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:

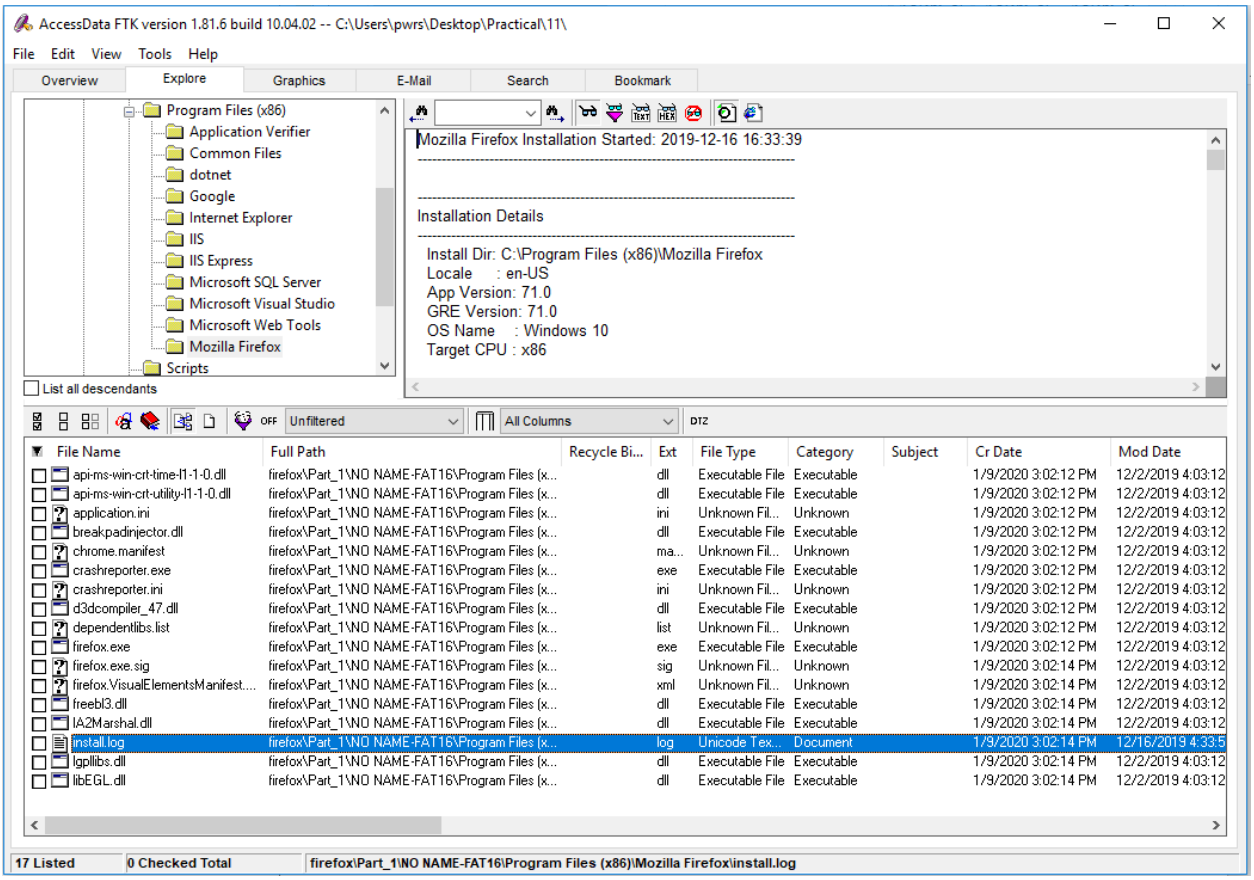
1. N/A

Lab Assessment:

1. N/A

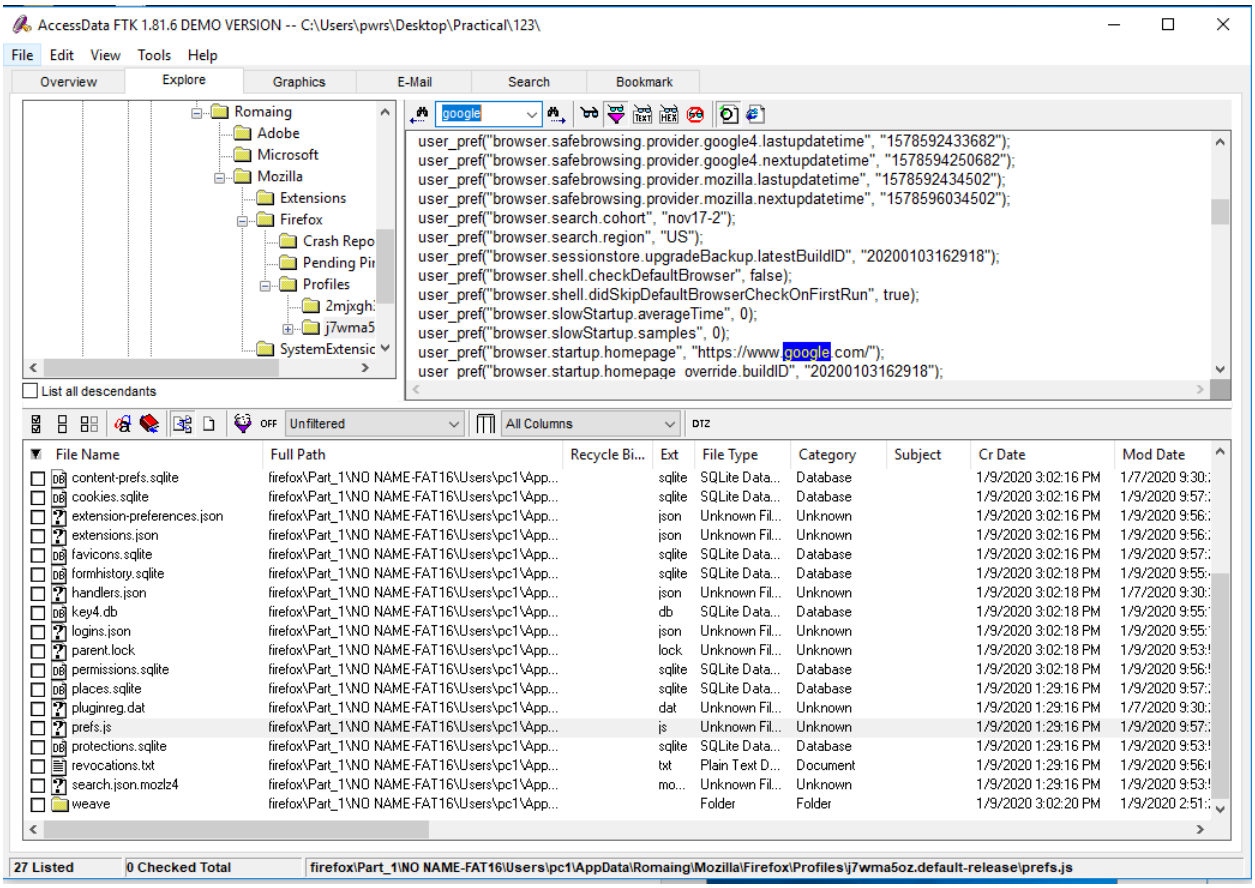
Lab Instructions:

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

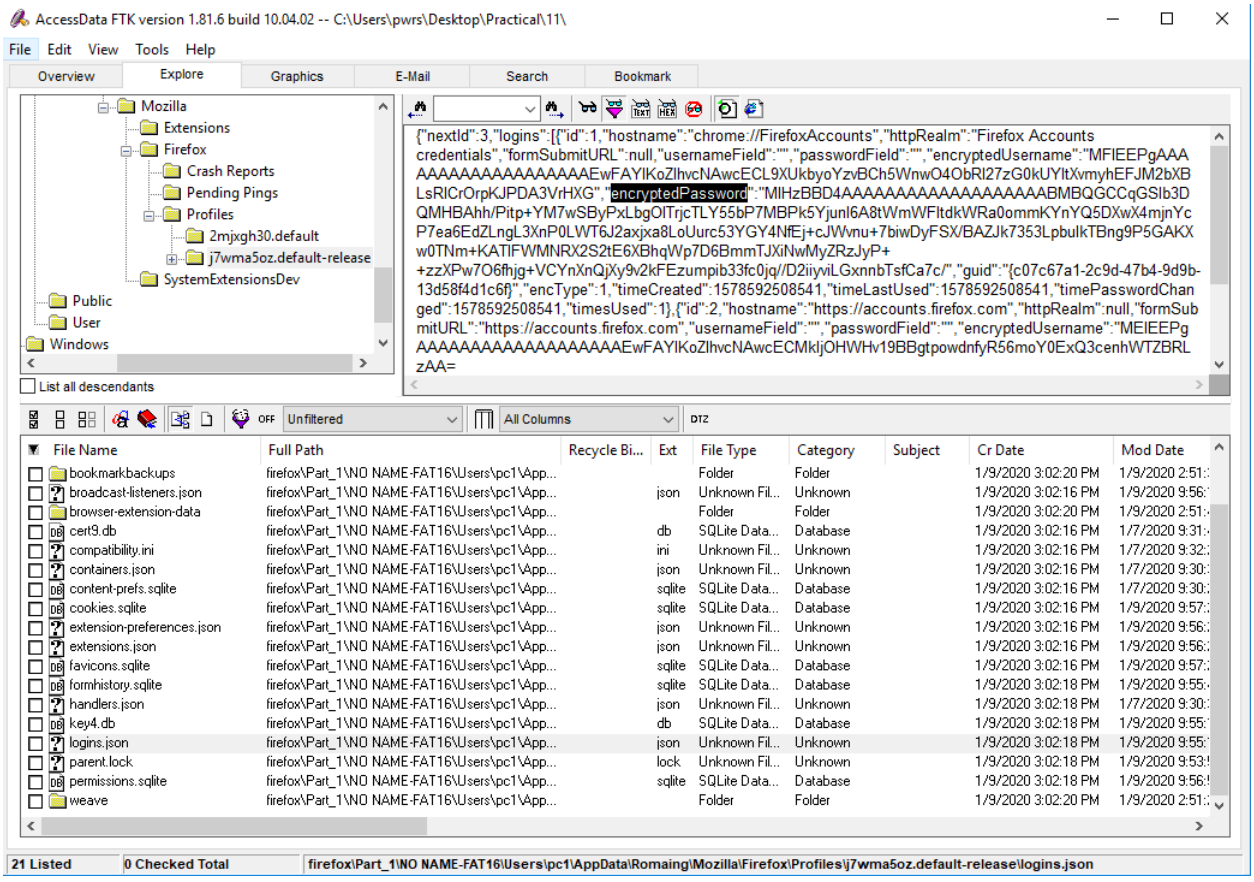
3. Navigate to **\Users\pc1\AppData\Roaming\Mozilla\Firefox\Profiles\Default**
   a. Click on file **Prefs.js**
   Note within this file
   Homepage of www.google.com



