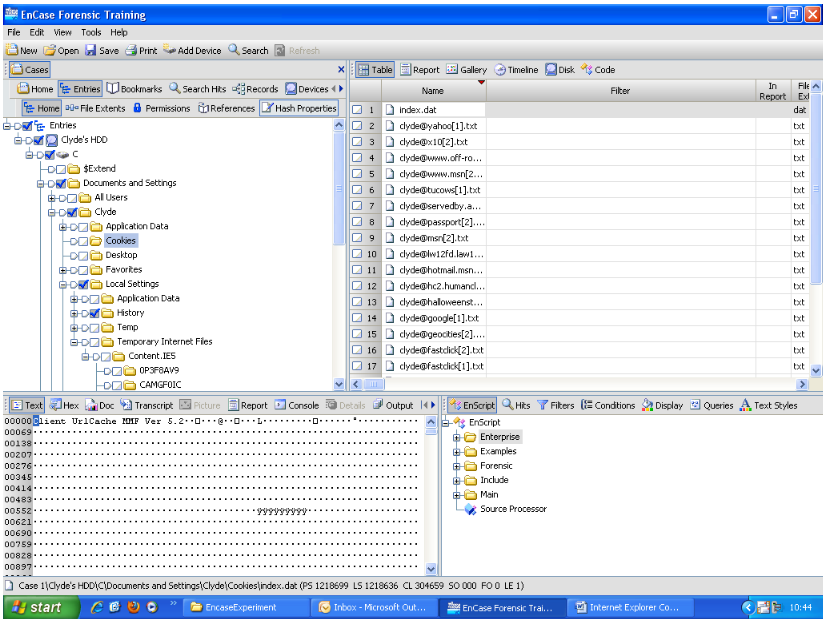
Internet Explorer Cookies: understanding index.dat (III)

Cookies are individual text files that can contain up to six individual values. Web sites use cookies to track visitors. The cookies are located in the following folder

C:\Documents and Setting\[username]\Cookies

1. Cookies location



	Name	Filter	In Report	File Ext
1	index.dat			dat
2	clyde@yahoo[1].txt			txt
3	clyde@x10[2].txt			txt
4	clyde@www.off-ro…			txt
5	clyde@www.msn[2…			txt
6	clyde@tucows[1].txt			txt
7	clyde@servedby.a…			txt
8	clyde@passport[2]….			txt
9	clyde@msn[2].txt			txt
10	clyde@lw12fd.law1…			txt
11	clyde@hotmail.msn…			txt
12	clyde@hc2.humancl…			txt
13	clyde@halloweenst…			txt
14	clyde@google[1].txt			txt
15	clyde@geocities[2]….			txt
16	clyde@fastclick[2].txt			txt
17	clyde@fastclick[1].txt			txt

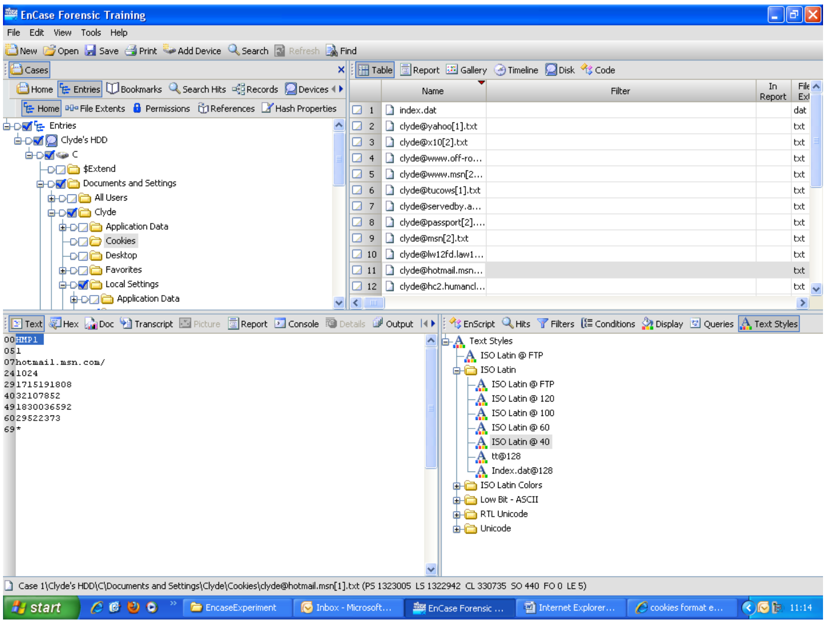
```
00000Client UrlCache MMF Ver 5.2··□···@··□···L·········□······°·············
00069··························································
00138··························································
00207··························································
00276··························································
00345··························································
00414··························································
00483··························································
00552·······························ÿÿÿÿÿÿÿÿÿÿ·················
00621··························································
00690··························································
00759··························································
00828··························································
00897··························································
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 000 FO 0 LE 1)

2. Cookies's Attributes

2.1 Cookies have 6 parameters including: name, value expiration date, path, domain, secure. Among of them, name and value are mandatory.

- **Name and value: you can just simply pairing them together sets the name of a cookie and its value: name (SITESERVER) &Value (ID=a52a7d93f43abe84472d36df59134a00). The value of cookie can be null.**
- **Expiration Date: the lifetime of the cookie. If not set, then means the end of the session**
- **Path: defines a subset of directories in a domain for which the cookie is valid. Pages outside of that path can not read or use the cookie.**
- **Domain: the domain parameter such as: yahoo.txt. If domain is not set, then it defaults to the full domain of the document creating the cookie.**
- **Secure: the secure parameter indicates a cookie will be used only for a secure server condition such as SSL. In most cases, it is set as FALSE**



	Name	Filter	In Report	File Ext
1	index.dat			dat
2	clyde@yahoo[1].txt			txt
3	clyde@x10[2].txt			txt
4	clyde@www.off-ro...			txt
5	clyde@www.msn[2...			txt
6	clyde@tucows[1].txt			txt
7	clyde@servedby.a...			txt
8	clyde@passport[2]....			txt
9	clyde@msn[2].txt			txt
10	clyde@lw12fd.law1...			txt
11	clyde@hotmail.msn...			txt
12	clyde@hc2.humancl...			txt

```
00HMP1
051
07hotmail.msn.com/
241024
291715191808
4032107852
491830036592
6029522373
69*
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\clyde@hotmail.msn[1].txt (PS 1323005 LS 1322942 CL 330735 SO 440 FO 0 LE 5)

3. Cookie’s data structure

- Each cookie contains one or more record
- Nine fields in each record (including terminating field)
- Each field ends in hex 0A (linefeed)
- Each records ends in hex 2A 0A

Name	value	DOMAIN	type	Expired date/time	Modified date/time	end
HMP1	1	hotmail.msn.com /	1024	1715191808/32107852	1830036592 /29522373	*

4. Index.dat

In the cookies folder, there is an index.dat file as well (you have already learned that index.dat files in history folders and cache folders are very different. The index.dat file is to keep track of the cookies files within the folder.

