

**第四回 調査技術ゼミ**  
**2005年11月22日**

**『ブラウザ履歴の調査』**  
**Index.dat の解析**

**ネットエージェント株式会社**

# Index.dat (1)

- 4種類のINDEX.DAT
  - (1)クッキー
  - (2)ヒストリー(メイン)
  - (3)ヒストリー(デイリー/ウィークリー)
  - (4)キャッシュ
- Documents and Settings¥*UserName*¥
  - Cookies¥**index.dat**
  - Local Settings¥History¥History.IE5¥**index.dat**
  - Local Settings¥History¥History.IE5¥MSHist01 2005103120051107¥**index.dat**
  - Local Settings¥Temporary Internet Files¥Content.IE5¥**index.dat**

※MSHist01～配下には日・週フォルダ毎にIndex.datが作成される※

# Index.dat (2)

- Index.dat 内部に記録される日本語文字列の文字コードはCP932(いわゆるShift\_JIS) \* 1
- Index.dat を検索する方法
  - (a)ファイル名の検索
  - (b)ヘッダパターン(文字列)の検索

(例)IE6 の index.dat ヘッダ部分

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	01	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	43	6C	69	65	6E	74	20	55	72	6C	43	61	63	68	65	20	Client UrlCache														
00000010	4D	4D	46	20	56	65	72	20	35	2E	32	00	00	00	18	00	MMF_Ver_5.2...														
00000020	00	50	00	00	80	2F	00	00	42	2F	00	00	00	00	00	00	.P.../..B/.....														

\* 1:History の Index.dat に記録される Title 文字列は UTF-16LE で記録

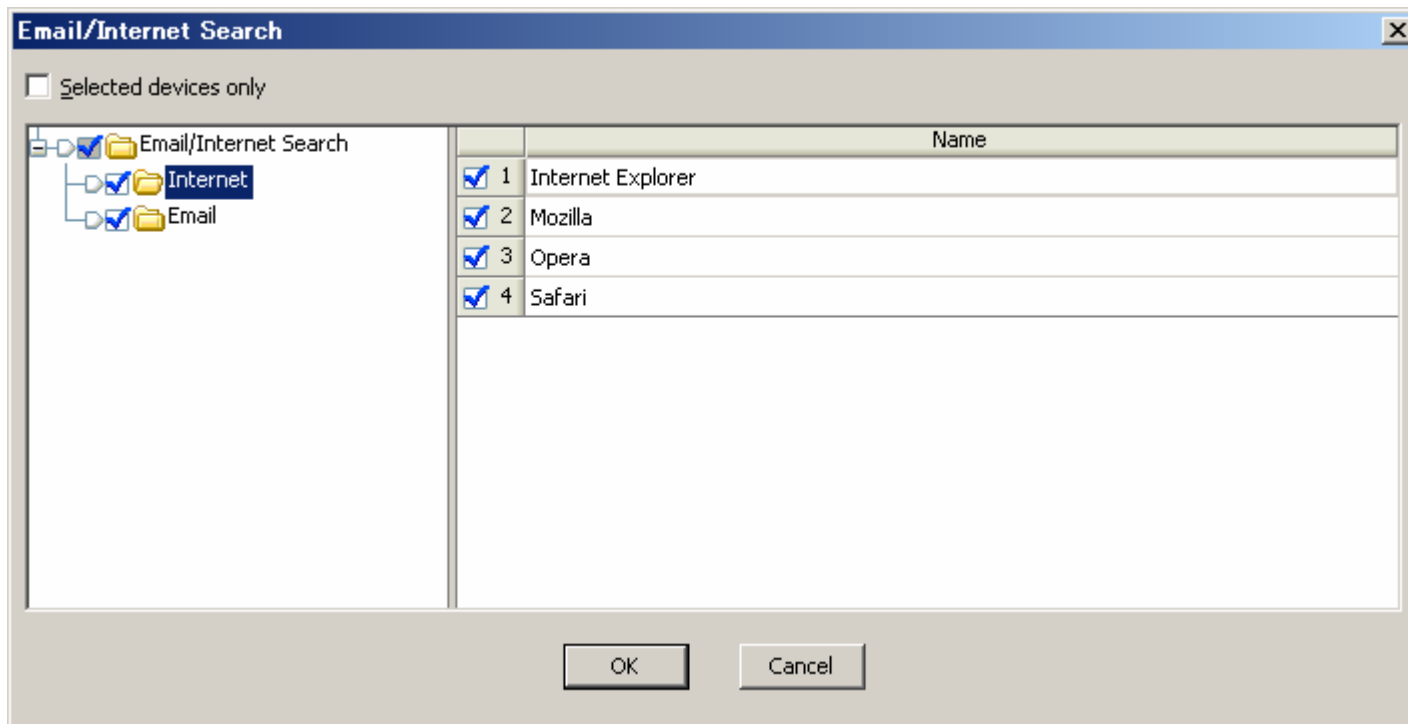
# Index.dat (3)

