

Module B4: Firefox Browser Forensics Analysis

Pre-requisite Knowledge and Skills:

1. Understand the basic of NTFS File Systems

Learning Objectives

1. Be familiar to

Recommended Running Environment/Tools:

1. Windows OS
2. AccessData FTK Imager
3. Forensic Toolkit 1.8.6.exe

Material:

1. ADS Image.E01

Video Lecture:

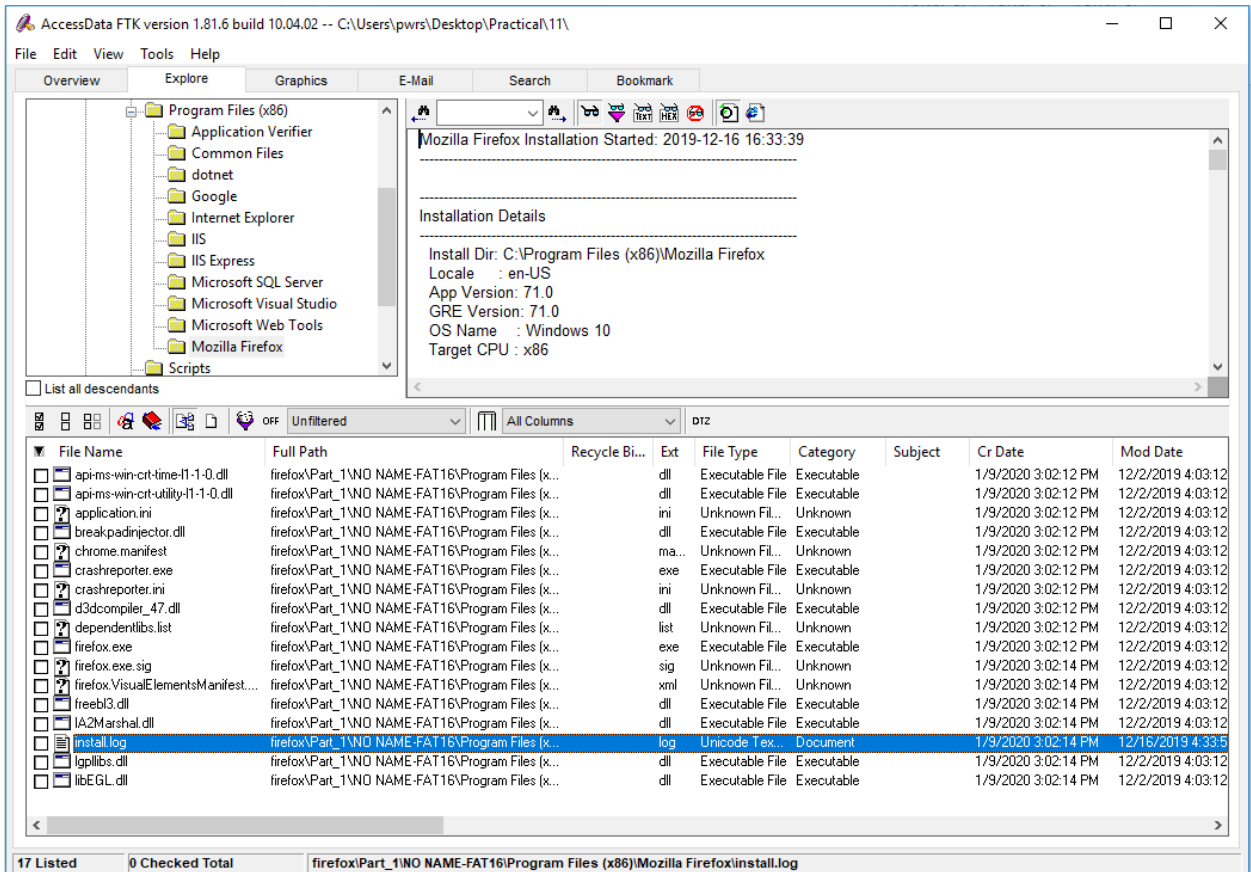
1. N/A

Lab Assessment:

