Module B13: IE Browser Forensics Analysis

Pre-requisite Knowledge and Skills:

1.

Learning Objectives

1. .

Recommended Running Environment/Tools:

1. Windows OS
2. AccessData FTK Imager
3. Registry Eidtor

Material:

1.

Video Lecture:

1. N/A

Lab Assessment:

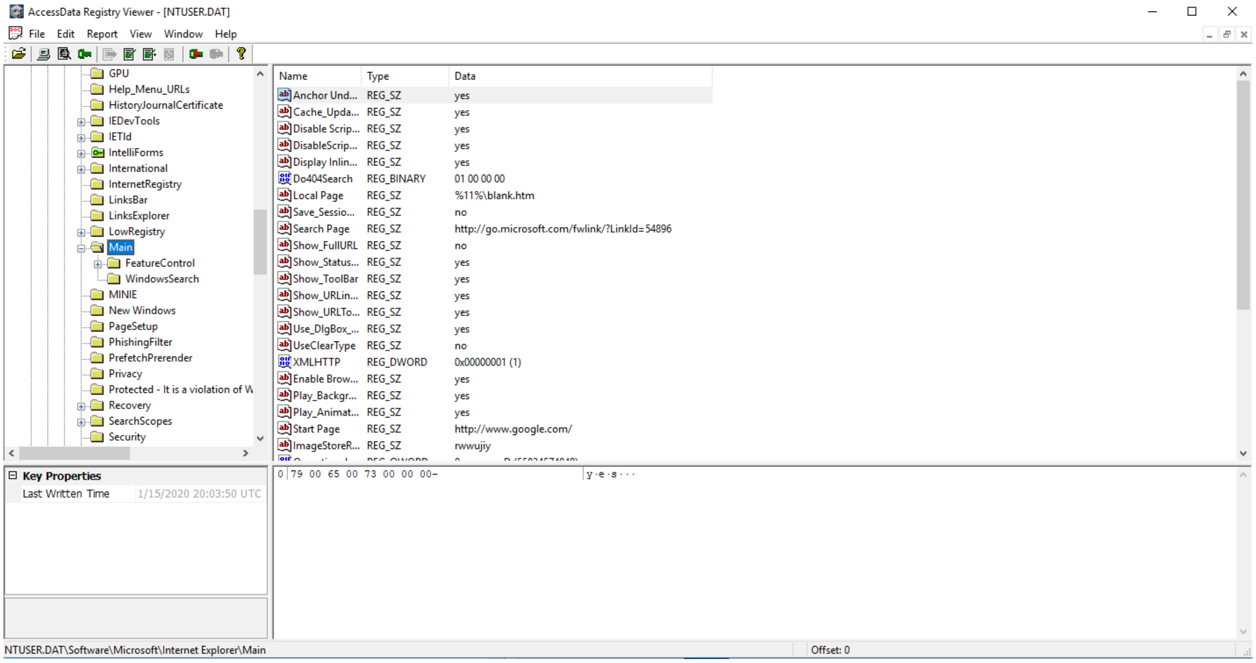
Lab Instructions:

1. In the FTK Explore tab, Locate the NTUSER.DAT file for the Instruct account.

a. Right-click NTUSER.DAT, then select Open in Registry Viewer.

b. In the Key pane, expand the **Software\Microsoft\Internet Explorer\Main** key stricture.

c. Select the Main key.



Name	Type	Data
Anchor Und...	REG_SZ	yes
Cache_Upda...	REG_SZ	yes
Disable Scrip...	REG_SZ	yes
DisableScrip...	REG_SZ	yes
Display Inlin...	REG_SZ	yes
Do404Search	REG_BINARY	01 00 00 00
Local Page	REG_SZ	%11%\blank.htm
Save_Sessio...	REG_SZ	no
Search Page	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=54896
Show_FullURL	REG_SZ	no
Show_Status...	REG_SZ	yes
Show_ToolBar	REG_SZ	yes
Show_URLin...	REG_SZ	yes
Show_URLTo...	REG_SZ	yes
Use_DlgBox_...	REG_SZ	yes
UseClearType	REG_SZ	no
XMLHTTP	REG_DWORD	0x00000001 (1)
Enable Brow...	REG_SZ	yes
Play_Backgr...	REG_SZ	yes
Play_Animat...	REG_SZ	yes
Start Page	REG_SZ	http://www.google.com/
ImageStoreR...	REG_SZ	rwwujiy

Key Properties

Last Written Time	1/15/2020 20:03:50 UTC

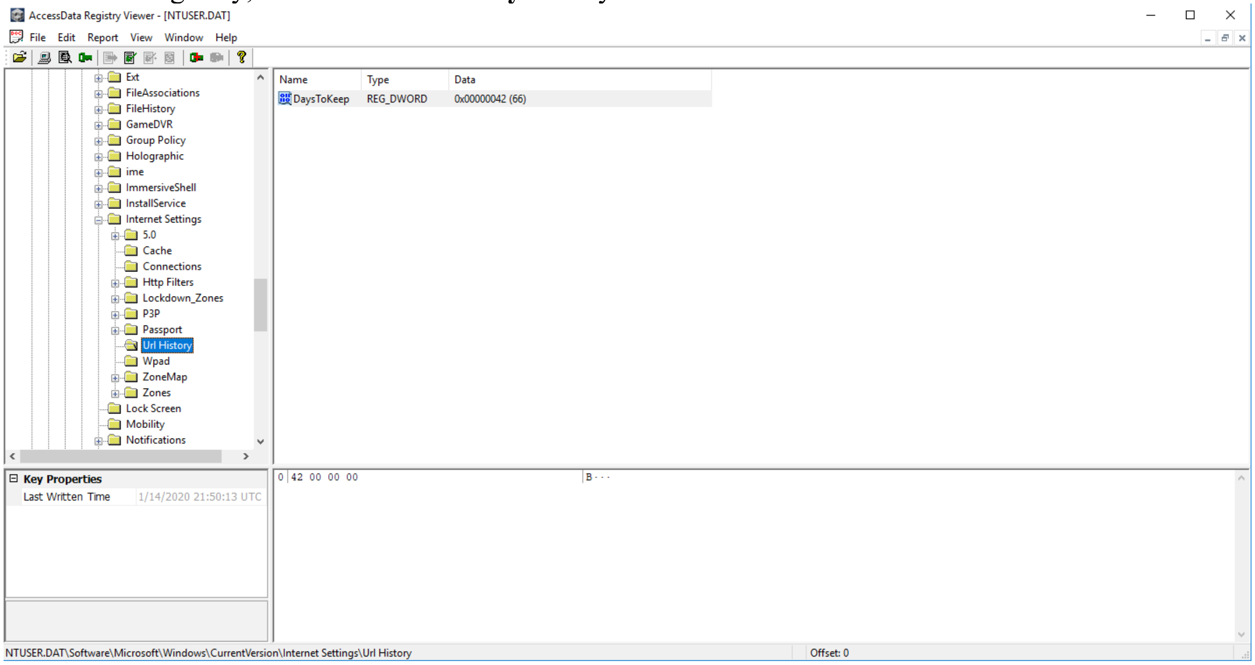
```
0 | 79  00  65  00  73  00  00  00-          y·e·s···
```

NTUSER.DAT\Software\Microsoft\Internet Explorer\Main   Offset: 0

d. Note the entries in the Value List pane in the upper-right comer.

e. Scroll through the values.

f. In the key pane, expand **Software\Microsoft\Windows\CurrentVersion\Internet Settings**. In the Internet Settings key, select the **Url History** subkey.



Name	Type	Data
DaysToKeep	REG_DWORD	0x00000042 (66)

Key Properties

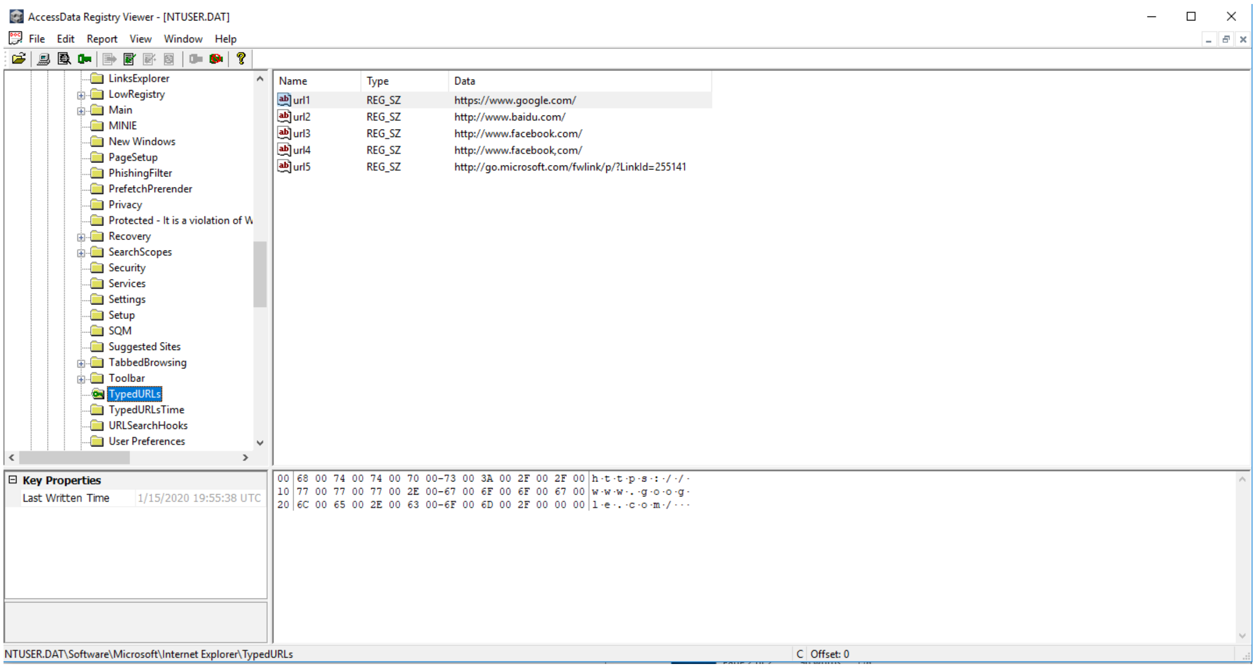
Last Written Time	1/14/2020 21:50:13 UTC

```
0 | 42  00  00  00          B···
```

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Url History   Offset: 0

g. Note: The DaysToKeep value in the Value List pane. DaysToKeep 0x00000042 (66)

h. In the Key pane, expand **Software\Microsoft\Internet Explorer\TypedURLs.**



Name	Type	Data
url1	REG_SZ	https://www.google.com/
url2	REG_SZ	http://www.baidu.com/
url3	REG_SZ	http://www.facebook.com/
url4	REG_SZ	http://www.facebook.com/
url5	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