Index.dat file	Type
Cookie	URL
History	URL
Cache	URL、REDR、LEAK
ALL	HASH

# EnCase

## WebCache・History(1)

- Ver 5.x からの新機能
- Email/Internet Search を実行することで  
キャッシュと履歴を自動的に検索し解析



# EnCase

## WebCache・History (2)

- ・ EFE 5.04a での現象
- ・ Email/Internet Search の初回表示では、Deleted が適切な表示を行わない？  
回避方法：EFE 再起動
- ・ Historyの表示でハングアップ状態に陥る場合がある  
回避方法：プロセスの強制終了
- ・ History 表示で URL, HOST 部分の日本語 (CP 932)が化ける

# NetAnalysis (1)

- NetAnalysis v1.36 – Standard  
<http://www.digital-detective.co.uk/>  
<http://www.paraben-forensics.com/>
- インターネット履歴専用調査ツール  
IE、Netscape、Mozilla、Opera に対応
- レイアウトの再現、クッキーのデコードなどが可能

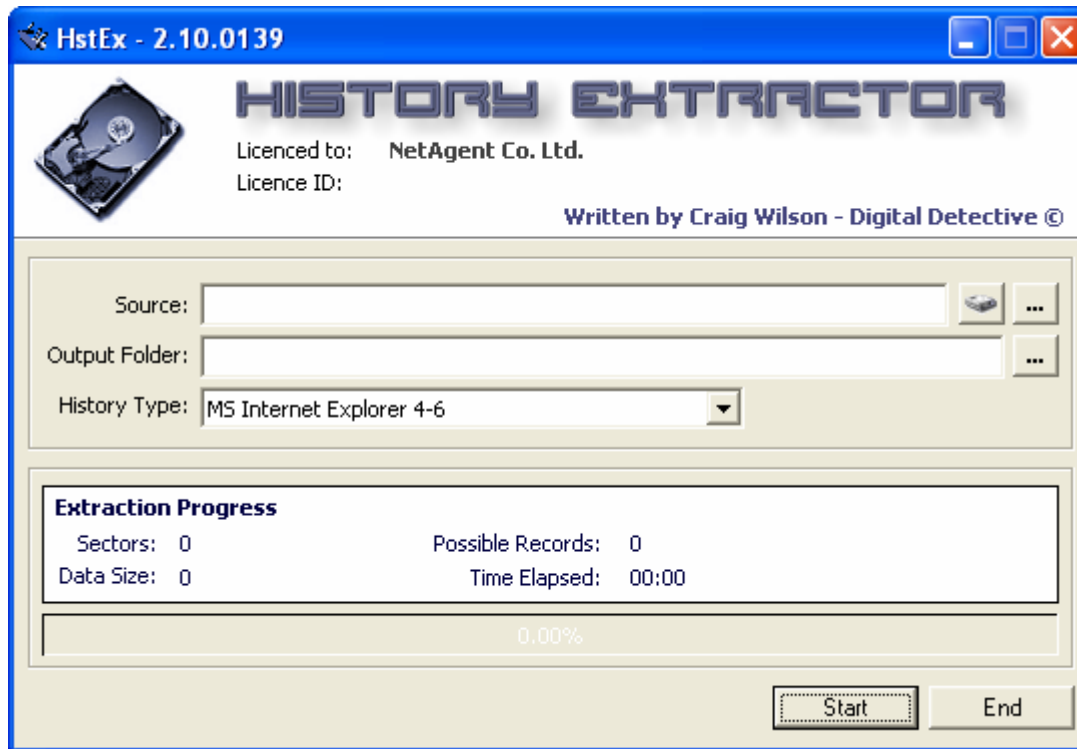
*英語版 Windows XP上で使用  
(日本語版XP上ではうまく動作しない)*

