HOW TO USE REMOTE DEVICE MOUNTING SERVICES

The Remote Data Mounting Services (RDMS) lets you acquire live evidence from active and remote network computers. You can gather many types of active information from network computers, including volatile data, memory data (RAM), and preview and image physical and logical drives. In addition, you can forensically mount physical devices and logical volumes on the examiner's machine from a single live system. SSL is used to ensure communication between the agent and examiner is protected using either a self-signed certificate or one signed by a Certificate Authority (CA). The examiner can utilize one of two methods to analyze a remote system; a Temporary Agent or the permanent Enterprise Agent.

The FTK Temporary Agent is an application for short-term use on client computers to access and acquire specific remote live evidence. It is set to expire after a period of inactivity and then it automatically uninstalls itself. The agent is only viable on the computer until the system is either turned off or rebooted. The Temporary Agent allows the examiner to image a drive remotely, acquire the active RAM, and/or mount physical devices and logical volumes.

The FTK Enterprise Agent is an application for long-term use on client computers to access and acquire specific remote live evidence. The agent can be either pushed to the remote system with FTK or can be embedded on the system manually. By using the permanent agent, the examiner can obtain the volatile data, active RAM, preview or acquire remote systems, and/or mount physical devices and logical volumes.

Prerequisites for Using FTK Agents

- FTK installed with a license.
- The FTK user account must have the Application Administrator or the Case Administrator role. Case Reviewers cannot access the **Add Remote Evidence** dialog.
- The examiner must have the administrator credentials for the remote system.
- For Windows XP systems, Simple File Sharing must be disabled on a target system. The default setting is enabled, so you must make this change manually.
- System date and time on all machines must be synchronized, or at least close. If the target machine is behind by more than 24 hours the agent connection will work, but you will not be able to acquire data.
- The port that is used must be open on any hardware or software firewalls in the network. The default port is 3999.

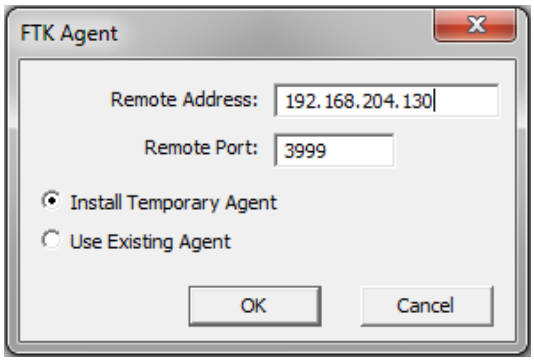
Using the FTK Temporary Agent

You can deploy the FTK Temporary Agent to a remote computer to acquire data for FTK. The temporary agent remains active until it has not had any activity for a period of 5 minutes, it then automatically uninstalls itself. It also uninstalls itself when the remote system is shutdown or rebooted. You can manually disconnect the agent from the **Tools** menu in FTK Examiner.

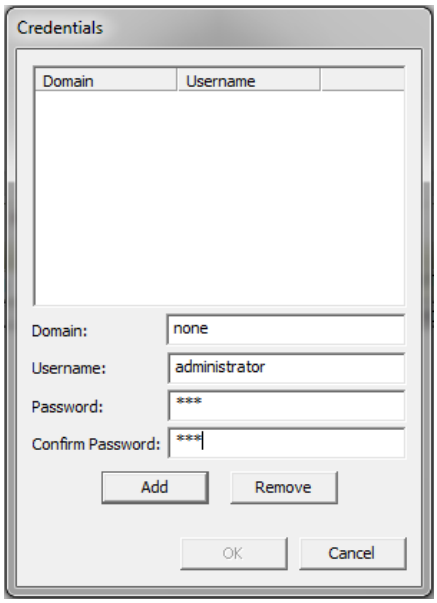
When you deploy the FTK Temporary Agent, it automatically creates and uses a temporary certificate for secure SSL communications. This certificate automatically expires and is only valid for a limited scope.

