oscheckerの流れ

Windows
レジストリハイヴ
ファイルの抽出

The Sleuth Kitでファイル抽出
1. ディスクイメージ展開のために必要な値を取得
2. ディスクイメージを展開して、目的ファイル*1の
   inode番号を捜索
3. 目的ファイルを抽出

*1 above window XP7s PATH(case-sensitive)
%SystemRoot%¥System32¥config¥SOFTWARE
windows98 , Me , 2000 ‘s PATH
%SystemRoot%¥SYSTEM.DAT

抽出したファイルから
レジストリの値を
読み込む

hivexでレジストリから値を読み取る
・抽出したレジストリハイヴの目的パス*2の**key**を
  読み取る

*2 above window XP7s PATH(case-sensitive)
HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion
windows98 , Me , 2000 ‘s PATH
HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion

Determine Windows Version!

The Sleuth Kitでファイル抽出

1. **ディスクイメージ展開のために必要な値を取得**

→読み込むイメージのファイル形式、ファイルシステム、パーティション情報を取得

2. **ディスクイメージを展開して、目的ファイルのinode番号*3を捜索**

→ 目的ファイルを目指して、上位フォルダのinode番号から順に捜索していく

3. **目的ファイルを抽出**

*3 inodeとは、ファイル、ディレクトリのアクセス権限、サイズ、更新時刻などを管理するデータ

　inode番号はinode領域の中でのアドレスの役割をしており、ファイルシステムはinode番号を基に対象inodeの検索を行う

oscheckerの流れ

Windows
レジストリハイヴ
ファイルの抽出

The Sleuth Kitでファイル抽出
1. ディスクイメージ展開のために必要な値を取得
2. ディスクイメージを展開して、目的ファイル*1の
   inode番号を捜索
3. 目的ファイルを抽出

*1 above window XP7s PATH(case-sensitive except for config)
%SystemRoot%¥System32¥config¥SOFTWARE
windows98 , Me , 2000 ‘s PATH
%SystemRoot%¥SYSTEM.DAT

抽出したファイルから
レジストリの値を
読み込む

hivexでレジストリから値を読み取る
・抽出したレジストリハイヴの目的パス*2のkeyを
  読み取る

*2 above window XP7s PATH(case-sensitive)
HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion
windows98 , Me , 2000 ‘s PATH
HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion

Determine Windows Version!

hivexで
レジストリから値を読み取る

- **抽出したレジストリハイヴの目的パスのkeyを読み取る**。

→windowsのレジストリのとある場所に目的の値がある。レジストリの実態はレジストリハイヴであるが、レジストリハイヴは階層的構造になっておりそのままでは値が読めない。

そこで、hivexの機能を使って値を読み取る。

oscheckerの流れ

Windows
レジストリハイヴ
ファイルの抽出

The Sleuth Kitでファイル抽出
1. ディスクイメージ展開のために必要な値を取得
2. ディスクイメージを展開して、目的ファイル*1の
   inode番号を捜索
3. 目的ファイルを抽出

*1 above window XP7s PATH(case-sensitive)
%SystemRoot%¥System32¥config¥SOFTWARE
windows98 , Me , 2000 ‘s PATH
%SystemRoot%¥SYSTEM.DAT

抽出したファイルから
レジストリの値を
読み込む

hivexでレジストリから値を読み取る
・抽出したレジストリハイヴの目的パス*2のkeyを
  読み取る

*2 above window XP7s PATH(case-sensitive)
HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion
windows98 , Me , 2000 ‘s PATH
HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion

Determine Windows Version!