SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Forensic Analysis

POSTER

You Can't Protect What You Don't Know About

digital-forensics.sans.org

$25.00
DFPS_FOR500_v4.7_1-19

Poster Created by Rob Lee with support of the SANS DFIR Faculty

翻訳:櫻井祐亮、佐藤圭太、川崎隆哉

Windows® Time Rules

$STANDARD_INFORMATION

File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion
Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
Access – Time of File Creation	Access – Time of Access (No Change only on NTFS Win7+)	Access – No Change	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Time of File Copy	Metadata – Time of Local File Move	Metadata – Inherited from Original	Metadata – Inherited from Original	Metadata – No Change
Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change

$FILENAME

File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion
Modified – Time of File Creation	Modified – No Change	Modified – No Change	Modified – No Change	Modified – Time of File Copy	Modified – No Change	Modified – Time of Move via CLI	Modified – Time of Cut/Paste	Modified – No Change
Access – Time of File Creation	Access – No Change	Access – No Change	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of Move via CLI	Access – Time of Cut/Paste	Access – No Change
Metadata – Time of File Creation	Metadata – No Change	Metadata – No Change	Metadata – No Change	Metadata – Time of File Copy	Metadata – No Change	Metadata – Time of Move via CLI	Metadata – Time of Cut/Paste	Metadata – No Change
Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of Move via CLI	Creation – Time of Cut/Paste	Creation – No Change

Windows Artifact Analysis: Evidence of...

このカテゴリはSANS Digital Forensics and Incidence Response facultyがFOR500:Windows Forensic Analysisコース用に作成したものです。分析に役立つように各アーティファクトをカテゴリごとにマッピングしています。このポスターをチートシートとして使用するとコンピュータへの侵入、知的財産の盗難、サイバー犯罪捜査などのために、Windowsの重要なアーティファクトをどこで見つけることができるか覚えておくのに役立ちます。

File Download

Open/Save MRU

説明
Windowsダイアログボックスから開かれたファイル、または保存されたファイルの一覧を参照できます。
このアーティファクトはInternet ExplorerやFirefoxなどのWebブラウザだけでなく一般的に使用されているアプリケーションの多くを内包するため、巨大なデータセットとして保存されることがあります。

場所
XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

解説
- **"*"キー –** このサブキーでは直近で保存、もしくは開かれたファイルを確認できます。
- **.??? (拡張子) –** このサブキーでは保存、もしくは開かれたファイルを拡張子ごとに確認できます。

Email Attachments

説明
電子メールの80%は添付ファイルを含むというデータがあります。しかし標準規格ではテキストの記載のみが許可されています。
そのため添付ファイルはMIME / base64フォーマットでエンコードされメールに添付されています。

場所
Outlook
XP:
%USERPROFILE%\Local Settings\ApplicationData\Microsoft\Outlook
Win7/8/10:
%USERPROFILE%\AppData\Local\Microsoft\Outlook
キャッシュされた添付ファイル
XP:
%USERPROFILE%\Local Settings\Temporary Internet Files\OLK...
Win7/8/10:
%USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook

解説
MS Outlookデータファイルには OST形式とPST形式があります。OLKフォルダ、Content. Outlookフォルダも併せて確認する必要があります。保存先フォルダは使用されているOutlookのバージョンによっては移動する可能性があります。
OLKフォルダの場所の詳細については以下のリンクを参照してください。
http://www.hancockcomputertech.com/blog/2010/01/06/find-the-microsoft-outlook-temporary-olk-folder/"

Skype History

説明
- Skypeの履歴は端末から送受信したチャットセッションをログとして保持します。
- この機能は初期設定で有効になっています。

場所
XP:
C:\Documents and Settings\<username>\Application\Skype\<skype-name>
Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Skype\<skype-name>

解説
これらのエントリにはSkypeで使用しているユーザー名が関連づけられ、実施した操作の日時が確認できます。

Browser Artifacts

説明
直接的なファイルのダウンロードだけではなく、Webサイトへのアクセス回数等ユーザーアカウントごとに詳細を記録しています。

場所
Internet Explorer
- IE8-9:
  %USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat
- IE10-11:
  %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Firefox
- v3-25:
  %USERPROFILE%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite
- v26+:
  %USERPROFILE%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\places.sqlite

Table:moz_annos

Chrome:
- Win7/8/10:
  %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

解説
Historyにはリモートサイトで開かれたファイルやローカルマシンにダウンロードされたファイルの履歴が含まれるケースが多くあります。
Historyはリンクを介したWebサイト上のファイルアクセスの記録も保持しています。

Downloads

説明
FirefoxとIEにはユーザがダウンロードしたすべてのファイルの履歴を保存するビルトインのダウンロードマネージャーがあります。
このアーティファクトはユーザーのWebアクセスおよびダウンロードしたファイルに関する情報を確認できます。

場所
Firefox:
- XP:
  %USERPROFILE%\Application Data\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite
- Win7/8/10:
  %USERPROFILE%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite

Internet Explorer:
- IE8-9:
  %USERPROFILE%\AppData\Roaming\Microsoft\Windows\ IEDownloadHistory
- IE10-11:
  %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV*.dat