Deploying the FTK Temporary Agent

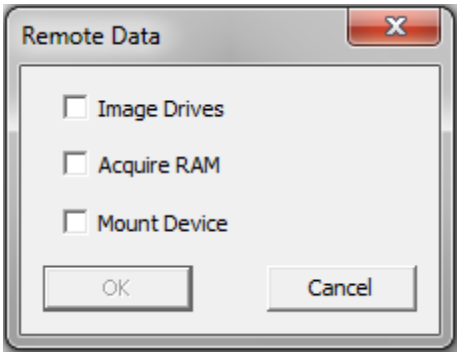
1. In the FTK examiner interface, click on **Evidence** > **Add Remote Data**.
2. Enter the IP Address of target computer.



3. Define the port for the agent to use for communication – port 3999 is the default port.
4. Choose **Install a Temporary Agent**.
5. Click **OK**.



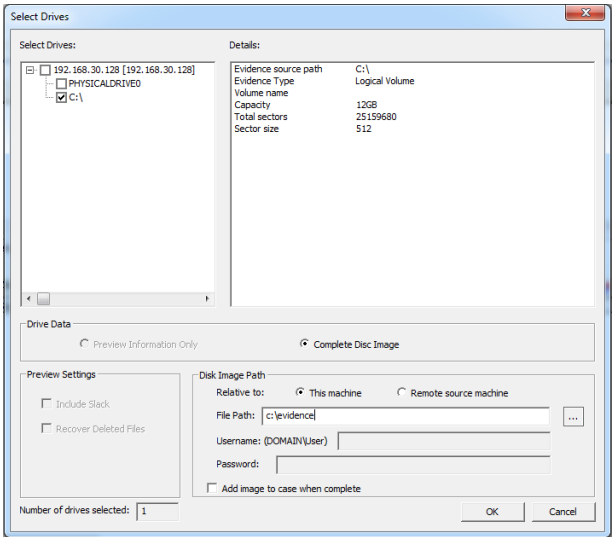
6. Enter the credentials of a user who is a member of the local administrators group on the target computer. **Note:** The authentication domain is required for both domain accounts and local accounts. If using a local account, type "none."
7. Click **Add** to add the set of credentials to the list.
8. Click **OK**.



9. In the **Remote Data** dialog, select from the following options to acquire and click **OK**.
    - **Image Drives**: Lets you create an image of a drive or device on the remote system. You can store the image on the remote computer or store it on the examiner computer. You can also automatically add the image into a case in FTK. (Refer to page 4 for more information).
    - **Acquire RAM**: Lets you acquire the data currently held in memory on the target machine. You can also capture and automatically import a memory dump, or save the memory dump to a location. (Refer to page 5 for more information).
    - M**ount Device**: lets you mount a remote drive or device and view it in Windows Explorer as if it were attached to your drive. It can be a CD or DVD, a USB storage device, or a drive or partition. (Refer to page 6 for more information).
        - **Note:** The **Preview Information Only** option is not available for the FTK Temporary Agent.

Imaging Drives with the FTK Temporary Agent

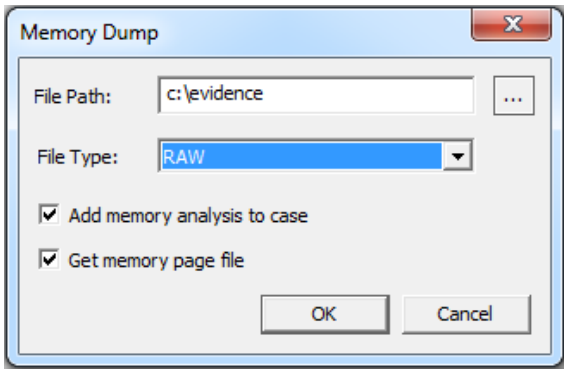
1. Follow the initial steps to deploy the Temporary FTK Agent. (Refer to page 2 for more information).
2. On the Remote Data dialog window, select **Image Drives**.



3. On the Select Drives dialog window:
    a. Select the type of image:
        1. **Physical**
        2. **Logical**
    b. Enter the path to place the image file
        1. **This machine**
        2. **Remote source machine**
        3. **File Path**
    c. If you want to add the image to the current case, check the box **Add image to case when complete**.
    d. Click **OK**.

