

---

---

# *FTK 1.81.6 Release Notes*

## **INTRODUCTION**

This readme is a document listing important information necessary for the use of this release of FTK 1.81.6.

## **NEW FEATURES**

- A new option was added to pre-processing that enables the image name to be put in the file path .
- FTK now provides the option for segments of files to be exported and bookmarked, rather than automatically exporting or bookmarking the whole file when a segment was selected.
- Added support for the new Network License Server. This requires upgrading CodeMeter Runtime software to v4.10

## **FIXES**

- Improved indexing of email.
- Resolved several crash/hang problems in processing.
- The processing of some images was being rejected because the sector count was too high. FTK can now handle images with many more sectors.

- 
- The filter for determining which carved items get added to the case (by size or pixel count) was on by default even though it was grayed out. It is now off by default and the user setting is persistent.
  - In order to improve memory management, the time a particular view remains cached in memory has been reduced.
  - Improved file handling capability to resolve errors in opening OLE files during processing and in the user interface.
  - The date column was fixed in Firefox history to be compatible with changes in newer versions of Firefox .

## COMMENTS?

- We value all feedback from our customers. Please contact us at **support@accessdata.com**, or send documentation issues to **documentation@accessdata.com**.

---

---

# *FTK 1.81.5 Release Notes*

## INTRODUCTION

This readme is a document listing important information necessary for the use of this release of FTK 1.81.5.

## FIXES

- Fixed a processing crash that caused a C++ runtime error.

## COMMENTS?

- We value all feedback from our customers. Please contact us at [support@accessdata.com](mailto:support@accessdata.com), or send documentation issues to [documentation@accessdata.com](mailto:documentation@accessdata.com).

---

---

# *FTK 1.81.4 Release Notes*

## **INTRODUCTION**

This readme is a document listing important information necessary for the use of this release of FTK 1.81.4.

## **NEW AND IMPROVED**

- Faster report generation when large amounts of data are selected from inside zip and email archives.
- Added viewer support for Firefox 3 file types (bookmarks, Browse history, Input history, Search Engines).
- Now supports carving of partial/incomplete buddy lists (Bag files).
- FTK now installs on 64-bit machines in 32-bit compatibility mode.
- FTK now has default values for minimum pixel height and width for graphics carving. Any graphic smaller than 130 x 130 pixels will not be added by default. This will reduce the number of unimportant graphics that get added to the case.
- FTK now uses a default minimum file size of 12 KB for carved files. Non-graphic carved files smaller than 12 KB will not be added to the case by default.
- Bookmarks can now be backed up and restored even when a case has been reprocessed and item numbers have changed.

---

# FIXES

The following issue has been fixed with this release of FTK 1.81.4:

- Truncated (incomplete or partial) AOL Bag files no longer causes FTK to crash.
- Improved error handling if FTK loses connection to the evidence file.
- Improved handling of .search-ms files.
- Improved handling of larger PST files (over 2 GB).
- Fixed an error with “Dongle not found” messages interfering with processing.
- Fixed a crash that occurred when trying to create an Access database using Copy Special.

**Important:** The following is an addition to instructions for **FTK VIRTUAL MEMORY USAGE AND CONFIGURATION**, as seen in the 1.8.3 Release Notes included below:

- When setting up the extra memory for the FTK processing, if your video memory is shared with system memory you should set userva to 2.5 GB instead of 3 GB. Otherwise login problems can occur.  
Syntax is as follows:  
`/userva=2560`

# COMMENTS?

We value all feedback from our customers. Please contact us at [support@accessdata.com](mailto:support@accessdata.com), or send documentation issues to [documentation@accessdata.com](mailto:documentation@accessdata.com).

---

---

# *FTK 1.81.3 Release Notes*

## **INTRODUCTION**

This readme is a document listing important changes to FTK 1.81.

## **NEW FEATURES**

- New export options that allow users to choose the format of files exported when HTML views are available. (User no longer has to export both the binary and html formats of these files)
- FTK can now use a larger virtual memory space (see instructions at the end of the release notes for details).

## **FIXES**

- Improved performance while data carving during pre-processing.
- Improved stability when processing certain PGP files.
- Improved stability when processing certain AOL Bag files.
- Improved stability when handling Unicode filenames.

- 
- Other general stability fixes in UI and processing.

## FTK VIRTUAL MEMORY USAGE AND CONFIGURATION

FTK 1.x uses an architecture that can utilize a significant amount of memory. Sometimes it uses more memory than is available in real memory. The operating system facilitates this by giving FTK virtual memory. It gives the operating system 2 gigabytes, and 2 gigabytes to the FTK processes (of the 32 bit, 4 gigabyte address space that is available to the program). The processor maps virtual memory to wherever the real memory is when FTK accesses that memory. When FTK asks for memory, the operating system gives a contiguous block of address space (memory) of the size requested. Over time, the 2 gigabytes of address space becomes fragmented between allocated blocks. FTK sometimes asks for a block of memory that is bigger than the largest free block of physical memory available. This causes the program to crash because it can't get the memory it requires to continue. This used to happen infrequently but as cases have gotten larger FTK encounters this much more frequently.

