



Collect Features Manual

V2.0.30

OCT 20, 2009

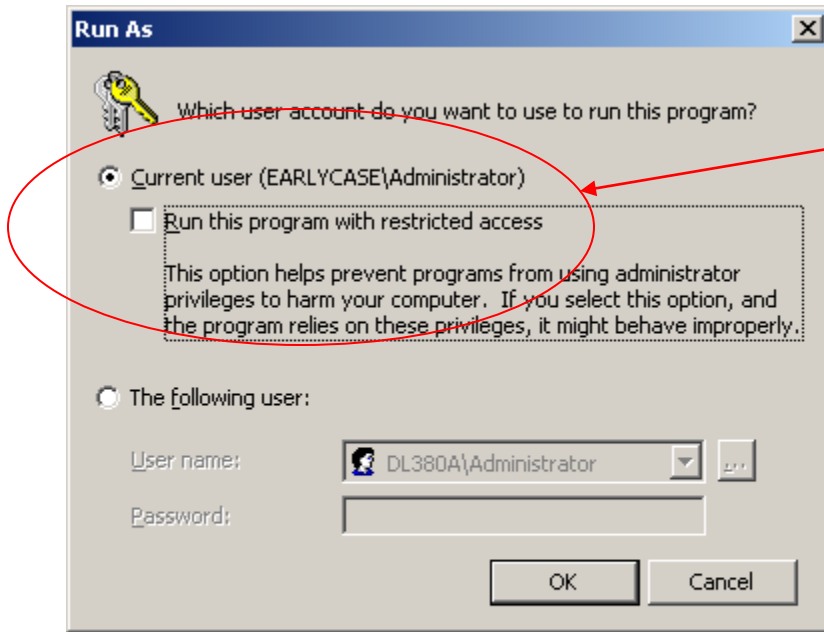
Introduction:

Version V2.0.30 of earlyCASE implements an extensive set of features related to collecting data and making forensically sound copy of ESI and disk drives. Along with the ability to collect ESI in more ways V2.0.30 also expands the types of drive images that can be analyzed natively when using the professional version of earlyCASE. This manual will go through the screens and features that are new to V2.0.30. Following this will be some practical notes on how to use these features in various real life scenarios you may encounter.

Types of Data Collections available using “Collect”:

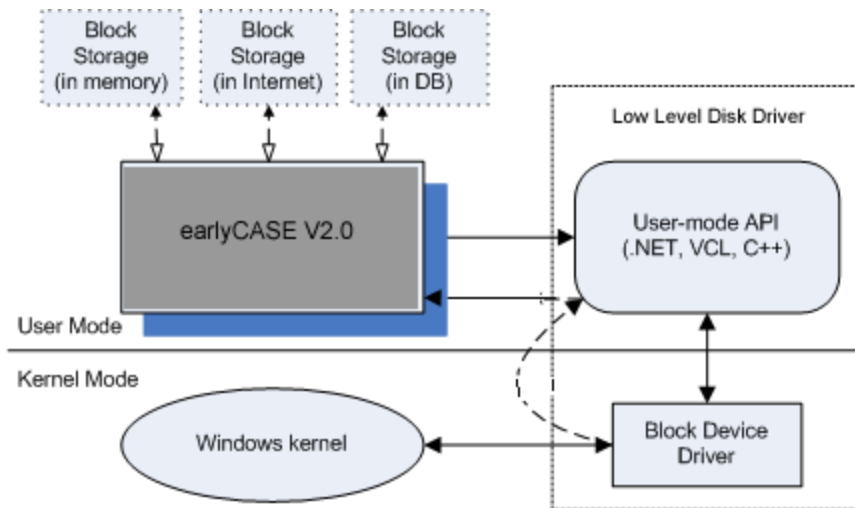
- Images of Logical Drives – anything that you have a drive letter assigned to. This includes thumb drives, ipods, memory cards, USB Drives, CD & DVD’s, local and mapped network drives. You will have the option to create a DD (Raw) image or an Advanced Forensic Format “AFF” of the drive. When using “AFF” you will have options for compression type, signing the image with a Digital ID (Key), and encrypting the image. AFF is the default image type and is slower than DD, but yields a more protected and recoverable image than DD produces.
- Contents of a Folder and its sub folders – this option is very useful when you are interested in a specific folder(s) and want to make a forensically sound copy of the folder and files (including the folder structure). This option will allow you to make a straight Native copy of the ESI, or you can select to compress the content into a Zip file to insure portability and protection of the data you are collecting. Collecting Folders and Files into a container (like a Zip File) have many advantages over just using the Native copy. Beside space, the Compress Zip container can be password protected, contains error checking to insure non of the files are corrupt, and provides a much cleaner means of moving collect ESI between sites, computers or vendors.
- Image of a Physical Drive (all partitions and unallocated space) – Only Locally attached drives can be imaged using the physical image option. The physical drives DO NOT have to mounted (assigned a drive letter) by the machine, but do need to be readable by the machine you are running earlyCASE on. If the drive shows when you when you select “Disk Management”, earlyCASE will be able to see it as well. The physical drive image will collect all of the sectors of the drive including unallocated space, deleted blocks, etc. Because it images the entire drive it will take the longest of the image types, and if the drive you are imaging is 250Gb it could produce an image file of the same size. You will have the option to create a DD (Raw) image or an Advanced Forensic Format “AFF” of the drive. When using “AFF” you will have options for compression type, signing the image with a Digital ID (Key), and encrypting the image. AFF is the default image type and is slower than DD, but yields a more protected and recoverable image than DD produces.