Acquiring RAM with the FTK Temporary Agent

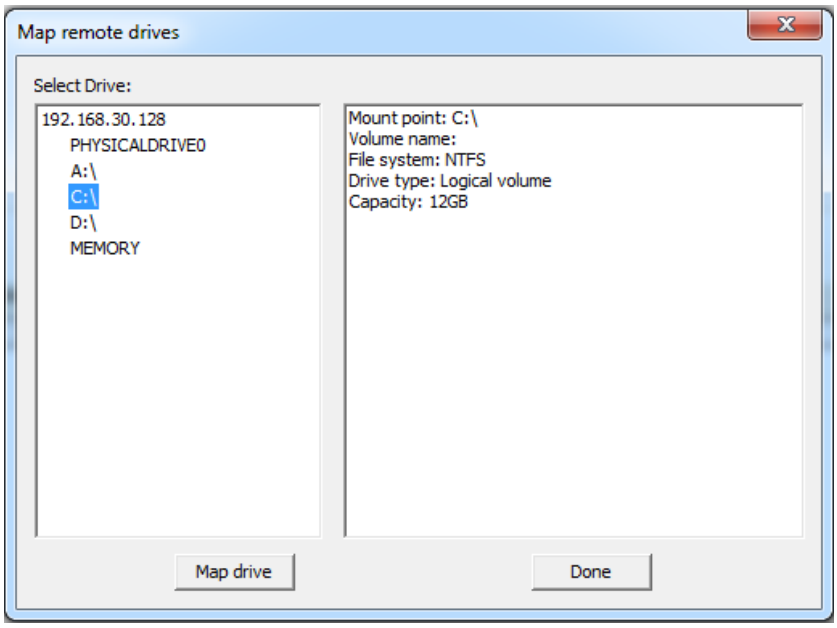
1. Follow the initial steps to deploy the Temporary FTK Agent. (Refer to page 2 for more information).
2. On the Remote Data dialog window, select **Acquire RAM.**



3. On the Memory Dump dialog window:
    a. Enter the File Path to save the memory file and page file to.
    b. Select the File Type:
        1. **RAW**
        2. **AD1**
    c. If you want to add the memory file to the current case, check **Add memory analysis to case.**
    d. To also obtain the Windows Paging file, check **Get memory page file**.
    e. Click **OK**.

Mounting a Device with the FTK Temporary Agent

1. Follow the initial steps to deploy the Temporary FTK Agent. (Refer to page 2 for more information).
2. On the Remote Data dialog window, select **Mount Device.**



3. On the Map remote drives dialog window do the following:
    a. Select the type of image:
        1. **Physical**
        2. **Logical**
    b. Click **Map drive**.
    c. Select the drive letter to use on the examiner machine.
    d. Click **OK**.
    e. Click **Done**.
4. You can now open Windows Explorer and access the remote system via the assigned drive letter.

Unmounting the FTK Temporary Agent

1. Click **Tools > Unmount Agent Drive**.
2. In the **Unmount Agent Drive** dialog, do one of the following:
    - Select a drive to unmount.
    - Select **All Agents** to unmount all drives from all agents at the same time.

Disconnecting the FTK Temporary Agent

1. Click **Tools > Disconnect Agent.**

Using the FTK Enterprise Agent

The FTK Enterprise Agent provides for the real-time acquisition of live remote evidence from a single Agent that you can install on workstations within the network.

Types of Remote Data you can Acquire with the FTK Enterprise Agent

- Volatile Data
  - Process Info
  - Services Info
  - DLL Info
  - Driver Info
  - User Info
  - Open Handles
  - Network Sockets
  - Network Devices
  - Registry Info
- Include Memory Data
  - RAM
  - Memory Search
- Include Drive Data
  - Physical Drive Info
  - Logical Drive Info
- Mount a Device

Methods of Deploying the FTK Enterprise Agent

You can use the following methods to deploy the FTK Enterprise Agent:

- A**uto Deployment**: Agents can be deployed with FTK.
- **Manual Deployment**: Agents can be installed using the agent binary and pre-created certificate running on the target machine.