解説
上記のアーティファクトから以下の情報を確認できます。
- ファイル名, サイズ, タイプ
- ダウンロード元、参照元ページ
- ファイル保存場所
- ファイルを開くために利用されたアプリケーション
- ダウンロードの開始時間と終了時間

ADS Zone.Identifer

説明
Windows XP SP2以降、Internet Zoneからブラウザを介してNTFSボリュームへファイルがダウンロードされる際、代替データストリーム(ADS)がファイルに追加されます。代替データストリームは"Zone.Identifier"と呼ばれます。

解説
ファイルダウンロード時に作成されたZone.Identifier がZoneID=3 の場合、インターネットからのダウンロードであることを示しています。
- URLZONE_TRUSTED(信頼済みサイト) ZoneID = 2
- URLZONE_INTERNET(インターネット) ZoneID = 3
- URLZONE_UNTRUSTED(制限付きサイト) ZoneID = 4

Program Execution

UserAssist

説明
Windows上で実行されたGUIプログラムの履歴はUserAssistに記録されます。

場所
NTUSER.DATハイブ:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

解説
全ての値はROT-13でエンコードされています。
- GUID for XP
  - 75048700 アクティブ・デスクトップ
- GUID for Win7/8/10
  - CEBFF5CD 実行ファイルの起動
  - F4E57C4B ショートカットファイルからの実行

Windows 10 Timeline

説明
Windows10では最近使ったアプリケーションやファイルの情報はタイムライン(Windowsキー+Tabキーで表示可能)に表示されます。この情報はSQLiteデータベースに格納されています。

場所
C:\Users\%USERPROFILE%\AppData\Local\ConnectedDevicesPlatform\L.%USERPROFILE%

解説
- 実行したアプリケーション
- アプリケーションがフォーカスされた回数

RecentApps

説明
Windows10で実行されたGUIプログラムの履歴はRecentAppsに記録されます。

場所
Win10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps

解説
各GUIDはアプリケーションと紐づいています。
AppID = アプリケーション名
LastAccessTime = 最終実行時刻(UTC)
LaunchCount = 実行回数

Shimcache

説明
- Application Compatibility Database(Shimcache)は実行ファイルやアプリケーションの互換性問題を識別するために使用されます。
- このキーからは実行ファイル名、ファイルサイズおよび最終更新日時を確認できます。Windows XPにおいてはレジストリキーの最終更新日時を確認できます。

場所
XP:
SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility
Win7/8/10:
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

解説
起動された実行ファイルはすべてこのキーに記録されます。特定のマルウェアが実行されたシステムの識別に役立つことに加え、時系列で情報を整理することで日時情報やアクティビティの特定に役立ちます。
- Windows XPには最大96エントリが含まれます。
  - ファイルの実行によりLast Update Timeが更新されます。
- Windows 7以降では最大1,024のエントリが含まれます。
  - LastUpdateTimeはWindows7以降含まれなくなりました。

Jump Lists

説明
- Windows 7タスクバー(Jump List)はユーザーが頻繁に利用する、または最近利用したアイテムへのアクセスを補助します。この機能は最近開いたメディアファイルだけでなくタスクも対象です。
- AutomaticDestinationsフォルダには各アプリケーションに紐づく一意のAppIDが先頭に付けられたファイルが格納されています。

場所
Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

解説
Jump Listでは時間情報を以下のように解釈します。
- 作成日時:対象のAppIDを持つアプリケーションを初めて実行した日時
- 最終更新日時:対象のAppIDを持つアプリケーションを最後に実行した日時
- Jump List IDのリスト:
  http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs

Amcache.hve

説明
ProgramDataUpdaterはプロセス作成時の情報をレジストリAmcache.hveに記録します。
ProgramDataUpdaterはApplication Experienceに関連付けられているタスクです。Application Experienceは起動するアプリケーションに対して互換性キャッシュ要求を処理します。

場所
Win7/8/10:
C:\Windows\AppCompat\Programs\Amcache.hve
Amcache.hve\Root\File\{Volume GUID}\#######

解説
- Volume GUID以下のサブキーから、以下の情報が確認できます。
- 全ての実行ファイルの起動履歴、フルパス情報、$StandardInfoの最終更新日時、実行ファイルが起動されたディスクボリューム
- キーの最終更新日時は初回実行日時に相当
- 実行ファイルのSHA1ハッシュ

System Resource Usage Monitor (SRUM)

説明
システムのパフォーマンスの履歴を30~60日分記録します。
アプリケーションが実行された際のユーザーアカウント、送受信したバイト数などを確認できます。
更新はシャットダウン時、もしくは1時間ごとに実行されます。

場所
SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions {d10ca2fe-6fcf4f6d-848e-b2e99266fa89} = Application Resource Usage Provider C:\Windows\System32\SRU

解説
srum_dump.exeなどのツールを使用して、レジストリキーとSRUM ESEデータベース間のデータを相互に関連付けます。

BAM/DAM

説明
Windows Background Activity Moderator (BAM)