earlyCASE version 2 requires low level access to the machine / operating system to be able to create drive images. On certain operating systems (Windows XP and Windows Server 2003) you may see a security prompt as follows:



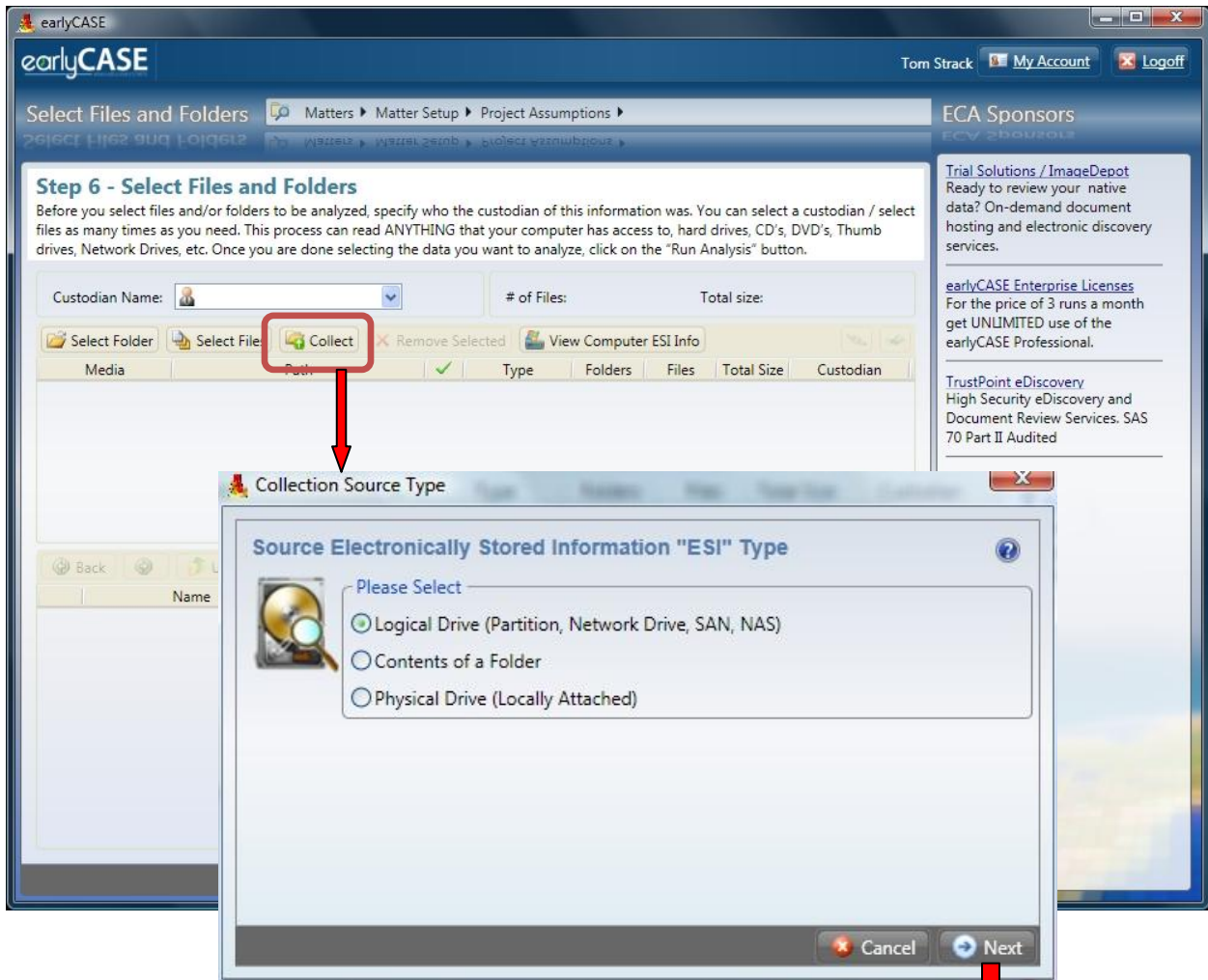
MAKE SURE: that you have specified an account with has LOCAL administrative privilege on the machine you are running earlyCASE on.