Most 32 bit operating systems from Microsoft have the ability to allow users to change the amount of virtual address space available to FTK and other applications. They call it 4GT RAM tuning. It is documented here, <http://msdn.microsoft.com/en-us/library/ms791558.aspx>, for the device driver people but it applies to applications as well. It states that:

*The 4GT RAM Tuning feature is fully functional on Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, and all editions of Windows XP, Windows Server 2003, Windows Vista, and later versions of Windows.*

Taking advantage of this feature will make it possible to avoid this crash except in extreme circumstances.

To make this work you will need FTK version 1.81.3 or greater. Then, you will do 1 of 2 things. For Windows XP and some Windows server operating systems, you simply edit boot.ini (a hidden system file at c:\boot.ini) and add /3GB switch to the end of the line.

For example, here is a sample boot.ini with the switch added

```
[boot loader]
```

---

timeout=30

default=multi(0)disk(0)rdisk(0)partition(2)\WINDOWS

[operating systems]

multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Microsoft Windows XP Professional" /noexecute=optin /fastdetect /3GB

You can also divide the space differently by using

**/3GB** [ **/userva=SizeInMB** ]

Where SizeInMB is between 0 and 1024.

In windows server 2008 and Vista, you have to set this up by starting a command prompt as admin and then typing

Bcdedit /set IncreaseUserVA=SizeInMB

Where SizeInMB is a number between 2048 and 3072

We hope that this recommended settings change will alleviate this crash for customers and make the product more useful and effective. FTK 1.81.3 *Release Notes*

## COMMENTS?

We value all feedback from our customers. Please contact us at **support@accessdata.com**, or send documentation issues to **documentation@accessdata.com**.

---

---

# *FTK 1.81.2 Release Notes*

## INTRODUCTION

This readme is a document listing important information necessary for the use of this release of FTK 1.81.2.

## FIXES

The following issue has been fixed with this release of FTK 1.81.2:

- FTK no longer crashes while trying to process **main.idx** file.

## COMMENTS?

We value all feedback from our customers. Please contact us at **support@accessdata.com**, or send documentation issues to **documentation@accessdata.com**.

---

---

# *FTK 1.81 Release Notes*

This document provides a brief overview of new features and enhancements in AccessData FTK 1.81.

## **NEW FEATURES**

The following sections list new features added to FTK since the last release.

### **FIREFOX SUPPORT**

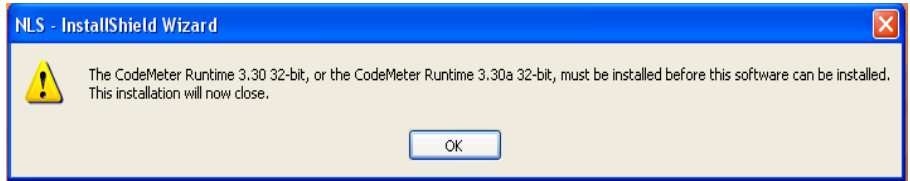
- FTK 1.81 now supports the new FireFox cookie format.  
Note: All cookie expiration times are shown in local machine time.

### **ACCESSDATA NETWORK LICENSE SERVICE**

The AccessData<sup>®</sup> (AD) Network License Service (NLS) extends the functionality of the WIBU\* CmStick\* and its licenses across a network to allow multiple machines on the network to run AD software without requiring a locally-installed and connected CmStick at each workstation.

**Important:** You must have the CmStick software installed before you install the AD NLS software. The system gives the following error message to remind you to do so:

Figure 1-1 CmStick Installation Reminder

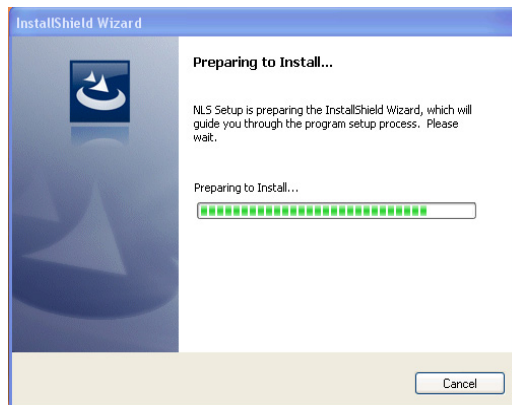


**Note:** The AD NLS CmStick ships from AccessData to serve solely as an AD NLS CmStick and will not function as a local license CmStick. If you need to run a local copy of FTK 2 or AD Enterprise, be sure to have a local license CmStick installed and connected. You can install both CmSticks on the same computer, but you can connect only one at a time.