1. N/A

Lab Instructions:

1. Using the firefox case
2. On the Explore Tab, Navigate to:
 - a. **ProgramFiles(x86)\Mozilla Firefox** and click on Install.log



b. Note install data and time

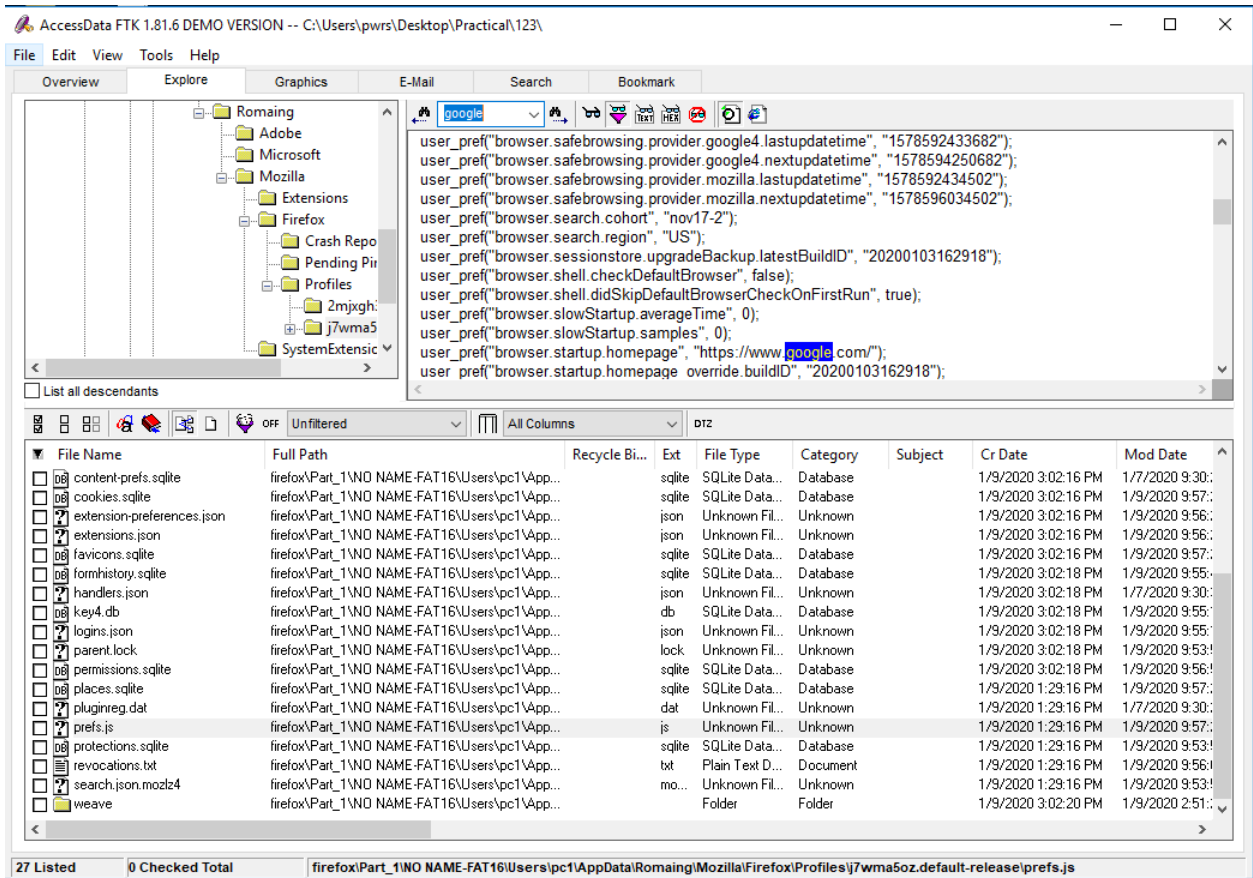
3. Navigate to

\Users\pc1\AppData\Roaming\Mozilla\Firefox\Profiles\Default

a. Click on file **Prefs.js**

Note within this file

Homepage of www.google.com



Username

```

user_pref("services.sync.tabs.lastSync", "0");
user_pref("services.sync.username", "1124802704@qq.com");
user_pref("signon.importedFromSqlite", true);

```

- a. Click on file Logins.json
 - i. Note presence encrypt password.