場所
Win10:
SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

解説
システム上で起動した実行ファイルのフルパスと最終実行日時を確認できます。

Last-Visited MRU

説明
LastVisitedMRUではOpenSaveMRUキーに記録されているファイルを開く際、アプリケーションによって利用された実行ファイルと最後にアクセスされたフォルダを確認できます。

場所
XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

解説
OpenSaveMRUキーに記録されたファイルを開く際、アプリケーションが使用する実行ファイルを確認できます。
記録されている値はアプリケーションが最後にアクセスしたフォルダ情報も保持しています。
例:テキストファイルを開く際に、Notepad.exeは最後に「**C:\%USERPROFILE%\Desktop**」にアクセスした、などの情報が得られます。

Prefetch

説明
よく使用されるアプリケーションのコードページを事前に読み込むことによりシステムのパフォーマンスを向上させます。
アプリケーションがシステム上で実行されたことを確認する際に使用します。

場所
C:\Windows\Prefetch

解説
- Cache Managerは各アプリケーションまたはプロセスで参照されるすべてのファイルとディレクトリを監視し、よく使われるアプリケーションを.pfファイルに登録します。
- WindowsXP から Windows 7までは128件、Windows 8-10では1024件まで登録されます。
- Prefetchファイルは (実行ファイル名)-(hash値).pfの命名規則で作成されます。
- Prefetchファイルには前回の実行日時、実行回数が含まれます。
- 初回実行日時、最終実行日時が確認できます。
- 初回実行日時はファイル作成日時、最終実行日時はファイルの最終更新日時から、それぞれ10秒を引いた時刻です。
- Windows8から10では過去8回の実行履歴を確認できます。

Deleted File or File Knowledge

XP Search – ACMRU

説明
Windows XPマシンではサーチアシスタントによって幅広い情報を検索できます。サーチアシスタントでは検索に利用されたファイル名、コンピュータ名およびファイルに含まれる単語などを記録しています。

場所
NTUSER.DAT\Software\Microsoft\Search Assistant\ACMru\####

解説
ACMruキーのサブキー名(####に相当)の一例です。
- インターネット検索 – ####=5001
- ファイル名の一部もしくは全て – ####=5603
- ファイルに含まれる単語 – ####=5604
- プリンタ、コンピュータ、もしくはユーザー – ####=5647

Thumbcache

説明
写真、Office文書およびフォルダのサムネイルはthumbcacheと呼ばれるデータベースに存在します。ユーザーが選択しているサムネイルの表示サイズに基づいてユーザー単位で独自のデータベースを持ちます。(小、中、大、特大)

場所
C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer

解説
- ユーザーがフォルダをサムネイルモードに切り替えたとき、またはスライドショーで写真を表示したときに作成されます。
- Windows7以降、4つのサイズがあり、それぞれ異なるデータベースに格納されています。キャッシュフォルダ内のファイルは、サムネイルのサイズに準じます。
  - 32 -> 小 -96 -> 中
  256 -> 大 -1024 -> 特大
- サムネイルのサイズに基づき、対応する画像のサムネイルコピーがそれぞれのデータベースに保存されます。

Thumbs.db

説明
画像ファイルに関連する隠しファイルで、フォルダごとに作成されます。
thumbs.dbはフォルダ内の画像ファイルをカタログ化し、オリジナルの画像が削除された場合でもサムネイルのコピーを保持しています。

場所
WinXP/Win8|8.1:
ホームグループが有効の場合、各フォルダに自動作成される
Win7/8/10:
UNCパスでアクセスされた場合、自動作成される(ローカル、リモートいずれも)

解説
以下の情報が含まれます。
- オリジナルの画像の縮小表示
- ドキュメントのサムネイル(削除されたファイルを含む)
- 最終更新日時(XPのみ)
- オリジナルのファイル名(XPのみ)

IE|Edge file://

説明
IE HistoryはWeb閲覧履歴に加えて、ローカル及びリモート(ネットワーク共有)によるファイルアクセスも記録しています。
ローカルおよびリモートのファイルアクセスも記録されるため、システム上のファイルおよびアプリケーションにアクセスしたかを判断するための手段となります。

場所
Internet Explorer:
IE6-7
%USERPROFILE%\LocalSettings\History\History.IE5
IE8-9
%USERPROFILE%\AppData\Local\Microsoft\WindowsHistory\History.IE5
IE10-11
%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

解説
- index.dat内に**"file:///C:/directory/filename.ext"**のような形で記録されています。
- ブラウザによってファイルが開かれたことを示しているわけではありません。

Search – WordWheelQuery

説明
WordWheelQueryはスタートメニューバーから検索したキーワードの情報を記録します。

場所
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

解説
キーワードはUnicodeで追加されMRUlistに時系列でリストされます。

Win7/8/10 Recycle Bin

説明
recycle binはWindowsのファイルシステムを理解する上で非常に重要なアーティファクトです。
削除したファイルをシステムが自動で配置するフォルダのため非常に有用な情報が得られます。