4.1 Data structure

File header

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

Hash table

Length	Description
4 bytes	Header
4 bytes	Length of hash table value *128
4 bytes	Pointer to file offset of next hash table
4 bytes	Hash table number

The beginning of the hash table will look like

File offset	Data (bytes)	Description

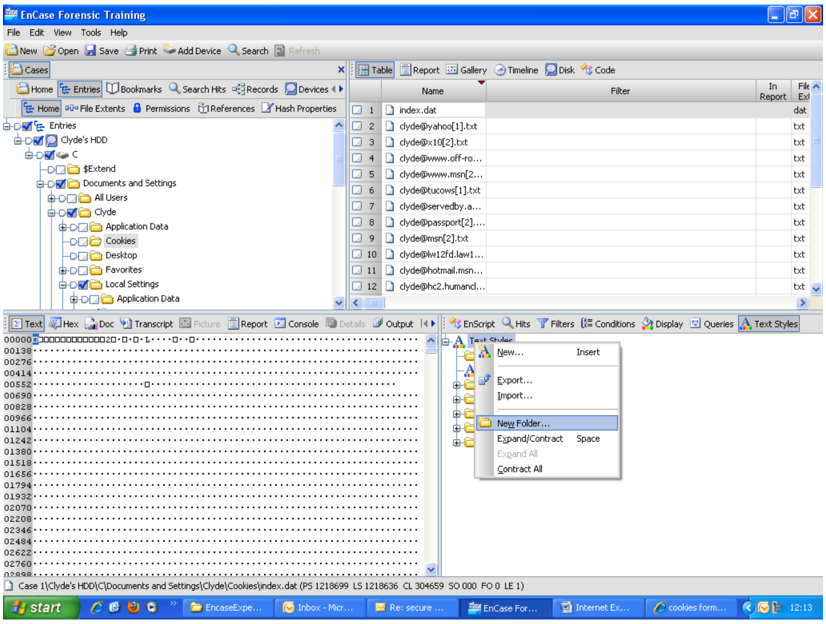
16400	3	3
16408	3	3
16416	Bb121380	26624
16424	3	3
16432	70c03ac0	31232
16440	3	3
16448	1	26624
16456	C5982dc0	23296
16464	73b53080	28416
16472	0252b300	27648
16480	3	3
16488	1	26624
16696	0	0

The first cookie record begins at the file offset 20480. Here is the record structure of the cache index.dat file.

Record offset	Length	Description
0	4 bytes	Type (URL)
4	4 bytes	Record size (value x 128 bytes)
8	8 bytes	Cookie modified: filetime format (GMT)
16	8 bytes	Cookie file last accessed time –Filetime format (GMT)
24	4 bytes	Cookies expiration date: DosDATE Time Format (GMT)
32	1 byte	Cookie file size
60	4 bytes	Record offset o cookie filename
80	4 bytes	Cookie file last accessed time-DosDATE Time Format (GMT)
84	4 bytes	Hit counter
92	4 bytes	Cookie file created time-DosDateTime format (GMT)
104	variable	Cookie:[username]@[website URL]. Ends in hex 00
variable	variable	Cookie filename, Ends in hex 00

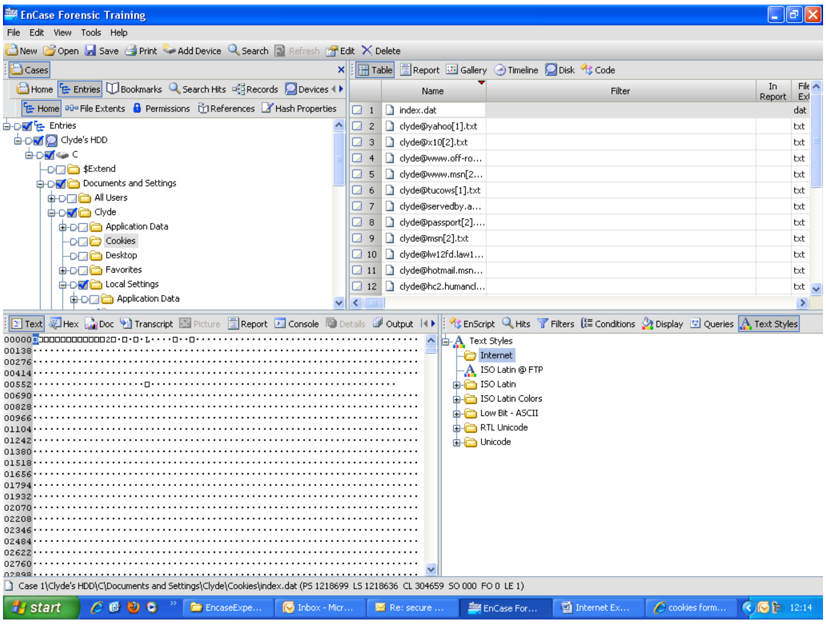
5. Creating a new folder in text styles

5.1 Go to View->Text Styles, then right click to create a new folder called 'Internet'


EnCase Forensic Training
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search Hits Records Devices
Home File Extents Permissions References Hash Properties
Entries
Clyde's HDD
C
$Extend
Documents and Settings
All Users
Clyde
Application Data
Cookies
Desktop
Favorites
Local Settings
Application Data
Table Report Gallery Timeline Disk Code
Text Hex Doc Transcript Picture Report Console Details Output
EnScript Hits Filters Conditions Display Queries Text Styles
Text Styles
New... Insert
Export...
Import...
New Folder...
Expand/Contract Space
Expand All
Contract All
start
EncaseExpe... Inbox - Micr... Re: secure ... EnCase For... Internet Ex... cookies form...
12:13

	Name	Filter	In Report	File Ext
1	index.dat			dat
2	clyde@yahoo[1].txt			txt
3	clyde@x10[2].txt			txt
4	clyde@www.off-ro...			txt
5	clyde@www.msn[2...			txt
6	clyde@tucows[1].txt			txt
7	clyde@servedby.a...			txt
8	clyde@passport[2]....			txt
9	clyde@msn[2].txt			txt
10	clyde@lw12fd.law1...			txt
11	clyde@hotmail.msn...			txt
12	clyde@hc2.humand...			txt

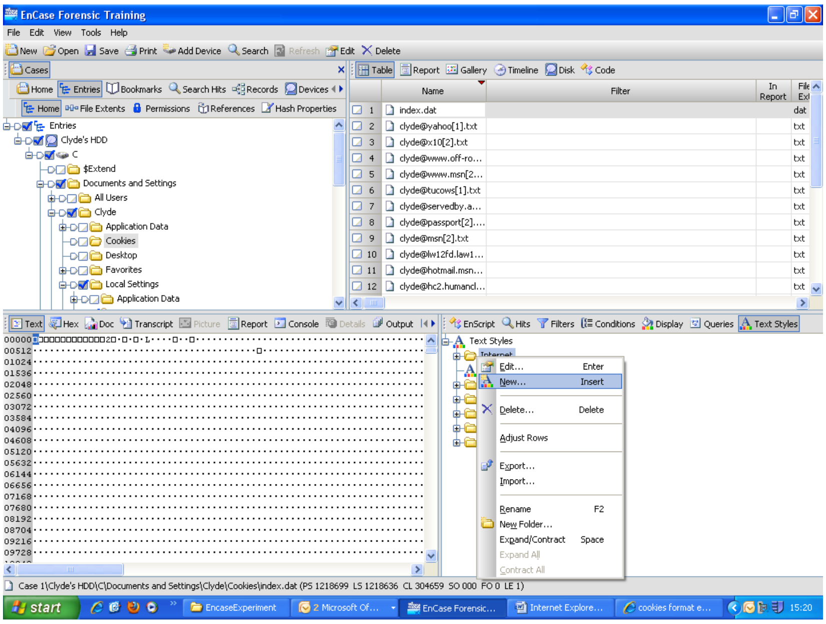
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 000 FO 0 LE 1)


EnCase Forensic Training
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Edit Delete
Cases
Home Entries Bookmarks Search Hits Records Devices
Home File Extents Permissions References Hash Properties
Entries
Clyde's HDD
C
$Extend
Documents and Settings
All Users
Clyde
Application Data
Cookies
Desktop
Favorites
Local Settings
Application Data
Table Report Gallery Timeline Disk Code
Text Hex Doc Transcript Picture Report Console Details Output
EnScript Hits Filters Conditions Display Queries Text Styles
Text Styles
Internet
ISO Latin @ FTP
ISO Latin
ISO Latin Colors
Low Bit - ASCII
RTL Unicode
Unicode
start
EncaseExpe... Inbox - Micr... Re: secure ... EnCase For... Internet Ex... cookies form...
12:14

