Internet Explorer History files – Understand index.dat (I)

The Internet History files are important evidence. To analyse evidence, it is necessary to examine index.dat files. Index.dat files log information that a user has performed.

1. **What is index.dat?**
   Index.dat is to keep track of a user activity, which can include surfing the Internet Explorer or opening files from within window Explorer or Outlook that have an extension listed as a registered file type. Other web-based programs can as also generate entries. Please do remember that index.dat files are not all created equal. This handbook mainly focus on Internet History files, which located, in windows, in C:\Documents and Settings\[username]\Local Settings\History\History.IE5

2. **Index.dat structure in Internet History Folder**
   The beginning of the data structure of the index.dat file

File offset	Length	Description
0	28bytes	File header (ends in hex 00)
28	4 bytes	Filesize of Index.dat
32	4 bytes	Pointer to file offset of hash table

The hash table structure

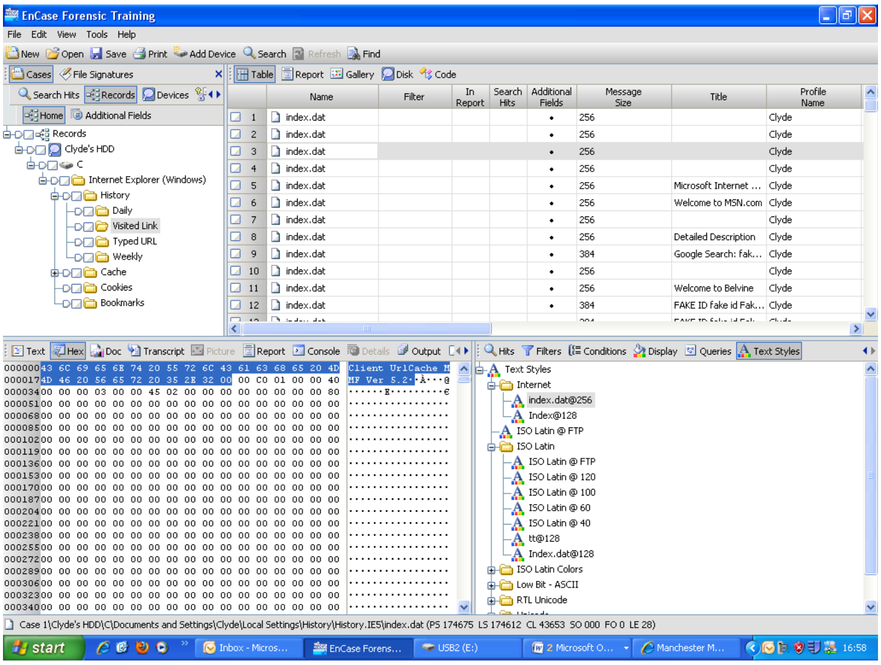
Length	Description
4 bytes	Header
4 bytes	Length of hash
4 bytes	Pointer to file offset of next hash table
4 bytes	Hash table number

The record structure

Record offset	Length	Description
0	4 bytes	Type (URL)
4	4 bytes	Record size (value x 128 bytes)
8	8 bytes	Last visited time –Filetime format (GMT)
16	8 bytes	Last visited time –Filetime format (GMT)
24	4 bytes	Expiration date –DosDate Time format (GMT)
68	4 bytes	Record offset to tile Bar Parameters
80	4 bytes	Last visited time-DocsdATE Time Format (GMT
84	4 bytes	Hit counter
104	variable	Visited:[username]@[URL]
variable	20 bytes	Title bar parameters. Starting at the 17th byte (offset 16) read 2bytes is the length of the title bar data. The 20th byte(offset19) is the type: \x1f =USED –TITLE BAR DATA WILL BE IN UNICODE \X1E ={guid} \X00= Not used
variable	variable	Title bar data

3. **Understanding the structure of index.dat file (an example)**
Use "search" Internet history with comprehensive search for the Internet History Files. After search, go to "Records" and find an index.dat file. Now we start to understand the structure of index.dat.