場所
Win7/8/10:
C:\$Recycle.bin

解説
- SIDごとにサブフォルダが作成されるため、レジストリの解析を行うことでどのユーザーの削除ファイルであるかの特定に役立ちます。
- Windows7以降では$I######ファイル、$R######ファイルが作成され、以下の情報を確認できるようになりました。
  - $I#######ファイル:オリジナルのPath情報、削除された日時情報
  - $R#######ファイル:オリジナルのファイル内容

Last-Visited MRU

説明
LastVisitedMRUではOpenSaveMRUキーに記録されているファイルを開く際、アプリケーションによって利用された実行ファイルと、最後にアクセスされたフォルダを確認できます。

場所
XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

解説
OpenSaveMRUキーに記録されたファイルを開く際、アプリケーションが使用する実行ファイルを確認できます。
記録されている値はアプリケーションが最後にアクセスしたフォルダ情報も保持しています。

XP Recycle Bin

説明
XP recycle binはWindowsのファイルシステムを理解する上で非常に重要なアーティファクトです。
削除したファイルをシステムが自動で配置するフォルダのため非常に有用な情報が得られます。

場所
Win2000/NT/XP/2003:
C:\RECYCLER

解説
- SIDごとにサブフォルダが作成されるため、レジストリの解析を行うことでどのユーザーの削除ファイルであるかの特定に役立ちます。
- ゴミ箱内のファイルが、以前はどのフォルダに保存されていたかをマッピングできます。
- サブフォルダ内の隠しファイルINFO2ファイルには削除日時、オリジナルファイル名が含まれます。(ASCII/UNICODE両方のファイル名)

Network Activity/Physical Location

Timezone

説明
システムに設定されている現在のタイムゾーンを確認できます。

場所
SYSTEM ハイブ:
SYSTEM\CurrentControlSet\Control\TimeZoneInformation

解説
- 内部のログ、タイムスタンプ情報はシステムのタイムゾーン情報に基づいています。
- 異なるネットワークに属する機器を併せて調査する場合はタイムゾーン情報を加味する必要があります。

Cookies

説明
CookieはアクセスしたWebサイト上でどのようなアクティビティが行われたかを確認する際に役立ちます。

場所
Internet Explorer
- **IE8-9:**
  %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- **IE10:**
  %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- **IE11:**
  %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies
- **Edge:**
  %USERPROFILE%\AppData\Local\Packages\microsoft.
- **microsoftedge_<APPID>\AC\MicrosoftEdge\Cookies**

Firefox
- **XP:**
  %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite
- **Win7/8/10:**
  %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite

Chrome
- **XP:**
  %USERPROFILE%\Local Settings\Application Data\Google\Chrome\UserData\Default\Local Storage
- **Win7/8/10:**
  %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Local Storage

Network History

説明
コンピュータが接続されていたネットワーク関連の情報はレジストリSoftwareから確認することができます。

場所
Win7/8/10 SOFTWAREハイブ:
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache**

解説
- コンピュータが接続していたイントラネットやネットワークを特定することができます。
- キーの最終更新日時は、ネットワークに最後に接続した日時を示します。
- VPN経由で接続されているネットワークも一覧表示されます。
- ゲートウェイのMACアドレスにより物理的な位置特定が可能になる場合があります。
- SSIDの識別が可能です。
- 接続方式（有線・無線）を判別できます。

WLAN Event Log

説明
システムに関連付けされたワイヤレスネットワークおよび認証された場所を確認できます。

場所
%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-WLAN-AutoConfig Operational.evtx

解説
- 以下のIDを参照します。
  －11000：無線ネットワークの関連付けが開始
  －8001：ワイヤレスネットワークへの接続に成功
  －8002：ワイヤレスネットワークへの接続に失敗
  －8003：ワイヤレスネットワークからの切断
  －6100：ネットワーク診断（システムログ）
- ワイヤレスネットワークの接続履歴を参照できます。
- SSIDとBSSID（MACアドレス）を含むため、アクセスポイントの地理情報が識別できます。（BSSIDはWindows8以降記録されていません）

Browser Search Terms

説明
アクセスしたWebサイトやアクセス回数、アクセス日時がユーザーごとに記録されています。
ローカルシステム上のファイルアクセスやブラウザ上で検索した検索ワードも残されています。

場所
Internet Explorer
- **IE6-7:**
  %USERPROFILE%\Local Settings\History\History.IE5
- **IE8-9:**
  %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5
- **IE10-11:**
  %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Firefox
- **XP:**
  %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite
- **Win7/8/10:**
  %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite

System Resource Usage Monitor (SRUM)

説明
システムのパフォーマンスの履歴を30~60日分記録します。
アプリケーションが実行された際のユーザーアカウント、送受信したバイト数などを確認できます。更新はシャットダウン時、もしくは1時間ごとに実行されます。

場所
SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions
{973F5D5C-1D90-4944-BE8E-24B94231A174} = ネットワークのデータ使用量・方法
{DD6636C4-8929-4683-974E-22C046A43763} = ネットワークの接続方法
SOFTWARE\Microsoft\WlanSvc\Interfaces
C:\Windows\System32\SRU