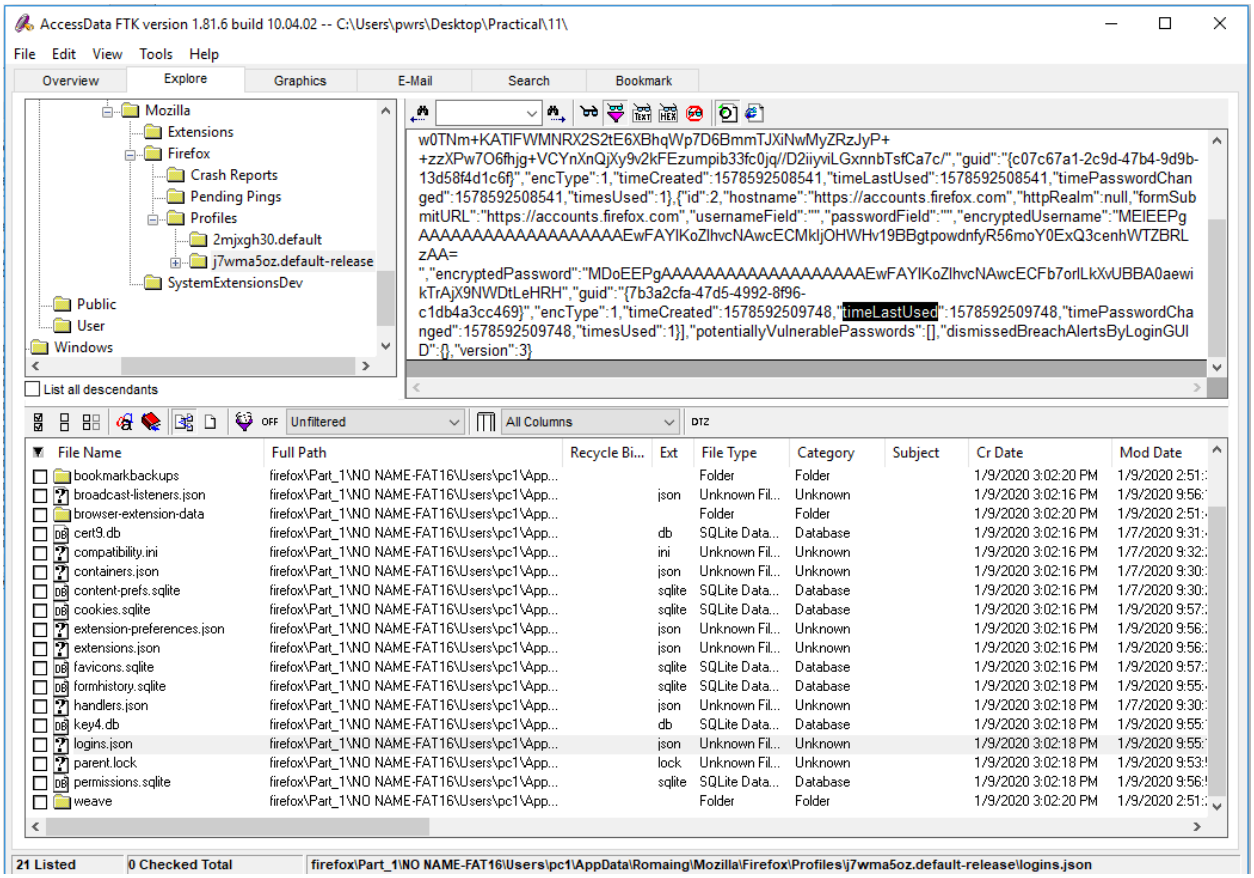
Username

```
user_pref("services.sync.tabs.lastSync", "0");
user_pref("services.sync.username", "1124302704@qq.com");
user_pref("signon.importedFromSqlite", true);
```