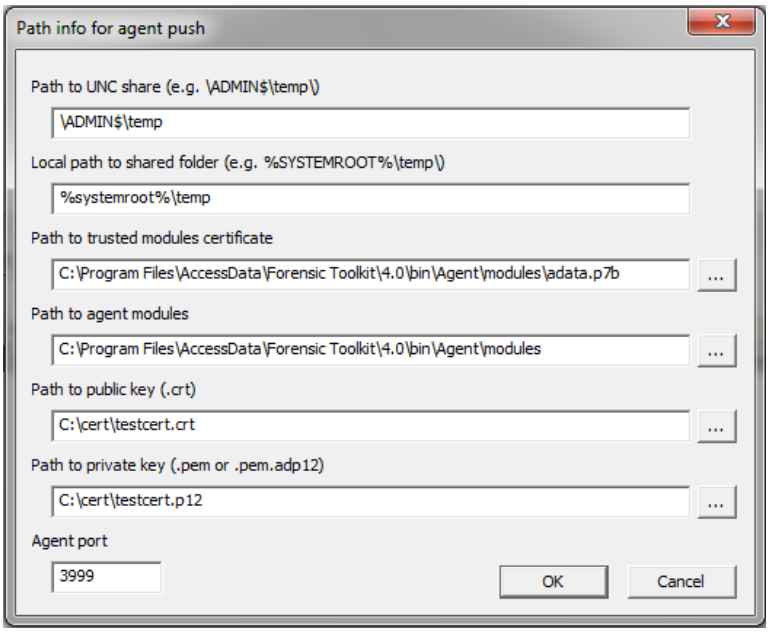
  Note: You only need to create only one set of certificate keys. All deployment methods can use the same certificate.

Preparing Certificates for Agent Deployment

1. To create your own certificates:
    - Create a new folder on the examiner computer.
    - Copy **certman.exe, libeay32.dll,** and **boost_thread-vc100-mt-1_49.dll** from the FTK bin directory (c:\Program Files\AccessData\Forensic Toolkit\5.0\bin) to the new folder.
2. From a command window, go to the directory where you copied the files.
3. Run the following command in the window: "certman –n <name of issuer> <name of certificate>"
    - Example "certman –n accessdata.com ExaminerCert"
4. Three files are created –
    - .crt <public key>
    - .p12 <private key>
    - .key <licensing info>

Setting Certificates for Agent Deployment

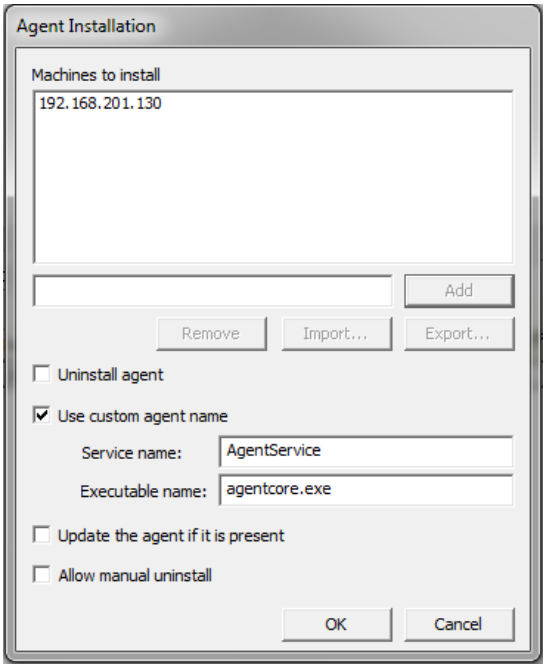
1. In order to push the Enterprise Agent from FTK, you must configure the system.
2. In the Examiner interface, select **Tools** > **Configure Agent Push**.



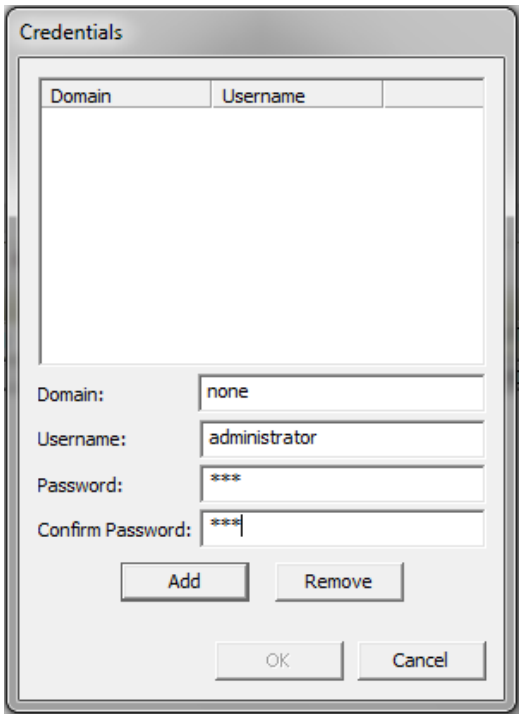
3. In the Path to public key, browse to the directory where you created the certificates and select the .crt file. (For more information on how to create a certificate, see Preparing Certificates for Agent Deployment).
4. In the Path to the private key, browse to the same directory and select the .p12 file.