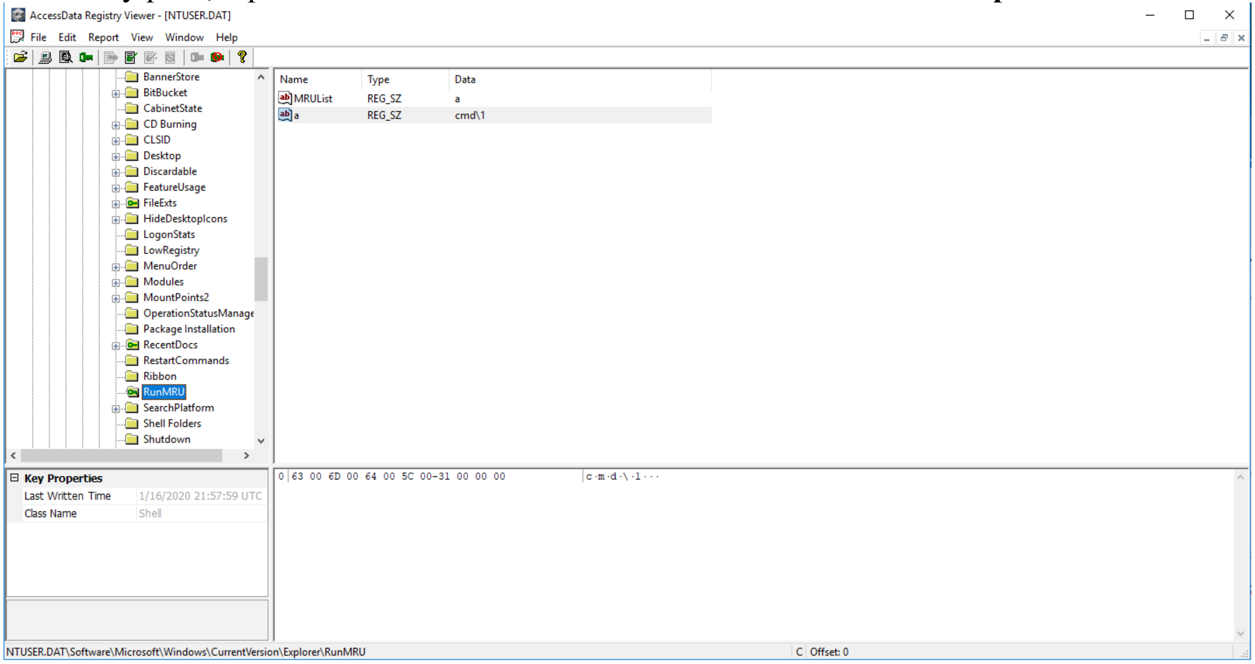
Last Written Time	1/15/2020 19:55:38 UTC

```
00 68 00 74 00 74 00 70 00-73 00 3A 00 2F 00 2F 00 h·t·t·p·s·:·/·/·
10 77 00 77 00 77 00 2E 00-67 00 6F 00 6F 00 67 00 w·w·w·.·g·o·o·g·
20 6C 00 65 00 2E 00 63 00-6F 00 6D 00 2F 00 00 00 l·e·.·c·o·m·/···
```

NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs   C Offset: 0

Note: The web address entires in the Value List pane.

i. In the Key pane, expand **Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**



Name	Type	Data
MRUList	REG_SZ	a
a	REG_SZ	cmd\1

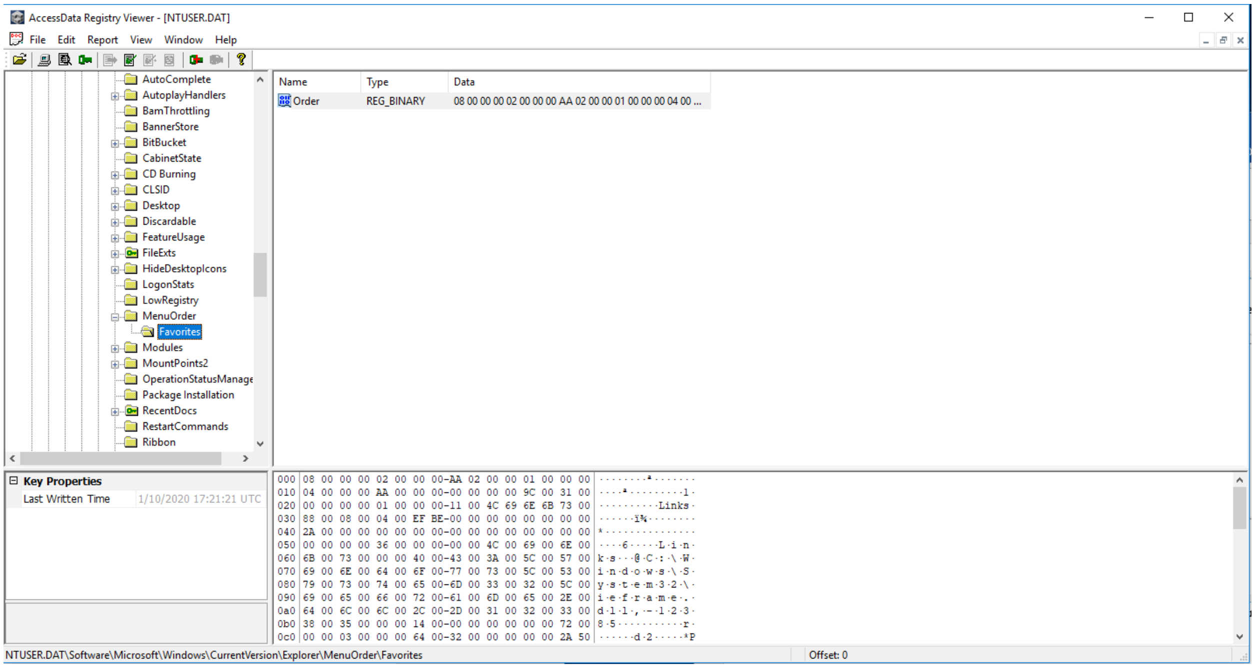
Last Written Time	1/16/2020 21:57:59 UTC
Class Name	Shell

```
0 63 00 6D 00 64 00 5C 00-31 00 00 00              c·m·d·\·1···
```

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU   C Offset: 0

Note: The history of most recently used commands from the Run command on the Start menu are stored

j. Expand **Software\Microsoft\Windows\Current Version\Explorer\MenuOrder\Favorites**, then expand the Instruct Favorites subkey.



Name	Type	Data
Order	REG_BINARY	08 00 00 00 02 00 00 00 AA 02 00 00 01 00 00 00 04 00 ...

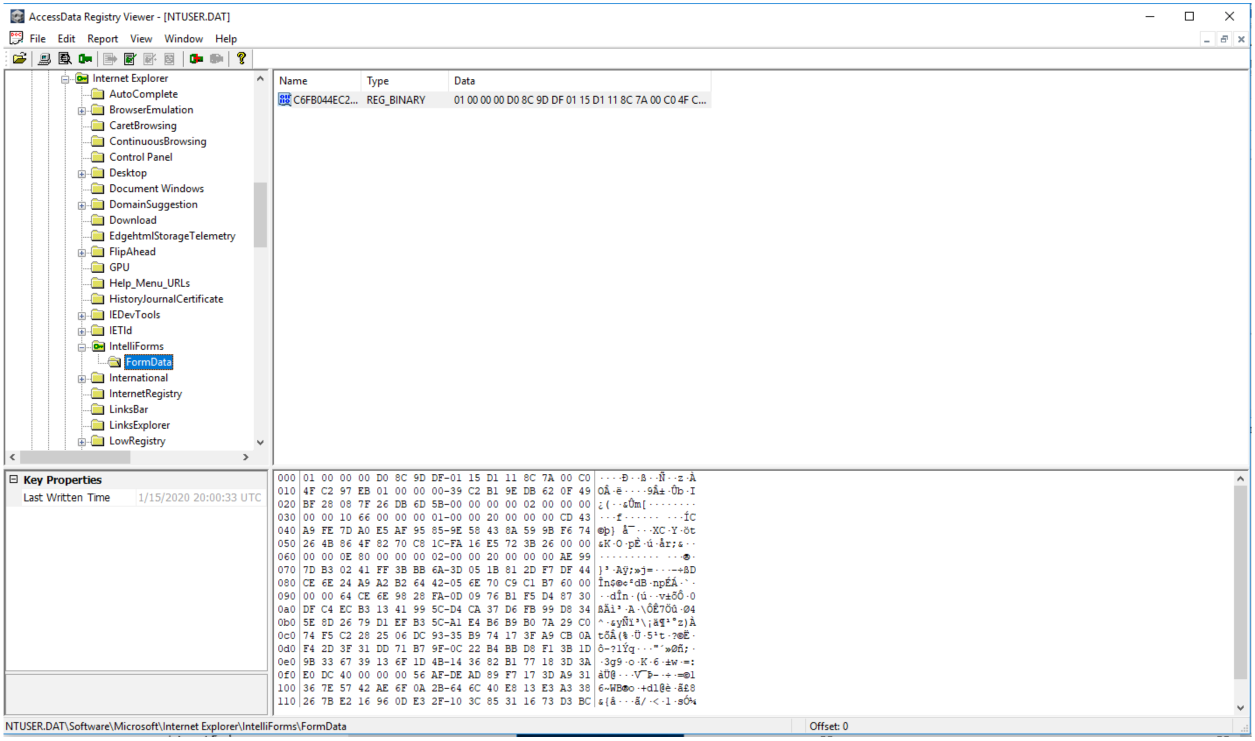
Key Properties
Last Written Time 1/10/2020 17:21:21 UTC

```
000 08 00 00 00 02 00 00 00-AA 02 00 00 01 00 00 00  ········ª·······
010 04 00 00 00 AA 00 00 00-00 00 00 00 9C 00 31 00  ····ª·········1·
020 00 00 00 00 01 00 00 00-11 00 4C 69 6E 6B 73 00  ··········Links·
030 88 00 08 00 04 00 EF BE-00 00 00 00 00 00 00 00  ······ï¾········
040 2A 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *···············
050 00 00 00 00 36 00 00 00-00 00 4C 00 69 00 6E 00  ····6·····L·i·n·
060 6B 00 73 00 00 00 40 00-43 00 3A 00 5C 00 57 00  k·s···@·C·:·\·W·
070 69 00 6E 00 64 00 6F 00-77 00 73 00 5C 00 53 00  i·n·d·o·w·s·\·S·
080 79 00 73 00 74 00 65 00-6D 00 33 00 32 00 5C 00  y·s·t·e·m·3·2·\·
090 69 00 65 00 66 00 72 00-61 00 6D 00 65 00 2E 00  i·e·f·r·a·m·e·.·
0a0 64 00 6C 00 6C 00 2C 00-2D 00 31 00 32 00 33 00  d·l·l·,·-·1·2·3·
0b0 38 00 35 00 00 00 14 00-00 00 00 00 00 00 72 00  8·5···········r·
0c0 00 00 03 00 00 00 64 00-32 00 00 00 00 00 2A 50  ······d·2·····*P
```

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites Offset: 0

Note: The subkey structure and naming conventions. The subkeys have the same names as the folders in the pc1\Favorites directory in Windows.

k. Expand the **Software\Micosoft\Internet Explporer\IntelliForms**



Name	Type	Data
C6FB044EC2...	REG_BINARY	01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C...