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



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

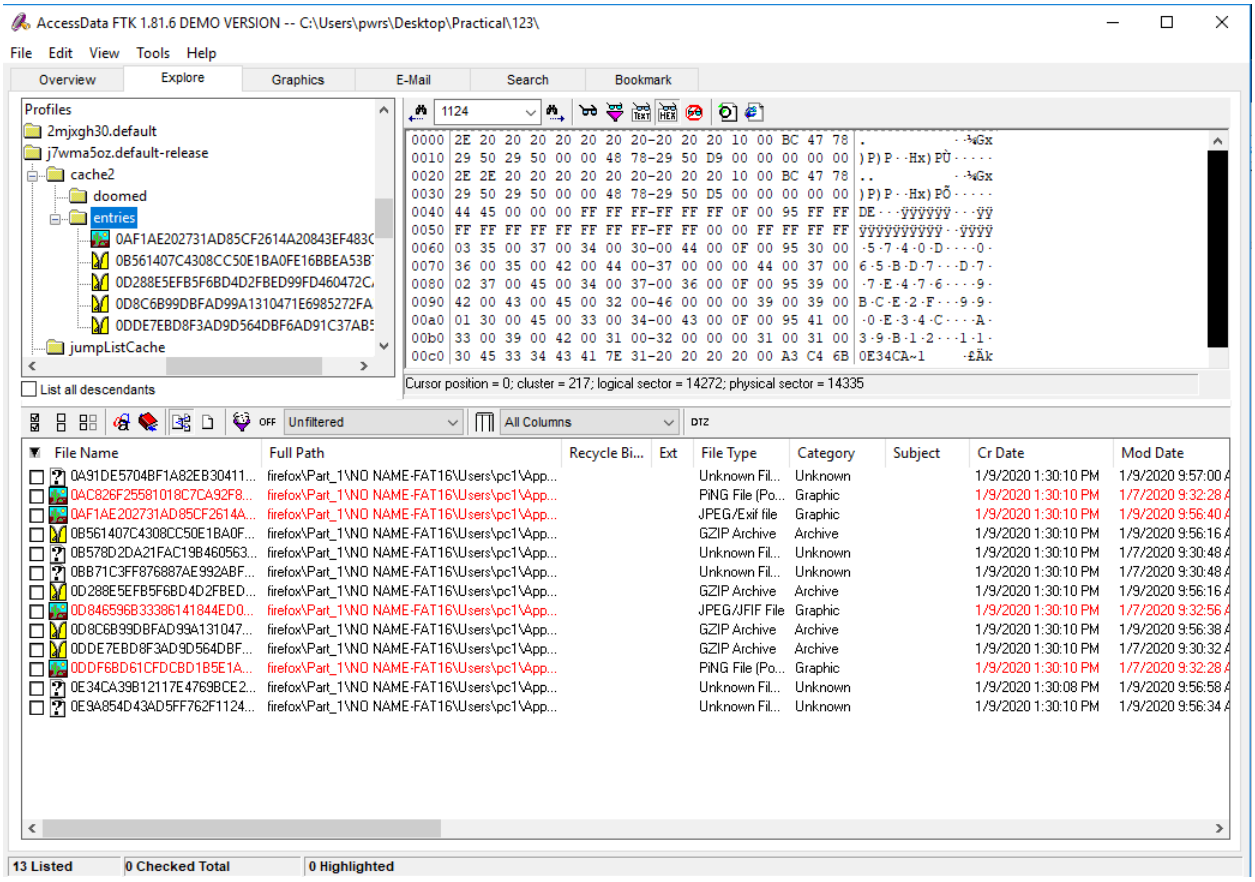
ix. Review the Profile Data

x. Click View Selected Data

xi. Click Save as .csv file

4. Navigate to