3.1 File header (highlighted hexadecimal representation)

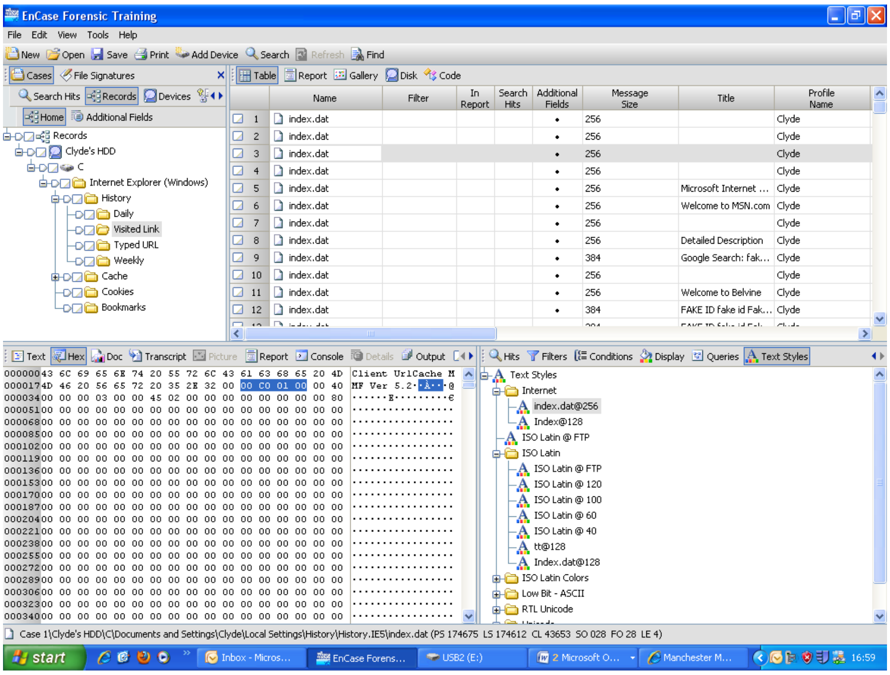


	Name	Filter	In Report	Search Hits	Additional Fields	Message Size	Title	Profile Name
1	index.dat				•	256		Clyde
2	index.dat				•	256		Clyde
3	index.dat				•	256		Clyde
4	index.dat				•	256		Clyde
5	index.dat				•	256	Microsoft Internet ...	Clyde
6	index.dat				•	256	Welcome to MSN.com	Clyde
7	index.dat				•	256		Clyde
8	index.dat				•	256	Detailed Description	Clyde
9	index.dat				•	384	Google Search: fak...	Clyde
10	index.dat				•	256		Clyde
11	index.dat				•	256	Welcome to Belvine	Clyde
12	index.dat				•	384	FAKE ID fake id Fak...	Clyde

```
00000043 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4D  Client UrlCache M
0000174D 46 20 56 65 72 20 35 2E 32 00 00 C0 01 00 00 40  MF Ver 5.2··À···@
00003400 00 00 03 00 00 45 02 00 00 00 00 00 00 00 00 80  ······E·········€
00005100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00006800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00008500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00010200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00011900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00013600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00015300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00017000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00018700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00020400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00022100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00023800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00025500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00027200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00028900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00030600 00 00 00 00 00 45 02 00 00 00 00 00 00 00 00 00  ·················
00032300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00034000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 174675 LS 174612 CL 43653 SO 000 FO 0 LE 28)

3.2 File size (highlighted hexadecimal representation)

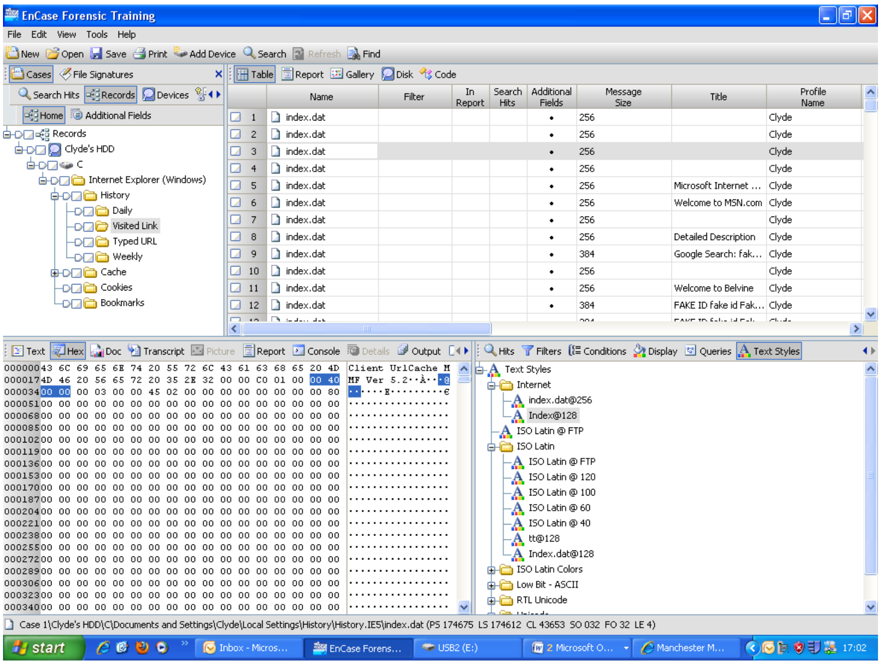


	Name	Filter	In Report	Search Hits	Additional Fields	Message Size	Title	Profile Name
1	index.dat				•	256		Clyde
2	index.dat				•	256		Clyde
3	index.dat				•	256		Clyde
4	index.dat				•	256		Clyde
5	index.dat				•	256	Microsoft Internet ...	Clyde
6	index.dat				•	256	Welcome to MSN.com	Clyde
7	index.dat				•	256		Clyde
8	index.dat				•	256	Detailed Description	Clyde
9	index.dat				•	384	Google Search: fak...	Clyde
10	index.dat				•	256		Clyde
11	index.dat				•	256	Welcome to Belvine	Clyde
12	index.dat				•	384	FAKE ID fake id Fak...	Clyde

```
00000043 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4D  Client UrlCache M
0000174D 46 20 56 65 72 20 35 2E 32 00 00 C0 01 00 00 40  MF Ver 5.2··À···@
00003400 00 00 03 00 00 45 02 00 00 00 00 00 00 00 00 80  ······E·········€
00005100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00006800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00008500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00010200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00011900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00013600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00015300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00017000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00018700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00020400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00022100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00023800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00025500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00027200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00028900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00030600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00032300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00034000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 174675 LS 174612 CL 43653 SO 028 FO 28 LE 4)