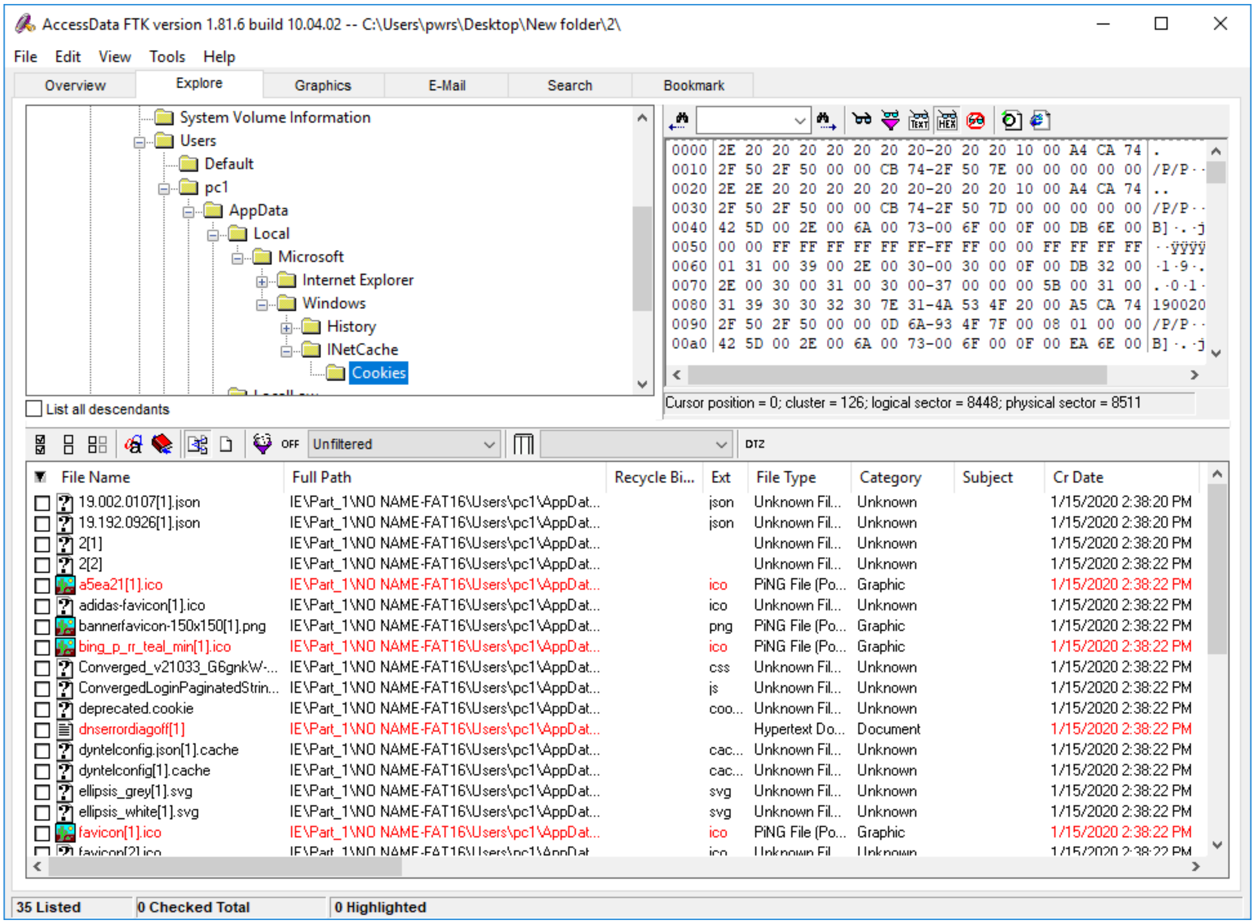
Key Properties
Last Written Time 1/15/2020 20:00:33 UTC

```
000 01 00 00 00 D0 8C 9D DF-01 15 D1 11 8C 7A 00 C0  ····Ð··ß··Ñ··z·À
010 4F C2 97 EB 01 00 00 00-39 C2 B1 9E DB 62 0F 49  OÂ·ë····9Â±·Ûb·I
020 BF 28 08 7F 26 DB 6D 5B-00 00 00 00 02 00 00 00  ¿(··&Ûm[········
030 00 00 10 66 00 00 00 01-00 00 20 00 00 00 CD 43  ···f······ ···ÍC
040 A9 FE 7D A0 E5 AF 95 85-9E 58 43 8A 59 9B F6 74  ©þ} å¯···XC·Y·öt
050 26 4B 86 4F 82 70 C8 1C-FA 16 E5 72 3B 26 00 00  &K·O·pÈ·ú·år;&··
060 00 00 0E 80 00 00 00 02-00 00 20 00 00 00 AE 99  ·········· ···®·
070 7D B3 02 41 FF 3B BB 6A-3D 05 1B 81 2D F7 DF 44  }³·Aÿ;»j=···-÷ßD
080 CE 6E 24 A9 A2 B2 64 42-05 6E 70 C9 C1 B7 60 00  În$©¢²dB·npÉÁ·`·
090 00 00 64 CE 6E 98 28 FA-0D 09 76 B1 F5 D4 87 30  ··dÎn·(ú··v±õÔ·0
0a0 DF C4 EC B3 13 41 99 5C-D4 CA 37 D6 FB 99 D8 34  ßÄì³·A·\ÔÊ7Öû·Ø4
0b0 5E 8D 26 79 D1 EF B3 5C-A1 E4 B6 B9 B0 7A 29 C0  ^·&yÑï³\¡ä¶¹°z)À
0c0 74 F5 C2 28 25 06 DC 93-35 B9 74 17 3F A9 CB 0A  tõÂ(%·Ü·5¹t·?©Ë·
0d0 F4 2D 3F 31 DD 71 B7 9F-0C 22 B4 BB D8 F1 3B 1D  ô-?1Ýq···"´»Øñ;·
0e0 9B 33 67 39 13 6F 1D 4B-14 36 82 B1 77 18 3D 3A  ·3g9·o·K·6·±w·=:
0f0 E0 DC 40 00 00 00 56 AF-DE AD 89 F7 17 3D A9 31  àÜ@···V¯Þ-·÷·=©1
100 36 7E 57 42 AE 6F 0A 2B-64 6C 40 E8 13 E3 A3 38  6~WB®o·+dl@è·ã£8
110 26 7B E2 16 96 0D E3 2F-10 3C 85 31 16 73 D3 BC  &{â···ã/·<·1·sÓ¼
```

NTUSER.DAT\Software\Microsoft\Internet Explorer\IntelliForms\FormData Offset: 0

Note: The encrypted values for the saved webpage authentication user names/passwords and search queries.

2. In the Explorer tab, expand the following path: **Users\pc1\AppData\Local\Microsoft\Windows\INetCache\Cookies**



```
0000 2E 20 20 20 20 20 20 20-20 20 20 10 00 A4 CA 74 .
0010 2F 50 2F 50 00 00 CB 74-2F 50 7E 00 00 00 00 00 /P/P··
0020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 A4 CA 74 ..
0030 2F 50 2F 50 00 00 CB 74-2F 50 7D 00 00 00 00 00 /P/P··
0040 42 5D 00 2E 00 6A 00 73-00 6F 00 0F 00 DB 6E 00 B]·.·j
0050 00 00 FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ··ÿÿÿÿ
0060 01 31 00 39 00 2E 00 30-00 30 00 0F 00 DB 32 00 ·1·9·.
0070 2E 00 30 00 31 00 30 00-37 00 00 00 5B 00 31 00 .·0·1·
0080 31 39 30 30 32 30 7E 31-4A 53 4F 20 00 A5 CA 74 190020
0090 2F 50 2F 50 00 00 0D 6A-93 4F 7F 00 08 01 00 00 /P/P··
00a0 42 5D 00 2E 00 6A 00 73-00 6F 00 0F 00 EA 6E 00 B]·.·j
```

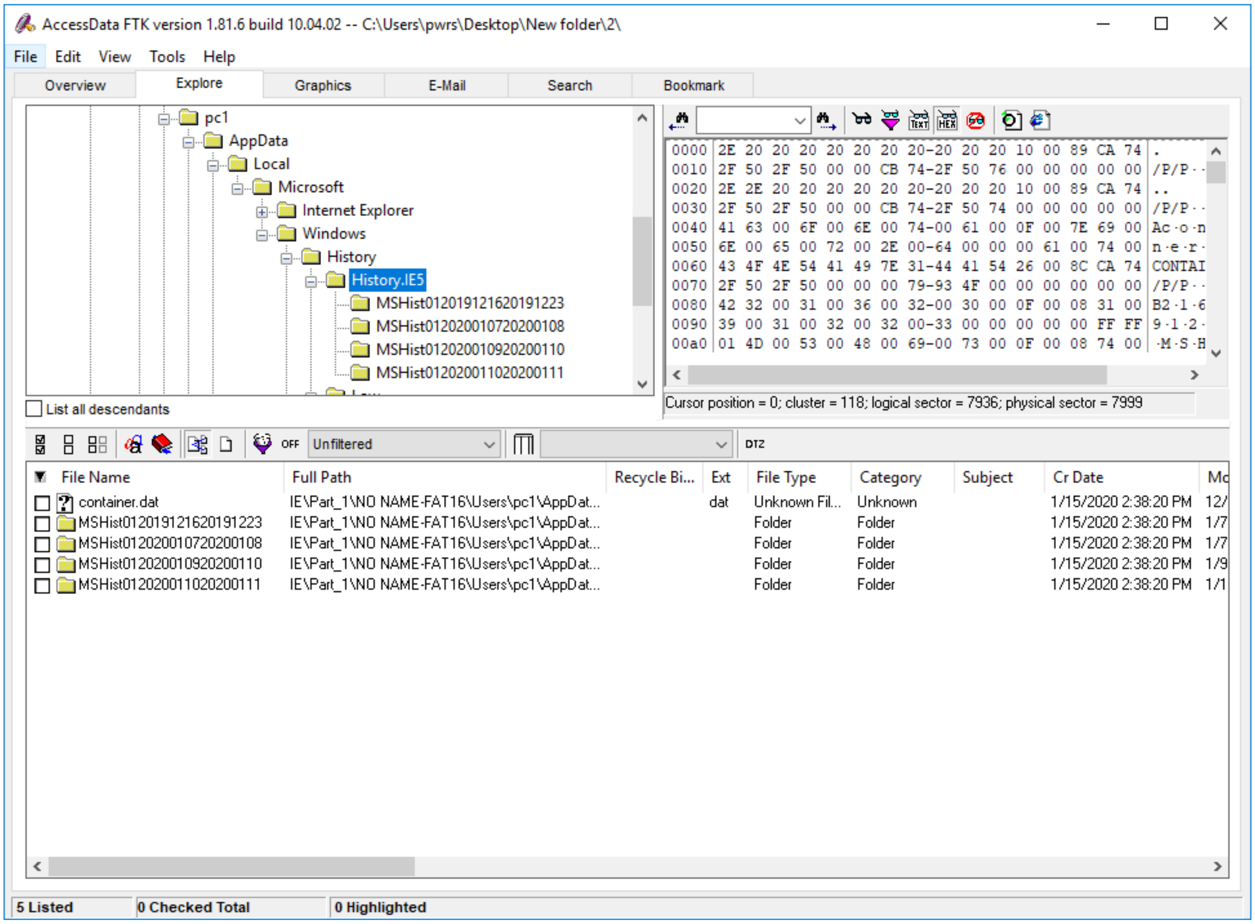
Cursor position = 0; cluster = 126; logical sector = 8448; physical sector = 8511