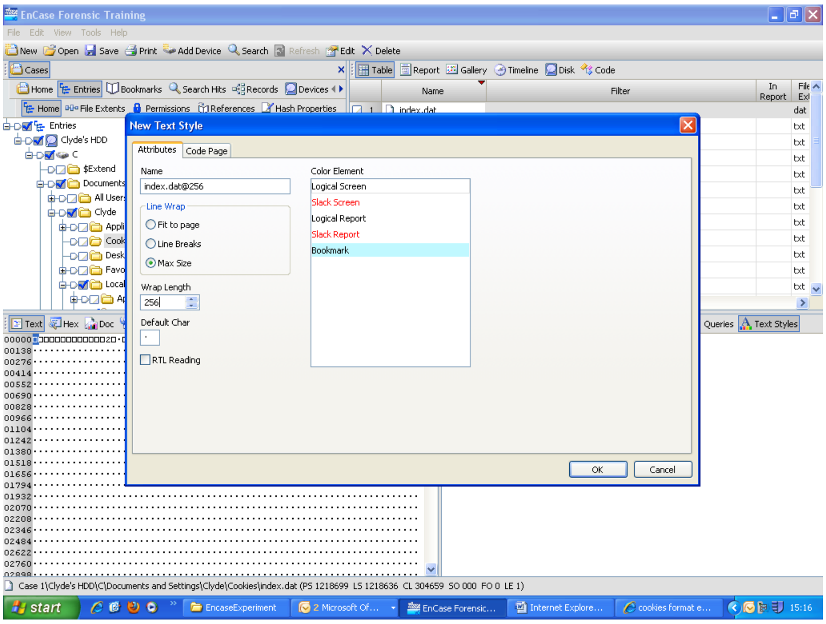
	Name	Filter	In Report	File Ext
1	index.dat			dat
2	clyde@yahoo[1].txt			txt
3	clyde@x10[2].txt			txt
4	clyde@www.off-ro...			txt
5	clyde@www.msn[2...			txt
6	clyde@tucows[1].txt			txt
7	clyde@servedby.a...			txt
8	clyde@passport[2]....			txt
9	clyde@msn[2].txt			txt
10	clyde@lw12fd.law1...			txt
11	clyde@hotmail.msn...			txt
12	clyde@hc2.humand...			txt

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 000 FO 0 LE 1)

5.2 Creating a new text style



Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 000 FO 0 LE 1)


New Text Style

Attributes | Code Page

Name: index.dat@256

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

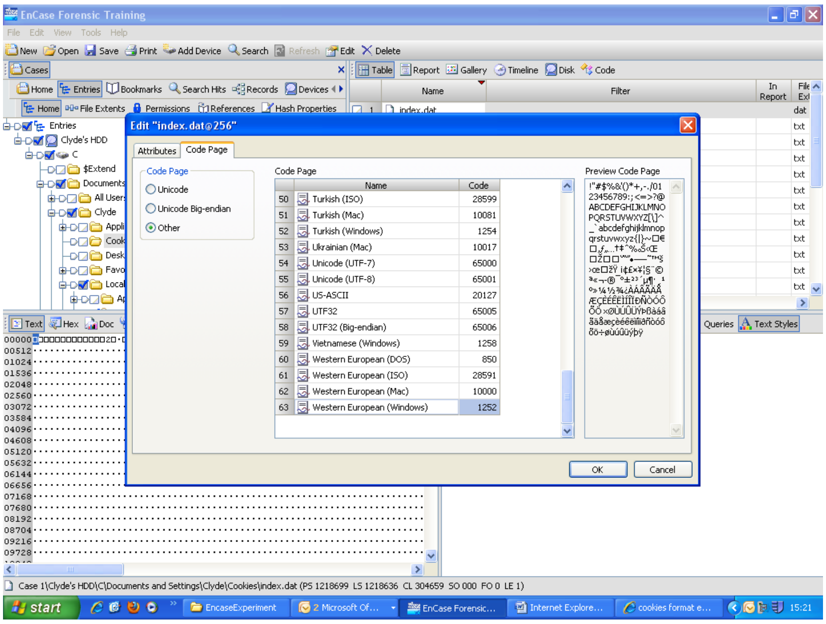
Wrap Length: 256

Default Char: .

□ RTL Reading

Color Element:
Logical Screen
Slack Screen
Logical Report
Slack Report
Bookmark

Then on the code page tab, set the code page to other and then highlight Western European (windows) and click ‘ok’



Edit "index.dat@256"

Code Page

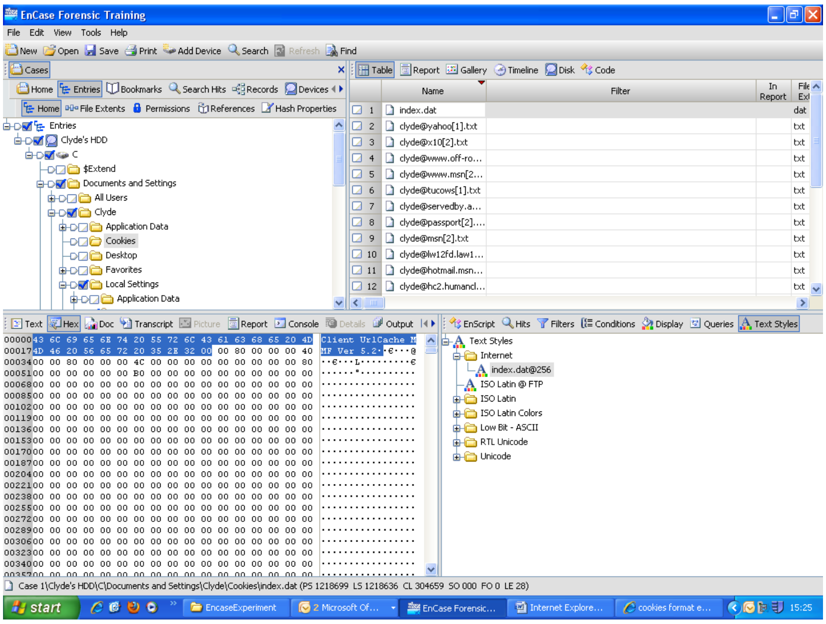
○ Unicode
○ Unicode Big-endian
● Other

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

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 000 FO 0 LE 1)