3.2 Hash table offset

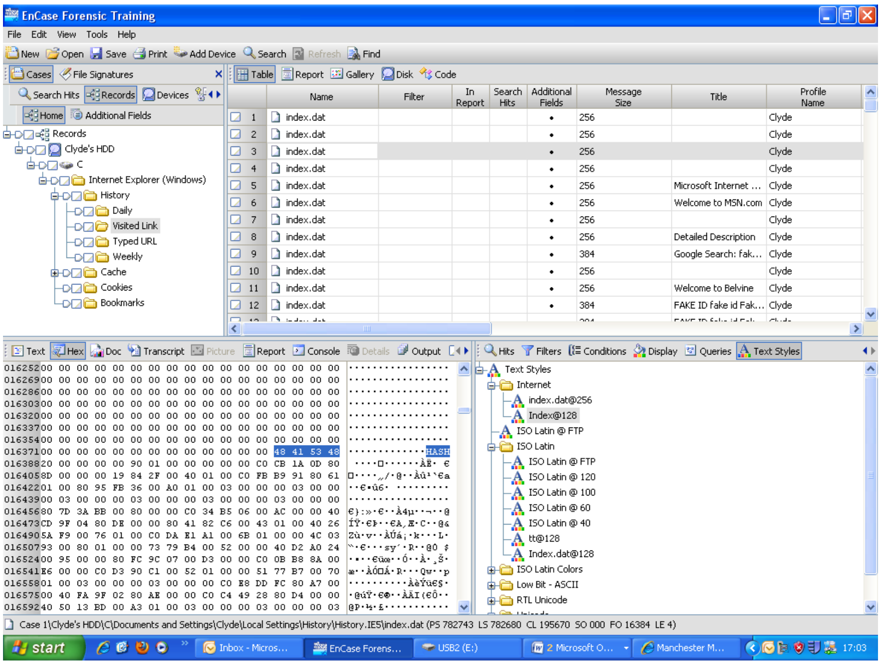


	Name	Filter	In Report	Search Hits	Additional Fields	Message Size	Title	Profile Name
1	index.dat				•	256		Clyde
2	index.dat				•	256		Clyde
3	index.dat				•	256		Clyde
4	index.dat				•	256		Clyde
5	index.dat				•	256	Microsoft Internet ...	Clyde
6	index.dat				•	256	Welcome to MSN.com	Clyde
7	index.dat				•	256		Clyde
8	index.dat				•	256	Detailed Description	Clyde
9	index.dat				•	384	Google Search: fak...	Clyde
10	index.dat				•	256		Clyde
11	index.dat				•	256	Welcome to Belvine	Clyde
12	index.dat				•	384	FAKE ID fake id Fak...	Clyde

```
00000043 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4D  Client UrlCache M
0000174D 46 20 56 65 72 20 35 2E 32 00 00 C0 01 00 00 40  MF Ver 5.2··À···@
00003400 00 00 03 00 00 45 02 00 00 00 00 00 00 00 00 80  ······E·········€
00005100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00006800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00008500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00010200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00011900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00013600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00015300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00017000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00018700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00020400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00022100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00023800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00025500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00027200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00028900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00030600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00032300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
00034000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 174675 LS 174612 CL 43653 SO 032 FO 32 LE 4)

3.3 Hash header



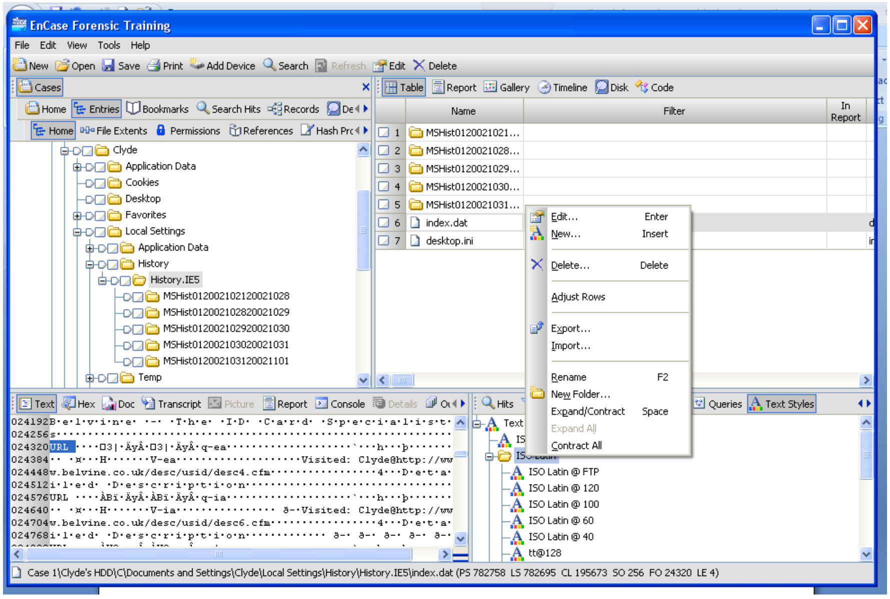
	Name	Filter	In Report	Search Hits	Additional Fields	Message Size	Title	Profile Name
1	index.dat				•	256		Clyde
2	index.dat				•	256		Clyde
3	index.dat				•	256		Clyde
4	index.dat				•	256		Clyde
5	index.dat				•	256	Microsoft Internet ...	Clyde
6	index.dat				•	256	Welcome to MSN.com	Clyde
7	index.dat				•	256		Clyde
8	index.dat				•	256	Detailed Description	Clyde
9	index.dat				•	384	Google Search: fak...	Clyde
10	index.dat				•	256		Clyde
11	index.dat				•	256	Welcome to Belvine	Clyde
12	index.dat				•	384	FAKE ID fake id Fak...	Clyde

```
01625200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
01626900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
01628600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
01630300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
01632000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
01633700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
01635400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ·················
01637100 00 00 00 00 00 00 00 00 00 00 00 00 00 48 41 53 48  ·············HASH
01638820 00 00 00 00 90 01 00 00 00 00 00 C0 CB 1A 0D 80   ····□······ÀË· €
0164058D 00 00 00 19 84 2F 00 40 01 00 C0 FB B9 91 80 61  □····„/·@··Àû¹`€a
01642201 00 80 95 FB 36 00 A0 01 00 03 00 00 00 03 00 00  ··€•û6· ·········
01643900 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00  ·················
01645680 7D 3A BB 00 80 00 00 C0 34 B5 06 00 AC 00 00 40  €}:»·€··À4µ··¬··@
016473CD 9F 04 80 DE 00 00 80 41 82 C6 00 43 01 00 40 26  ÍŸ·€Þ··€A‚Æ·C··@&
0164905A F9 00 76 01 00 C0 DA E1 A1 00 6B 01 00 00 4C 03  Zù·v··ÀÚá¡·k···L·
01650793 00 80 01 00 00 73 79 B4 00 52 00 00 40 D2 A0 24  "·€···sy´·R··@Ò $
01652400 95 00 00 80 FC 9C 07 00 D3 00 00 C0 0B B8 8A 00  ·•··€üœ··Ó··À·¸Š·
016541E6 00 00 C0 D3 90 C1 00 52 01 00 00 51 77 B7 00 70  æ··ÀÓ□Á·R···Qw··p
01655801 00 03 00 00 00 03 00 00 00 C0 E8 DD FC 80 A7 00  ··········ÀèÝü€§·
01657500 40 FA 9F 02 80 AE 00 00 C0 C4 49 28 80 D4 00 00  ·@úŸ·€®··ÀÄI(€Ô··
01659240 50 13 BD 00 A3 01 00 03 00 00 00 03 00 00 00 03  @P·½·£···········
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 782743 LS 782680 CL 195670 SO 000 FO 16384 LE 4)