解説
srum_dump.exeなどのツールを使用して、レジストリキーとSRUM ESEデータベースの間のデータを相互に関連付けます。

File/Folder Opening

Open/Save MRU

説明
Windowsダイアログボックスから開かれたファイル、または保存されたファイルの一覧を参照できます。
このアーティファクトはInternet ExplorerやFirefoxなどのWebブラウザだけでなく、一般的に使用されているアプリケーションの多くを内包するため、巨大なデータセットとして保存されていることがあります。

場所
XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

解説
- **“ *”キー** – このサブキーは直近で保存された、もしくは開かれたファイルを確認できます。
- **.??? （拡張子）** – このサブキーでは保存、もしくは開かれたファイルを拡張子ごとに確認できます。

Recent Files

説明
“Recent（最近使用したファイル）”として知られる、直近で開かれたファイルやフォルダの情報を記録しています。

場所
NTUSER.DAT:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

解説
- **RecentDocs –** RecentDocsキーには直近150のファイル・フォルダオープンの履歴が記録されています。MRU listには各ファイルやフォルダが開かれた順序が記録され、最も直近のエントリとキーの最終更新日時から、最後に開かれたファイル名と時間を知ることができます。
- **.??? –** 拡張子ごとにサブキーが作成され、拡張子毎に開かれたファイルが記録されています。MRU listには各ファイルが開かれた順序が記録されています。最も直近のエントリとキーの最終更新日時から、最後に開かれたファイル名と時間を知ることができます。
- **Folder –** このサブキーは、最後に開かれたフォルダが記録されています。MRU listには各フォルダが開かれた順序が記録されています。最も直近のエントリとキーの最終更新日時から、最後に開かれたフォルダ名と時間を知ることができます。

Jump Lists

説明
- Windows 7タスクバー（Jump List）はユーザーが頻繁に利用する、または最近利用したアイテムへのアクセスを補助します。この機能は最近開いたメディアファイルだけでなくタスクも対象です。
- AutomaticDestinationsフォルダには各アプリケーションに紐づく一意のAppIDが先頭に付けられたファイルが格納されています。

場所
Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

解説
- Structured Storage ViewerなどのツールはJump Listを解析する際に役立ちます。
- Jumplistには各ストリームにLNKファイルが埋め込まれます。最も古い履歴（通常は1）から直近の履歴（最大の整数値）まで順番に数値で格納されます。

Shell Bags

説明
ローカル、もしくはネットワーク上でアクセスされたフォルダ、デバイスを参照できます。 以前存在しすでに削除されたり上書きされたフォルダの痕跡を確認できる場合があります。

場所
Explorer Access:
- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags**
- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU**

Desktop Access:
- **NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU**
- **NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags**

解説
ユーザが最近閲覧したフォルダの情報を格納しています。

Shortcut (LNK) Files

説明
ローカル、もしくはリモートのファイルを開くことで、ショートカット（LNK）ファイルが自動生成される場合があります。

場所
XP:
- **%USERPROFILE%\Recent**

Win7/8/10:
- **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent**
- **%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent**

Note:主な場所は上記の通りですが他の場所に存在することもあります。

解説
ショートカット（LNK）ファイルを解析すると以下の情報を確認できます。
- ファイルを最初に開いた時間：ショートカット（LNK）ファイルの作成日時
- ファイルを最後に開いた時間：ショートカット（LNK）ファイルの最終更新日時
- 開かれたファイル自身の更新,アクセス,作成日時
- 開かれたファイル自身の保存先
- ボリューム情報（名前,タイプ,シリアル番号）
- ネットワーク共有情報
- システム名

Prefetch

説明
よく使用されるアプリケーションのコードページを事前に読み込むことにより、システムのパフォーマンスを向上させます。
アプリケーションがシステム上で実行されたことを確認する際に使用します。Prefetchファイルを調べることで最近使用されたファイル、デバイスを確認できます。

場所
WinXP/7/8/10:
C:\Windows\Prefetch

解説
- Cache Managerは各アプリケーションまたはプロセスで参照されるすべてのファイルとディレクトリを監視し、よく使われるアプリケーションは.pfファイルに登録します。
- WindowsXP から Windows 7までは128件、Windows 8-10では1024件まで登録されます。
- Prefetchファイルは（実行ファイル名）-（hash値）.pfの命名規則で作成されます。

Last-Visited MRU

説明
LastVisitedMRUでは、OpenSaveMRUキーに記録されているファイルを開く際、アプリケーションによって利用された実行ファイルと、最後にアクセスされたフォルダを確認できます。

場所
XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

解説
OpenSaveMRUキーに記録されたファイルを開く際、アプリケーションが使用する実行ファイルを確認できます。
記録されている値はアプリケーションが最後にアクセスしたフォルダ情報も保持しています。
例：テキストファイルを開く際に、Notepad.exeは最後に「**C:\Users\Rob\Desktop**」にアクセスした、などの情報が得られます。

IE|Edge file://

説明
IE HistoryはWeb閲覧履歴に加えて、ローカル及びリモート（ネットワーク共有）によるファイルアクセスも記録しています。
どのようなファイルやアプリケーションがアクセスされたかを知ることができます。