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
□ 19.002.0107[1].json	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		json	Unknown Fil...	Unknown		1/15/2020 2:38:20 PM
□ 19.192.0926[1].json	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		json	Unknown Fil...	Unknown		1/15/2020 2:38:20 PM
□ 2[1]	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...			Unknown Fil...	Unknown		1/15/2020 2:38:20 PM
□ 2[2]	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...			Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ a5ea21[1].ico	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		ico	PiNG File (Po...	Graphic		1/15/2020 2:38:22 PM
□ adidas-favicon[1].ico	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		ico	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ bannerfavicon-150x150[1].png	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		png	PiNG File (Po...	Graphic		1/15/2020 2:38:22 PM
□ bing_p_rr_teal_min[1].ico	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		ico	PiNG File (Po...	Graphic		1/15/2020 2:38:22 PM
□ Converged_v21033_G6gnkW-...	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		css	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ ConvergedLoginPaginatedStrin...	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		js	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ deprecated.cookie	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		coo...	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ dnserrordiagoff[1]	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...			Hypertext Do...	Document		1/15/2020 2:38:22 PM
□ dyntelconfig.json[1].cache	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		cac...	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ dyntelconfig[1].cache	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		cac...	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ ellipsis_grey[1].svg	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		svg	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ ellipsis_white[1].svg	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		svg	Unknown Fil...	Unknown		1/15/2020 2:38:22 PM
□ favicon[1].ico	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		ico	PiNG File (Po...	Graphic		1/15/2020 2:38:22 PM
□ favicon[2].ico	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat		ico	Unknown Fil	Unknown		1/15/2020 2:38:22 PM

35 Listed | 0 Checked Total | 0 Highlighted

Note: The individual cookie entries in the File List pane, resulting from the Expand Compound Files evidence processing option.

3. In the FTK Explore tab, expand the following path for the Instruct user account: User\pc1\AppData\Local\Microsoft\Windows\History\History.IE5



```
0000 2E 20 20 20 20 20 20 20-20 20 20 10 00 89 CA 74 .
0010 2F 50 2F 50 00 00 CB 74-2F 50 76 00 00 00 00 00 /P/P··
0020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 89 CA 74 ..
0030 2F 50 2F 50 00 00 CB 74-2F 50 74 00 00 00 00 00 /P/P··
0040 41 63 00 6F 00 6E 00 74-00 61 00 0F 00 7E 69 00 Ac·o·n
0050 6E 00 65 00 72 00 2E 00-64 00 00 00 61 00 74 00 n·e·r·
0060 43 4F 4E 54 41 49 7E 31-44 41 54 26 00 8C CA 74 CONTAI
0070 2F 50 2F 50 00 00 00 79-93 4F 00 00 00 00 00 00 /P/P··
0080 42 32 00 31 00 36 00 32-00 30 00 0F 00 08 31 00 B2·1·6
0090 39 00 31 00 32 00 32 00-33 00 00 00 00 00 FF FF 9·1·2·
00a0 01 4D 00 53 00 48 00 69-00 73 00 0F 00 08 74 00  ·M·S·H
```

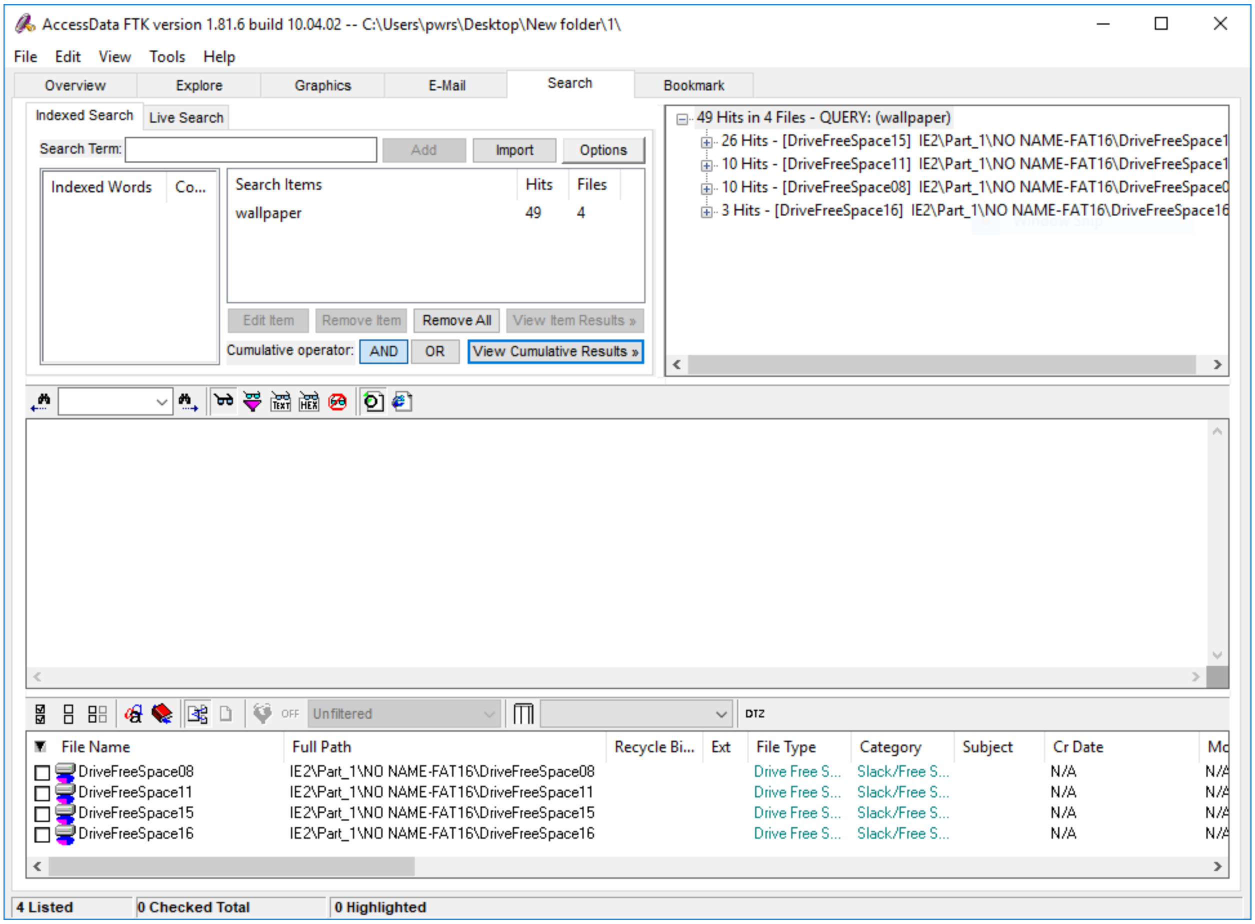
Cursor position = 0; cluster = 118; logical sector = 7936; physical sector = 7999

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mo
□ container.dat	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...		dat	Unknown Fil...	Unknown		1/15/2020 2:38:20 PM	12/
□ MSHist012019121620191223	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...			Folder	Folder		1/15/2020 2:38:20 PM	1/7
□ MSHist012020010720200108	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...			Folder	Folder		1/15/2020 2:38:20 PM	1/7
□ MSHist012020010920200110	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...			Folder	Folder		1/15/2020 2:38:20 PM	1/9
□ MSHist012020011020200111	IE\Part_1\NO NAME-FAT16\Users\pc1\AppDat...			Folder	Folder		1/15/2020 2:38:20 PM	1/1

5 Listed | 0 Checked Total | 0 Highlighted

In the Evidence Items pane, note the MSHIST01YYYYMMDDYYYYMMDD subfolders representing daily and weekly Internet Explorer history activity.

4. In FTK, go to the Search tab.
5. Enter the following
   i. wallpaper
6. Conduct an index search for all terms, then select Search Now and Include AllFiles.



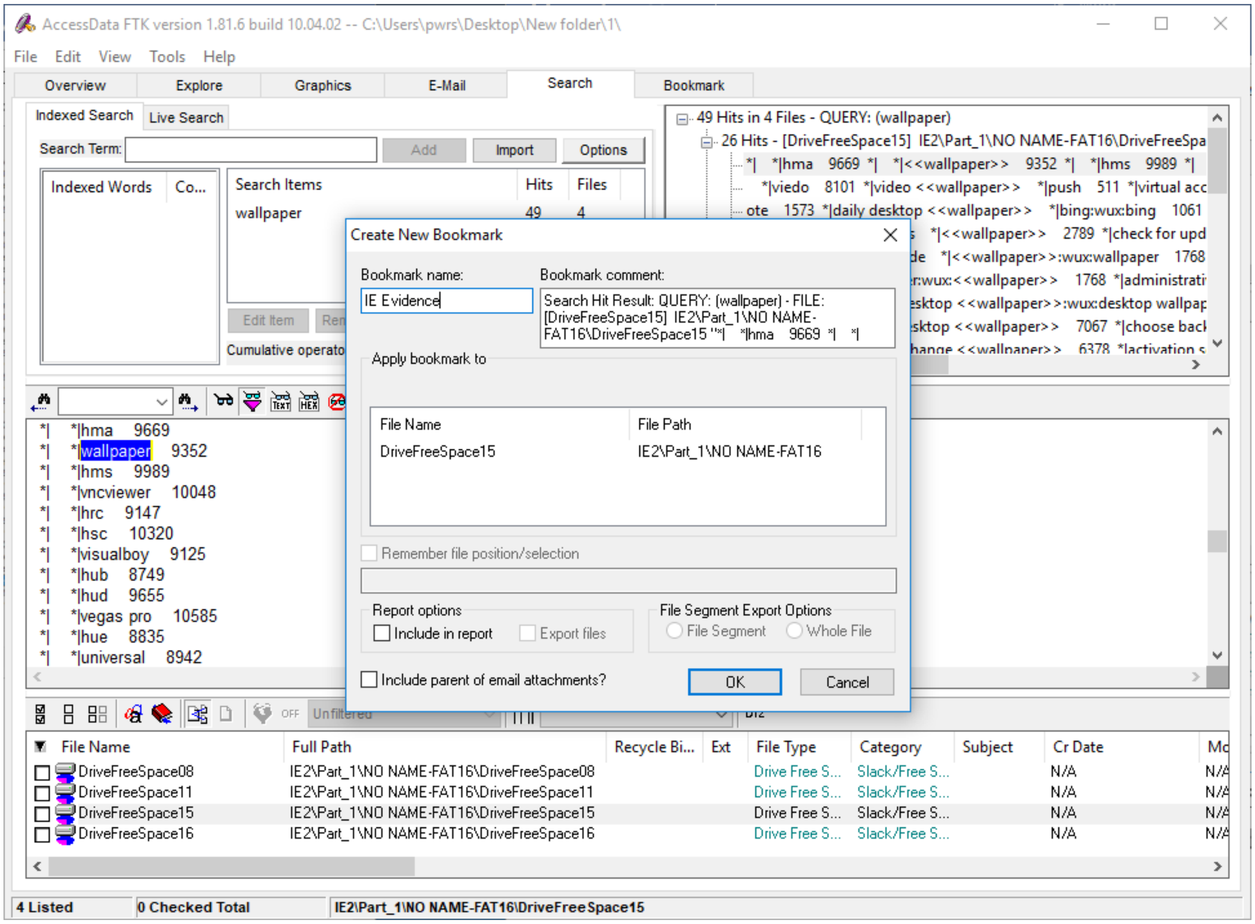
Search Items	Hits	Files
wallpaper	49	4

```
49 Hits in 4 Files - QUERY: (wallpaper)
  26 Hits - [DriveFreeSpace15]  IE2\Part_1\NO NAME-FAT16\DriveFreeSpace1
  10 Hits - [DriveFreeSpace11]  IE2\Part_1\NO NAME-FAT16\DriveFreeSpace1
  10 Hits - [DriveFreeSpace08]  IE2\Part_1\NO NAME-FAT16\DriveFreeSpace0
  3 Hits - [DriveFreeSpace16]  IE2\Part_1\NO NAME-FAT16\DriveFreeSpace16
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mo
□ DriveFreeSpace08	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace08			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace11	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace11			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace15	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace15			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace16	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace16			Drive Free S...	Slack/Free S...		N/A	N/A

4 Listed | 0 Checked Total | 0 Highlighted

7. In the Index Search Results window, select the DriveFreeSpace15 hits.
8. Right-click the first entry, select Create Bookmark, name the bookmark “IE Evidence,” then save the book mark in the admin directory.



AccessData FTK version 1.81.6 build 10.04.02 -- C:\Users\pwrs\Desktop\New folder\1\

Indexed Words	Co...

Search Items	Hits	Files
wallpaper	49	4