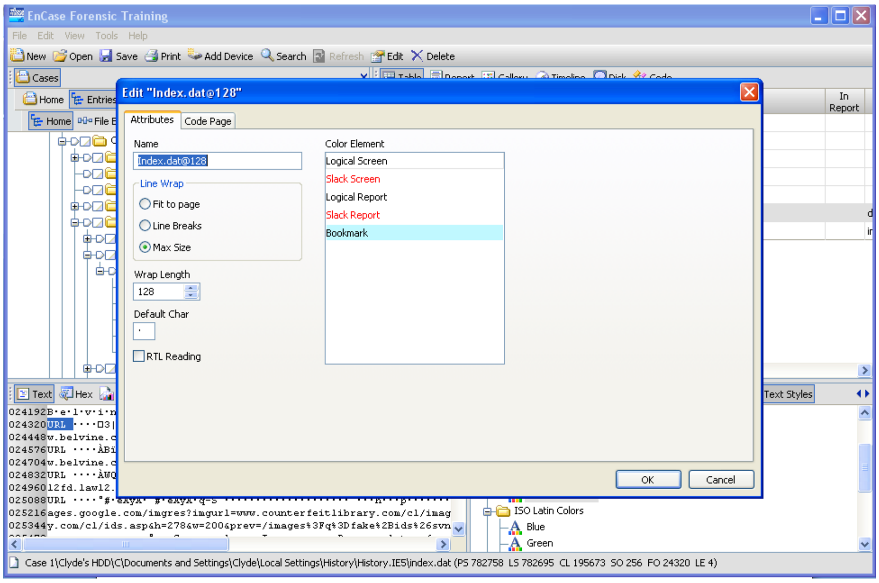
4. **Creating new text style for the index.dat file, the purpose is to set the proper text style for the history INDEX.DAT files in the view pane.**

4.1 Go to text style in the filter pane and create a new style using "new"



Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 782758 LS 782695 CL 195673 SO 256 FO 24320 LE 4)

4.2 Fill index.dat@128 and choose MAX SIZE and the wrap length is 128.



Name: Index.dat@128

Line Wrap: ○ Fit to page ○ Line Breaks ● Max Size

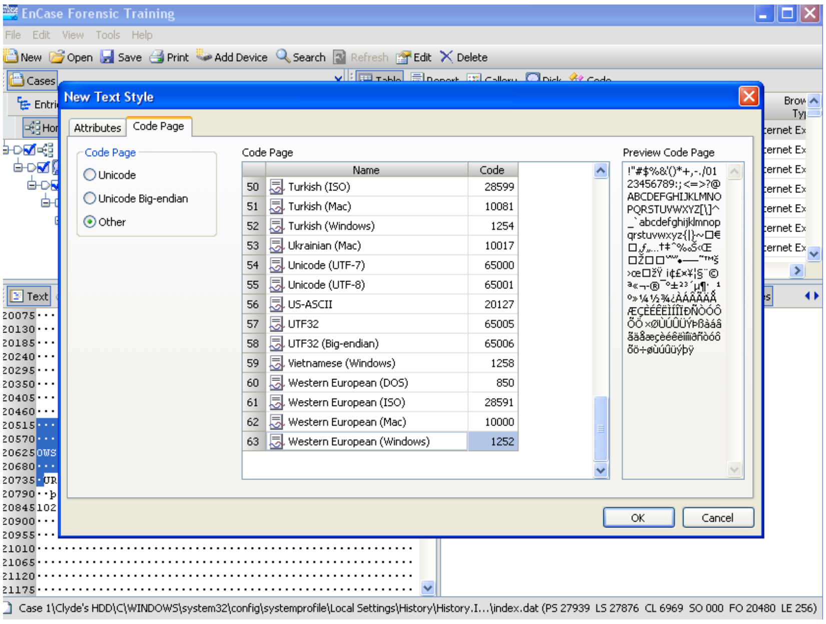
Wrap Length: 128

Default Char: .

□ RTL Reading

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 782758 LS 782695 CL 195673 SO 256 FO 24320 LE 4)

4.3 Click on the code page tab, select “other” and then choose Western European (windows) click “ok”



EnCase Forensic Training
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Edit Delete
New Text Style
Attributes
Code Page
OK
Cancel

Code Page

○ Unicode
○ Unicode Big-endian
● Other

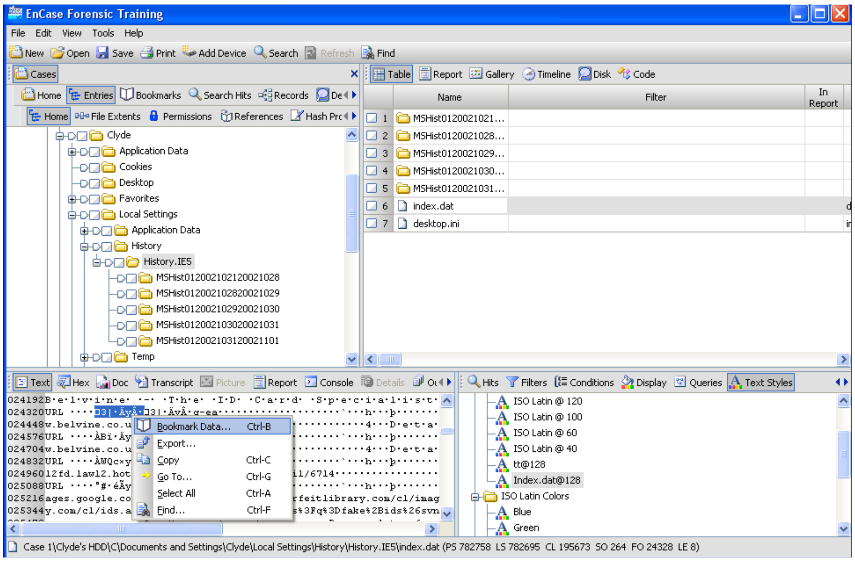
Code Page

	Name	Code
50	Turkish (ISO)	28599
51	Turkish (Mac)	10081
52	Turkish (Windows)	1254
53	Ukrainian (Mac)	10017
54	Unicode (UTF-7)	65000
55	Unicode (UTF-8)	65001
56	US-ASCII	20127
57	UTF32	65005
58	UTF32 (Big-endian)	65006
59	Vietnamese (Windows)	1258
60	Western European (DOS)	850
61	Western European (ISO)	28591
62	Western European (Mac)	10000
63	Western European (Windows)	1252