Deploying the Enterprise Agent

1. In the Examiner interface, click **Tools** > **Push Agents**.



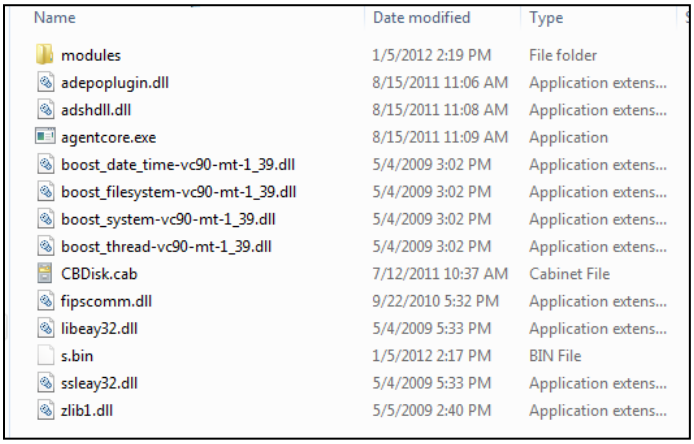
2. From the Agent Installation dialog window, enter the IP address of the system you want to push the agent to, and then click **Add**.
3. From this window you can:
    - (Optional) Select **Use a custom agent name**.
        1. Enter a custom **Service name** to hide the service.
        2. Enter a custom **Executable name** to hide the process.
    - Update an existing agent if one already exists.
    - Allow manual uninstall.
4. Click **OK**.



5. Enter the credentials of an account who is a member of the local administrators group on the target computer.

   Note: The authentication domain is required for both domain accounts and local accounts. If using a local account, enter "none."

6. Click **Add** to add the set of credentials to the list.
7. Click **OK**.
8. A directory is created on the target system at c:\Program Files\AccessData\Agent that will contain the files necessary for access to the system.



9. After the agent installation is complete, the service and process will start on the remote system.

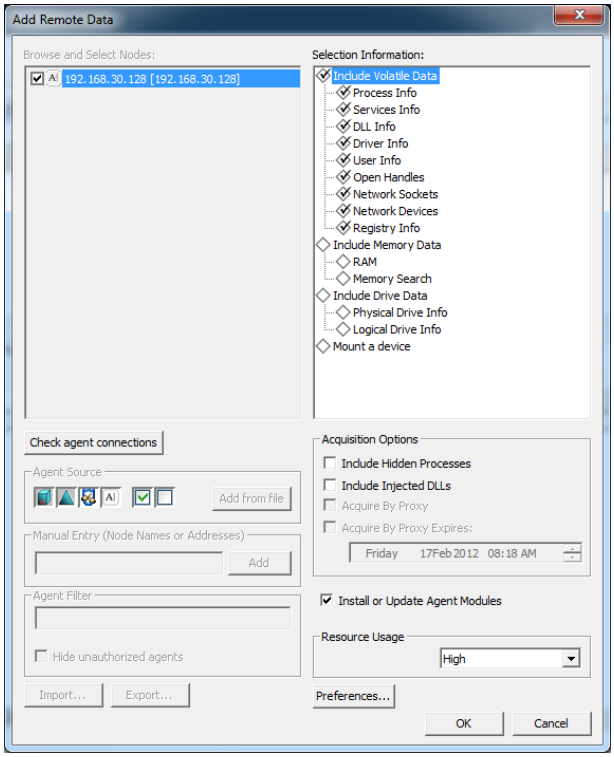
Manually Deploying the FTK Enterprise Agent