6. Index.dat file header

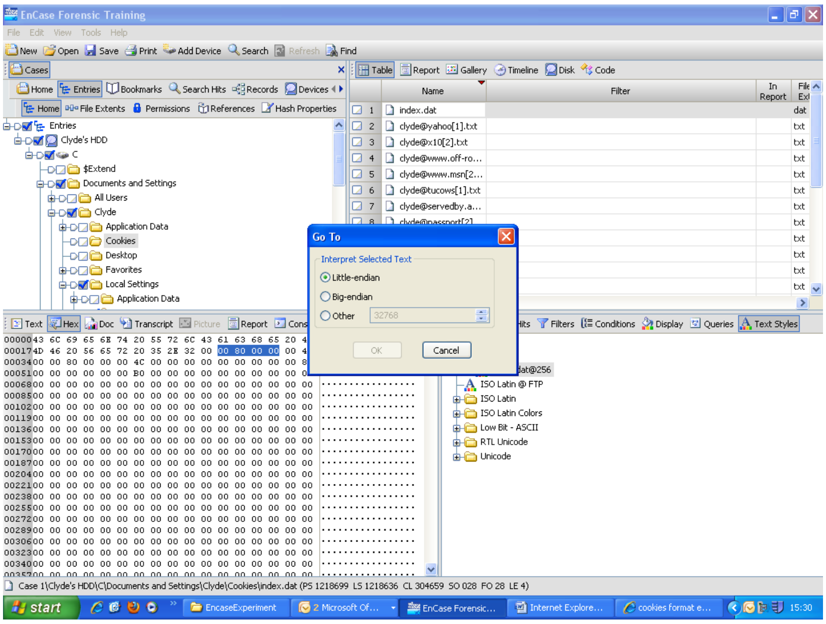


	Name	File Ext
1	index.dat	dat
2	clyde@yahoo[1].txt	txt
3	clyde@x10[2].txt	txt
4	clyde@www.off-ro…	txt
5	clyde@www.msn[2…	txt
6	clyde@tucows[1].txt	txt
7	clyde@servedby.a…	txt
8	clyde@passport[2]….	txt
9	clyde@msn[2].txt	txt
10	clyde@lw12fd.law1…	txt
11	clyde@hotmail.msn…	txt
12	clyde@hc2.humand…	txt

```
0000043 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4D Client UrlCache M
000174D 46 20 56 65 72 20 35 2E 32 00 00 80 00 00 00 40 MF Ver 5.2··€···@
0003400 00 80 00 00 00 4C 00 00 00 00 00 00 00 00 00 80 ··€···L·········€
0005100 00 00 00 00 00 B0 00 00 00 00 00 00 00 00 00 00 ······°··········
0006800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0008500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0010200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0011900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0013600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0015300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0017000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0018700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0020400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0022100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0023800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0025500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0027200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0028900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0030600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0032300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·················
0034000 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\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 000 FO 0 LE 28)

6.1 Filesize: the netx field is the file size of the index.dat file, which is 4 bytes in length


EnCase Forensic Training
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Find
Cases
Home Entries Bookmarks Search Hits Records Devices
Home File Extents Permissions References Hash Properties
Entries
Clyde's HDD
C
$Extend
Documents and Settings
All Users
Clyde
Application Data
Cookies
Desktop
Favorites
Local Settings
Application Data
Table Report Gallery Timeline Disk Code
Name Filter In Report File Ext
Text Hex Doc Transcript Picture Report Cons
Hits Filters Conditions Display Queries Text Styles
ISO Latin @ FTP
ISO Latin
ISO Latin Colors
Low Bit - ASCII
RTL Unicode
Unicode
start
EncaseExperiment
2 Microsoft Of...
EnCase Forensic...
Internet Explore...
cookies format e...
15:30

	Name	File Ext
1	index.dat	dat
2	clyde@yahoo[1].txt	txt
3	clyde@x10[2].txt	txt
4	clyde@www.off-ro...	txt
5	clyde@www.msn[2...	txt
6	clyde@tucows[1].txt	txt
7	clyde@servedby.a...	txt
8	clyde@passport[2]	txt

Go To

Interpret Selected Text

● Little-endian

○ Big-endian

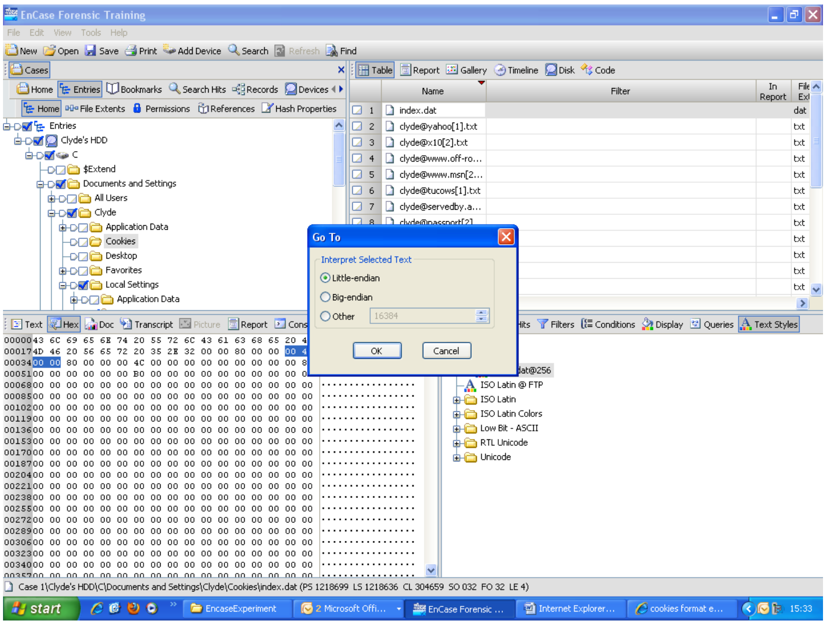
○ Other 32768

OK Cancel

```
0000043 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4
000174D 46 20 56 65 72 20 35 2E 32 00 00 80 00 00 00 4
0003400 00 80 00 00 00 4C 00 00 00 00 00 00 00 00 00 8
0005100 00 00 00 00 00 B0 00 00 00 00 00 00 00 00 00 0
0006800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0008500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0010200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0011900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0013600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0015300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0017000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0018700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0020400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0022100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0023800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0025500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0027200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0028900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0030600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0032300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0034000 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\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 028 FO 28 LE 4)

6.2. pointer to hash, the next field that is 4 bytes in length


EnCase Forensic Training
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Find
Cases
Home Entries Bookmarks Search Hits Records Devices
Home File Extents Permissions References Hash Properties
Entries
Clyde's HDD
C
$Extend
Documents and Settings
All Users
Clyde
Application Data
Cookies
Desktop
Favorites
Local Settings
Application Data
Table Report Gallery Timeline Disk Code
Name Filter In Report File Ext
Text Hex Doc Transcript Picture Report Cons
Hits Filters Conditions Display Queries Text Styles
ISO Latin @ FTP
ISO Latin
ISO Latin Colors
Low Bit - ASCII
RTL Unicode
Unicode
start
EncaseExperiment
2 Microsoft Offi...
EnCase Forensic ...
Internet Explorer...
cookies format e...
15:33

	Name	File Ext
1	index.dat	dat
2	clyde@yahoo[1].txt	txt
3	clyde@x10[2].txt	txt
4	clyde@www.off-ro...	txt
5	clyde@www.msn[2...	txt
6	clyde@tucows[1].txt	txt
7	clyde@servedby.a...	txt
8	clyde@passport[2]	txt

