200/1201700200
0/C:/Program Files/Internet Explorer/Connection Wizard/phone.icw/4949-128-3/r/
rrwxrwxrwx/0/0/2921/1201700184/1057579200/1201700184/1201700184
```

Dữ liệu này xuất hiện trong phần giữa tệp và sau đó có thể được phân tích cú pháp bởi tập lệnh Peract mactime để tạo thông tin dòng thời gian. Thời gian được liên kết với tệp là 32 bit thời gian Epoch, ngay cả khi thời gian được duy trì bởi hệ thống tệp (hình ảnh là của một hệ thống sử dụng hệ thống tệp NTFS) dưới dạng đối tượng FILETIME 64 bit. Ngoài ra, bạn có thể phân tích nội dung phần giữa tệp bằng công cụ Ex-Tip của Michael Cloppert, (<http://sourceforge.net/projects/ex-tip/>) và xem đầu ra ở

một định dạng khác. Chúng tôi sẽ thảo luận về Ex-Tip với độ dài lớn hơn trong Chương 8.

## 5.5. Summary (Tóm lược)

Hầu hết chúng ta đều biết, hoặc đã nghe nói, rằng không có hai sự nghiên cứu nào giống nhau. Mỗi sự nghiên cứu mà chúng tôi thực hiện dường như khác với lần trước, giống như những “bông tuyết”. Tuy nhiên, một số khái niệm cơ bản có thể phổ biến trong các cuộc nghiên cứu, và biết nơi để tìm kiếm thông tin chứng thực có thể là một chìa khóa quan trọng. Quá thường xuyên, chúng ta có thể bị kéo mạnh hoặc bị thúc đẩy bởi các lực lượng bên ngoài và thời hạn, và biết nơi để tìm kiếm thông tin hoặc bằng chứng về hoạt động, ngoài những gì được trình bày bởi GUI phân tích điều tra số, có thể rất quan trọng. Nhiều cuộc điều tra bị giới hạn do thời gian và tài nguyên chỉ đơn thuần là tìm kiếm từ khóa hoặc các tệp cụ thể, trong khi rất nhiều thông tin có thể có sẵn nếu chúng ta biết tìm ở đâu và hỏi gì. Bên cạnh sự tồn tại của các tệp cụ thể (hình ảnh bất hợp pháp, phần mềm độc hại), chúng tôi có thể kiểm tra một số định dạng tệp không có giấy tờ (hoặc tài liệu kém) để phát triển sự hiểu biết nhiều hơn về những gì xảy ra trên hệ thống và khi nào.

Biết nơi để tìm và nơi dấu hiệu tồn tại dựa trên cách hệ thống vận hành và ứng dụng phản ứng với hành động của người dùng là hai khía cạnh rất quan trọng của phân tích điều tra số. Biết nơi các tệp nhật ký tồn tại, cũng như định dạng của chúng, có thể cung cấp manh mối có giá trị trong quá trình điều tra - có lẽ nhiều hơn nếu không có những thứ do con người tạo ra.

Việc thiếu tài liệu rõ ràng về các định dạng tệp khác nhau (cũng như sự tồn tại của một số tệp nhất định) là một thách thức đối với các cuộc điều tra điều tra số. Chìa khóa để vượt qua thử thách này là điều tra kỹ lưỡng, tài liệu của các định dạng tệp và chia sẻ thông tin này. Điều này bao gồm không chỉ các tệp và định dạng tệp từ các phiên bản của hệ điều hành Windows hiện đang được điều tra (Windows 2000, XP và 2003), mà cả các phiên bản mới hơn như Vista.

## 5.6. Solutions Fast Track (Giải pháp theo dõi nhanh)

### Log File

- Rất nhiều phân tích điều tra số máy tính truyền thống xoay quanh sự tồn tại của các tệp hoặc các đoạn tệp. Các hệ thống Windows lưu trữ một số tệp có thể được tích hợp vào chế độ xem truyền thống này để cung cấp mức độ chi tiết phân tích cao hơn.

- Nhiều tệp nhật ký được lưu trữ bởi các hệ thống Windows bao gồm các dấu thời gian có thể được tích hợp vào phân tích dòng thời gian của điều tra viên về hoạt động trên hệ thống.

## **File Metadata**

- Thuật ngữ siêu dữ liệu đề cập đến dữ liệu về dữ liệu. Tổng số dữ liệu bổ sung về một tệp tách biệt với nội dung thực tế của tệp (tức là, nơi nhiều nhà phân tích thực hiện tìm kiếm văn bản).
- Nhiều ứng dụng duy trì siêu dữ liệu về một tệp hoặc tài liệu trong chính tệp đó.

## **Alternative Methods of Analysis (Phương pháp phân tích thay thế)**

- Ngoài các phương pháp phân tích điều tra số máy tính truyền thống, các phương pháp phân tích bổ sung có sẵn cho điều tra viên.
- Việc khởi động một hình ảnh thu được vào một môi trường ảo có thể cung cấp cho điều tra viên một phương tiện hữu ích cho cả phân tích hệ thống cũng như trình bày dữ liệu thu thập được cho người khác (chẳng hạn như bồi thẩm đoàn).
- Truy cập hình ảnh dưới dạng hệ thống tệp chỉ đọc cung cấp cho điều tra viên phương tiện để quét nhanh vi-rút, Trojan và phần mềm độc hại khác.

## **5.7. Frequently Asked Questions (Các câu hỏi thường gặp)**

**Q:** Tôi đang thực hiện tìm kiếm hoạt động duyệt Internet trong một hình ảnh và tôi thấy rằng “Người dùng Mặc định” có một số lịch sử duyệt web. Điều đó có nghĩa là gì?

**A:** Mặc dù chúng tôi không thảo luận về lịch sử duyệt Internet trong chương này (chủ đề này đã được giải quyết triệt để thông qua các phương tiện khác), đây là một câu hỏi tôi đã nhận được, và trên thực tế, tôi đã tự mình nhìn thấy nó trong các cuộc nghiên cứu. Robert Hensing (một nhân viên của Microsoft) đã giải quyết vấn đề này trong blog của anh ấy ([http://blogs.technet.com/robert\\_hensing/default.aspx](http://blogs.technet.com/robert_hensing/default.aspx)). Tóm lại, Người dùng mặc định không có bất kỳ tệp Internet tạm thời hoặc lịch sử duyệt theo mặc định. Nếu lịch sử duyệt được phát hiện cho tài khoản này, nó cho biết ai đó có quyền truy cập cấp HỆ THỐNG sử dụng các hàm API WinInet. Tôi đã thấy điều này trong trường hợp kẻ tấn công có thể truy cập cấp độ HỆ THỐNG và chạy một công cụ có tên wget.exe để tải các công cụ về hệ thống bị xâm nhập. Vì tệp wget.exe sử dụng API WinInet, nên “lịch sử duyệt web” đã được hiển thị trong thư mục Tệp Internet tạm thời cho Người

dùng mặc định. Robert cung cấp một ví dụ tuyệt vời để chứng minh tình huống này bằng cách khởi chạy Internet Explorer dưới dạng Tác vụ theo lịch để khi nó chạy, nó sẽ thực hiện với thông tin HỆ THỐNG. Lịch sử duyệt web sau đó sẽ được điền cho Người dùng mặc định. Phân tích sau đó có thể được thể hiện trên tệp lịch sử duyệt / index.dat bằng Trình xem lịch sử Internet trong ProDiscover hoặc Nhà sử học web từ Mandiant.com.

Q: Tôi có hình ảnh của một ổ đĩa cứng, và thoát nhìn, dường như không có nhiều dữ liệu trên hệ thống. Theo hiểu biết của tôi là người dùng sở hữu hệ thống này đã gắn bó với tổ chức này trong vài năm và gần đây đã rời đi trong tình huống đáng ngờ. Ngày cài đặt được duy trì trong Registry là khoảng một tháng trước. Một số cách tiếp cận tôi có thể thực hiện từ góc độ phân tích là gì?

A: Câu hỏi này thường xuất hiện khi phân tích một hệ thống, điều tra viên tin rằng hệ điều hành đã được cài đặt lại ngay trước khi hình ảnh được thu nhận. Điều này có thể kết thúc, nhưng trước khi chúng ta đi tuyến đường đó, có những nơi điều tra viên có thể tìm kiếm để thu thập thêm dữ liệu về vấn đề này. Dấu ngày / giờ khi hệ thống hoạt động được ghi vào giá trị InstallDate trong khóa Sổ đăng ký khi cài đặt:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion
```

