**Distributed Processing**

For more information contact: info@syntricate.com

---

**What is Distributed Processing?**

An FTK examiner machine can be configured to utilize three additional machines to assist case creation / data processing as remote "workers". These additional processing engines are in addition to the local machine FTK installation engine. Distributed processing increases productivity while decreasing processing time.

**What is needed to configure Distributed Processing?**

The additional components needed for distributed processing with FTK:

- .NET 3.5 Service Pack 1
- Microsoft Windows Installer 4.5
- AccessData Distributed Processing Engine (DPE executable)

This document assumes an existing installation of FTK as outlined in Chapter 3 of the FTK user guide. The Distributed Processing Engine is not to be installed on the examiner FTK examiner machine.

**Configuring Distributed Processing:**

**BEFORE BEGINNING!**

It is important to note the remote worker machines should have only the distributed processing engine installed. Remote worker machines should not have stand alone FTK with the single processing engine installed.

It is also essential that the remote worker machines have unimpeded network permissions and connectivity to the machine that contains the cases folder and evidence folder to be utilized in the distributed processing environment. These folders need to be shared with full read / write control (illustrated later in this document).
Distributed Processing

For more information contact: info@syntricate.com

Environment Setup

This environment represents a standard FTK installation on a single examiner machine with evidence files and the database residing together with FTK. Optional host and evidence storage machines are displayed but not used in this configuration (see FAQ #12 for more information on that type of configuration).

The following configuration steps assume a Windows XP or Vista operating system and full network connectivity between all machines. For assistance with creating a network, contact your IT department or network administrator. Using the above environment setup, gather the following information from each machine:

- Machine IP address on the network (Steps for Windows XP and Vista are the same)
  - Click on the Start or Windows button and select the "Run" option.
  - In the Run box, type the command "cmd" as illustrated below.

![Run dialog box](https://via.placeholder.com/150)

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Syntricate makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, Inc. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.
o In the resulting command box, utilize the “ipconfig /all” command to determine the IP address of the network connection adaptor (if unfamiliar with network addressing, consult IT or the network administrator for assistance with this).

- User account credentials (logon name and password)

**NOTE**: The easiest way to ensure that the remote worker machines can fully communicate with the FTK examiner machine hosting the cases and evidence folders is to have all machines logged in to Windows with mirrored user accounts. This means all machines log in with the same user name and account password. Create Administrator privileged user accounts with the same user name and account passwords on all machines in the environment via the following steps:
Distributed Processing

For more information contact: info@syntricate.com

See the FAQ #8, #9 and #10 at the end of this document for important notes regarding using mirrored accounts vs. individual accounts and installing in a domain environment.

In Windows XP:

- Click on the Start or Windows button and select the "Control Panel" option.
- In the Control Panel, select the "User Accounts" application as illustrated (#1).
- In User Accounts, select "Create a new account" as illustrated (#2).
- In User Accounts, name the new account as illustrated (#3).
- In User Accounts, pick an account type of "Administrator" as illustrated (#4).

---

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Syntricate makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, Inc. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.
In Windows Vista and Windows 7:

- Click on the Start or Windows button and select the "Control Panel" option.
- In the Control Panel, select the "User Accounts" application as illustrated (#1).
- In User Accounts, select "Manage another account" as illustrated (#2).
- In Manage Accounts, select "Create New Account" as illustrated (#3).
- In Create New Account, name the account and select an account type of "Administrator" as illustrated (#4).
NOTE: Remote worker machines require access to the cases folder and evidence folder(s) on whichever machine they reside. This access must be unimpeded and these folders must be shared with read / write permissions. To ensure this state, perform the following actions with these folders.