MAKE SURE: That you have UNCHECKED the box which restricts programs access to the machine. To do low level (DISK I/O) required to image drives earlyCASE requires this type of access privilege.



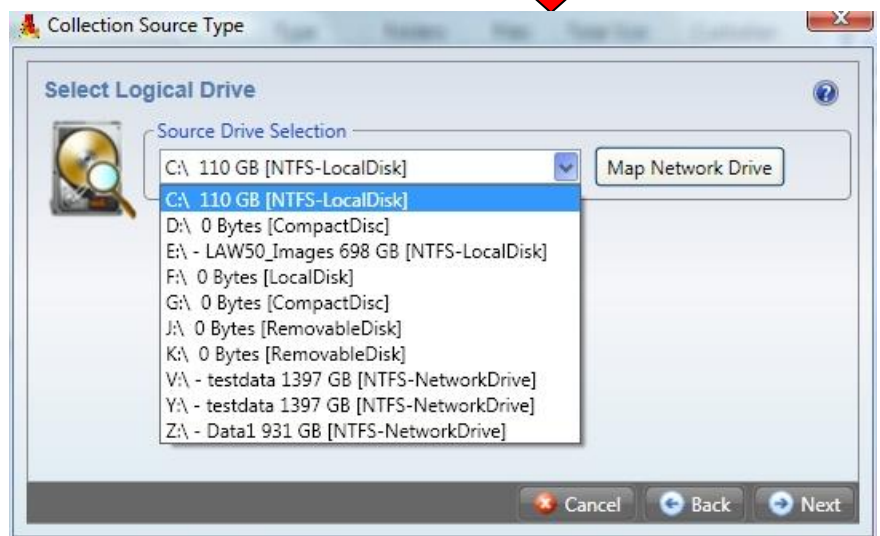
From a Technical Perspective here is why kernel mode access is required to image a drive while it is mounted on a machine.

Let's have a look at how to use each of these as well as some new features available in earlyCASE.



A logical drive is in essence anything that has a drive letter assigned to it. If you have a specific network share or need to create an image of a machine on the network you can use [Map Network Drive] to assign a drive letter and then use the "Logical Drive" type of source for your data collection.