Preview Code Page

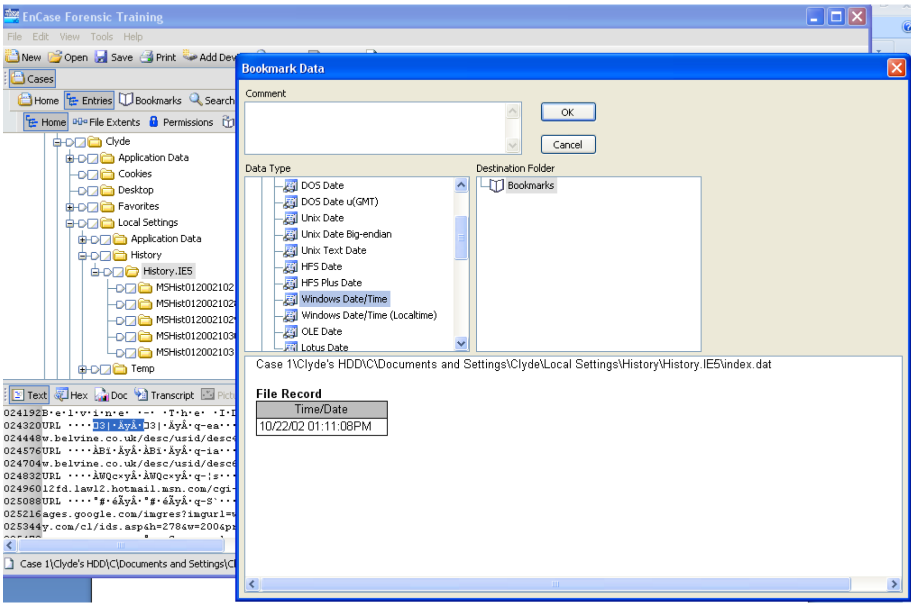
Case 1\Clyde's HDD\C\WINDOWS\system32\config\systemprofile\Local Settings\History\History.I...\index.dat (PS 27939 LS 27876 CL 6969 SO 000 FO 20480 LE 256)

5. **Decoding the windows date/time within the record**
   5.1 Find Record offset. The identifier is URL. To try to find the beginning of last accessed date/time field (record offset 8), highlight the first 8 bytes of the record, the next byte begins that field. Beginning at that byte, highlight for 8 bytes to decide the last accessed field. Use the bookmark feature to decode the windows date/time by choosing "Windows Date/time" or "Windows Date/Time (Localtime)".



	Name	Filter	In Report
1	MSHist0120021021...		
2	MSHist0120021028...		
3	MSHist0120021029...		
4	MSHist0120021030...		
5	MSHist0120021031...		
6	index.dat		
7	desktop.ini		

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 782758 LS 782695 CL 195673 SO 264 FO 24328 LE 8)



```
024192B·e·l·v·i·n·e· ·-· ·T·h·e· ·I·
024320URL ····03|·ÅyÅ·03|·ÅyÅ·q-ea··
024448w.belvine.co.uk/desc/usid/desc
024576URL ····ÀBi·ÅyÅ·ÀBi·ÅyÅ·q-ia··
024704w.belvine.co.uk/desc/usid/desc
024832URL ····ÀWQc×yÅ·ÀWQc×yÅ·q-¦s··
02496012fd.lawl2.hotmail.msn.com/cgi
025088URL ····"#·éÅyÅ·"#·éÅyÅ·q-S`··
025216ages.google.com/imgres?imgurl=
025344y.com/cl/ids.asp&h=278&w=200&p
```

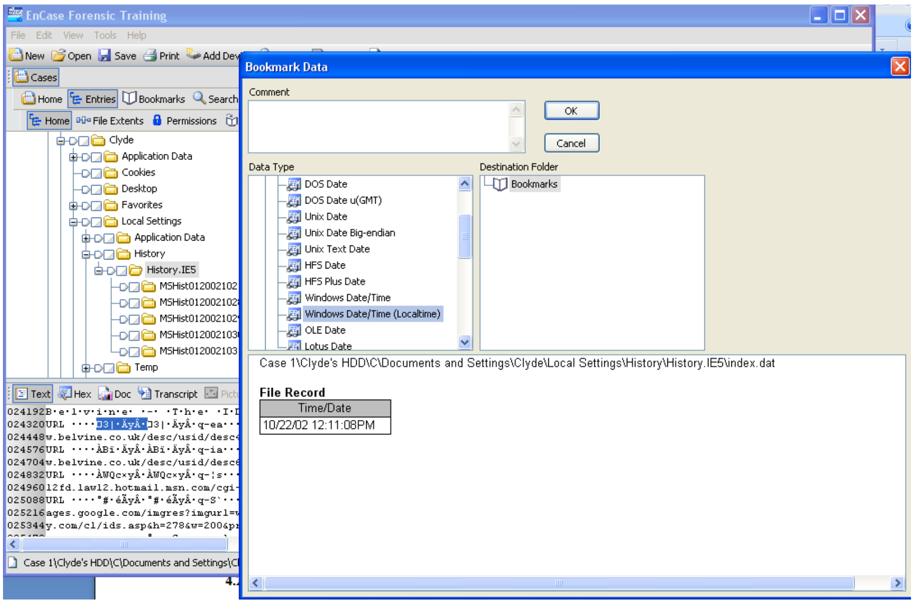
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat

File Record

Time/Date
10/22/02 01:11:08PM

Case 1\Clyde's HDD\C\Documents and Settings\C

Or you can choose Windows Date (local time)



```
024192B·e·l·v·i·n·e· ·-· ·T·h·e· ·I·
024320URL ····03|·ÅyÅ·03|·ÅyÅ·q-ea··
024448w.belvine.co.uk/desc/usid/desc
024576URL ····ÀBi·ÅyÅ·ÀBi·ÅyÅ·q-ia··
024704w.belvine.co.uk/desc/usid/desc
024832URL ····ÀWQc×yÅ·ÀWQc×yÅ·q-¦s··
02496012fd.lawl2.hotmail.msn.com/cgi
025088URL ····"#·éÅyÅ·"#·éÅyÅ·q-S`··
025216ages.google.com/imgres?imgurl=
025344y.com/cl/ids.asp&h=278&w=200&p
```