AccessData FTK version 1.81.6 build 10.04.02 -- C:\Users\pws\Desktop\Practical\11\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

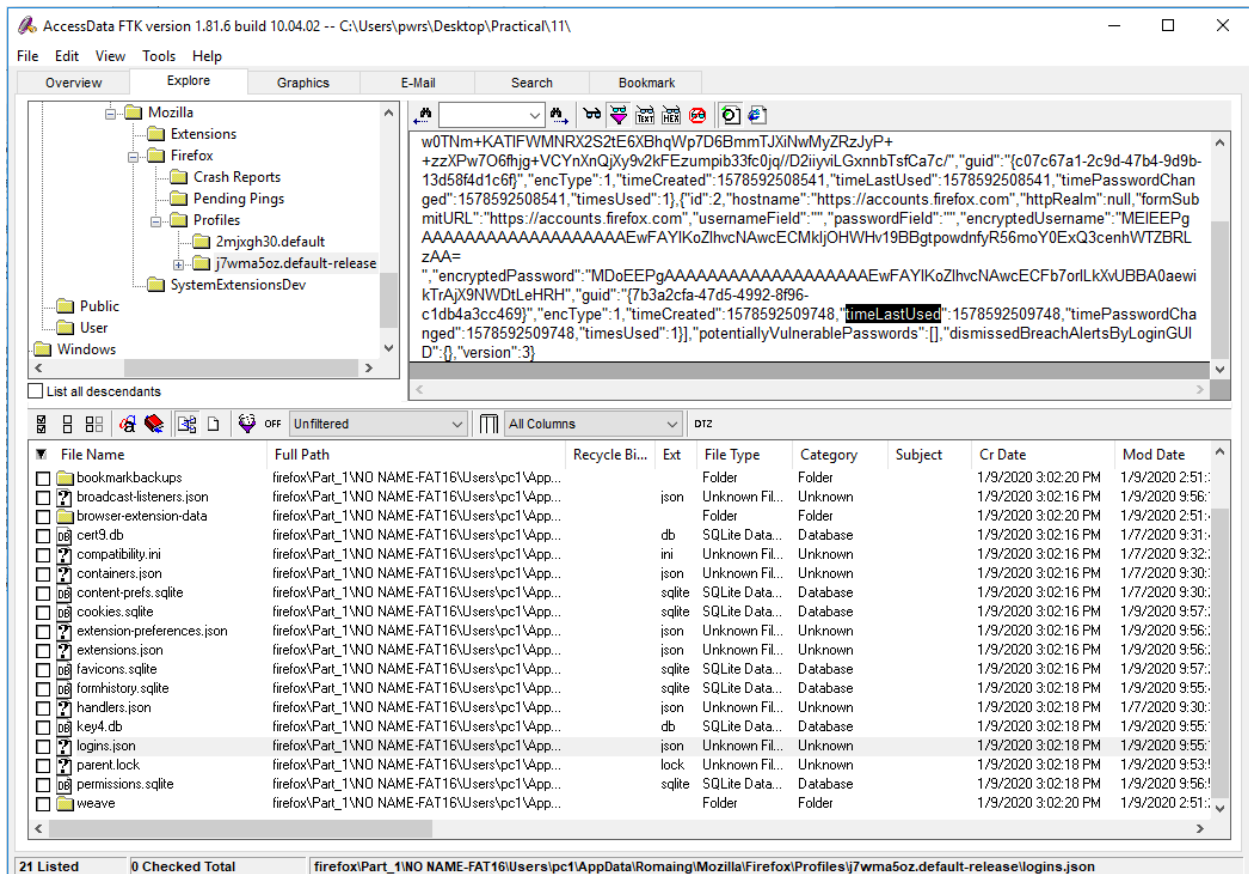
Mozilla
 Extensions
 Firefox
 Crash Reports
 Pending Pings
 Profiles
 2mjxgh30.default
 j7wma5oz.default-release
 SystemExtensionsDev

```
{
  "nextId": 3,
  "logins": [
    {
      "id": 1,
      "hostname": "chrome://FirefoxAccounts",
      "httpRealm": "Firefox Accounts credentials",
      "formSubmitURL": null,
      "usernameField": "",
      "passwordField": "",
      "encryptedUsername": "MFIEEPgAAAAA...EwFAYIKoZlhvcNAwcECL9XUkbyoYzvBCh5WnwO4ObRI27zG0kUYitXmyhEFJM2bxBLsRiCrOrpKJPDa3VHXG",
      "encryptedPassword": "MIHzBBd4AAAAA...AAAAABMQGCCqGSib3DQMhBAhh/Pitp+YM7wSBypXlbgOITrjCLY55bP7MBPky5Yjunl6A8tWmWfItkdWRa0omkKYnYQ5DXwX4mjnYcP7ea6EdZLngL3XnP0LWT6J2axjx8LoUjrc53YGy4NEj+cjVWnu+7biwDyFSX/BAZJk7353LpbulktBng9P5GAKXw0TNm+KATIFWMNRX2S2tE6xBhqWp7D6BmmTjXiNwMyZRzJyP++zXPw7O6fhjg+VCYnXnQjy9v2kFEzumpib33fc0jq/D2iiyviLgXnnbTsfCa7c",
      "guid": "c07c67a1-2c9d-47b4-9d9b-13d58f4d1c6f",
      "encType": 1,
      "timeCreated": 1578592508541,
      "timeLastUsed": 1578592508541,
      "timePasswordChanged": 1578592508541,
      "timesUsed": 1,