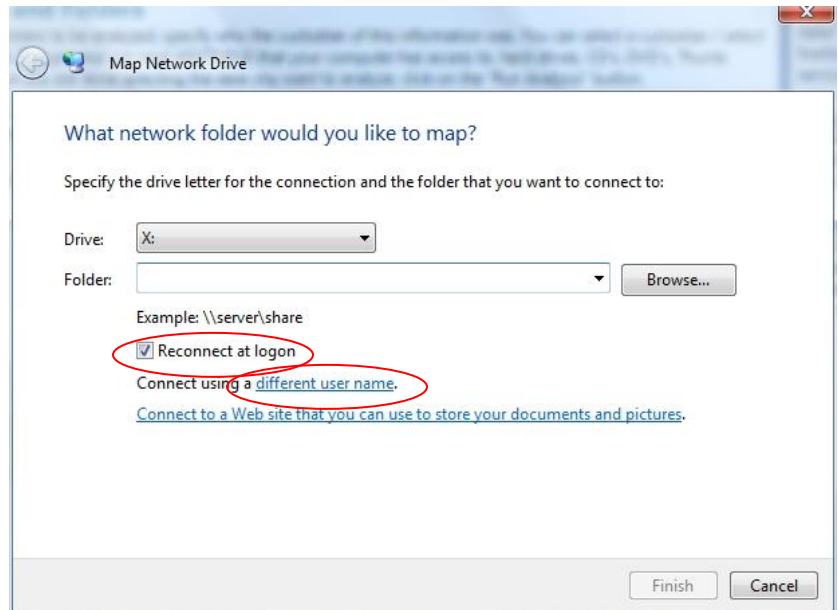
Remember that imaging drives across the network will be a lot slower than creating an image locally from the physical machine the data is on.



Mapping Network Drives

This is the same interface that you use from Explorer on your computer to map a network drive. Pay attention to the options circled in red: “Reconnect at Logon” and “Connect using a different user name”.

For more information on how network drive works refers to windows help files.

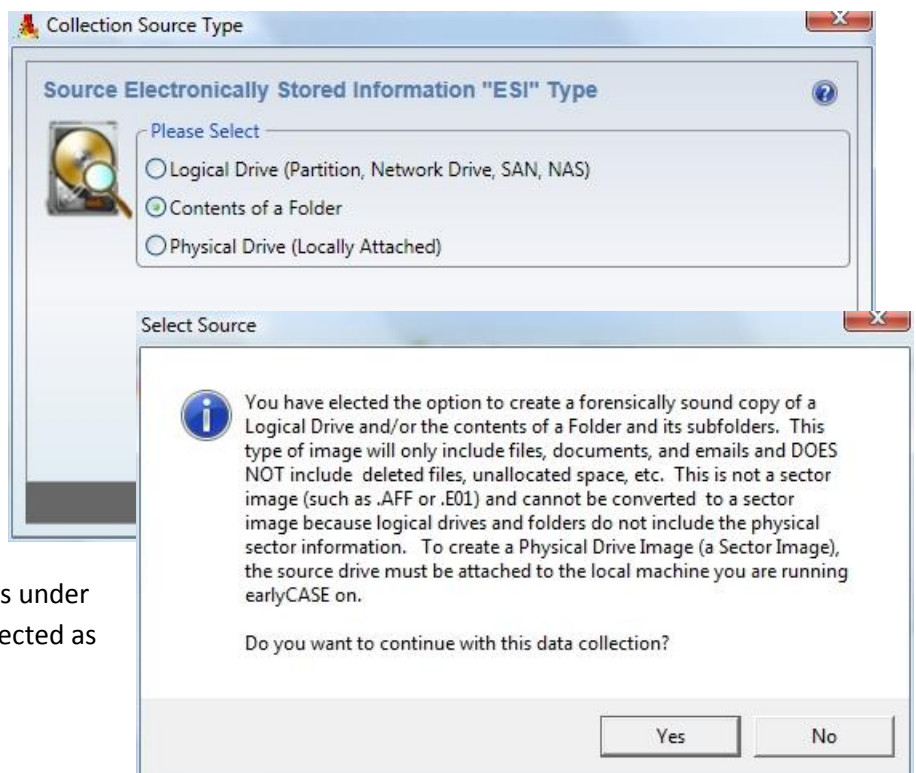


Collecting data from a Folder (i.e. not a complete drive)

This option is useful when you are interested in getting a sound collection of what is in a folder and subfolders underneath that folder. For instance “C:\Documents and Settings” or a shared folder on the network. This option will warn you that you are not making a sector copy etc.