Go To

Interpret Selected Text

● Little-endian

○ Big-endian

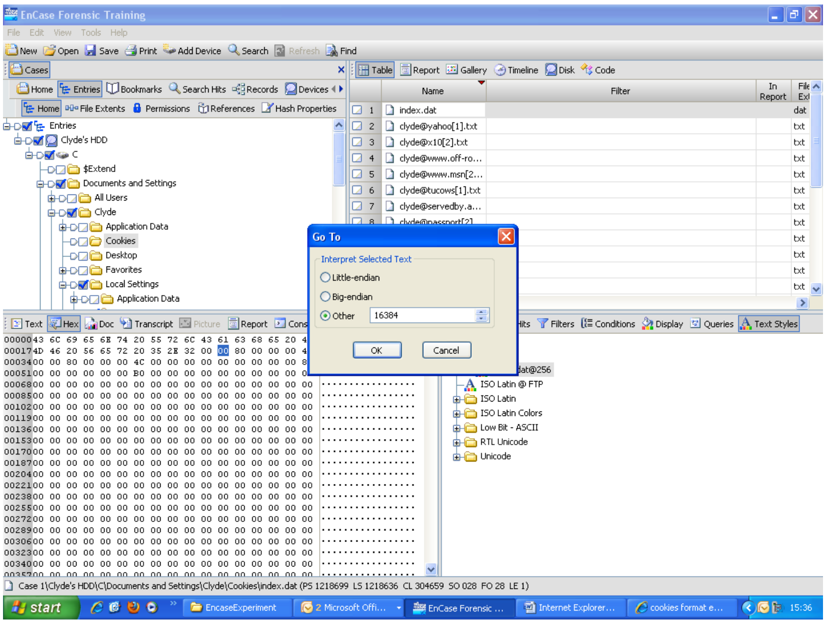
○ Other 16384

OK Cancel

```
0000043 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4
000174D 46 20 56 65 72 20 35 2E 32 00 00 80 00 00 00 4
0003400 00 80 00 00 00 4C 00 00 00 00 00 00 00 00 00 8
0005100 00 00 00 00 00 B0 00 00 00 00 00 00 00 00 00 0
0006800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0008500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0010200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0011900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0013600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0015300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0017000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0018700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0020400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0022100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0023800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0025500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0027200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0028900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0030600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0032300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
0034000 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\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 032 FO 32 LE 4)

6.3 Beginning of the hash table (fileoffset 16384)



Go To

Interpret Selected Text

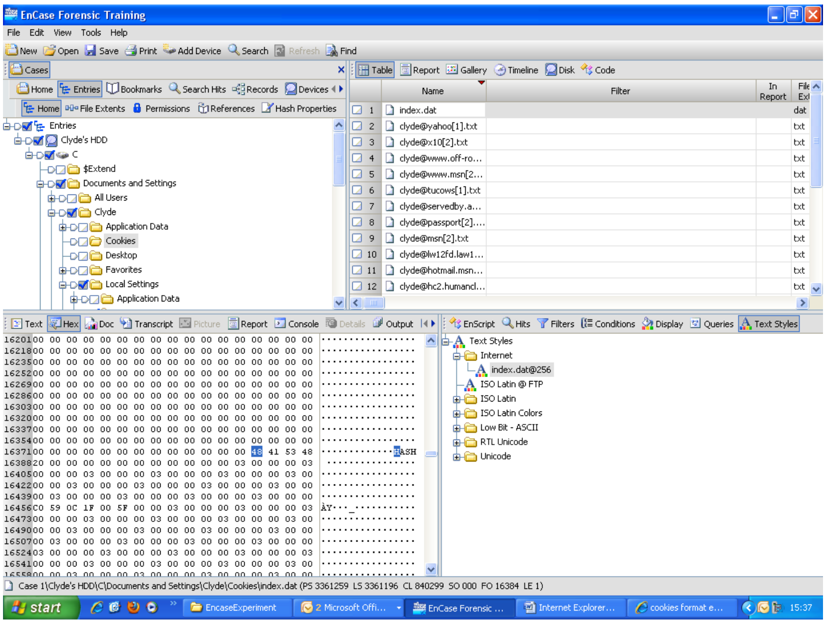
○ Little-endian

○ Big-endian

● Other 16384

```
0000043 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4
000174D 46 20 56 65 72 20 35 2E 32 00 00 80 00 00 00 4
0003400 00 80 00 00 00 4C 00 00 00 00 00 00 00 00 00 8
0005100 00 00 00 00 00 B0 00 00 00 00 00 00 00 00 00 0
0006800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0008500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0010200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0011900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0013600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0015300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0017000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0018700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0020400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0022100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0023800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0025500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0027200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0028900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0030600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0032300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
0034000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
```

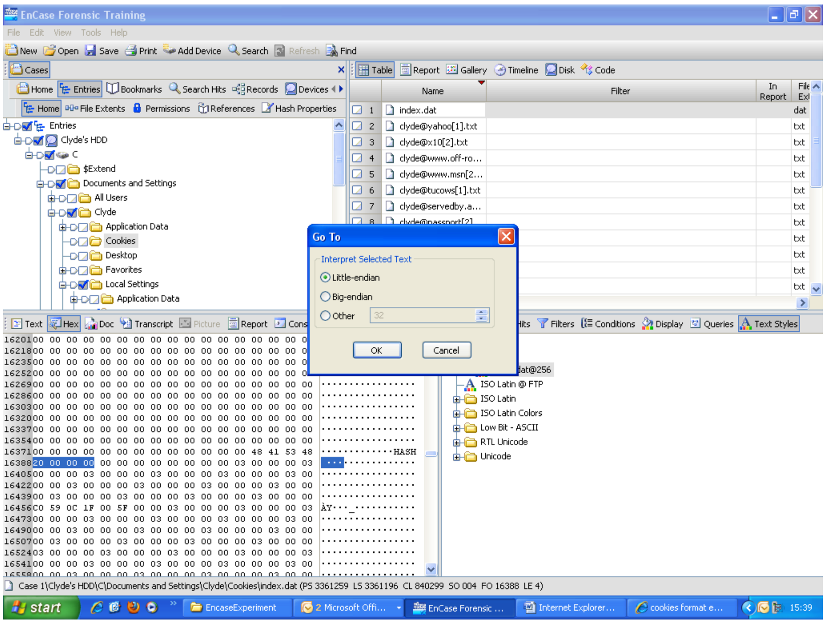
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 1218699 LS 1218636 CL 304659 SO 028 FO 28 LE 1)