場所
Internet Explorer:
- **IE6-7:**
  %USERPROFILE%\LocalSettings\History\History.IE5
- **IE8-9:**
  %USERPROFILE%\AppData\Local\Microsoft\WindowsHistory\History.IE5
- **IE10-11:**
  %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

解説
- index.dat内に**“file:///C:/directory/filename.ext”**のような形で記録されています。
- ファイルがブラウザによって開かれたことを示しているわけではありません。

Office Recent Files

説明
MS Officeのアプリケーションはユーザーが参照、編集していたファイルを管理しています。

場所
NTUSER.DAT\Software\Microsoft\Office\VERSION
- 14.0 = Office 2010
- 12.0 = Office 2007
- 11.0 = Office 2003
- 10.0 = Office XP

NTUSER.DAT\Software\Microsoft\O˜ce\VERSION\UserMRU\LiveID_####\FileMRU
- 15.0 = Office 365

解説
Recentファイルと同様に各MS Officeアプリケーションによって最近開かれたファイルを記録します。 MRUに追加された最後のエントリは各MS Officeアプリケーションによって最後にファイルが開かれた日時を示します。

Account Usage

Last Login

説明
SAMのサブキーからユーザーアカウントの最終ログイン日時を確認できます。

場所
- **C:\windows\system32\config\SAM**
- **SAM\Domains\Account\Users**

解説
システムローカルアカウントのSIDを一覧で表示します。
サブキーには最終ログイン日時が記録されます。

Last Password Change

説明
特定のローカルユーザーによる最終パスワード変更日時が記録されています。

場所
- **C:\windows\system32\config\SAM**
- **SAM\Domains\Account\Users**

解説
- レジストリキーには最終パスワード変更日時のみを保持します。

RDP Usage

説明
リモートデスクトッププロトコル（RDP）によるログオンを追跡します。

場所
Win7/8/10:
%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

解説
- SECURITYイベントログの以下のIDを参照します。
  -4778-セッション接続/再接続
  -4779-セッション切断
- SECURITYイベントログはホスト名と接続しているリモートマシンのIPアドレスを提供します。
- ワークステーション上では現在のコンソールセッションが切断され（4779）、続いてRDP接続（4778）になることがよくあります。

Services Events

説明
- OS起動時に実行されている疑わしいサービスのログを確認する際に使用します。
- 侵害された可能性のある時間帯に開始、または停止したサービスのログを確認する際に使用します。

場所
Win7/8/10:
%system root%\System32\winevt\logs\System.evtx
%system root%\System32\winevt\logs\Security.evtx

解説
- SYSTEMイベントログの以下のIDを参照します。
  7034 – サービスが突然クラッシュしました
  7035 – サービスが開始/停止コントロールを送信しました
  7036 – サービスが開始または停止しました
  7040 – 起動タイプが変更されました
  （Boot | On Request | Disabled）
  7045 – システムにサービスがインストールされました
  （Win2008R2+）
- SECURITYイベントログの以下のIDを参照します。
  4697 - サービスがシステムにインストールされました
- 多くのマルウェアやワームが実際に利用するサービス内容です
- OS起動時に開始されたサービスは永続性を示します（マルウェア）
- プロセスインジェクションなどの攻撃によりサービスがクラッシュする可能性があります。

Logon Types

説明
ログオンイベントはアカウントのログオン認証の確認に役立ちます。試行時間、ユーザ名、ホスト名、ログオンの成功/失敗などの情報を得ることができ、どのようなログオンが試行されたのか判断することができます。

場所
Win7/8/10:
%system root%\System32\winevt\logs\security.evtx

解説
ID4624のイベントでは、ログオンタイプが識別できます。
2 – 対話型ログオン（キーボード等を用いた対話型ログオン）
3 – ネットワークログオン（ユーザーまたはコンピュータによるネットワーク上のコンピュータへのログオン）
4 – バッチログオン（サーバプロセスによる自動ログオン）
5 – サービスログオン
7 – ロック解除（スクリーン）
8 – ネットワークログオン（プレーンテキスト送信）
9 – 新しい資格情報を用いたログオン
10 – リモート対話型ログオン
（RDP、もしくはターミナルによるログオン）
11 – キャッシュされたクレデンシャルによる対話型ログオン
（ローカルに保存された資格情報を用いたログオン）
12 – キャッシュされたリモートによるログオン
13 – キャッシュされたロック解除

Authentication Events

説明
認証イベントのログを確認する際に使用します。

場所
認証イベントは次の場所に記録されます。
ローカルアカウント/Workgroup = ワークステーション上
ドメインアカウント/Active Directory = ドメインコントローラー上
Win7/8/10:
%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

解説
イベントID（NTLMプロトコル）
- 4776 – アカウント認証の成功/失敗

イベントID（Kerberosプロトコル）
- 4768 – Kerberos認証チケット（TGT）が要求されました
- 4769 – Kerberos サービス チケットが要求されました
- 4771 – Kerberos 事前認証に失敗しました