      "id": 2,
      "hostname": "https://accounts.firefox.com",
      "httpRealm": null,
      "formSubmitURL": "https://accounts.firefox.com",
      "usernameField": "",
      "passwordField": "",
      "encryptedUsername": "MEIEEPgAAAAA...EwFAYIKoZlhvcNAwcECMkljOHWHv19BBgtpowdnfyR56moY0ExQ3cenhWTZBRlzAA="
    }
  ]
}
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
bookmarkbackups	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\bookmarkbackups			Folder	Folder		1/9/2020 3:02:20 PM	1/9/2020 2:51:00 PM
broadcast-listeners.json	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\broadcast-listeners.json		json	Unknown Fil...	Unknown		1/9/2020 3:02:16 PM	1/9/2020 9:56:00 PM
browser-extension-data	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\browser-extension-data			Folder	Folder		1/9/2020 3:02:20 PM	1/9/2020 2:51:00 PM
cert9.db	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\cert9.db		db	SQLite Data...	Database		1/9/2020 3:02:16 PM	1/7/2020 9:31:00 PM
compatibility.ini	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\compatibility.ini		ini	Unknown Fil...	Unknown		1/9/2020 3:02:16 PM	1/7/2020 9:32:00 PM
containers.json	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\containers.json		json	Unknown Fil...	Unknown		1/9/2020 3:02:16 PM	1/7/2020 9:30:00 PM