1. Create a new folder on your Examiner machine.
    - Example c:\agent
2. Copy the .crt certificate you created. (For more information on how to create a certificate, see Preparing Certificates for Agent Deployment on page 9).
3. Copy the appropriate agent from the examiner computer - c:\Program Files\ AccessData\Forensic Toolkit\5.0\bin\Agent.
4. There are two sub-directories – one for 32 bit and 64 bit installers
5. Go to the correct version folder and copy the AccessData Agent.msi or AccessData Agent (64-bit).msi to the c:\agent folder.
6. In the c:\agent directory, create a batch file to execute the install –
    - msiexec /i “accessdata agent.msi” CER=certname.crt
7. Copy the folder to a USB flash drive.
8. Insert the USB flash drive into the target machine.
9. On the remote machine – execute the batch file with admin privileges.
10. After the agent installation is complete, the service and process will start on the remote system.

    Note: You can uninstall the Agent manually by modifying the batch file. To modify the batch file from a command window, manually type:
    - msiexec /x “accessdata agent.msi” CER=certname.crt

Acquiring Volatile Data with the Enterprise Agent

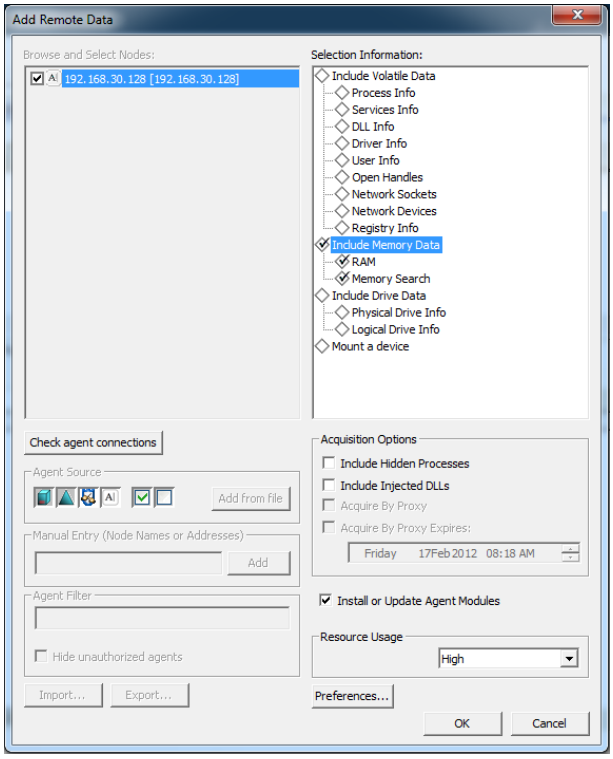
1. In the Examiner interface, select **Evidence** > **Add Remote Data**.
2. Enter the IP Address of target machine.
3. Define the port the agent will use for communication.
4. Select **Use Existing Agent**.
5. Press **OK**.
6. Enter the credentials of a user who is a member of the local administrators group on the target computer.
    a. **Domain** – Enter the domain name. If using a local account, type "none."
    b. **Username** – Administrative account username.
    c. **Password** – Administrative account password.
    d. **Confirm Password** – Re-enter the administrative account password.
    e. Click **Add**.
7. Press **OK**.



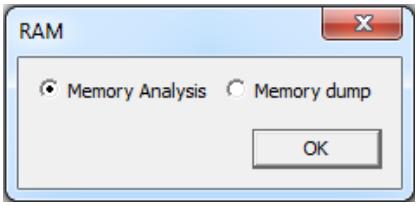
8. On the Add Remote Data dialog window:
    a. Select **Include Volatile Data**.
    b. Uncheck any Volatile Data collection you do not want.
    c. Optional Acquisition Options include:
        1. **Include Hidden Processes**
        2. **Include Injected DLL's**
9. Click **OK**.

