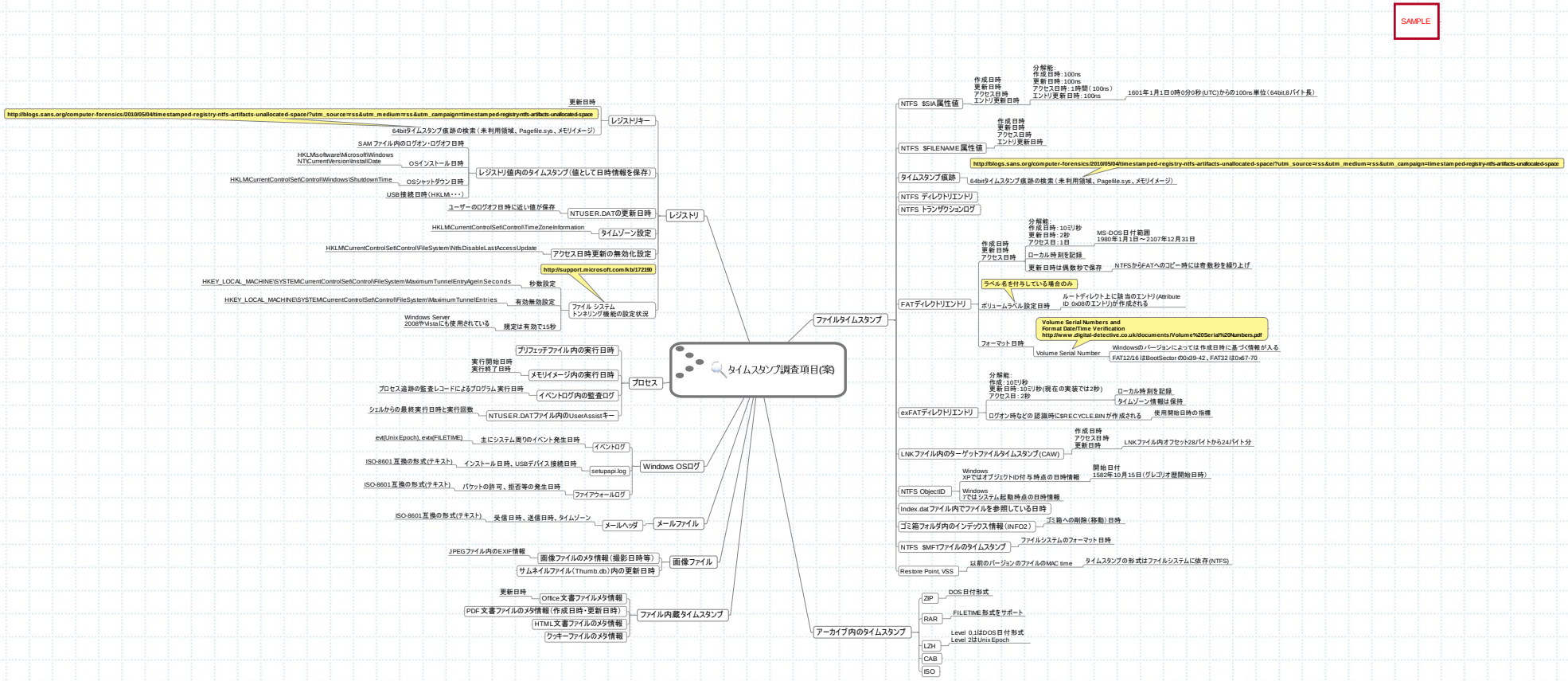
タイムスタンプ調査項目(案)
SAMPLE
レジストリ
レジストリキー
更新日時
http://blogs.sans.org/computer-forensics/2010/05/04/timestamped-registry-ntfs-artifacts-unallocated-space/?utm_source=rss&utm_medium=rss&utm_campaign=timestamped-registry-ntfs-artifacts-unallocated-space
64bitタイムスタンプ痕跡の検索（未利用領域、Pagefile.sys、メモリイメージ）
レジストリ値内のタイムスタンプ（値として日時情報を保存）
SAM ファイル内のログオン・ログオフ日時
HKLM\software\Microsoft\Windows NT\CurrentVersion\InstallDate
OSインストール日時
HKLM\CurrentControlSet\Control\Windows\ShutdownTime
OSシャットダウン日時
USB接続日時（HKLM・・・）
NTUSER.DATの更新日時
ユーザーのログオフ日時に近い値が保存
タイムゾーン設定
HKLM\CurrentControlSet\Control\TimeZoneInformation
アクセス日時更新の無効化設定
HKLM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate
ファイル システム トンネリング機能の設定状況
http://support.microsoft.com/kb/172190
秒数設定
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\MaximumTunnelEntryAgeInSeconds
有効無効設定
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\MaximumTunnelEntries
規定は有効で15秒
Windows Server 2008やVistaにも使用されている
プロセス
プリフェッチファイル内の実行日時
メモリイメージ内の実行日時
実行開始日時
実行終了日時
イベントログ内の監査ログ
プロセス追跡の監査レコードによるプログラム実行日時
NTUSER.DATファイル内のUserAssistキー
シェルからの最終実行日時と実行回数
Windows OSログ
イベントログ
ext(Unix Epoch), etx(FILETIME)
主にシステム周りのイベント発生日時
setupapi.log
インストール日時、USBデバイス接続日時
ISO-8601互換の形式(テキスト)
ファイアウォールログ
パケットの許可、拒否等の発生日時
ISO-8601互換の形式(テキスト)
メールファイル
メールヘッダ
受信日時、送信日時、タイムゾーン
ISO-8601互換の形式(テキスト)
画像ファイル
画像ファイルのメタ情報（撮影日時等）
JPEGファイル内のEXIF情報
サムネイルファイル（Thumb.db）内の更新日時
ファイル内蔵タイムスタンプ
Office文書ファイルメタ情報
更新日時
PDF文書ファイルのメタ情報（作成日時・更新日時）
HTML文書ファイルのメタ情報
クッキーファイルのメタ情報
ファイルタイムスタンプ