Once you have acknowledged the informational box you will be presented the dialog box to point to folder you wish to collect.

Remember that ALL of the subfolders under the folder you select will also be collected as well.



You can drill down to the specific folder you wish to collect here. You can also use this to drill down into network locations you have access to and collect data from remote folders as well.

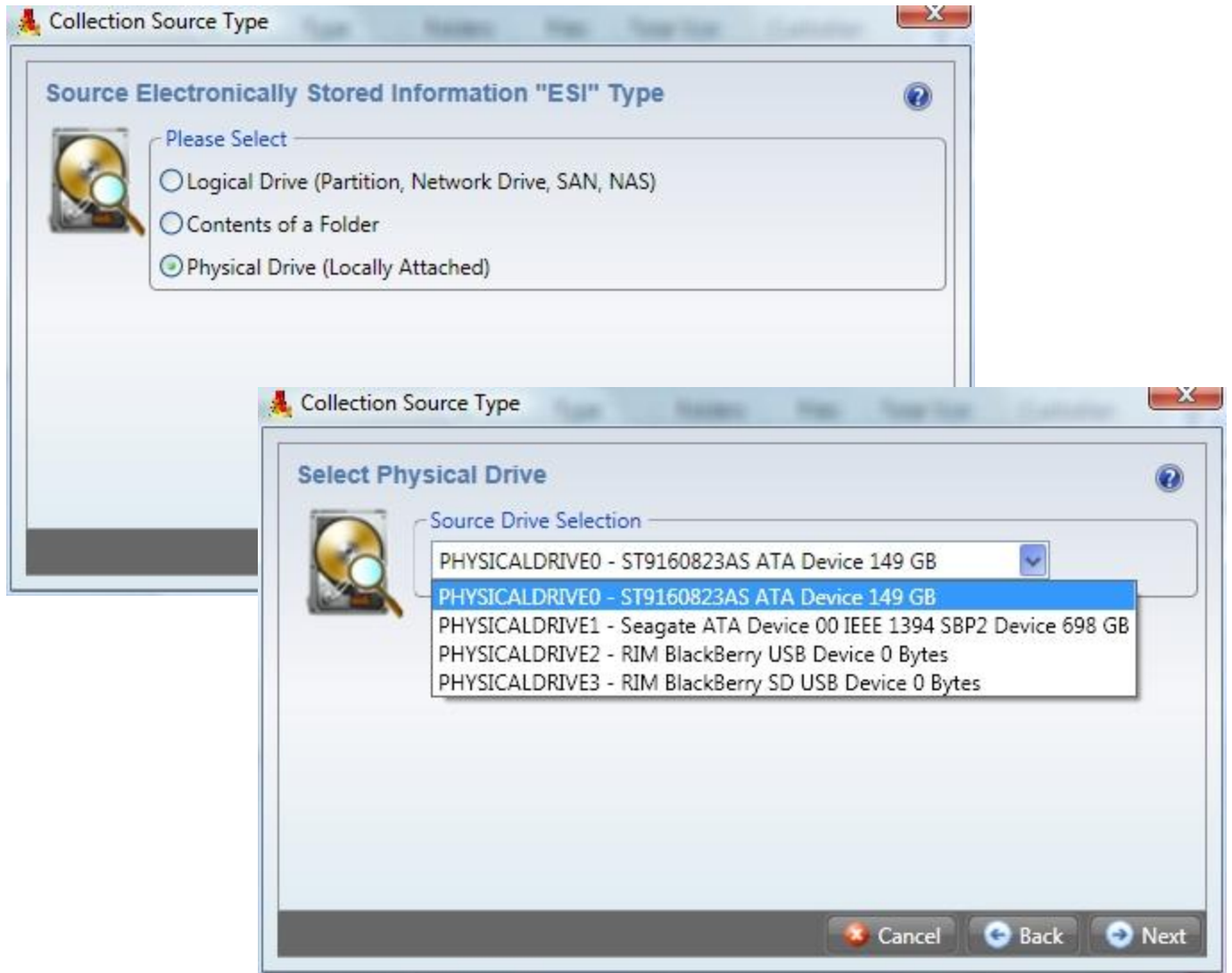
Once you have selected the folder, click on OK.