Success/Fail Logons

説明
ログオン試行時に使用されたアカウント、もしくは既知の侵害されたアカウントの使用状況を確認する際に使用します。

場所
Win7/8/10:
%system root%\System32\winevt\logs\Security.evtx

解説
以下のIDを参照します。
- 4624 – ログオン成功
- 4625 – ログオン失敗
- 4634 | 4647 – ログオフ成功
- 4648 – 明示的な認証情報を使用してログオン（Runas）
- 4672 – 管理者権限を持つアカウントのログオン
- 4720 – アカウントが作成されました

External Device/USB Usage

Key Identification

説明
接続したUSBデバイスが記録されます。

場所
SYSTEM\CurrentControlSet\Enum\USBSTOR
SYSTEM\CurrentControlSet\Enum\USB

解説
- 接続されたUSBのベンダー、プロダクト及びバージョンなどを記録しています。
- 接続された一意のUSBデバイスを識別します。
- 接続されたUSBの最終接続日時を確認できる場合があります。
- デバイス固有のシリアルナンバーを持たない接続機器は値の前から2文字目に"&"が入ります。

First/Last Times

説明
USBデバイスが接続・切断された時間情報を確認する際に使用します。

初回接続日時（デバイスドライバインストールログ）
XP:
C:\Windows\setupapi.log
Win7/8/10:
C:\Windows\inf\setupapi.dev.log

解説
- 上記のログはUSBデバイスのシリアル番号で検索を行うと時間情報が確認できます。
- ログファイルの日時は設定されているタイムゾーンで記録されます。
- Windows7以降では上記のログファイルの他にレジストリからもデバイスの使用状況を確認できます。

SYSTEMハイブ：
SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####
0064：初回接続（Win7-10）
0066：最終接続（Win8-10）
0067：最終切断（Win8-10）

User

説明
ユーザーが使用したUSBデバイスを確認する際に使用します。

場所
- **SYSTEM\MountedDevices**
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**

解説
MountedDevicesからGUIDを確認することでUSBデバイスを接続したユーザーを識別することができます。
このキーの最終更新日時はデバイスの最終接続日時に相当します。
GUIDはNTUSER.DATのMount Points2キーと紐づけて参照することができます。

PnP Events

説明
Plug and Play driverのインストール試行時にイベントログに記録が残ります。このイベントはUSBだけでなくFirewireやPCMCIAデバイス等のPlug and Play可能なあらゆるデバイスにより記録されます。

場所
Win7/8/10:
%system root%\System32\winevt\logs\System.evtx

解説
- イベントID：20001「プラグアンドプレイドライバのインストールが試行されました」として記録が残ります。
- 日時情報
- デバイスの概要
- シリアル番号
- ステータス（正常に完了した場合は「0 = エラーなし」）

Volume Serial Number

説明
USBのファイルシステムパーティションにあるボリュームシリアル番号（VSN）を調べることができます。
（注記: これはデバイスファームウェアにハードコードされた、USBのユニークなシリアル番号ではありません。）

場所
- **SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt**
- ボリューム名とUSB固有のシリアル番号を使用して、次の操作を行います。
  - 行の最後の整数を検索
  - 10進数シリアル番号を16進数シリアル番号に変換

解説
- VSNとボリューム名を用いて、SHORTCUTファイル（LNK）分析とRECENTDOCキーの間でデータを相互に関連付けることができます。
- ショートカットファイル（LNK）には、ボリュームシリアル番号と名前が含まれています。
- RecentDocsレジストリキーは、多くの場合エクスプローラでUSBデバイスを開いた際のボリューム名を含みます。

Drive Letter and Volume Name

説明
USBデバイスを接続した際に割り振られたドライブレター情報を参照します。

場所
XP:
SYSTEM\CurrentControlSet\Enum\USBSTOR
- デバイスの固有識別子を確認します。

SYSTEM\MountedDevices
- デバイスの固有識別子を元にドライブレターを確認できます。

Win7/8/10:
SOFTWARE\Microsoft\Windows Portable Devices\Devices
- デバイスの固有識別子を確認します。

SYSTEM\MountedDevices
- デバイスの固有識別子を元にドライブレターを確認できます。

解説
ドライブレターに最後に割り当てられたUSBデバイスを識別します。 最後に割り当てられたドライブに対してのみ機能し、全てのドライブレターの履歴記録は含まれていません。

Shortcut (LNK) Files

説明
ローカル、もしくはリモートのファイルを開くことで、ショートカット（LNK）ファイルが自動生成される場合があります。

場所
XP:
- **%USERPROFILE%\Recent**

Win7/8/10:
- **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent**
- **%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent**

Note:主な場所は上記の通りですが他の場所に存在することもあります。

解説
ショートカット（LNK）ファイルを解析すると、以下の情報を確認できます。
- ファイルを最初に開いた時間
  - ショートカット（LNK）ファイルの作成日時
- ファイルを最後に開いた時間
  - ショートカット（LNK）ファイルの更新日時
- LNKターゲットファイルの情報（LNKファイルに含まれる情報）
  - 開かれたファイル自身の更新, アクセス, 作成日時
  - 開かれたファイル自身の保存先
  - ボリューム情報（名前, タイプ, シリアル番号）
  - ネットワーク共有情報
  - システム名