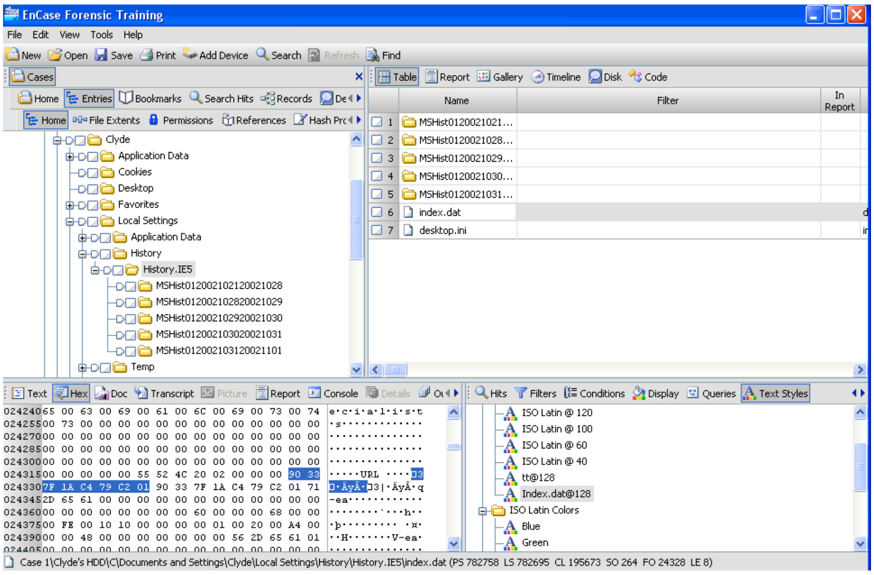
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat

File Record

Time/Date
10/22/02 12:11:08PM

Case 1\Clyde's HDD\C\Documents and Settings\C

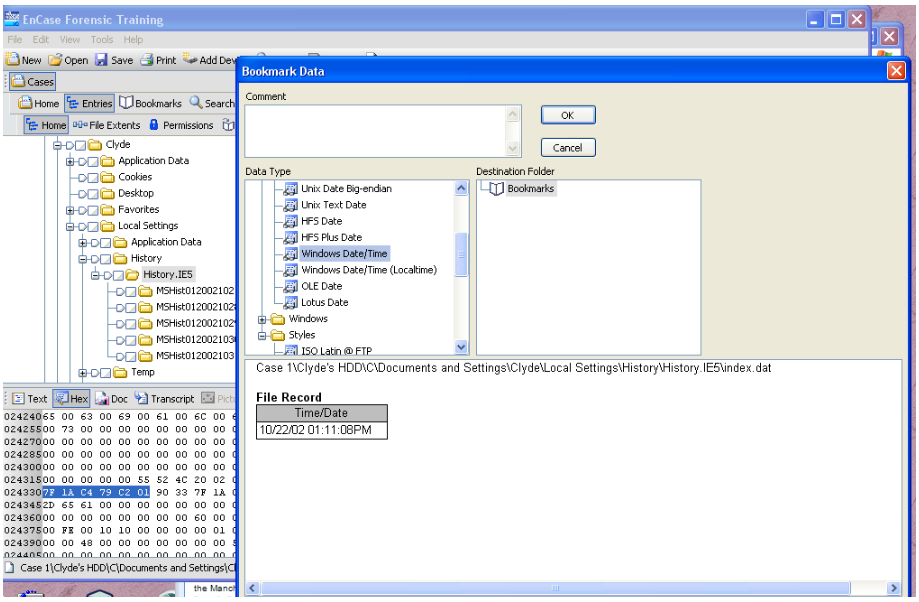
5.2 You can also decode from HEX to date/time using bookmark



	Name	Filter	In Report
1	MSHist0120021021…		
2	MSHist0120021028…		
3	MSHist0120021029…		
4	MSHist0120021030…		
5	MSHist0120021031…		
6	index.dat		
7	desktop.ini		

```
02424065 00 63 00 69 00 61 00 6C 00 69 00 73 00 74  e·c·i·a·l·i·s·t
02425500 73 00 00 00 00 00 00 00 00 00 00 00 00 00  ·s·············
02427000 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············
02428500 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············
02430000 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············
02431500 00 00 00 00 55 52 4C 20 02 00 00 00 90 33  ·····URL ····□3
0243307F 1A C4 79 C2 01 90 33 7F 1A C4 79 C2 01 71  □·ÄyÂ·□3|·ÄyÂ·q
0243452D 65 61 00 00 00 00 00 00 00 00 00 00 00 00  -ea············
02436000 00 00 00 00 00 00 00 60 00 00 00 68 00 00  ········`···h··
02437500 FE 00 10 10 00 00 00 00 01 00 20 00 A4 00  ·þ·········  ·¤·
02439000 00 48 00 00 00 00 00 00 00 56 2D 65 61 01  ··H·······V-ea·
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 782758 LS 782695 CL 195673 SO 264 FO 24328 LE 8)



Comment

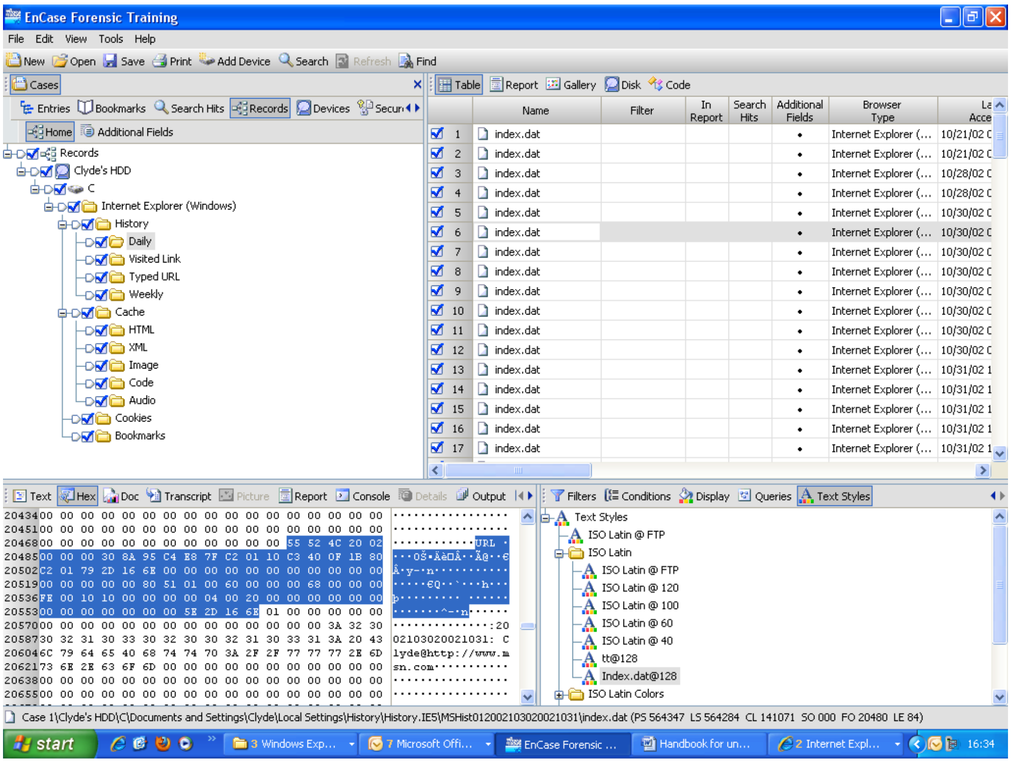
Data Type: Windows Date/Time

Destination Folder: Bookmarks

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat

File Record

Time/Date
10/22/02 01:11:08PM



	Name	Filter	In Report	Search Hits	Additional Fields	Browser Type	Last Acce
☑ 1	index.dat				•	Internet Explorer (...	10/21/02 C
☑ 2	index.dat				•	Internet Explorer (...	10/21/02 C
☑ 3	index.dat				•	Internet Explorer (...	10/28/02 C
☑ 4	index.dat				•	Internet Explorer (...	10/28/02 C
☑ 5	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 6	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 7	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 8	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 9	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 10	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 11	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 12	index.dat				•	Internet Explorer (...	10/30/02 C
☑ 13	index.dat				•	Internet Explorer (...	10/31/02 1
☑ 14	index.dat				•	Internet Explorer (...	10/31/02 1
☑ 15	index.dat				•	Internet Explorer (...	10/31/02 1
☑ 16	index.dat				•	Internet Explorer (...	10/31/02 1
☑ 17	index.dat				•	Internet Explorer (...	10/31/02 1