```
⊟ 49 Hits in 4 Files - QUERY: (wallpaper)
  ⊟ 26 Hits - [DriveFreeSpace15]  IE2\Part_1\NO NAME-FAT16\DriveFreeSpa
      *|   *|hma   9669  *|   *|<<wallpaper>>   9352  *|   *|hms   9989  *|
      *|viedo   8101  *|video <<wallpaper>>   *|push   511  *|virtual acc
      ote   1573  *|daily desktop <<wallpaper>>   *|bing:wux:bing   1061
      s   *|<<wallpaper>>   2789  *|check for upd
      de   *|<<wallpaper>>:wux:wallpaper   1768
      r:wux:<<wallpaper>>   1768  *|administrati
      esktop <<wallpaper>>:wux:desktop wallpap
      sktop <<wallpaper>>   7067  *|choose back
      hange <<wallpaper>>   6378  *|activation s
```

```
*|   *|hma   9669
*|   *|wallpaper   9352
*|   *|hms   9989
*|   *|vncviewer   10048
*|   *|hrc   9147
*|   *|hsc   10320
*|   *|visualboy   9125
*|   *|hub   8749
*|   *|hud   9655
*|   *|vegas pro   10585
*|   *|hue   8835
*|   *|universal   8942
```

Create New Bookmark

Bookmark name: IE Evidence

Bookmark comment: Search Hit Result: QUERY: (wallpaper) - FILE: [DriveFreeSpace15] IE2\Part_1\NO NAME-FAT16\DriveFreeSpace15 "*| *|hma   9669 *| *|

Apply bookmark to

File Name	File Path
DriveFreeSpace15	IE2\Part_1\NO NAME-FAT16

□ Remember file position/selection

Report options: □ Include in report □ Export files

File Segment Export Options: ○ File Segment ○ Whole File

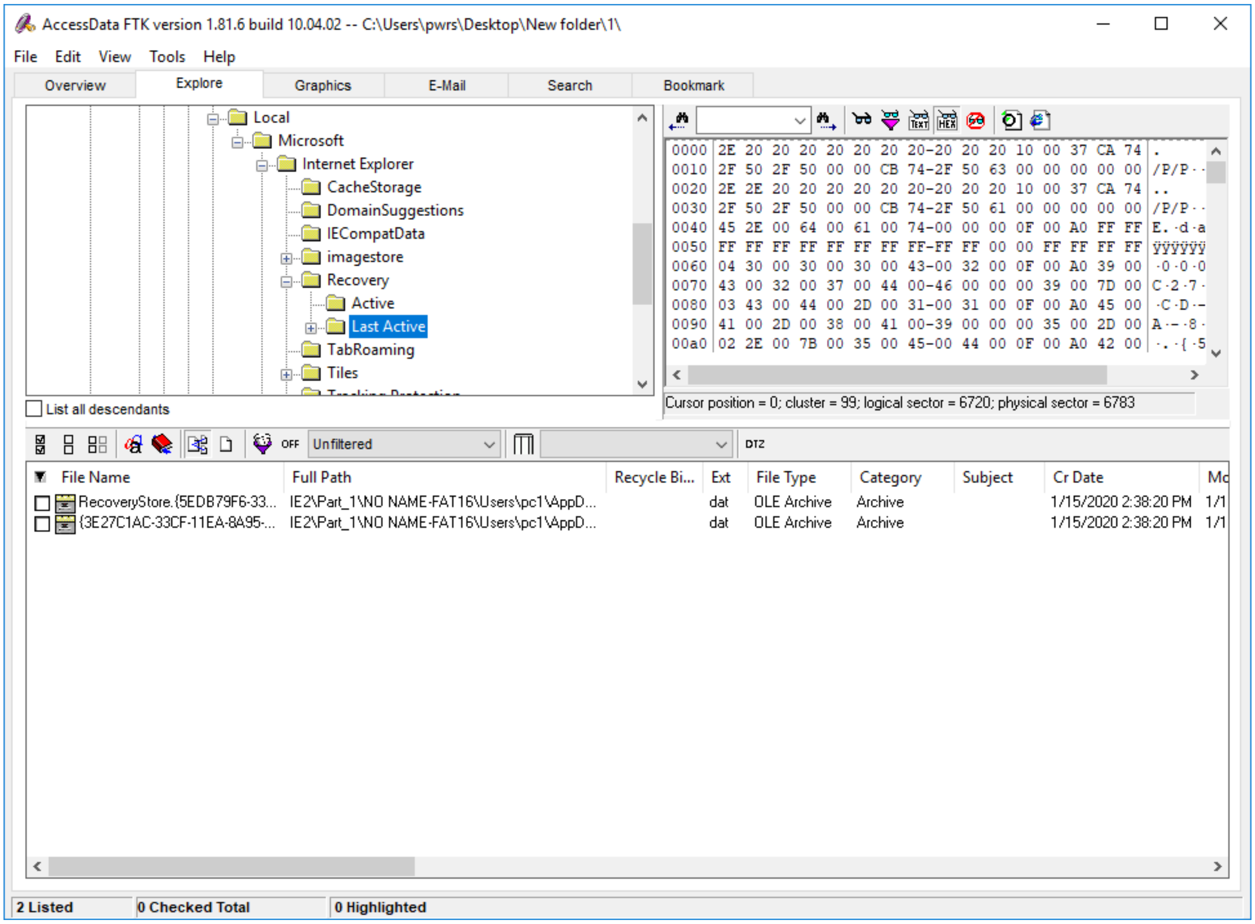
□ Include parent of email attachments?

OK   Cancel

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mo
□ DriveFreeSpace08	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace08			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace11	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace11			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace15	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace15			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace16	IE2\Part_1\NO NAME-FAT16\DriveFreeSpace16			Drive Free S...	Slack/Free S...		N/A	N/A

4 Listed | 0 Checked Total | IE2\Part_1\NO NAME-FAT16\DriveFreeSpace15

9. In the Explorer tab, expand the following path: Users\Instruct\AppData\Local\Microsoft\Internet Explorer\Recovery\LastActive



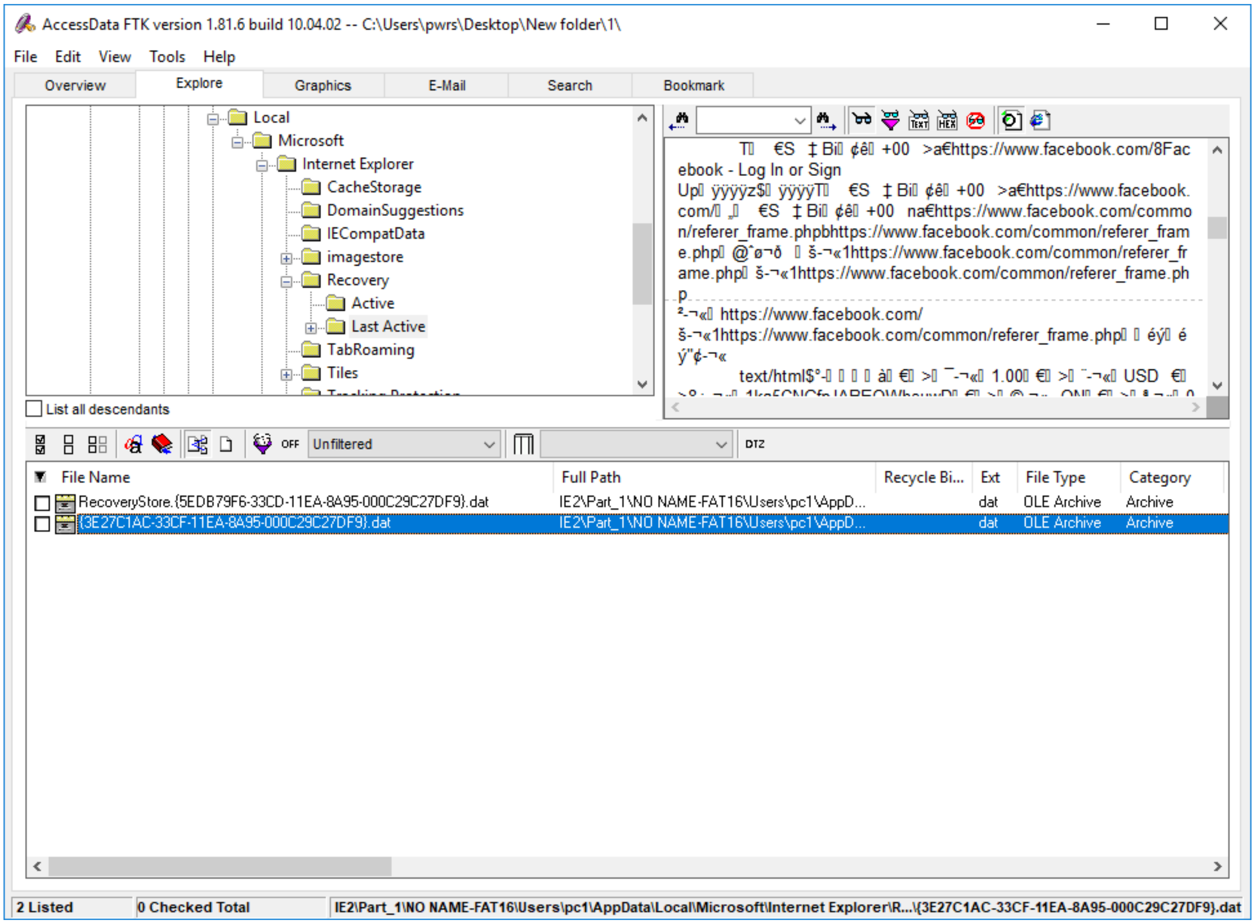
```
0000 2E 20 20 20 20 20 20 20-20 20 20 10 00 37 CA 74 .
0010 2F 50 2F 50 00 00 CB 74-2F 50 63 00 00 00 00 00 /P/P··
0020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 37 CA 74 ..
0030 2F 50 2F 50 00 00 CB 74-2F 50 61 00 00 00 00 00 /P/P··
0040 45 2E 00 64 00 61 00 74-00 00 00 0F 00 A0 FF FF E.·d·a
0050 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿ
0060 04 30 00 30 00 30 00 43-00 32 00 0F 00 A0 39 00 ·0·0·0
0070 43 00 32 00 37 00 44 00-46 00 00 00 39 00 7D 00 C·2·7·
0080 03 43 00 44 00 2D 00 31-00 31 00 0F 00 A0 45 00 ·C·D·-
0090 41 00 2D 00 38 00 41 00-39 00 00 00 35 00 2D 00 A·-·8·
00a0 02 2E 00 7B 00 35 00 45-00 44 00 0F 00 A0 42 00 ·.·{·5
```

Cursor position = 0; cluster = 99; logical sector = 6720; physical sector = 6783

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mc
□ RecoveryStore.{5EDB79F6-33...	IE2\Part_1\NO NAME-FAT16\Users\pc1\AppD...		dat	OLE Archive	Archive		1/15/2020 2:38:20 PM	1/1
□ {3E27C1AC-33CF-11EA-8A95-...	IE2\Part_1\NO NAME-FAT16\Users\pc1\AppD...		dat	OLE Archive	Archive		1/15/2020 2:38:20 PM	1/1

2 Listed | 0 Checked Total | 0 Highlighted

10. In the evidence items pane, select the GUID session recovery folder that begins with 3E27C1AC