Acquiring RAM / Memory Search with the Enterprise Agent

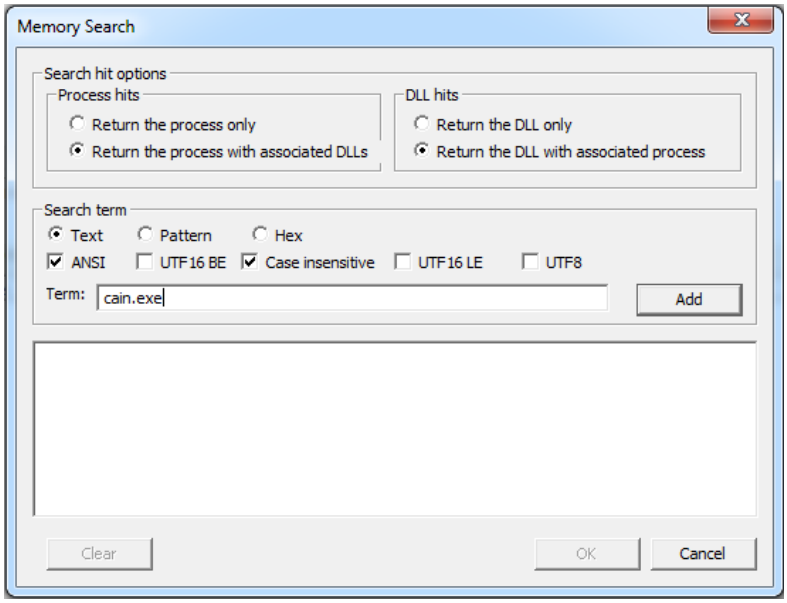
1. In the Examiner interface, select **Evidence** > **Add Remote Data**.
2. Enter the IP Address of target machine.
3. Define the port the agent will use for communication.
4. Select **Use Existing Agent**.
5. Press **OK**.
6. Enter the credentials of a user who is a member of the local administrators group on the target computer.
    a. **Domain** – Enter the domain name. If using a local account, type "none."
    b. **Username** – Administrative account username.
    c. **Password** – Administrative account password.
    d. **Confirm Password** – Re-enter the administrative account password.
    e. Click **Add**.
7. Press **OK**.



8. On the Add Remote Data dialog window:
    a. Select **RAM** or **Memory Search**.



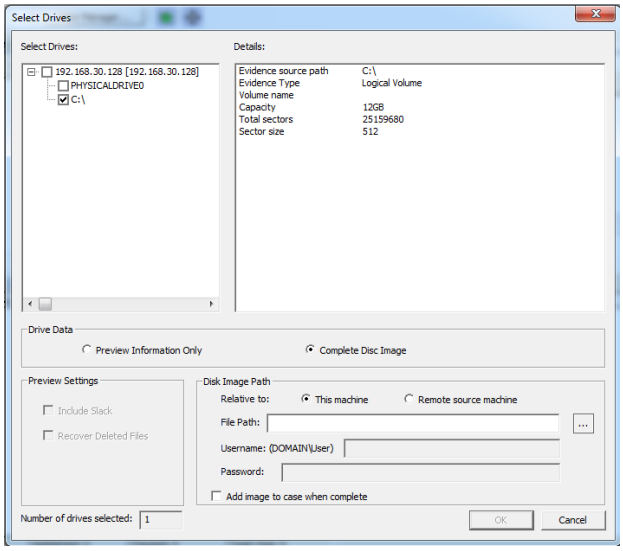
9. To acquire or analyze the memory or acquire the RAM, select:
    a. **Memory Analysis** to complete an analysis in FTK and display on the Volatile tab.
    b. **Memory Dump** to acquire RAM.
    c. Click **OK.**



10. To conduct a search of the memory, on the Memory Search dialog window, you can:
    a. Select your **Search hit Options**.
    b. Enter **Search term**.
    c. Click **Add**.
    d. Click **OK**.