```
1620100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1621800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1623500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1625200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1626900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1628600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1630300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1632000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1633700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1635400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ················
1637100 00 00 00 00 00 00 00 00 00 00 00 00 00 48 41 53 48 ·············HASH
1638820 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 03  ················
1640500 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00 ················
1642200 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 ················
1643900 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00 ················
16456C0 59 0C 1F 00 5F 00 00 03 00 00 00 03 00 00 00 03 ÀY··_···········
1647300 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00 ················
1649000 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 ················
1650700 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00 ················
1652403 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 ················
1654100 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00 ················
```

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361259 LS 3361196 CL 840299 SO 000 FO 16384 LE 1)

6.4. Hash table size is 4 bytes in length after hash header



		Name	Filter	In Report	File Ext
□	1	index.dat			dat
□	2	clyde@yahoo[1].txt			txt
□	3	clyde@x10[2].txt			txt
□	4	clyde@www.off-ro...			txt
□	5	clyde@www.msn[2....			txt
□	6	clyde@tucows[1].txt			txt
□	7	clyde@servedby.a...			txt
□	8	clyde@passport[2]...			txt

Go To

Interpret Selected Text

● Little-endian

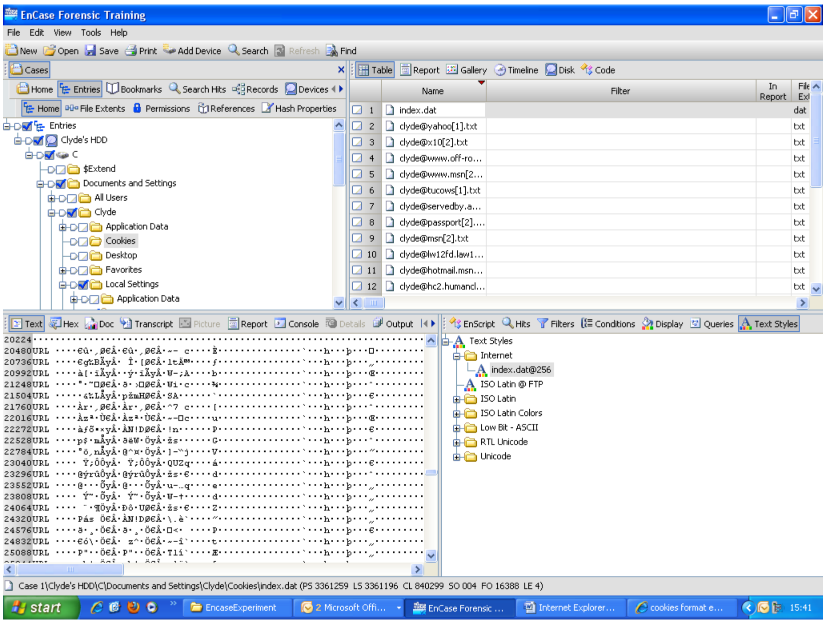
○ Big-endian

○ Other 32

OK Cancel

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361259 LS 3361196 CL 840299 SO 004 FO 16388 LE 4)

7. Index.dat records

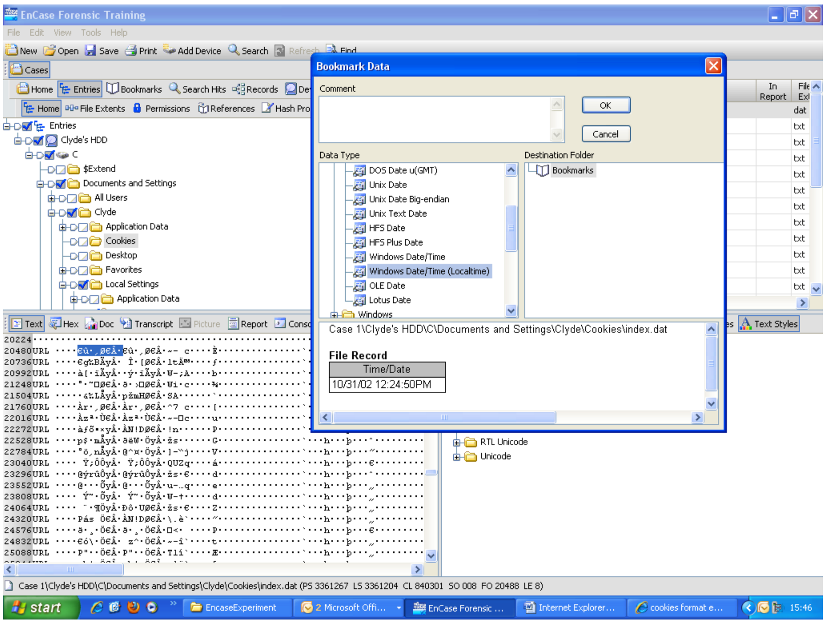


		Name	Filter	In Report	File Ext
□	1	index.dat			dat
□	2	clyde@yahoo[1].txt			txt
□	3	clyde@x10[2].txt			txt
□	4	clyde@www.off-ro...			txt
□	5	clyde@www.msn[2....			txt
□	6	clyde@tucows[1].txt			txt
□	7	clyde@servedby.a...			txt
□	8	clyde@passport[2]....			txt
□	9	clyde@msn[2].txt			txt
□	10	clyde@lw12fd.law1...			txt
□	11	clyde@hotmail.msn....			txt
□	12	clyde@hc2.humancl...			txt

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361259 LS 3361196 CL 840299 SO 004 FO 16388 LE 4)

8. Decoding the windows date/time within the record

To decode cookie modified date/time field within the record, highlight the first 8 bytes of the record. The next byte begins that field.



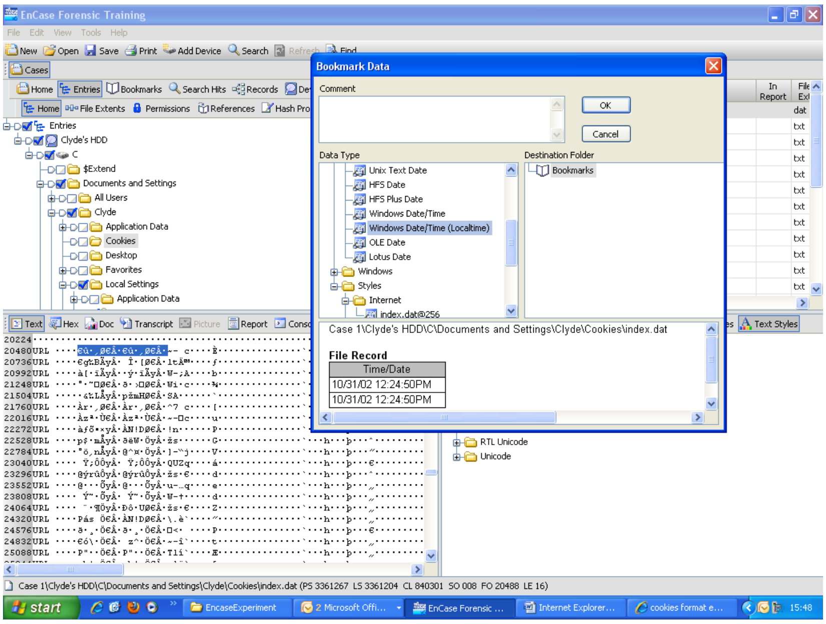
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat

File Record

Time/Date
10/31/02 12:24:50PM

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 008 FO 20488 LE 8)

Or highlight for 16 bytes o decode cookie modified and last accessed date/time



Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat

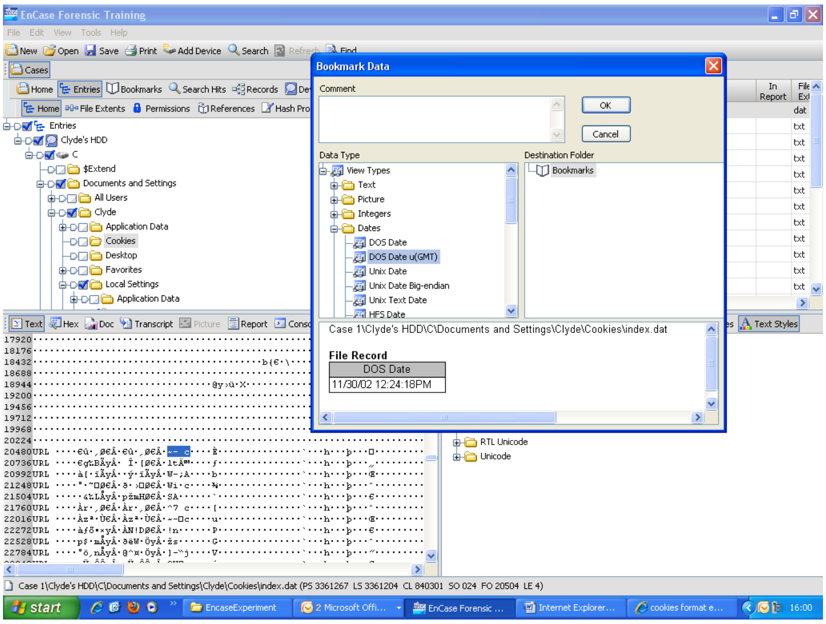
File Record

Time/Date
10/31/02 12:24:50PM
10/31/02 12:24:50PM

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 008 FO 20488 LE 16)

9. Decoding expiration time

9.1. The 4 bytes following the two windows date/time stamps is the cookie expiration date/time. This value is stored in DosDate Time format, which is almost like DOS time and is set to GMT as well.



Bookmark Data

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat

File Record

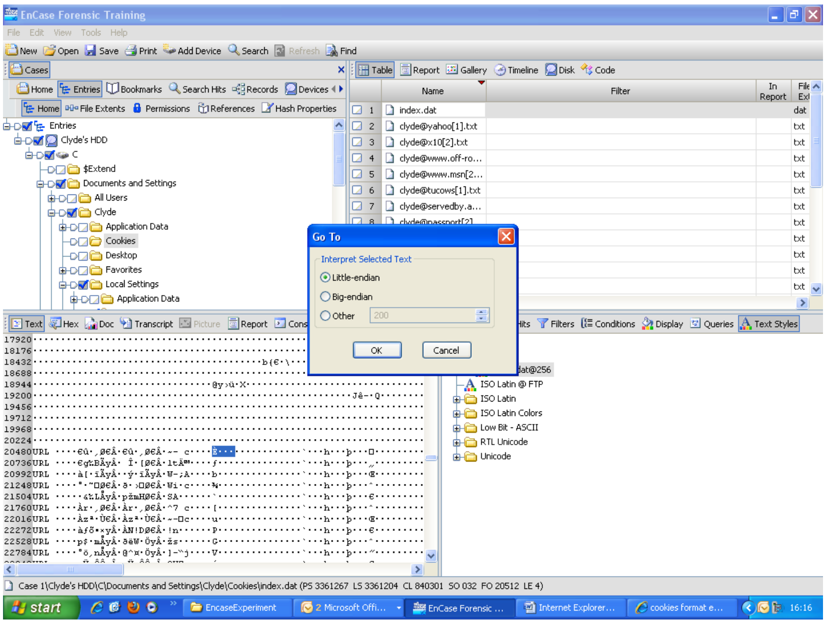
DOS Date
11/30/02 12:24:18PM

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 024 FO 20504 LE 4)

10. Decoding the remaining data within the record

10.1 Filesize of a cookie

Starting at the beginning of the record, sweep 32 bytes to arrive at record offset 32. Highlight for a length of 4 bytes to determine the filesize of the cookie file. The value is hex c8 00 00 00, which is 200 bytes



Go To

Interpret Selected Text

● Little-endian

○ Big-endian

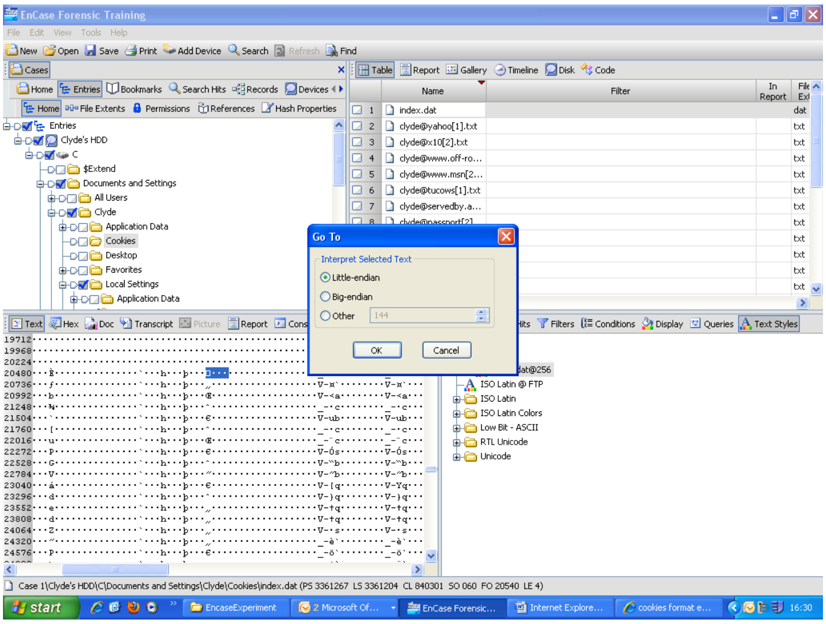
○ Other 200

OK Cancel

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 032 FO 20512 LE 4)

10.2 Filename pointer

A record offset 60 for a length of 4 bytes, you will find a pointer for the record offset for the cookie filename and this decoded as 144



Go To

Interpret Selected Text

● Little-endian

○ Big-endian

○ Other 144

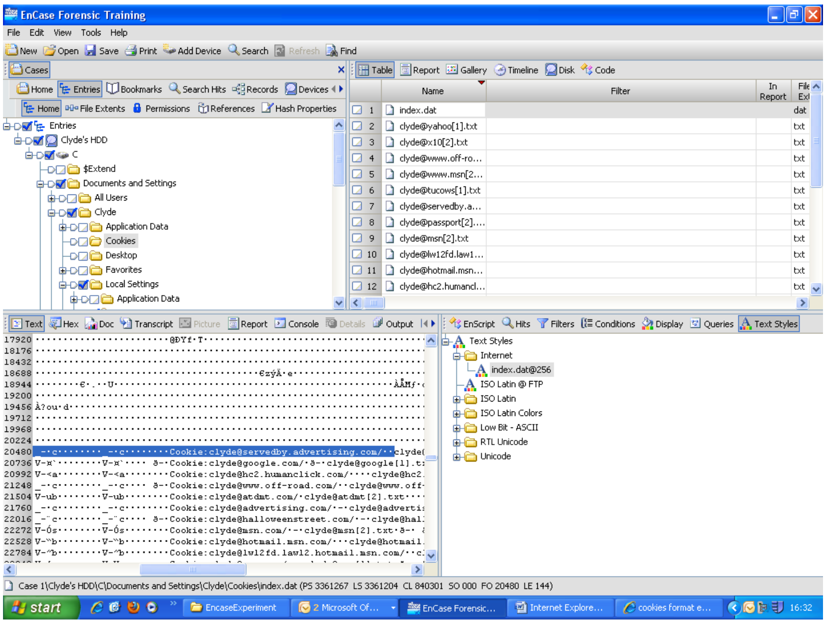
OK Cancel

	Name
1	index.dat
2	clyde@yahoo[1].txt
3	clyde@x10[2].txt
4	clyde@www.off-ro…
5	clyde@www.msn[2…
6	clyde@tucows[1].txt
7	clyde@servedby.a…

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 060 FO 20540 LE 4)

10.3 Filename of cookies

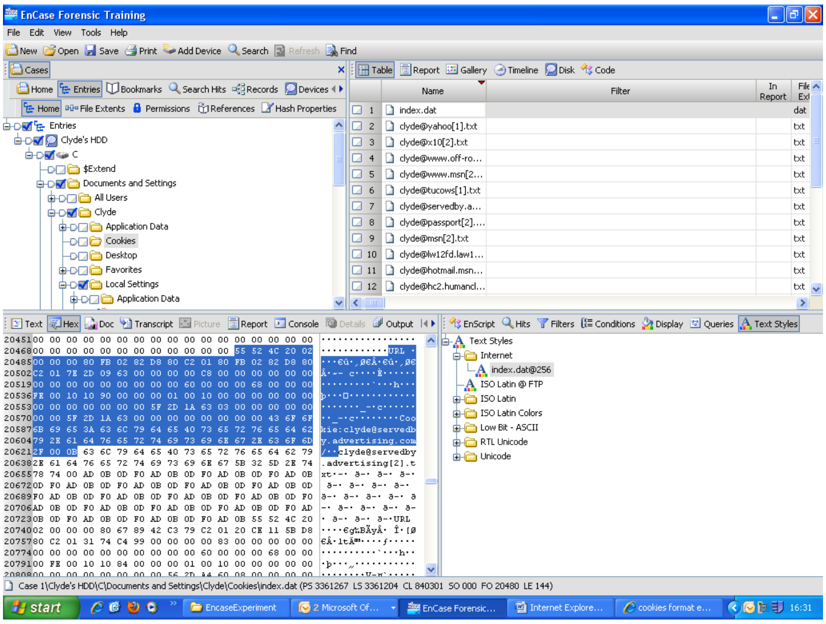
You can start from the beginning of the record and sweep for 144 and the next byte will be the start of the filename



	Name
1	index.dat
2	clyde@yahoo[1].txt
3	clyde@x10[2].txt
4	clyde@www.off-ro…
5	clyde@www.msn[2…
6	clyde@tucows[1].txt
7	clyde@servedby.a…
8	clyde@passport[2]….
9	clyde@msn[2].txt
10	clyde@lw12fd.law1…
11	clyde@hotmail.msn…
12	clyde@hc2.humancl…