```
        T▯   €S  ‡ Bi▯ ¢ê▯ +00  >a€https://www.facebook.com/8Fac
ebook - Log In or Sign
Up▯ ÿÿÿÿz$▯ ÿÿÿÿT▯   €S  ‡ Bi▯ ¢ê▯ +00  >a€https://www.facebook.
com/▯ „▯   €S  ‡ Bi▯ ¢ê▯ +00  na€https://www.facebook.com/commo
n/referer_frame.phpbhttps://www.facebook.com/common/referer_fram
e.php▯ @ˆø¬ð  ▯ š-¬«1https://www.facebook.com/common/referer_fr
ame.php▯ š-¬«1https://www.facebook.com/common/referer_frame.ph
p
²-¬«▯ https://www.facebook.com/
š-¬«1https://www.facebook.com/common/referer_frame.php▯ ▯ éý▯ é
ý"¢-¬«
        text/html$°-▯ ▯ ▯ ▯ à▯ €▯ >▯ ¯-¬«▯ 1.00▯ €▯ >▯ ¨-¬«▯ USD  €▯
```

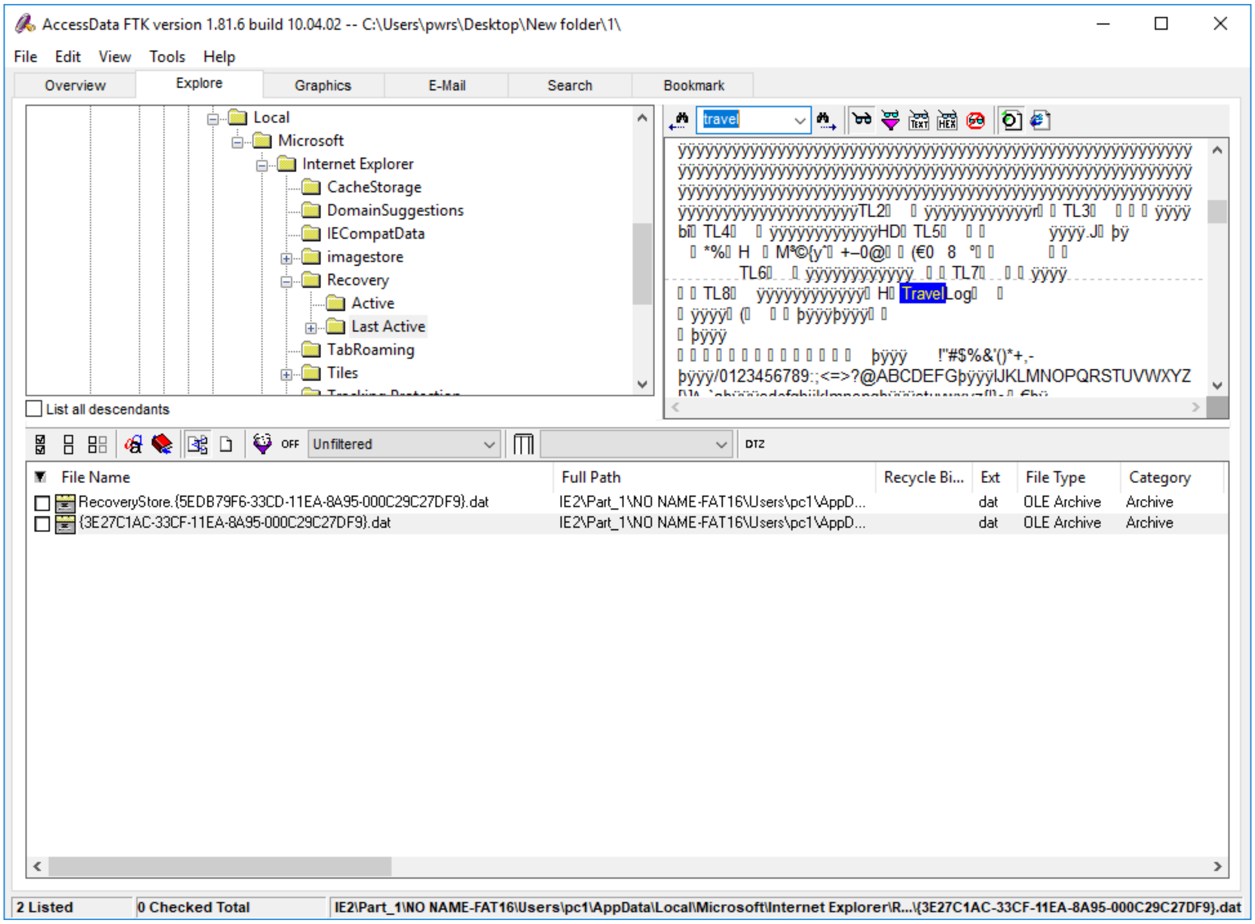
	File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□	RecoveryStore.{5EDB79F6-33CD-11EA-8A95-000C29C27DF9}.dat	IE2\Part_1\NO NAME-FAT16\Users\pc1\AppD...		dat	OLE Archive	Archive
□	{3E27C1AC-33CF-11EA-8A95-000C29C27DF9}.dat	IE2\Part_1\NO NAME-FAT16\Users\pc1\AppD...		dat	OLE Archive	Archive

2 Listed | 0 Checked Total | IE2\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\Microsoft\Internet Explorer\R...\{3E27C1AC-33CF-11EA-8A95-000C29C27DF9}.dat

Note the entries in the File List pane.

11. In the File List pane, select the Visit, or Travel Log file.

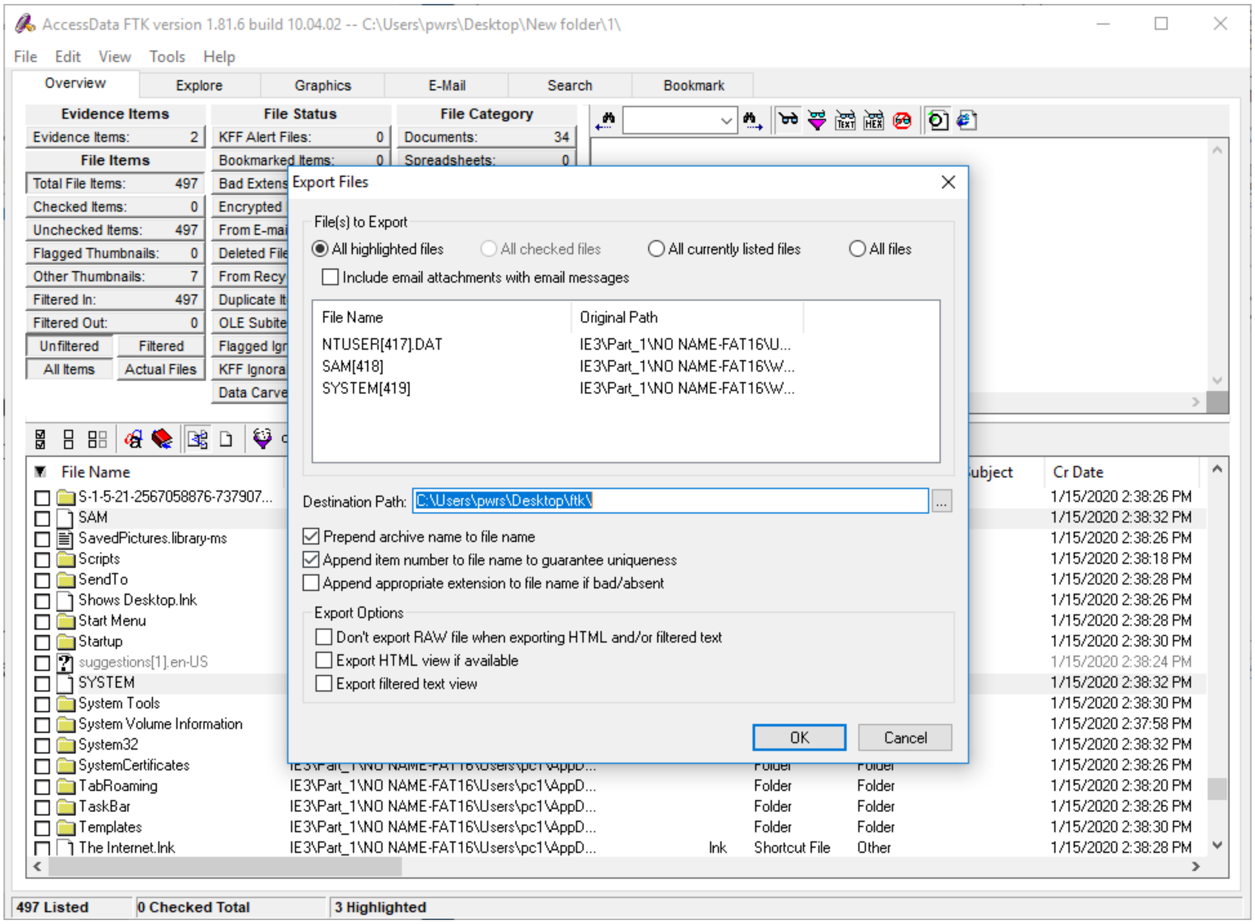
    Note the date in the File Content pane. This represents another open tab in the last active session.



File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□ RecoveryStore.{5EDB79F6-33CD-11EA-8A95-000C29C27DF9}.dat	IE2\Part_1\NO NAME-FAT16\Users\pc1\AppD...		dat	OLE Archive	Archive
□ {3E27C1AC-33CF-11EA-8A95-000C29C27DF9}.dat	IE2\Part_1\NO NAME-FAT16\Users\pc1\AppD...		dat	OLE Archive	Archive

2 Listed | 0 Checked Total | IE2\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\Microsoft\Internet Explorer\R...\{3E27C1AC-33CF-11EA-8A95-000C29C27DF9}.dat

12. In the File List pane, select the following files:
    - i. SAM
    - ii. System
    - iii. NTUSER.DAT


AccessData FTK version 1.81.6 build 10.04.02 -- C:\Users\pwrs\Desktop\New folder\1\

Export Files

File(s) to Export

● All highlighted files ○ All checked files ○ All currently listed files ○ All files