content-prefs.sqlite	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\content-prefs.sqlite		sqlite	SQLite Data...	Database		1/9/2020 3:02:16 PM	1/7/2020 9:30:00 PM
cookies.sqlite	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\cookies.sqlite		sqlite	SQLite Data...	Database		1/9/2020 3:02:16 PM	1/9/2020 9:57:00 PM
extension-preferences.json	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\extension-preferences.json		json	Unknown Fil...	Unknown		1/9/2020 3:02:16 PM	1/9/2020 9:56:00 PM
extensions.json	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\extensions.json		json	Unknown Fil...	Unknown		1/9/2020 3:02:16 PM	1/9/2020 9:56:00 PM
favicons.sqlite	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\favicons.sqlite		sqlite	SQLite Data...	Database		1/9/2020 3:02:16 PM	1/9/2020 9:57:00 PM
formhistory.sqlite	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\formhistory.sqlite		sqlite	SQLite Data...	Database		1/9/2020 3:02:18 PM	1/9/2020 9:55:00 PM
handlers.json	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\handlers.json		json	Unknown Fil...	Unknown		1/9/2020 3:02:18 PM	1/7/2020 9:30:00 PM
key4.db	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\key4.db		db	SQLite Data...	Database		1/9/2020 3:02:18 PM	1/9/2020 9:55:00 PM
logins.json	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\logins.json		json	Unknown Fil...	Unknown		1/9/2020 3:02:18 PM	1/9/2020 9:55:00 PM
parent.lock	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\parent.lock		lock	Unknown Fil...	Unknown		1/9/2020 3:02:18 PM	1/9/2020 9:53:00 PM
permissions.sqlite	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\permissions.sqlite		sqlite	SQLite Data...	Database		1/9/2020 3:02:18 PM	1/9/2020 9:56:00 PM
weave	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\weave			Folder	Folder		1/9/2020 3:02:20 PM	1/9/2020 2:51:00 PM

21 Listed 0 Checked Total firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\Mozilla\Firefox\Profiles\j7wma5oz.default-release\logins.json

ii. Also note dates and times for created, last used and changed



iii. Decryption steps:

Using Imager export the itser's logins.json and key4.db files to a folder called Firefox on Desktop

Install and run Firefox Password by

vi. Select Open Profile Select Search for Profiles

Select the folder where you exported the logins.json and key3.db files and click OK