```
2043400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
2045100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
2046800 00 00 00 00 00 00 00 00 00 00 00 55 52 4C 20 02 ············URL ·
2048500 00 00 30 8A 95 C4 E8 7F C2 01 10 C3 40 0F 1B 80 ···0Š•ÄèÂ··Ã@··€
20502C2 01 79 2D 16 6E 00 00 00 00 00 00 00 00 00 00 00 Â·y-·n···········
2051900 00 00 00 00 80 51 01 00 60 00 00 00 68 00 00 00 ·····€Q··`···h···
20536FE 00 10 10 00 00 00 00 04 00 20 00 00 00 00 00 00 þ·········  ······
2055300 00 00 00 00 00 00 5E 2D 16 6E 01 00 00 00 00 00 ·······^-·n······
2057000 00 00 00 00 00 00 00 00 00 00 00 00 00 3A 32 30 ··············:20
2058730 32 31 30 33 30 32 30 30 32 31 30 33 31 3A 20 43 02103020021031: C
206046C 79 64 65 40 68 74 74 70 3A 2F 2F 77 77 77 2E 6D lyde@http://www.m
2062173 6E 2E 63 6F 6D 00 00 00 00 00 00 00 00 00 00 00 sn.com···········
2063800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
2065500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
```

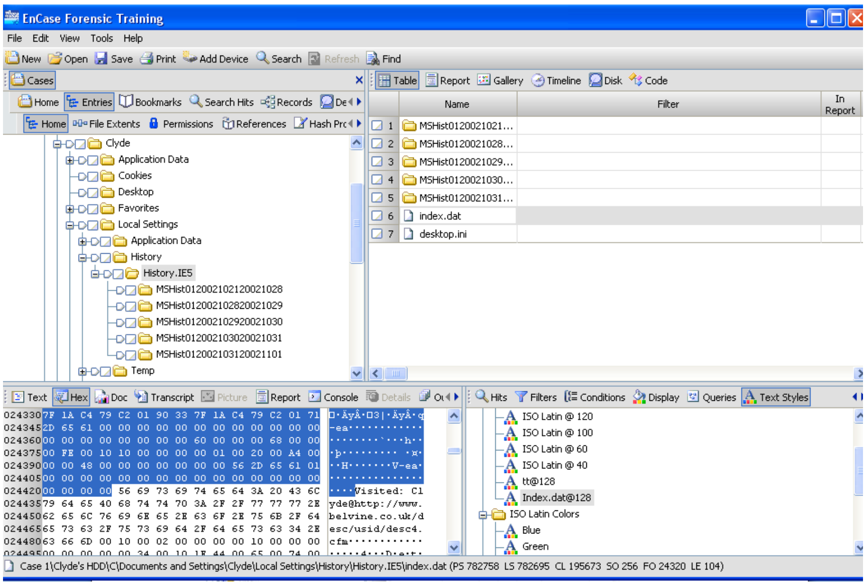
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\MSHist012002103020021031\index.dat (PS 564347 LS 564284 CL 141071 SO 000 FO 20480 LE 84)

6.2 Look at data record "visited: [username]@[url]", at record offset 104, you will find this data structure:

Visited:[username]@[URL]

[username] is at the URL that was visited

The data ends at hex 00



	Name	Filter	In Report
□ 1	MSHist0120021021...		
□ 2	MSHist0120021028...		
□ 3	MSHist0120021029...		
□ 4	MSHist0120021030...		
□ 5	MSHist0120021031...		
□ 6	index.dat		
□ 7	desktop.ini		

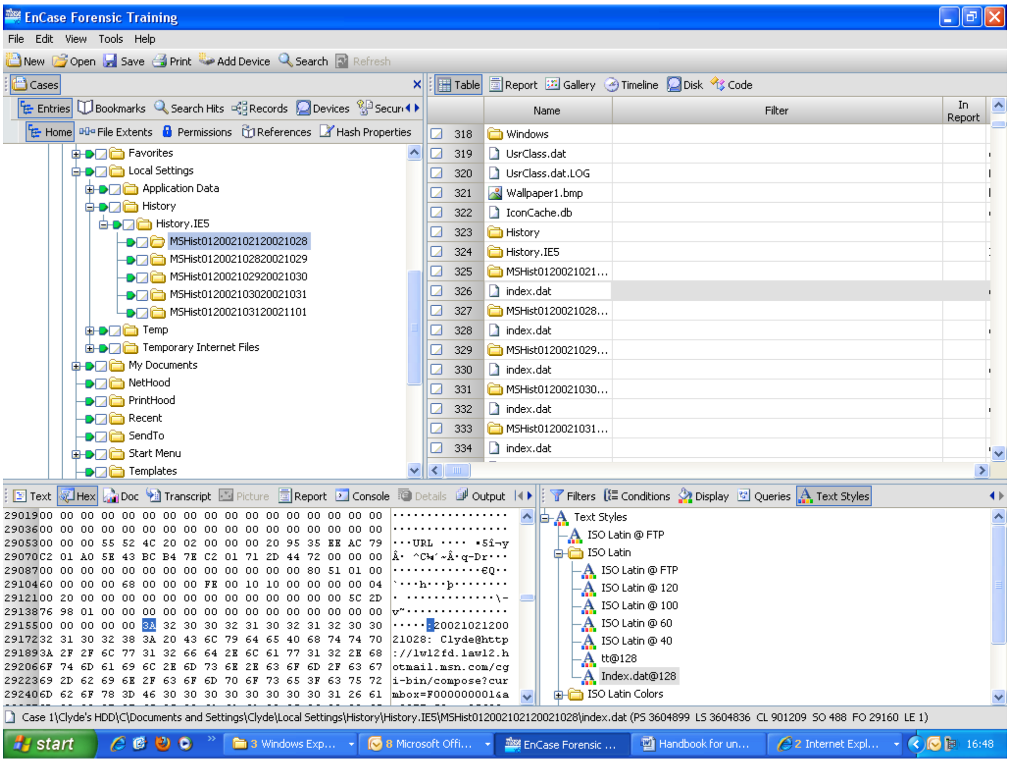
```
0243307F 1A C4 79 C2 01 90 33 7F 1A C4 79 C2 01 71 □·ÄyÂ·□3|·ÄyÂ·q
0243452D 65 61 00 00 00 00 00 00 00 00 00 00 00 00 -ea·············
02436000 00 00 00 00 00 00 00 60 00 00 00 68 00 00 ·········`···h··
02437500 FE 00 10 10 00 00 00 00 01 00 20 00 A4 00 ·þ·········  ·¤·
02439000 00 48 00 00 00 00 00 00 00 56 2D 65 61 01 ··H·······V-ea·
02440500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···············
02442000 00 00 00 56 69 73 69 74 65 64 3A 20 43 6C ····Visited: Cl
02443579 64 65 40 68 74 74 70 3A 2F 2F 77 77 77 2E yde@http://www.
02445062 65 6C 76 69 6E 65 2E 63 6F 2E 75 6B 2F 64 belvine.co.uk/d
02446565 73 63 2F 75 73 69 64 2F 64 65 73 63 34 2E esc/usid/desc4.
02448063 66 6D 00 10 00 02 00 00 00 00 10 00 00 00 cfm············
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\index.dat (PS 782758 LS 782695 CL 195673 SO 256 FO 24320 LE 104)