□ Include email attachments with email messages

File Name	Original Path
NTUSER[417].DAT	IE3\Part_1\NO NAME-FAT16\U...
SAM[418]	IE3\Part_1\NO NAME-FAT16\W...
SYSTEM[419]	IE3\Part_1\NO NAME-FAT16\W...

Destination Path: C:\Users\pwrs\Desktop\ftk\

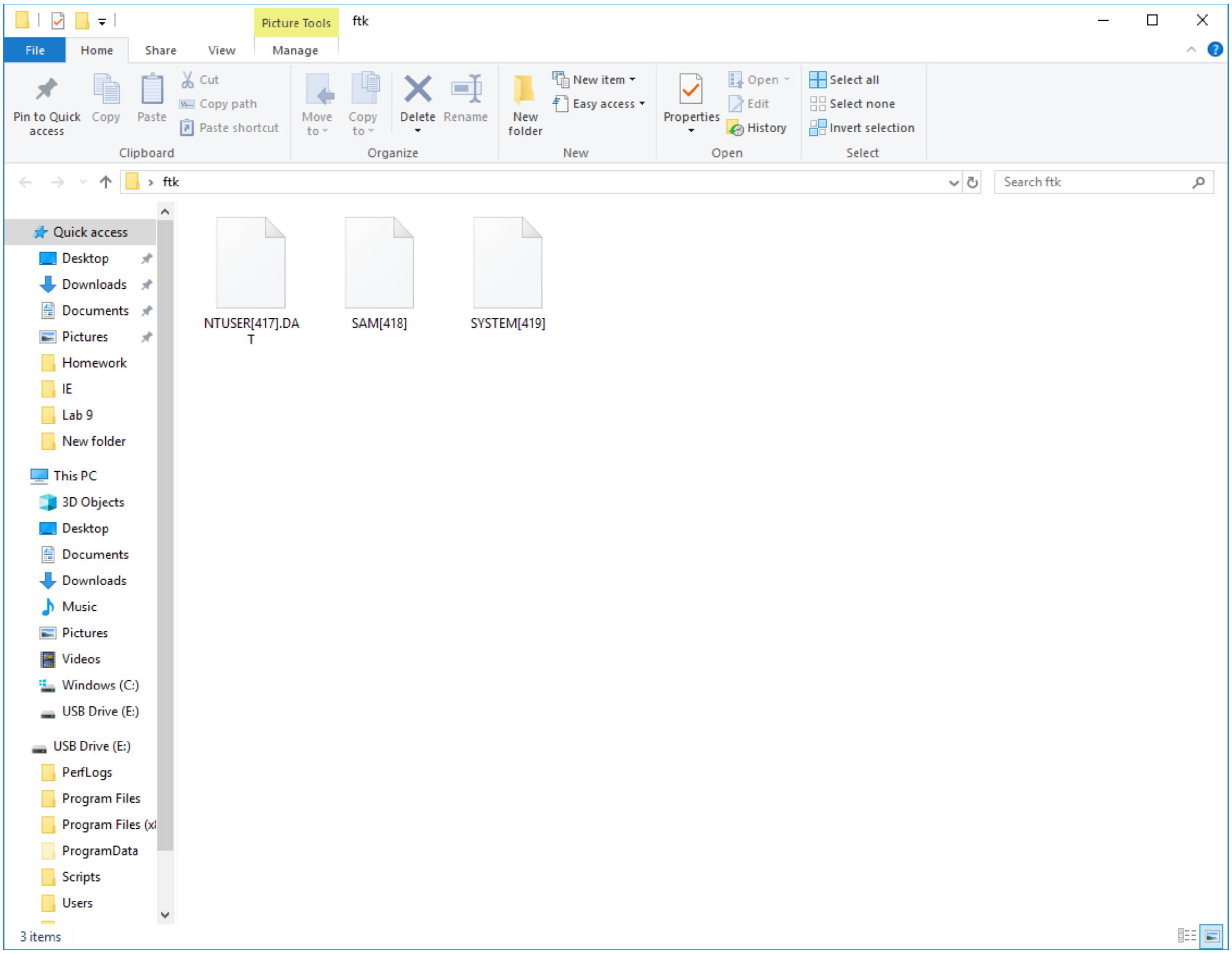
☑ Prepend archive name to file name
☑ Append item number to file name to guarantee uniqueness
□ Append appropriate extension to file name if bad/absent

Export Options

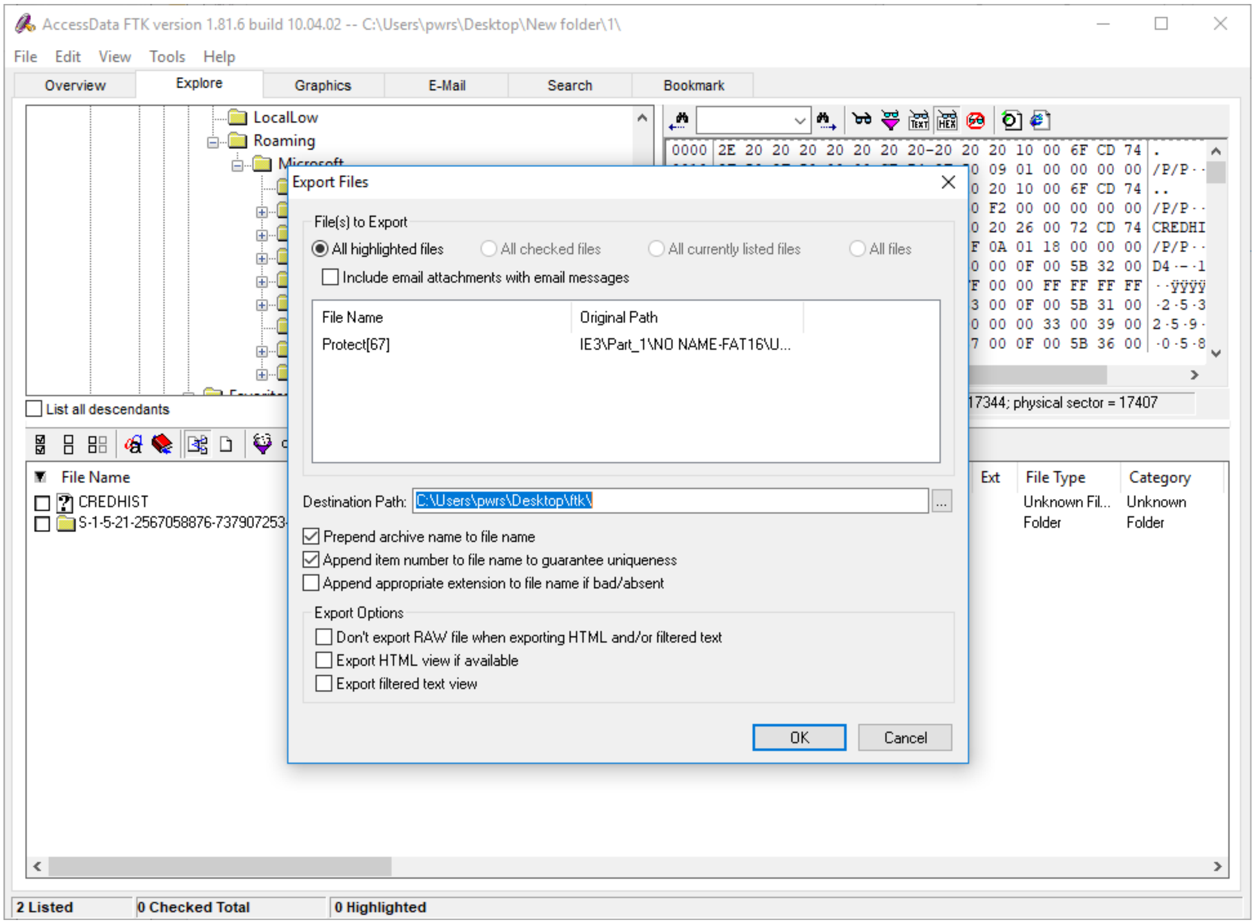
□ Don't export RAW file when exporting HTML and/or filtered text
□ Export HTML view if available
□ Export filtered text view

497 Listed | 0 Checked Total | 3 Highlighted

Right-click one of the checked files, then select Export



13. In the Explore tab, expand the following path: **Users\Instruct\AppData\Roaming\Microsoft**
14. In the Evidence Items pane, right-click the Protect folder, then select Export


AccessData FTK version 1.81.6 build 10.04.02 -- C:\Users\pwrs\Desktop\New folder\1\

File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
LocalLow
Roaming
Microsoft
□ List all descendants
File Name
CREDHIST
S-1-5-21-2567058876-737907253
Ext File Type Category
Unknown Fil... Unknown
Folder Folder
17344; physical sector = 17407

Export Files

File(s) to Export

● All highlighted files ○ All checked files ○ All currently listed files ○ All files

□ Include email attachments with email messages

File Name	Original Path
Protect[67]	IE3\Part_1\NO NAME-FAT16\U...

Destination Path: C:\Users\pwrs\Desktop\ftk\

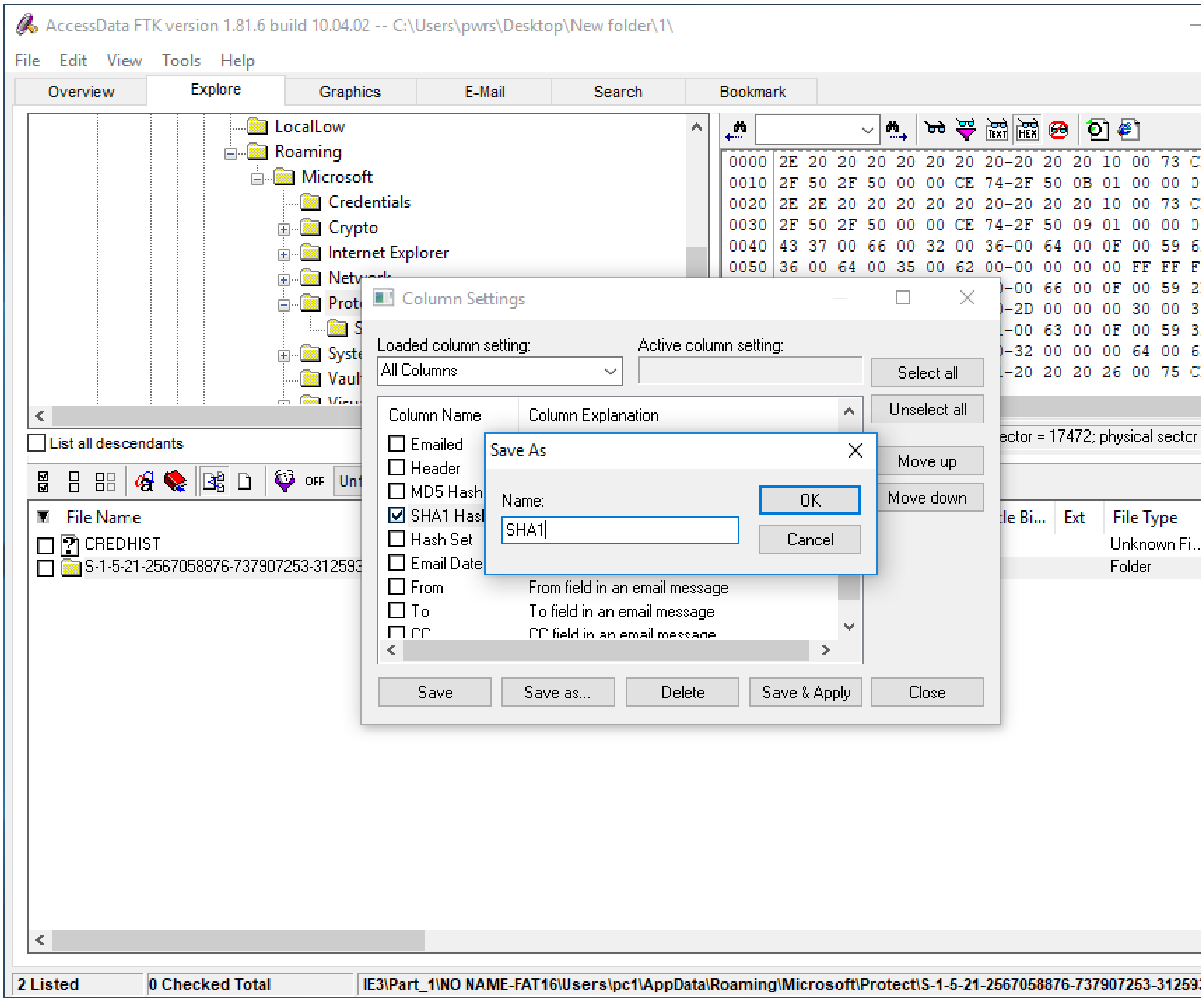
☑ Prepend archive name to file name
☑ Append item number to file name to guarantee uniqueness
□ Append appropriate extension to file name if bad/absent

Export Options
□ Don't export RAW file when exporting HTML and/or filtered text
□ Export HTML view if available
□ Export filtered text view

OK Cancel

2 Listed | 0 Checked Total | 0 Highlighted

15. Create new column setting. Add only SHA1. Name it SHA1 export.
16. In the File List view, right-click on column bars and select **Column Setting**.



AccessData FTK version 1.81.6 build 10.04.02 -- C:\Users\pwrs\Desktop\New folder\1\