In Windows XP:

- Locate the case and evidence folders in your networked environment.
- Right click on the folders and select "Sharing and Security...".
- In the next window, select "Share this folder" as illustrated (#1)
- Click the "Permissions" box (#1) and then select the box to allow "Full Control" as illustrated (#2). This will automatically select "Change" and "Read" as well.
- Click the “Apply” button on all windows as steps are completed.
In Windows Vista and Windows 7:

- Locate the case and evidence folders in your networked environment.
- Right click on the folder and select "Properties".
- In the next window, select the "Sharing" tab as illustrated (#1).
- In the next window, click the "Advanced Sharing" box as illustrated (#1).
- In the next window, select the "Share this folder" option as illustrated (#2).
- Click the "Permissions" box (#2) and select the box to allow "Full Control" as illustrated (#3). This will automatically select "Change" and "Read" as well.
- Click the "Apply" button on all windows as steps are completed.
At this stage, the environment should be in a state where all machines are logged in with Administrative accounts with the same user name and password, and all machine IP addresses have been documented. Use this template to assist documenting that information:

Username: __________________________
Password: __________________________
IP address: __________________________

* Cases folder should be shared with read / write access!

* Evidence folder should be shared with read / write access!
Installing the remote worker Distributed Processing Engines

The installer for a distributed worker is the same installer used in the FTK install for the main processing engine. On each machine, follow these installation steps:

1) **Launch** the FTK Installer and choose *Distributed Engine*.
   (Depending on your current machine configuration you may also have to install the .NET 3.5 SP1 and / or the Microsoft Windows Installer 4.5)
2) Click "Next" when prompted.
3) Accept the "License Agreement" - click "Next".
4) Note the Install destination Folder and click "Next".
   *Note: Do not uncheck the “Install as distributed engine” option*
5) Note the processing data path and change if needed.
   *Note: You should exclude this path from any virus scanning.*
6) Input the Administrative account name and password for the remote machine. This must be the account that has read / write access to the shared case and evidence folders. If the machine is on a domain, enter the domain name - leave "Domain" blank if none is present - click "Next".
7) Click "Install" to begin installation and "Finish" when complete.

Configuring FTK to utilize remote worker machines

When all remote worker machines have been configured, they can be added to the FTK client. Accomplish this configuration via these steps:

- In the FTK Database Management window select the menu option: "Tools \ Processing Engine Configuration".
- In the "Add engine" section, input the IP addresses of the remote machines. Click "Add" after inputting each remote machine IP address - each machine will propagate in the "Computer Name/IP" list as the Add button is clicked.
- Close the Processing Engine Configuration window when complete.
Creating a Case using Distributed Processing

- Create a new case. It is a requirement the "Case Folder Directory" be a UNC path to its location on the hosting machine in the distributed environment. *Remember*, this folder must be shared with read / write permissions (configured earlier in this document). Utilize the three dot ellipse on the "New Case Options" console to navigate to the UNC path of the shared Case Folder Directory as illustrated (#1).

- In the "Manage Evidence" console, it is a requirement the evidence "Path" be a UNC path to its location on the hosting machine in the distributed environment. *Remember*, this folder must be shared with read / write permissions (configured earlier in this document). When selecting the evidence to add to the case, be sure to browse to the evidence location via the network path when adding that evidence. In the "Manage Evidence" console, validate the UNC path of the shared evidence location as illustrated (#2).

- **With those two requirements met**, continue to create the case normally.
Distributed Processing

For more information contact: info@syntricate.com

#1

#2

SYNTRICTATE

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Syntricate makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, Inc. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.
NOTE: The remote machines will not immediately commence working on a case. New processes named "ADProcessor.exe" and "ADIndexer.exe" will spawn on the remote machines and can be observed in the remote worker machine process lists via the Windows Task Manager.