Previewing or Imaging a Drive with the Enterprise Agent

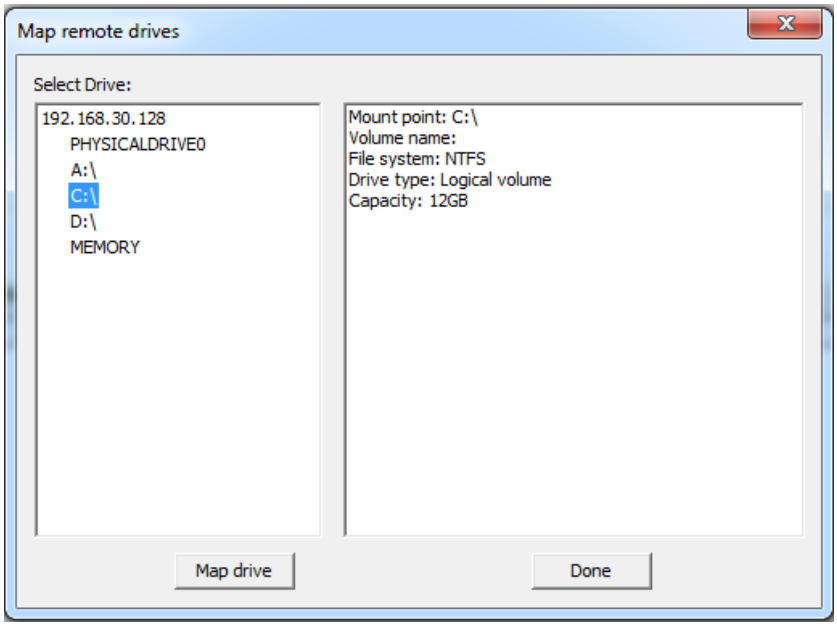
1. In the Examiner interface, select **Evidence** > **Add Remote Data**.
2. Enter the IP Address of target machine.
3. Define the port the agent will use for communication.
4. Select **Use Existing Agent**.
5. Press **OK**.
8. Enter the credentials of a user who is a member of the local administrators group on the target computer.
    a. **Domain** – Enter the domain name. If using a local account, type "none."
    b. **Username** – Administrative account username.
    c. **Password** – Administrative account password.
    d. **Confirm Password** – Re-enter the administrative account password.
    e. Click **Add**.
9. Press **OK**.



10. On the Select Drives dialog window:
    a. Select the type of image:
        1. **Physical**
        2. **Logical**
    b. In the Drive Data section, select:
        1. **Preview Information Only** (Takes a snapshot of the remote system and then adds it to the case).
        2. **Complete Disc Image**
    c. For Disk Image Path:
        1. Select **This machine**.
        2. Select **Remote source machine** to save image to remote storage location.
        3. Enter the **File Path**.
        4. If you want to add the image to the current case, check the box **Add image to case when complete**.
    d. Click **OK**.

Mounting a Device with the Enterprise Agent

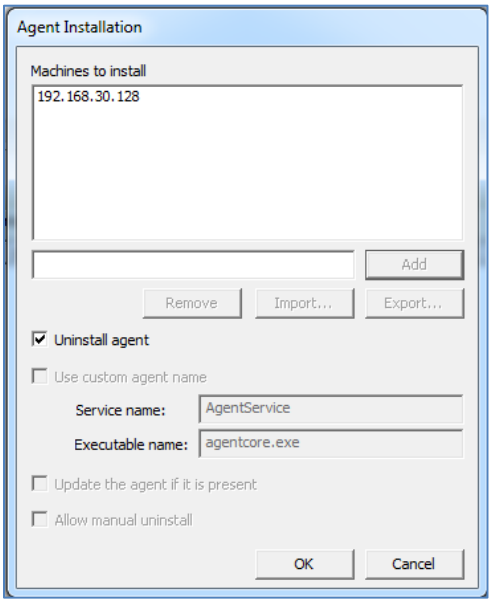
1. In the Examiner interface, select **Evidence** > **Add Remote Data**.
2. Enter the IP Address of target machine.
3. Define the port the agent will use for communication.
4. Select **Install Temporary Agent**.
5. Press **OK**.
6. Enter the credentials of a user who is a member of the local administrators group on the target computer.
    a. **Domain** – Enter the domain name. If using a local account, type "none."
    b. **Username** – Administrative account username.
    c. **Password** – Administrative account password.
    d. **Confirm Password** – Re-enter the administrative account password.
    e. Click **Add**.
7. Press **OK**.
8. On the Remote Data dialog window, select **Mount Device.**



9. On the Map remote drives dialog window:
    a. Select the type of image:
        1. **Physical**
        2. **Logical**
    b. Click **Map drive**.
    c. Select the drive letter to use on the examiner machine.
    d. Click **OK**.
    e. Click **Done**.
10. You can now open Windows Explorer and access the remote system from the assigned drive letter.

Uninstalling the Enterprise Agent from FTK

1. In the Examiner interface, click on **Tools** > **Push Agents**.



2. From the Agent Installation dialog window, enter the IP address of the system you want to uninstall the agent from, and then click **Add**.
3. Select **Uninstall agent**.
4. Click **OK**.