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

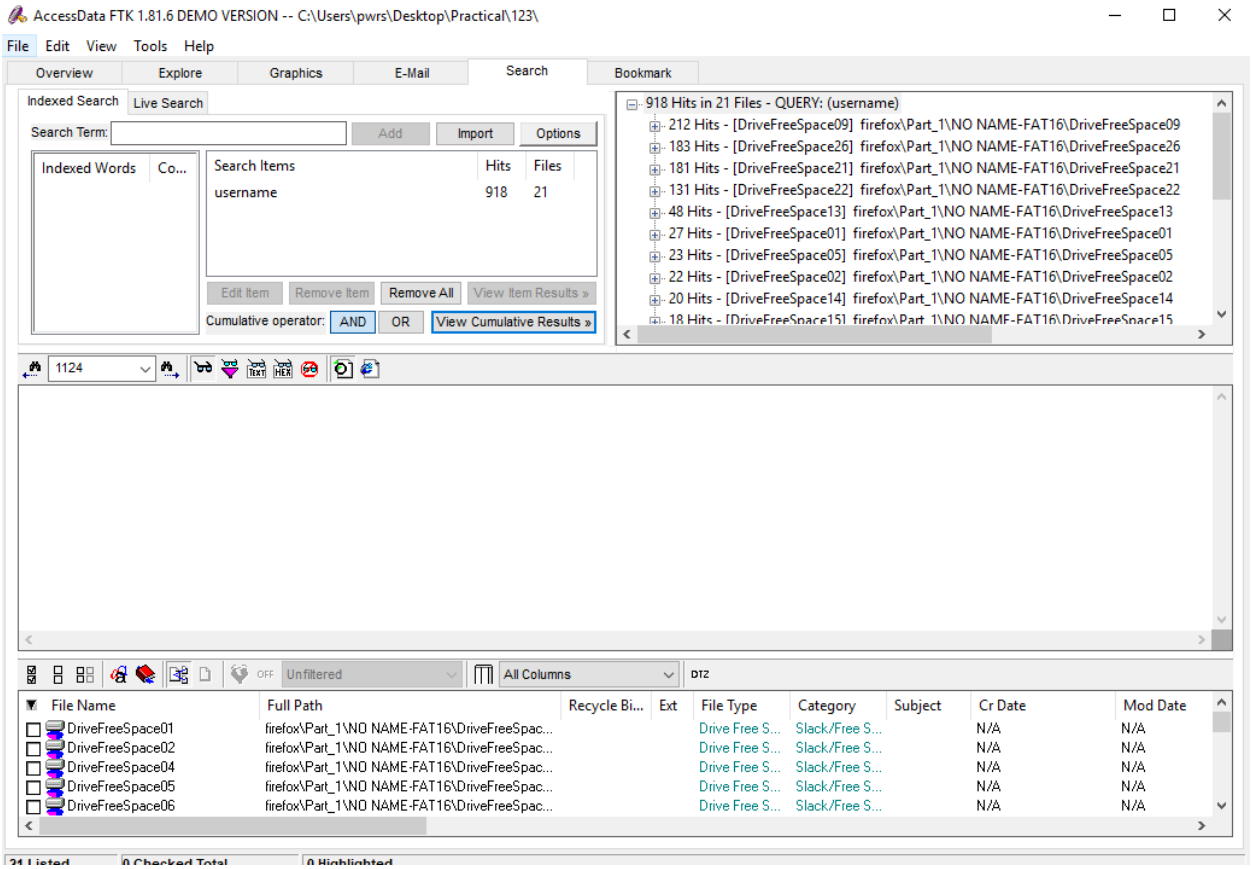


Firefox Temporary Internet Files (TIF) are here

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

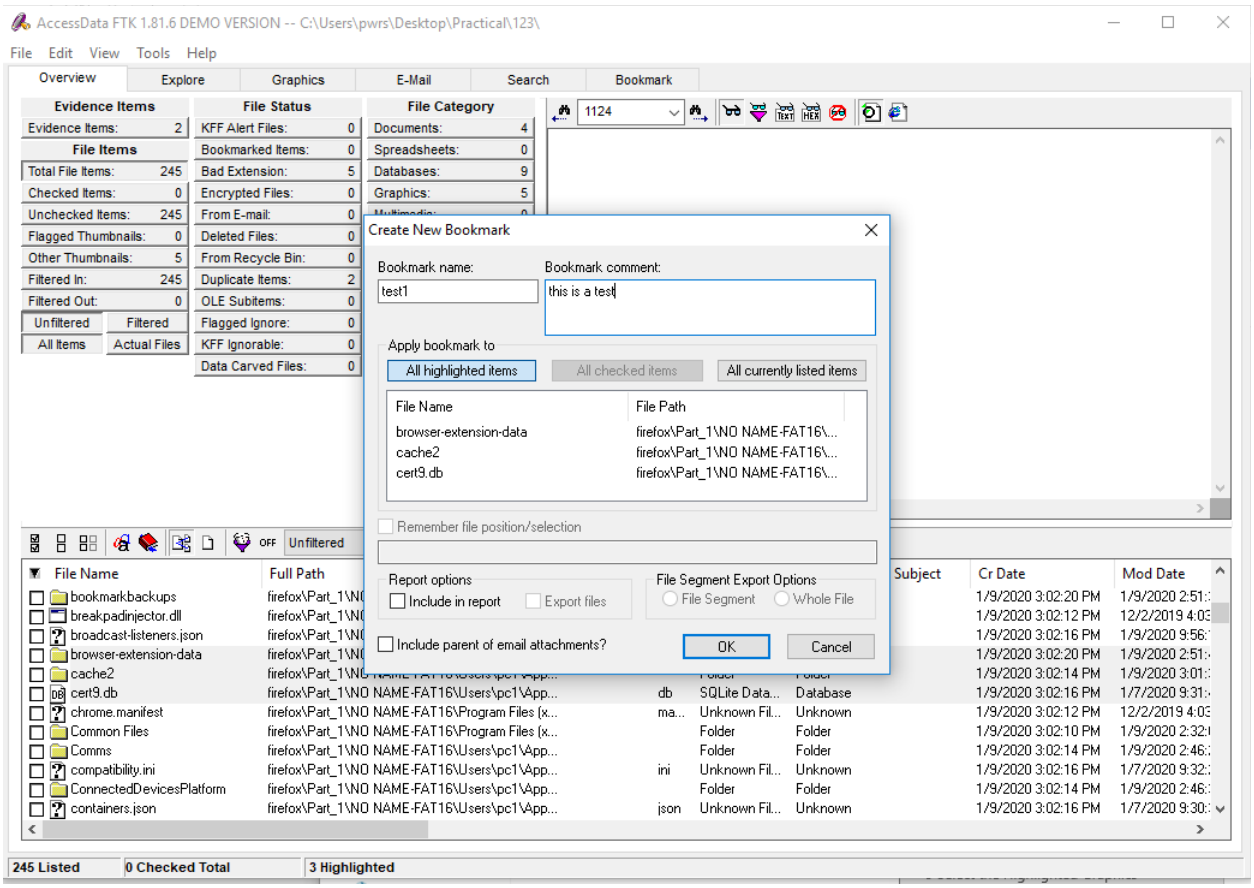