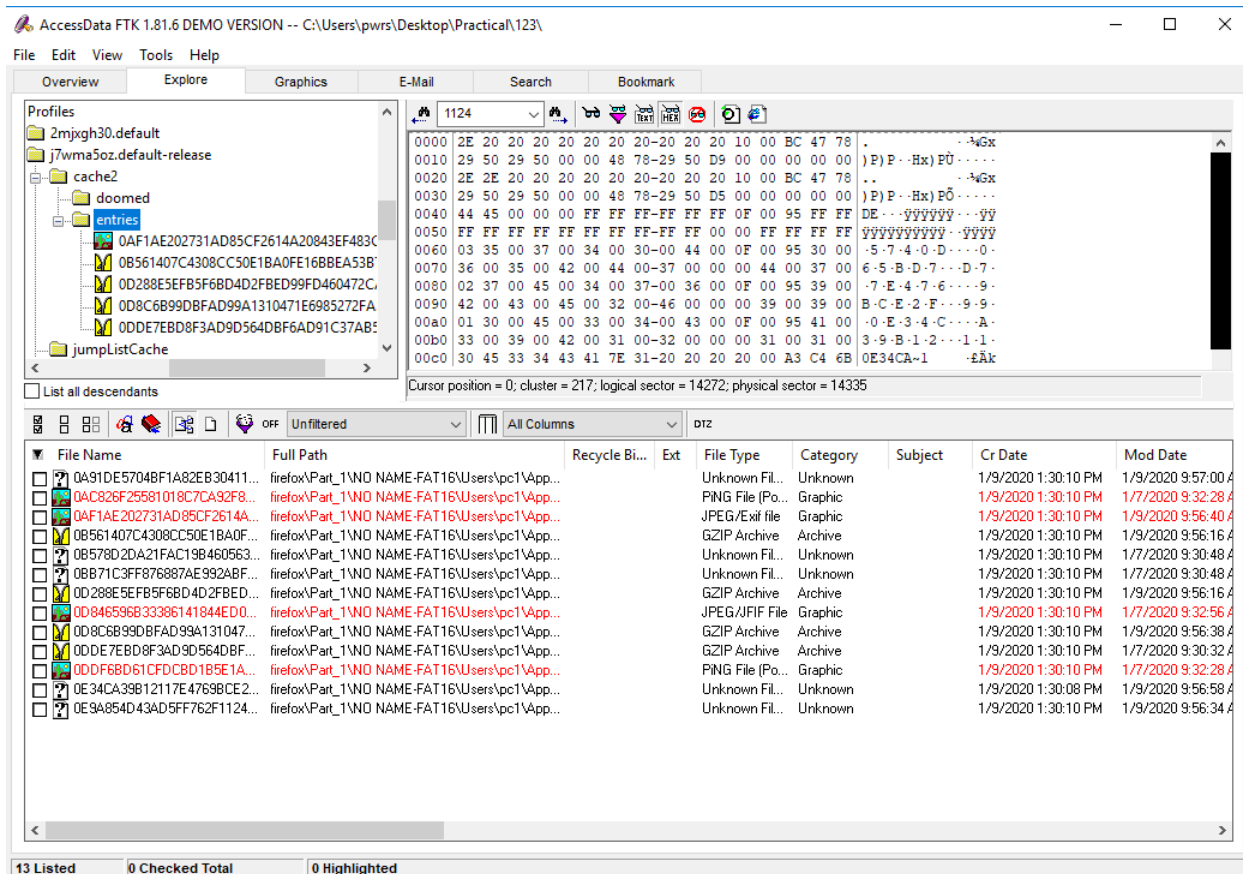
ix. Review the Profile Data

x. Click View Selected Data

xi. Click Save as .csv file

4. Navigate to

\Users\Everett\AppData\local\Mozilla\Firefoa\Profiles\Default\ Cache2\Entices

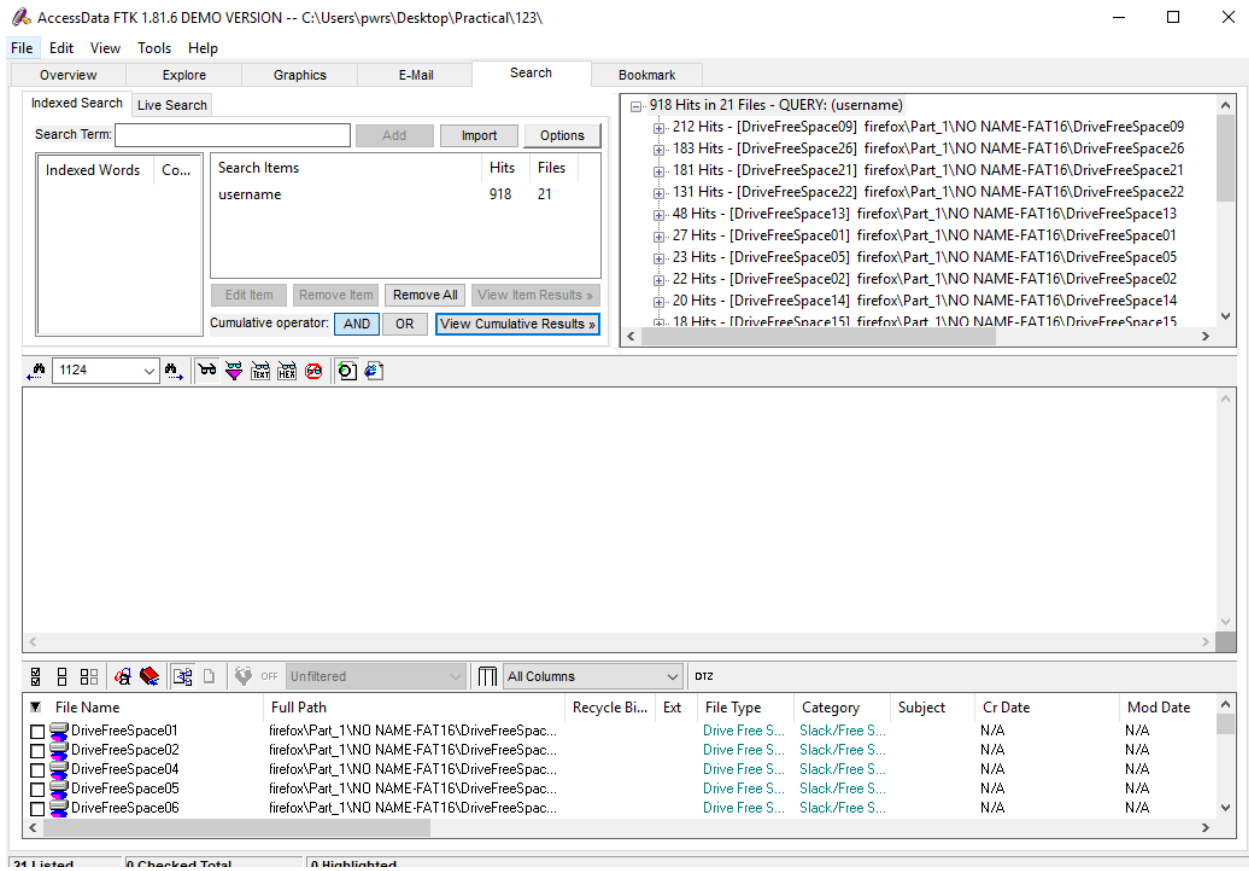


Firefox Temporary Internet Files (TIF) are here

File names are SHA1 hash of URL and are recorded in the index file.

5. Click the Search tab

An indexed search uses the index file to find search terms. FTK uses the search engine, dtSearch, to perform indexed searches.



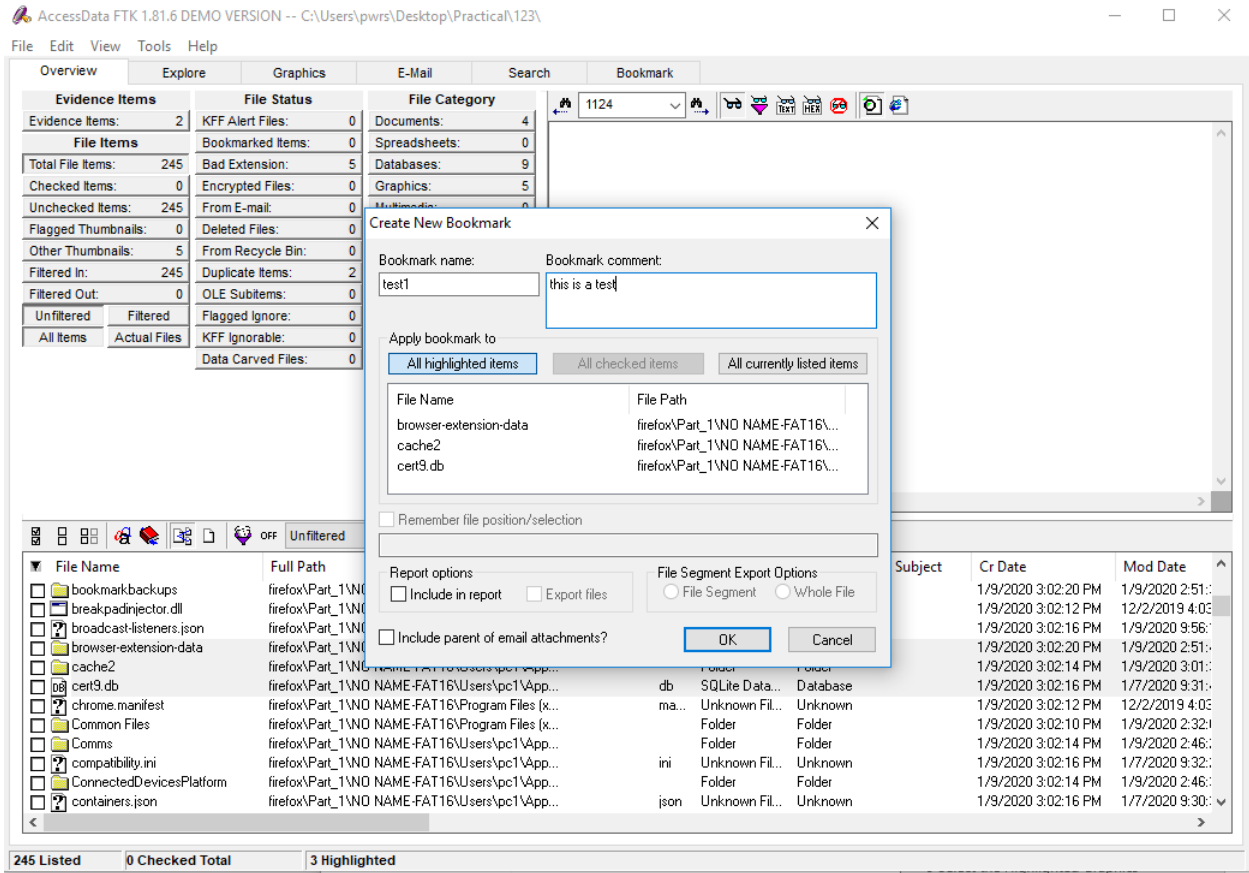
6. Bookmark part

Right-Click the graphics and select Create Bookmark

In the Create New Bookmark menu, name the bookmark

Highlighted Graphics. Then select All highlighted items and click OK

Add a comment in the Bookmark Comment field. Then click Save Changes



Go to the Bookmark tab.

AccessData FTK 1.81.6 DEMO VERSION -- C:\Users\pws\Desktop\Practical\123\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Bookmarks

- test1: this is a test
 - browser-extension-data
 - cache2
 - cert9.db

Bookmark Name: test1
Bookmark Comment: this is a test

Bookmarked Files: 3

File Name	File Path
browser-extension-data	firefox\Part_1\NO NAME-FAT16\...
cache2	firefox\Part_1\NO NAME-FAT16\...