Browser Usage

History

説明
Webサイトへのアクセス履歴、ブラウザを使用したローカルのファイルアクセスを記録しています。
ユーザープロファイルごとに作成され、アクセス先、日時情報及びアクセス回数が確認できます。

場所
Internet Explorer
- **IE6-7: %USERPROFILE%\Local Settings\History\History.IE5**
- **IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5**
- **IE10, 11, Edge: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat**

Firefox
- **XP: %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite**
- **Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite**

Chrome
- **XP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\UserData\Default\History**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History**

Cookies

説明
CookieはアクセスしたWebサイトでどのようなアクティビティがあったかを確認する際に役立ちます。

場所
Internet Explorer
- **IE8-9: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- **IE10: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- **IE11: %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies**
- **Edge: %USERPROFILE%\AppData\Local\Packages\microsoft.**
- **microsoftedge_<APPID>\AC\MicrosoftEdge\Cookies**

Firefox
- **WinXP: %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite**
- **Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite**

Chrome
- **winXP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\UserData\Default\Local Storage**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Local Storage**

Cache

説明
- キャッシュはWebページコンポーネントをローカルに保存することでその後のアクセスを高速化するものです。
- ユーザーがオンラインで閲覧していた内容を調査者に「スナップショット」として提供します。
  - アクセスしたWebサイトを識別します。
  - 指定された場所でユーザーが表示した実際のファイルを提供します。
  - キャッシュされたファイルは特定のローカルユーザーアカウントに関連づけられます。
  - タイムスタンプにはサイトへの初回訪問日時、最終訪問日時が記録されます。

場所
Internet Explorer
- **IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5**
- **IE10: %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5**
- **IE11: %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\IE**
- **Edge: %USERPROFILE%\AppData\Local\Packages\microsoft.microsoftedge_<APPID>\AC\MicrosoftEdge\Cache**

Firefox
- **XP: %USERPROFILE%\Local Settings\ApplicationData\Mozilla\Firefox\Profiles\<randomtext>.default\Cache**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\<randomtext>.default\Cache**

Chrome
- **XP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache - data_# and f_######**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Cache\ - data_# and f_######**

Flash & Super Cookies

説明
インターネットを介したFlashアプリケーションが浸透し、Local Stored Objects（LSOs）とFlash Cookieは多くのシステムに普及しました。ブラウザから消去されないために長期間保存されている傾向があります。多くのサイトがLSOsを追跡メカニズムとして使用する背景には従来のCookieのようにクリアされる頻度が少ないことがあげられます。

場所
Win7/8/10:
%APPDATA%\Roaming\Macromedia\FlashPlayer\#SharedObjects\<randomprofileid>

解説
- アクセスしたWebサイトを特定できます。
- LSOsとFlash Cookieはユーザアカウントと紐づけられています。
- LSOsとFlash Cookieの時間情報は作成日時が初回アクセス日時を、最終更新日時が最終アクセス日時を表します。

Session Restore

説明
ブラウザが予期せず終了した際の再構築に使用されます。

場所
Internet Explorer
%USERPROFILE%/AppData/Local/Microsoft/Internet Explorer/Recovery(Win7/8/10)
Firefox
%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\sessionstore.js(Win7/8/10)
Chrome
%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\(Win7/8/10)
Files = Current Session, Current Tabs, Last Session, Last Tabs

解説
- 各タブに表示されているWebサイトの履歴
- Webサイトの参照先
- 終了したセッション
- LastActiveフォルダ内の.datファイルの時刻の修正
- 各タブが開いた時間（クラッシュが発生したときのみ）
- Activeフォルダ内の.datファイルの作成時間

Google Analytics Cookies

説明
Google Analytics（GA）はWebサイトアクセス時のユーザアクティビティやアクセスに至る経路（サイトにアクセスするために用いたキーワード等）の情報を収集するための方法となるべく開発されました。
GAは基本的には無料なのでシェアの80%を占め全サイトの過半数が使用していると言われています。

解説
_utma – Unique visitors
主にアクセスしたユーザーの特定に用いられ、以下の情報を確認できます。
-ドメインHash
-Visitor ID
-Cookie作成日時
-前々回のアクセス日時
-前回のアクセス日時
-アクセス回数
_utmb – Session tracking
セッションを管理するCookieの一つで、セッション全体を管理する際に用いられます。以下の情報を確認できます。
-ドメインハッシュ
-現在のセッションで閲覧しているページ
-外部リンクへのクリック
-現在のセッションが開始された時間
_utmz – Traffic sources
参照元（リファラ）の計測に用いられ、以下の情報を確認できます。
-ドメインハッシュ
-最終アップデート日時
-アクセス回数
-タイプによるアクセス回数の統計
-よくアクセスされるリファラ情報
-Google Adwords campaign名
-アクセス方法（organic, referral, cpc, email, direct）
-サイトにアクセスするために用いたキーワード（non-SSL only）