```
20480 _-·c········ _-·c········Cookie:clyde@servedby.advertising.com/··clyde
20736 V-¤`········V-¤`····  ð-·Cookie:clyde@google.com/·ð-·clyde@google[1].t
20992 V-<a········V-<a········Cookie:clyde@hc2.humanclick.com/····clyde@hc2.
21248 _-·c········_-·c····  ð-·Cookie:clyde@www.off-road.com/··clyde@www.off-
21504 V-ub········V-ub········Cookie:clyde@atdmt.com/·clyde@atdmt[2].txt····
21760 _-·c········_-·c········Cookie:clyde@advertising.com/·-·clyde@advertis
22016 _-¨c········_-¨c····  ð-·Cookie:clyde@halloweenstreet.com/·-·clyde@hal
22272 V-Ós········V-Ós········Cookie:clyde@msn.com/·-·clyde@msn[2].txt·ð-·
22528 V-‵b········V-‵b········Cookie:clyde@hotmail.msn.com/···clyde@hotmail.
22784 V-‴b········V-‴b········Cookie:clyde@lwl2fd.lawl2.hotmail.msn.com/··c
```

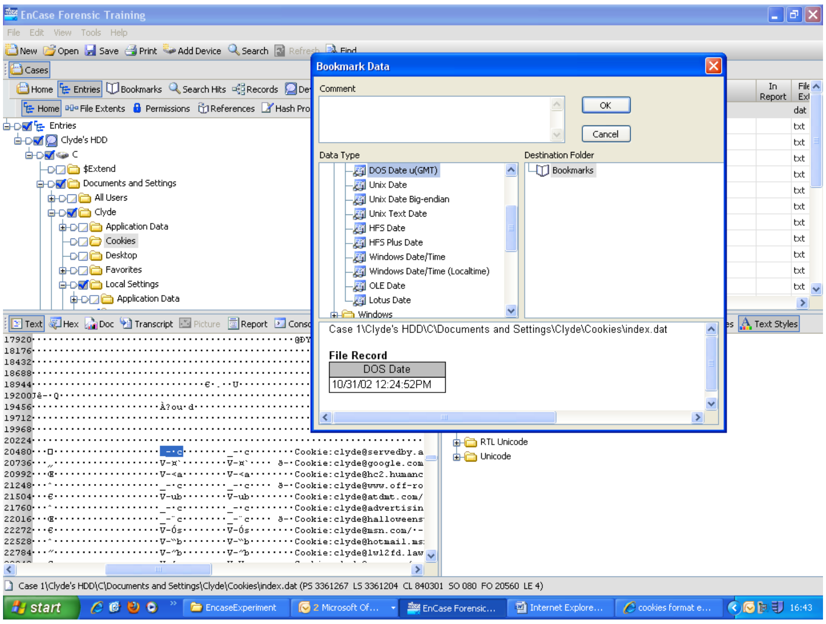
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 000 FO 20480 LE 144)