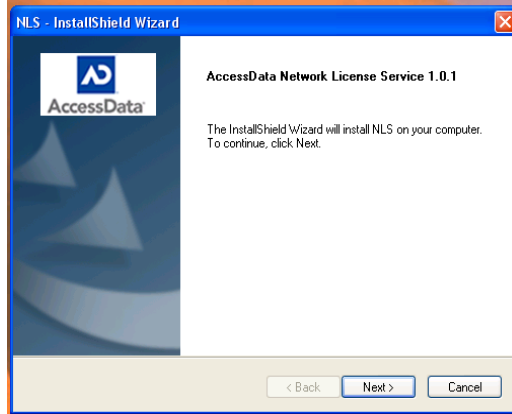
## INSTALLING AND SETTING UP THE LICENSING SERVICE

Before you can operate AD NLS, you need to set up a licensing service to serve as an AD NLS license check-out point. Perform the following steps:

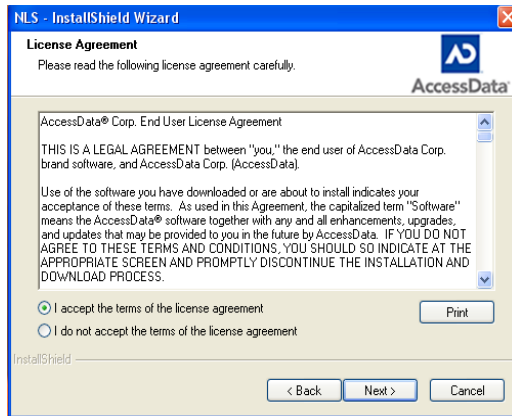
1. Open the folder with the NLS installer and double-click `nls_install.exe`.



2. Wait through the setup preparation.



3. Click *Next*.

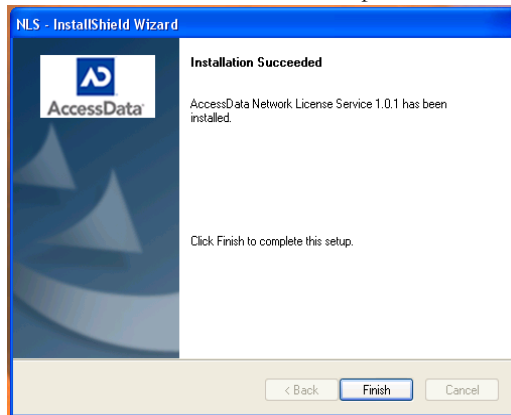


4. Read through and choose to accept the license agreement.

5. Click *Next*.

---

6. Wait for the installation to complete.



7. When the installation is complete, click *Finish* to close the installation dialogs.

**Note:** The AD NLS program should start automatically. Because it runs as a service, if you need to start it, or stop and restart it, you can do so by clicking *Start > Run >* and typing *services.msc*. Click *OK*. Right-click on the service and choose the option you need.

## AD NLS PORT INFORMATION

AD NLS communicates on the following ports:

- **dataPort:** 6921 (Data)
- **httpPort:** 5555 (Licensing)

Note: The httpPort remains hard-coded in the program.

## MANAGING LICENSES

To operate an AD product such as FTK 2 or AD Enterprise remotely from the licensing service, you must lease a license from the NLS. The NLS keeps, on its CmStick, the licenses you own for FTK 2 and AD Enterprise, and tracks the number of licenses either in use, or available for lease.

## VIEWING LICENSES

You can view the licenses available on your network CmStick by opening a browser window and entering <http://localhost:5555> into the address bar.

Figure 1-2 httpPort 5555 Displaying License Information

Leased licenses					
Locking Host	License product	License sub-product	License expiration date	Lease Time	Lease Expiration Time
<input type="button" value="Revoke licenses"/>					
Available licenses					
License product	License sub-product	License expiration date	Count		
Forensic Toolkit	Worker	05/31/2008	1		
Forensic Toolkit	Worker	11/30/2008	2		
Forensic Toolkit	Client	05/31/2008	1		
Forensic Toolkit	Client	11/30/2008	4		
eDiscovery	Worker	11/30/2008	1		
eDiscovery	Client	11/30/2008	1		
FTK Enterprise	Client	11/30/2008	1		

The httpPort screen displays the following frequently updated information for leased licenses:

**TABLE 1-1 Leased License Information**

Column	Information
Locking Host	The IP address of the host machine that is currently leasing the license listed in the product information to the right.
License Product	The name of the licensed product the Locking Host has leased from the NLS. These include: <ul style="list-style-type: none"> <li>• FTK 2</li> <li>• AD Enterprise</li> </ul>
License Sub-Product	The element of the licensed product that is actually checked out, as from the following list: <ul style="list-style-type: none"> <li>• Client</li> <li>• Worker</li> </ul>
License Expiration Date	The date on which the license expires from usability, not the date of the lease expiration.