NOTE: You can navigate your local computer or network to point to the folders you want to collect. earlyCASE supports UNC paths.



The most complex (technically) of the three types of images is the Physical Drive Image

ONLY drives that are physically attached to the machine you are running earlyCASE on can be imaged using the “Physical Drive” method.



The “Collect” Options Available:

All of the methods of collection share this common screen once you have selected the type of collection and the source of the ESI to be collected. Depending on the type of image you are doing, some of the options may or may not be available for that type of collection.

This screen is divided into three sections: Source, Protection and Target:

The source section identifies the source you selected as well as gives you the opportunity to document if the ESI is subject to a protective order or a subpoena, along with the credentials that were used (if any) to attached to the ESI.

The Protection section options vary with the type of the image.

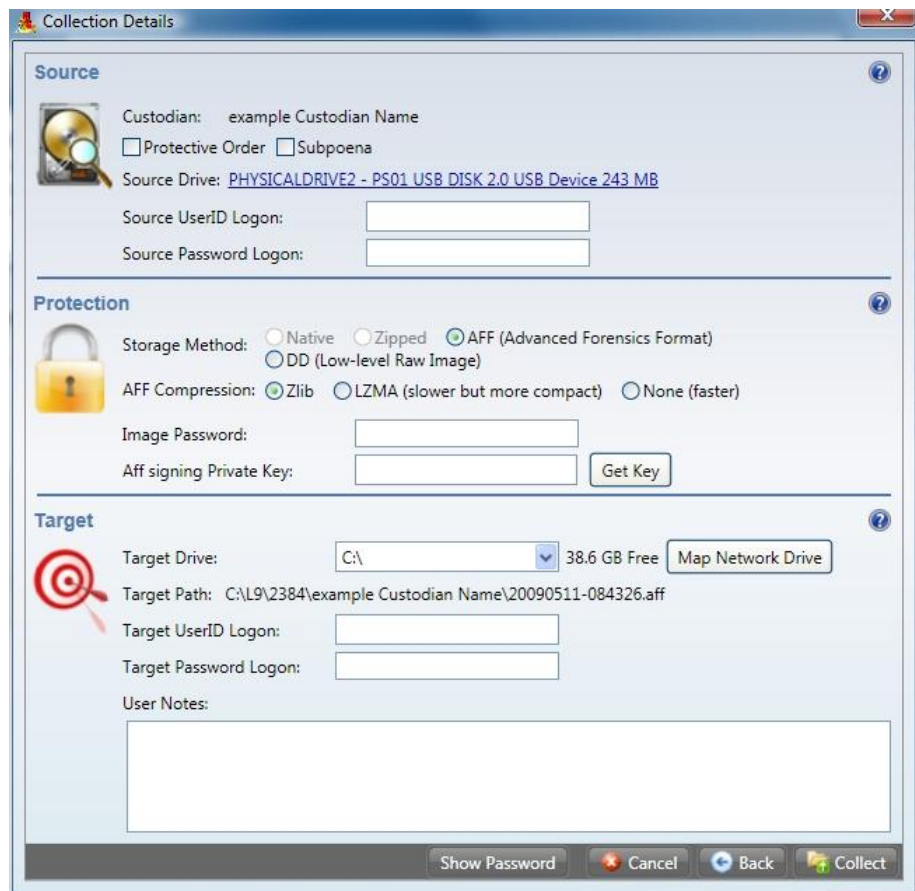
Content of Folder:

Native or Zipped, option to password protect the zip file.

Logical or Physical Drive:

DD or AFF image creation. If AFF is selected you have the option of ZLIB, LZMA or no compression. CD Rom devices also have the option of creating an ISO type of image.