```
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 000 FO 20480 LE 144)
```

10.4 Cookie file last accessed time

To find cookie file last accessed time, at record offset 80 for a length of 4 bytes, you will find another DosDateTime field, called last accessed time.



Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat

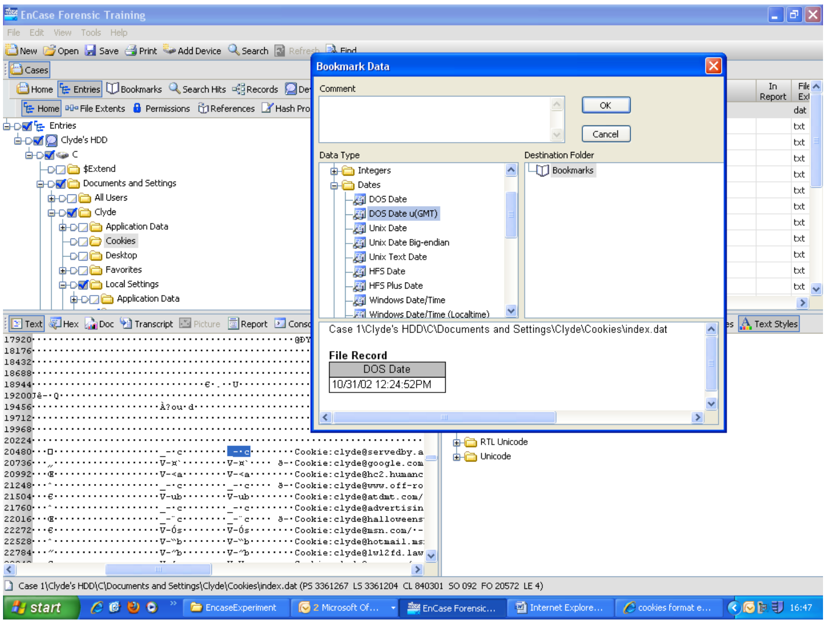
File Record

DOS Date
10/31/02 12:24:52PM

```
Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 080 FO 20560 LE 4)
```

10.5 Cookie file created time

At record offset 92 for a length 4 bytes and you will find the cookie file created time



Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat

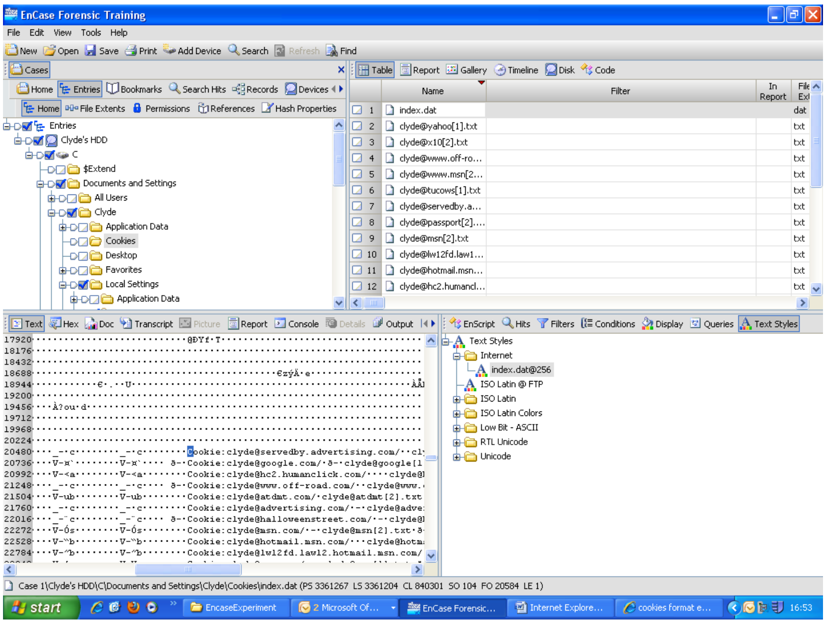
File Record

DOS Date
10/31/02 12:24:52PM

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 092 FO 20572 LE 4)

10.6 At record offset 104, you will find the following data structure:

Cookie:[username]@[website URL]. Ends in hex 00.



	Name	Filter	In Report	File Ext
1	index.dat			dat
2	clyde@yahoo[1].txt			txt
3	clyde@x10[2].txt			txt
4	clyde@www.off-ro…			txt
5	clyde@www.msn[2…			txt
6	clyde@tucows[1].txt			txt
7	clyde@servedby.a…			txt
8	clyde@passport[2]….			txt
9	clyde@msn[2].txt			txt
10	clyde@lw12fd.law1…			txt
11	clyde@hotmail.msn…			txt
12	clyde@hc2.humancl…			txt

Case 1\Clyde's HDD\C\Documents and Settings\Clyde\Cookies\index.dat (PS 3361267 LS 3361204 CL 840301 SO 104 FO 20584 LE 1)