---

**TABLE 1-1 Leased License Information**

<b>Column</b>	<b>Information</b>
Lease Time	The remaining time on the lease for the current license.
Lease Expiration Time	The time at which the lease expires. The lease can be renewed up until this time.

For information on the use of the Revoke Licenses button, see “Revoking a License” on page 16.

The screen also displays information on the licenses available on the network CmStick, as explained in the following table:

**TABLE 1-2 Available License Information**

<b>Column</b>	<b>Information</b>
License Product	The name of the product that is licensed and available for lease.
License Sub-Product	The element of the licensed product that is actually checked out, as from the following list: <ul style="list-style-type: none"><li>• Client</li><li>• Worker</li></ul>
License Expiration Date	The date on which the license expires from usability, not the date of the lease expiration.
Count	The number of each type of license available for lease.

## **ADDING LICENSES FOR LEASE**

To add licenses to an AD NLS CmStick, use AD LicenseManager. Add the licenses you purchase to the CmStick just as you normally do with the stand-alone CmStick. For more information on adding licenses using AD LicenseManager, please refer to your AD LicenseManager documentation. To purchase additional licenses, contact your AccessData Sales Rep.

---

## LEASING A LICENSE

When a request comes to the AD NLS for a license, the AD NLS checks for available licenses. If the AD NLS finds an available license, it leases that license to the requesting computer for the default period of eight hours.

After eight hours if no longer in use, the license expires, unless renewed prior to its expiration, as explained below.

## RENEWING A LICENSE

If a computer user running a product using a leased license needs to use the product lease for a longer period than the initial eight hours, the license automatically renews until the user releases the license. If the license attempts to renew and the service proves unable to renew the license, the user receives notification of the license renewal failure.

## RELEASING A LICENSE

When the local computer user is finished with the needed license, the user exits the program and the license releases immediately and returns to the pool of available licenses.

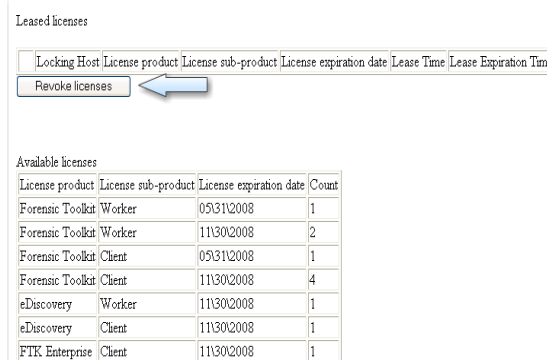
## REVOKING A LICENSE

You can revoke licenses in two ways:

- Individually, through the Localhost on port 5555
- Globally, by unplugging the AD NLS CmStick

To revoke an individual license, open the <http://localhost:5555> port and select a license. Then click the *Revoke License* button, as indicated in the following figure:

Figure 1-3 Localbost with Revoke Button Indicated



The screenshot shows the Localbost interface. At the top, there is a section titled 'Leased licenses' with a table containing columns: Locking Host, License product, License sub-product, License expiration date, Lease Time, and Lease Expiration Time. Below this table is a 'Revoke licenses' button, which is highlighted with a blue arrow pointing to it from the right. Below the 'Leased licenses' section is a section titled 'Available licenses' with a table containing columns: License product, License sub-product, License expiration date, and Count.

License product	License sub-product	License expiration date	Count
Forensic Toolkit	Worker	05/31/2008	1
Forensic Toolkit	Worker	11/30/2008	2
Forensic Toolkit	Client	05/31/2008	1
Forensic Toolkit	Client	11/30/2008	4
eDiscovery	Worker	11/30/2008	1
eDiscovery	Client	11/30/2008	1
FTK Enterprise	Client	11/30/2008	1

To revoke all licenses simultaneously, disconnect the CmStick from the machine.

## TURNING OFF THE SERVICE

If you turn off the service, the leased licenses remain leased for the remaining period of the lease. However, the expired leases send the user a message warning that the lease cannot be renewed.

## ENHANCEMENTS

The following sections list enhancements to FTK since the last release.

### EUDORA EMAIL

Improved processing and display of Eudora Email.

### FLOPPY DONGLE SUPPORT

Support for the floppy dongle is discontinued due to the addition of the Network License Service (NLS).

---

## MISCELLANEOUS

- Improved handling of large registry files when exported for Registry Viewer analysis.
- Improved canceling of backups; target backup folder will no longer be affected.
- Improved program performance and memory handling.

## FEEDBACK

We value all feedback from our customers. Please contact us at [support@accessdata.com](mailto:support@accessdata.com).