6.3 If the user opened a file, you would see a URL beginning with file:///; if the file name contained spaces, you would see that represented as %20(hex20). The delimiter between elements of the path is a forward slash ("/") instead of

a blackslash("\") an example of this would be:
file:///c:/My%20Files/Personal%20Information.txt

7. Looking at daily and history files (go to Entries and find History.IE5)



	Name	Filter	In Report
318	Windows		
319	UsrClass.dat		
320	UsrClass.dat.LOG		
321	Wallpaper1.bmp		
322	IconCache.db		
323	History		
324	History.IE5		
325	MSHist0120021021...		
326	index.dat		
327	MSHist0120021028...		
328	index.dat		
329	MSHist0120021029...		
330	index.dat		
331	MSHist0120021030...		
332	index.dat		
333	MSHist0120021031...		
334	index.dat		

```
2901900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................
2903600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................
2905300 00 00 55 52 4C 20 02 00 00 00 20 95 35 EE AC 79  ···URL ····  •5î¬y
29070C2 01 A0 5E 43 BC B4 7E C2 01 71 2D 44 72 00 00 00  Â· ^C¼´~Â·q-Dr···
2908700 00 00 00 00 00 00 00 00 00 00 00 00 80 51 01 00  ·············€Q··
2910460 00 00 00 68 00 00 00 FE 00 10 10 00 00 00 00 04  `···h···þ········
2912100 20 00 00 00 00 00 00 00 00 00 00 00 00 00 5C 2D  · ·············\-
2913876 98 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  v˜···············
2915500 00 00 00 00 3A 32 30 30 32 31 30 32 31 32 30 30  ·····:20021021200
2917232 31 30 32 38 3A 20 43 6C 79 64 65 40 68 74 74 70  21028: Clyde@http
291893A 2F 2F 6C 77 31 32 66 64 2E 6C 61 77 31 32 2E 68  ://lw12fd.law12.h
292066F 74 6D 61 69 6C 2E 6D 73 6E 2E 63 6F 6D 2F 63 67  otmail.msn.com/cg
2922369 2D 62 69 6E 2F 63 6F 6D 70 6F 73 65 3F 63 75 72  i-bin/compose?cur
292406D 62 6F 78 3D 46 30 30 30 30 30 30 30 31 26 61  mbox=F000000001&a
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Local Settings\History\History.IE5\MSHist012002102120021028\index.dat (PS 3604899 LS 3604836 CL 901209 SO 488 FO 29160 LE 1)

7.1 Look at history file folder naming
MSHist012002102120021028

MSHist01	2002	10	21		2002	10	28
	Year	Month	Day	through	year	Month	Day

Task: based on the naming, can you tell which folder is daily history and which folder is weekly history.
Search for a file and when this searching happened?

8. Notes : Daily and Weekly history
The daily history is a collection of records from a given day's activity. A day begins at 12am or 00:00:00 and ends at 11:59:59pm or 23:59:59
The weekly history is a collection of records from previous daily history files, the week begins on Monday at 12am.