NTFS $SIA属性値
作成日時
更新日時
アクセス日時
エントリ更新日時
分解能:
作成日時：100ns
更新日時：100ns
アクセス日時：1時間（100ns）
エントリ更新日時：100ns
1601年1月1日0時0分0秒(UTC)からの100ns単位（64bit,8バイト長）
NTFS $FILENAME属性値
作成日時
更新日時
アクセス日時
エントリ更新日時
タイムスタンプ痕跡
http://blogs.sans.org/computer-forensics/2010/05/04/timestamped-registry-ntfs-artifacts-unallocated-space/?utm_source=rss&utm_medium=rss&utm_campaign=timestamped-registry-ntfs-artifacts-unallocated-space
64bitタイムスタンプ痕跡の検索（未利用領域、Pagefile.sys、メモリイメージ）
NTFS ディレクトリエントリ
NTFS トランザクションログ
FATディレクトリエントリ
作成日時
更新日時
アクセス日時
分解能:
作成日時：10ミリ秒
更新日時：2秒
アクセス日：1日
MS-DOS日付範囲
1980年1月1日～2107年12月31日
ローカル時刻を記録
更新日時は偶数秒で保存
NTFSからFATへのコピー時には奇数秒を繰り上げ
ボリュームラベル設定日時
ラベル名を付与している場合のみ
ルートディレクト上に該当のエントリ(Attribute ID 0x08のエントリ)が作成される
フォーマット日時
Volume Serial Number
Volume Serial Numbers and Format Date/Time Verification
http://www.digital-detective.co.uk/documents/Volume%20Serial%20Numbers.pdf
Windowsのバージョンによっては 作成日時に基づく情報が入る
FAT12/16 はBootSector の0x39-42、FAT32 は0x67-70
exFATディレクトリエントリ
分解能:
作成：10ミリ秒
更新日時：10ミリ秒(現在の実装では2秒)
アクセス日：2秒
ローカル時刻を記録
タイムゾーン情報は保持
ログオン時などの認識時にSRECYCLE.BINが作成される
使用開始日時の指標
LNKファイル内のターゲットファイルタイムスタンプ(CAW)
作成日時
アクセス日時
更新日時
LNKファイル内オフセット28バイトから24バイト分
NTFS ObjectID
Windows XPではオブジェクトID付与時点の日時情報
Windows 7では システム起動時点の日時情報
開始日付
1582年10月15日（グレゴリオ歴開始日時）
Index.datファイル内でファイルを参照している日時
ゴミ箱フォルダ内のインデックス情報（INFO2）
ゴミ箱への削除（移動）日時
NTFS $MFTファイルのタイムスタンプ
ファイルシステムのフォーマット日時
Restore Point, VSS
以前のバージョンのファイルのMAC time
タイムスタンプの形式はファイルシステムに依存(NTFS)
アーカイブ内のタイムスタンプ
ZIP
DOS日付形式
RAR
FILETIME形式をサポート
LZH
Level 0,1はDOS日付形式
Level 2はUnix Epoch
CAB
ISO