Remember file position/selection

Include in Report Export files Export Segments Whole Files

1124

0000 2E 20 20 20 20 20 20 20 20 20 20 20 10 00 05 4A 78Jx
0010 29 50 29 50 00 00 4B 78-29 50 CE 01 00 00 00 00) P) P - -Kx) P I
0020 2E 2E 20 20 20 20 20 20 20-20 20 20 10 00 05 4A 78Jx
0030 29 50 29 50 00 00 4B 78-29 50 F1 00 00 00 00 00) P) P - -Kx) P I
0040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00

Cursor position = 0; cluster = 462; logical sector = 29952; physical sector = 30015

Unfiltered All Columns dtz

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
browser-extension-data	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\Temp\...			Folder	Folder		1/9/2020 3:02:20 PM	1/9/2020 2:51:40 PM
cache2	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\Temp\...			Folder	Folder		1/9/2020 3:02:14 PM	1/9/2020 3:01:32 PM
cert9.db	firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\Temp\...		db	SQLite Data...	Database		1/9/2020 3:02:16 PM	1/7/2020 9:31:46 AM

3 Listed 0 Checked Total firefox\Part_1\NO NAME-FAT16\Users\pc1\AppData\Local\Temp\moz-profiles\7wma5oz.default-release\browser-extension-data

Go to the Bookmark tab to verify that you have the files in the bookmark