```
0000 2E 20 20 20 20 20 20 20-20 20 20 10 00 73 C
0010 2F 50 2F 50 00 00 CE 74-2F 50 0B 01 00 00 0
0020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 73 C
0030 2F 50 2F 50 00 00 CE 74-2F 50 09 01 00 00 0
0040 43 37 00 66 00 32 00 36-00 64 00 0F 00 59 6
0050 36 00 64 00 35 00 62 00-00 00 00 00 FF FF F
```

Loaded column setting: All Columns

Active column setting:

☑ SHA1 Hash

From — From field in an email message

To — To field in an email message

CC — CC field in an email message

Name: SHA1

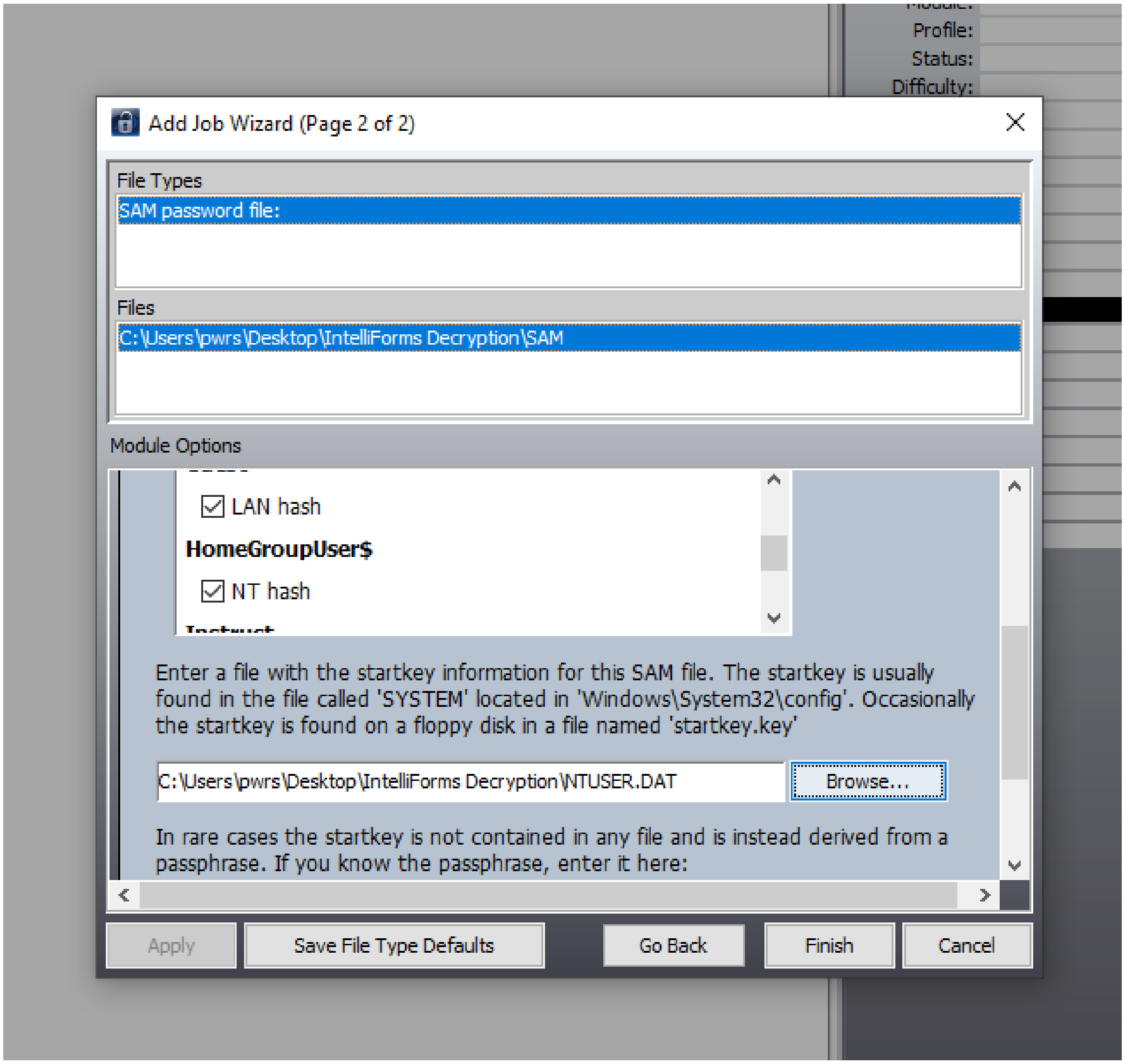
ector = 17472; physical sector

☐ CREDHIST — Unknown Fil..

☐ S-1-5-21-2567058876-737907253-312593 — Folder

2 Listed | 0 Checked Total | IE3\Part_1\NO NAME-FAT16\Users\pc1\AppData\Roaming\Microsoft\Protect\S-1-5-21-2567058876-737907253-31259

17. Using PRTK to Decrypting the windows logon password. (optional. If you have the license for PRTK.)
18.



Add Job Wizard (Page 2 of 2)

File Types

SAM password file:

Files

C:\Users\pwrs\Desktop\IntelliForms Decryption\SAM

Module Options

☑ LAN hash

HomeGroupUser$

☑ NT hash

Instruct

Enter a file with the startkey information for this SAM file. The startkey is usually found in the file called 'SYSTEM' located in 'Windows\System32\config'. Occasionally the startkey is found on a floppy disk in a file named 'startkey.key'

C:\Users\pwrs\Desktop\IntelliForms Decryption\NTUSER.DAT

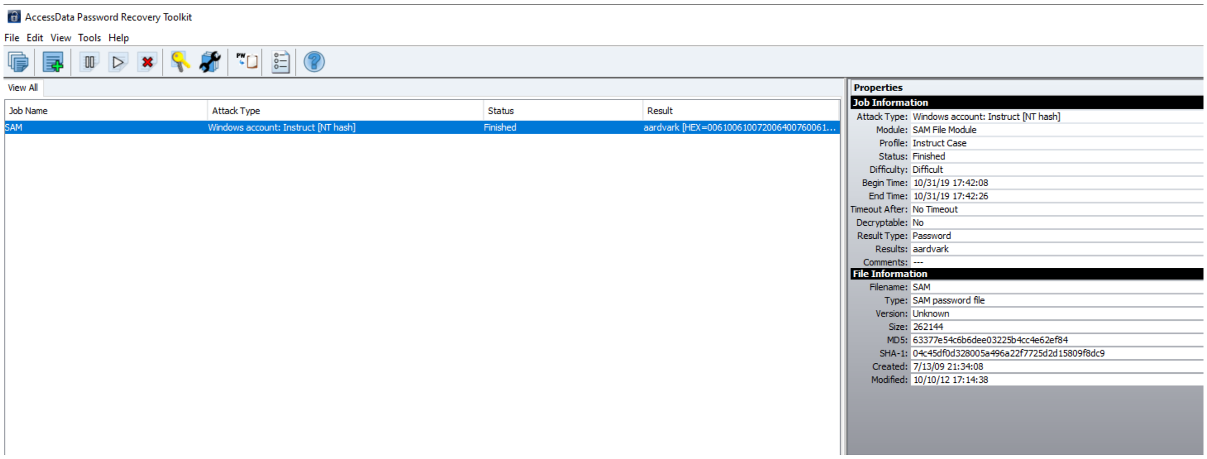
In rare cases the startkey is not contained in any file and is instead derived from a passphrase. If you know the passphrase, enter it here:

a. Add the exported SAM file to PRTK.

b. Select only the Instruct user account for processing.

19. When complete, right-click the results, then select Copy Password to Clipboard

20. The recovered password is “aardvark.



AccessData Password Recovery Toolkit
File Edit View Tools Help
PW
View All

Job Name	Attack Type	Status	Result
SAM	Windows account: Instruct [NT hash]	Finished	aardvark [HEX=006100610072006400760061...

Properties

Job Information

Attack Type:	Windows account: Instruct [NT hash]
Module:	SAM File Module
Profile:	Instruct Case
Status:	Finished
Difficulty:	Difficult
Begin Time:	10/31/19 17:42:08
End Time:	10/31/19 17:42:26
Timeout After:	No Timeout
Decryptable:	No
Result Type:	Password
Results:	aardvark
Comments:	---

File Information

Filename:	SAM
Type:	SAM password file
Version:	Unknown
Size:	262144
MD5:	63377e54c6b6dee03225b4cc4e62ef84
SHA-1:	04c45df0d328005a496a22f7725d2d15809f8dc9
Created:	7/13/09 21:34:08
Modified:	10/10/12 17:14:38