5. Click the Search tab

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

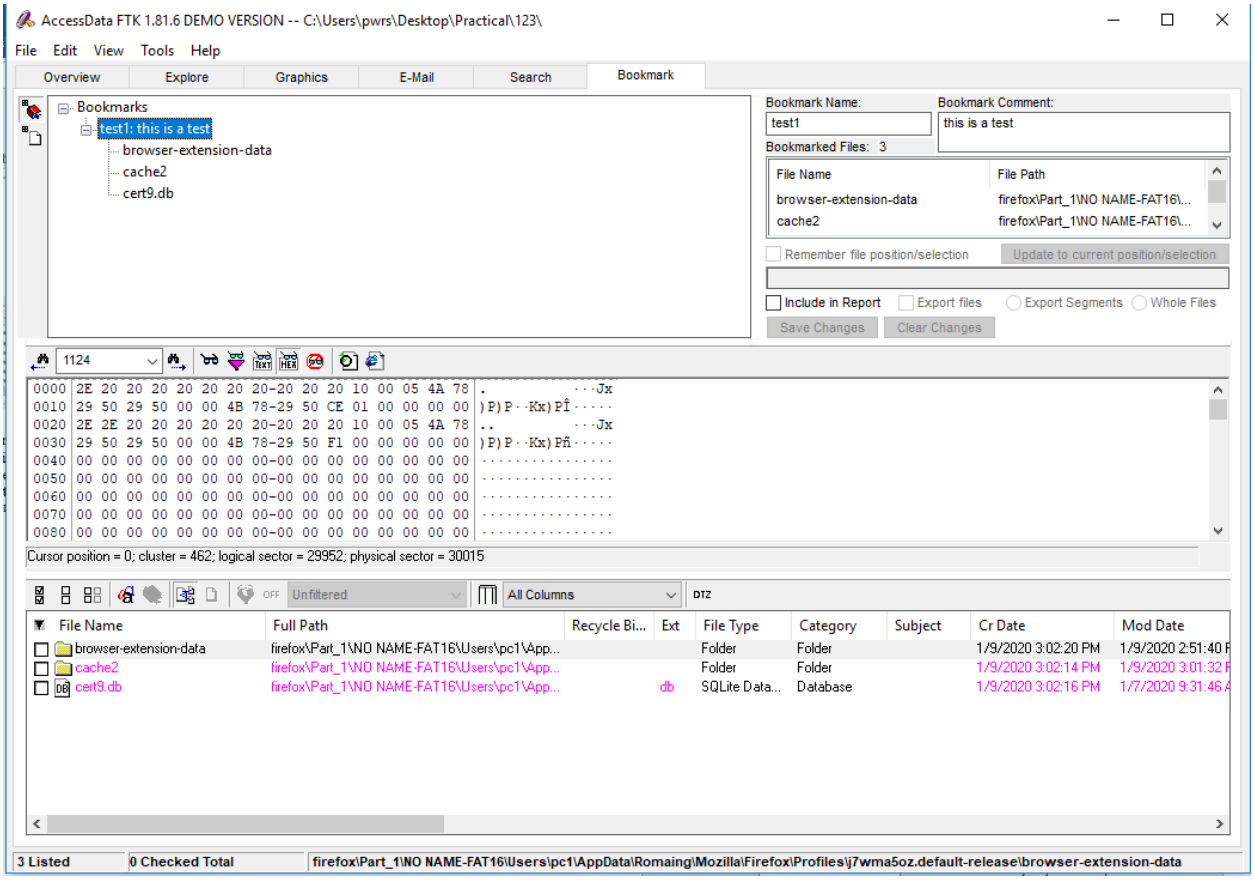


6. Bookmark part

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.



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