As the FTK examiner machine begins to enumerate (discover) items in the case, the enumeration builds to a point where the items are pushed into the database. At that stage, the enumerated items become "things to do" and will be assigned out to the remote worker machines previously configured in the FTK client. As these "item pushes" continue as the case "discovery" increases, the remote worker machines continue to function until case processing is complete.
Distributed processing install summary checklist / FAQ

- Add network connectivity between remote machines and FTK examiner machine
- Share cases and evidence folders with full read / write permissions
- Appropriately permission accounts for all machines in distributed environment
- Document IP address information for all machines in distributed environment
- Install Distributed Process Engines to remote machines (providing administrative credentials with read / write access to the shared case and evidence folders)
- Add remote machines to the FTK examiner machine (via FTK interface)
- Create FTK case with UNC paths for the case and evidence file locations

Q: The Distributed Processing Engine installation fails or the installed service fails to start because it needs appropriate logon rights - how is this overcome?
A: Follow these steps:

- Right click on the "My Computer" icon in Windows XP (the "Computer" icon in Windows Vista).
- Select "Manage" from the right click menu.
- In the Computer Management Console, expand "Services and Applications" and click on "Services" as illustrated (#1). The machine service list will populate.
- Locate the "AccessData Processing Engine Service" and view the "Properties" dialog box by double clicking on the AccessData Processing Engine Service (#1).
- In the Properties window, select the "Log On" tab. Verify the correct Administrative logon credentials for the service (#2).
- Stop and Restart this service after performing any credential update (#1).

-- OR --

- If the failure was during installation, click "Retry" on the installation window.

NOTE: When deploying, the credentials used by this service need to be part of the Administrator control group and must have read / write access to the shared case and evidence folders.
Distributed Processing

For more information contact: info@syntricate.com

Q: What is the option to "Maintain UI performance when processing"?
A: It allows the choice of making preprocessing or UI performance a precedent.

Q: What if a remote machine does not have the .NET 3.5 SP1 or the Microsoft Windows Installer 4.5?
A: The Distributed Processing Engine installer will provide these components during the installation process. This will cause the machine to reboot during the installation process - save any work before installation.

Q: In the FTK interface, what are the Processing Engine Configuration options: "Remove / Enable / Disable"?
A: Remove - removes a worker from the list. Enable - enables a worker. Disable - disables a worker (it will not receive work until re-enabled).

Q: ADProcessor.exe spawns remotely, but doesn't engage - what is wrong?
A: The most common problem in this scenario is pointing the case and / or evidence paths to local machine locations rather than the proper, fully shared, UNC path locations. Remember also, that a threshold of items must be enumerated and pushed into the database before remote workers will assist the FTK examiner machine. Also, check the entered IP addresses to ensure proper connectivity between the FTK examiner machine and remote worker machines.

Q: What other things can be done to fix issues preventing distributed processing?
A: Allow a firewall exception to the port used by the remote worker machines (default = 34097).
Q: Can machine names be used instead of machine IP addresses?
A: Yes, as long as proper name resolution is occurring on the network.

Q: Is it necessary for the remote worker machine accounts to be logged on for a remote worker machine engine to process data?
A: No, as long as the Distributed Processing Service Engine is installed with administrative credentials, and those credentials have full read / write permissions to the cases and evidence files folders on the FTK examiner machine.

In this graphic, ADProcessor is running as a service (Ken) that is not the logged on service user (Alice).

Q: Is it necessary to use mirrored accounts?
A: In a non-domain environment, this is the easiest way to facilitate machine communication. In a domain, users can be given individual permission to the case and evidence folders.
Q: What if the existing network for distributed implementation is domain based?
A: Add these steps to your installation process:

- When installing the Distributed Processing Engines, list your domain name at this step of the installation:

  ![Instillation Wizard](image)

- Be sure to install the engine with a domain-based user account.
- Ensure that domain-based user account has permission to install software.
- Ensure that domain-based user account has read / write permissions to the case and evidence folder.

Q: Can remote worker machines be added to FTK while a case is processing?
A: Yes, but they may not receive work until the next push of enumerated items.

Q: What if the distributed network environment is using standalone machines to separately host the database and evidence files?
A: The database configuration would have presumably been taken care of during the FTK examiner installation and the evidence files on the evidence host machine would need to be configured according to this document - SHARED to the remote worker machines, with full read / write access permissions (bet you never heard that before?).