# NetAnalysis (2)

1. タイムゾーンなどプロパティを設定
2. 解析したいデータをエクスポートする  
*case¥export¥Cookie¥*  
*case¥export¥Temporary Internet Files¥*  
*case¥export¥History¥*
3. ヒストリ ファイルを開く  
(INDEX.DATを直接指定してオープンも可)
4. 内部ビューアでオフライン表示  
(内部ビューアは日本語表示も可能)

# NetAnalysis (3)

- ・ 未使用領域から履歴レコードを抽出が可能
- ・ ドライブまたはバイナリファイルなどを指定



未使用領域を検索する場合は、事前にファイルとしてエクスポートしておき、そのファイル内容を解析

※EnCase用のスクリプトは現在は提供されていない模様※

# NetAnalysis (4)

- EnCase の外部ビューアとしても利用可能
- Web Page Title 部分でマルチバイト文字列の表示は不可？ (EnCaseは可能)
- History に含まれる日本語文字列 (CP932) は「？」に化けてしまう

# IECookiesView

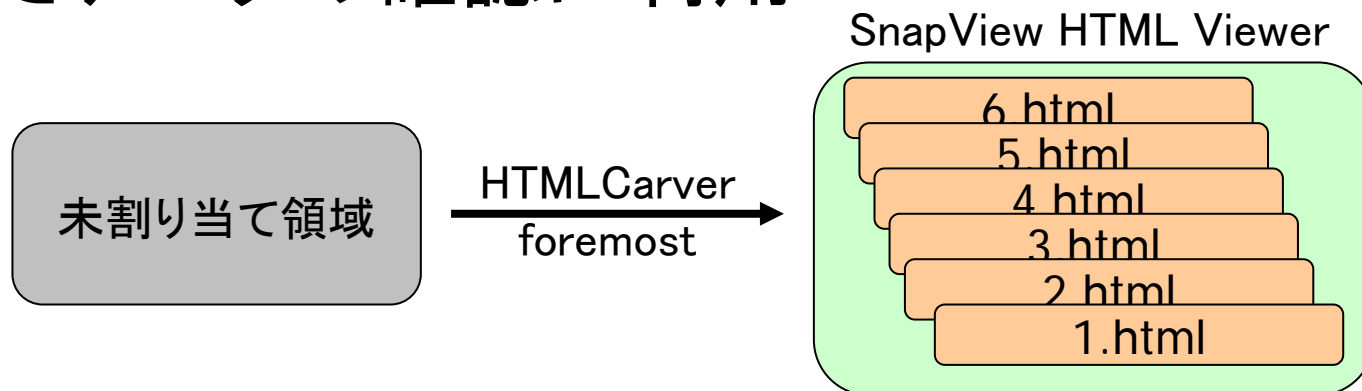
- IECookiesView (iecv)  
<http://www.nirsoft.net/utils/iecookies.html>
- IEが管理している Cookie を表示するツール  
任意のパスを指定することが可能
- 日時の表示方法  
実効環境で設定されているタイムゾーンに従って時刻を表示

# SnapView HTML Viewer

- SnapView HTML Viewer

<http://www.digital-detective.co.uk/freetools/snapview.asp>

- 未割り当て領域などから抽出した HTML ファイルを手軽に閲覧(表示にIEを利用)
- EnCase (HTMLCarver) やForemostで抽出したデータの確認に利用



**解き明かす力、今すぐにでも。  
フォレンジック・サービス**

**NetAgent**

**The Forensics Company**

**<http://forensic.netagent.co.jp/>**