Dữ liệu được liên kết với giá trị InstallDate là DWORD biểu thị số giây kể từ 00:00:00, ngày 1 tháng 1 năm 1970. Bài viết của Cơ sở tri thức Microsoft 235162 (<http://support.microsoft.com/?id=235162>) chỉ ra rằng giá trị này có thể được ghi lại không chính xác. Các vị trí khác mà điều tra viên có thể tìm kiếm thông tin để xác nhận hoặc chứng thực giá trị này là tem ngày / giờ trên các mục trong tệp setuplog.txt, trong lần LastWrite cho các khóa Đăng ký dịch vụ, v.v. Ngoài ra, hãy nhớ kiểm tra lần LastWrite cho các khóa Sổ đăng ký tài khoản người dùng trong tệp SAM. Tham khảo Chương 4 để biết thêm thông tin về việc trích xuất thông tin từ Registry (các khóa UserAssist và tương tự). Các lĩnh vực khác mà điều tra viên nên kiểm tra bao gồm thư mục Prefetch trên các hệ thống Windows XP và thời gian MAC trên các thư mục hồ sơ người dùng.

Q: Tôi đã nghe nói về một chủ đề gọi là pháp y chống máy tính, ai đó nỗ lực sử dụng các công cụ đặc biệt để che giấu chứng cứ từ một nhà phân tích điều tra số. Tôi có thể làm gì về điều đó?

A: Các nhà phân tích và điều tra số không bao giờ nên treo một lý thuyết hoặc phát hiện của họ trên một mẫu dữ liệu. Thay vào đó, bất cứ nơi nào có thể, các phát hiện nên được chứng thực bằng những sự việc xảy ra. Trong nhiều trường hợp, các nỗ lực ẩn dữ liệu sẽ tạo ra các vật của riêng chúng; hiểu cách hệ điều hành hoạt động và hoàn

cảnh và sự kiện nào tạo ra một số vật nhất định (lưu ý rằng nếu một giá trị được thay đổi, thì vẫn còn một vật giả mạo) cho phép một nhà điều tra viên nhìn thấy các dấu hiệu hoạt động. Ngoài ra, hãy nhớ xem xét sự vắng mặt của một vật trước đó được tạo ra mà ở đó đáng lẽ ra nên phải có một vật.