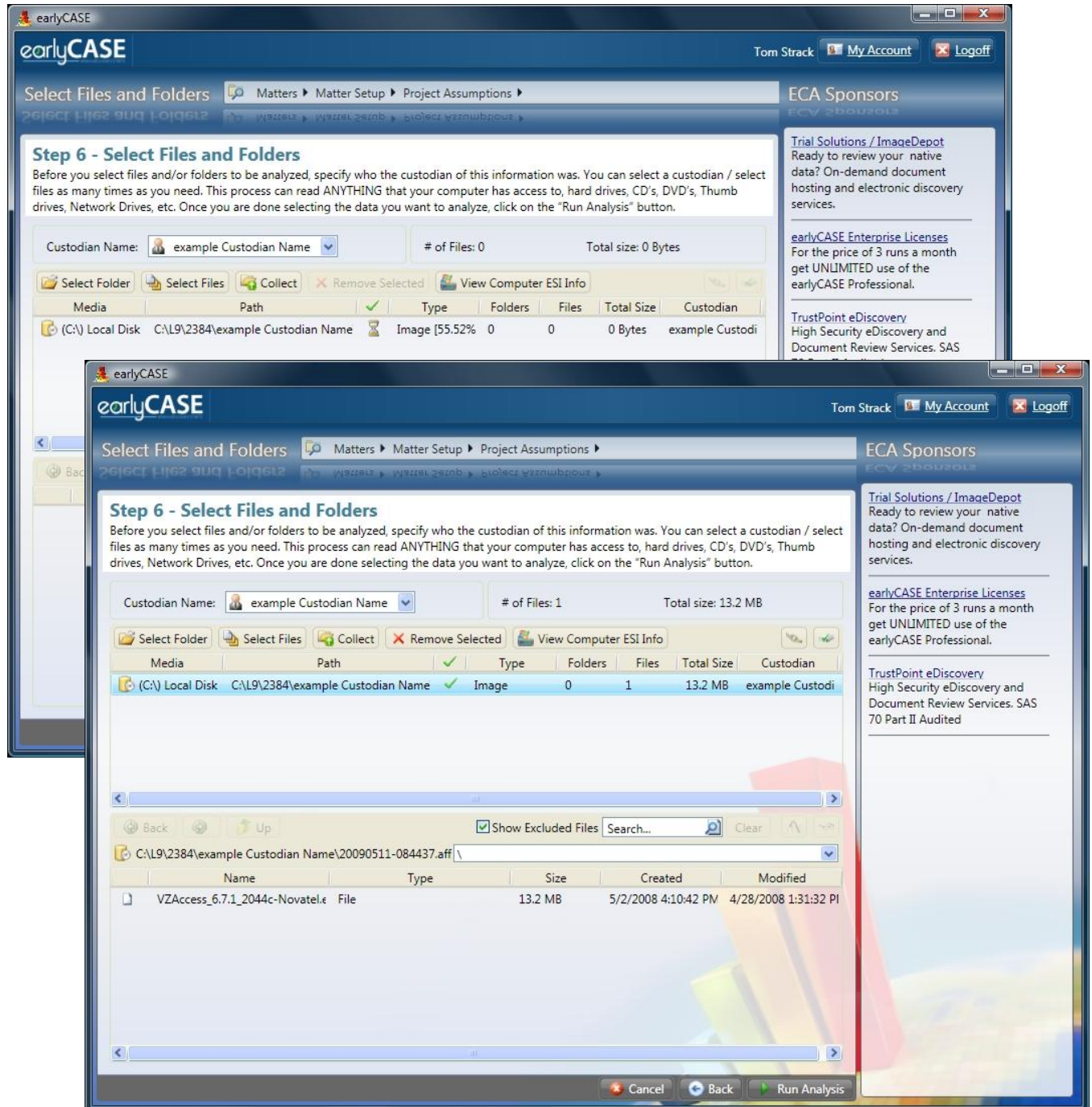
In addition AFF images can be Digitally Signed and encrypted. AFF images are recommended.



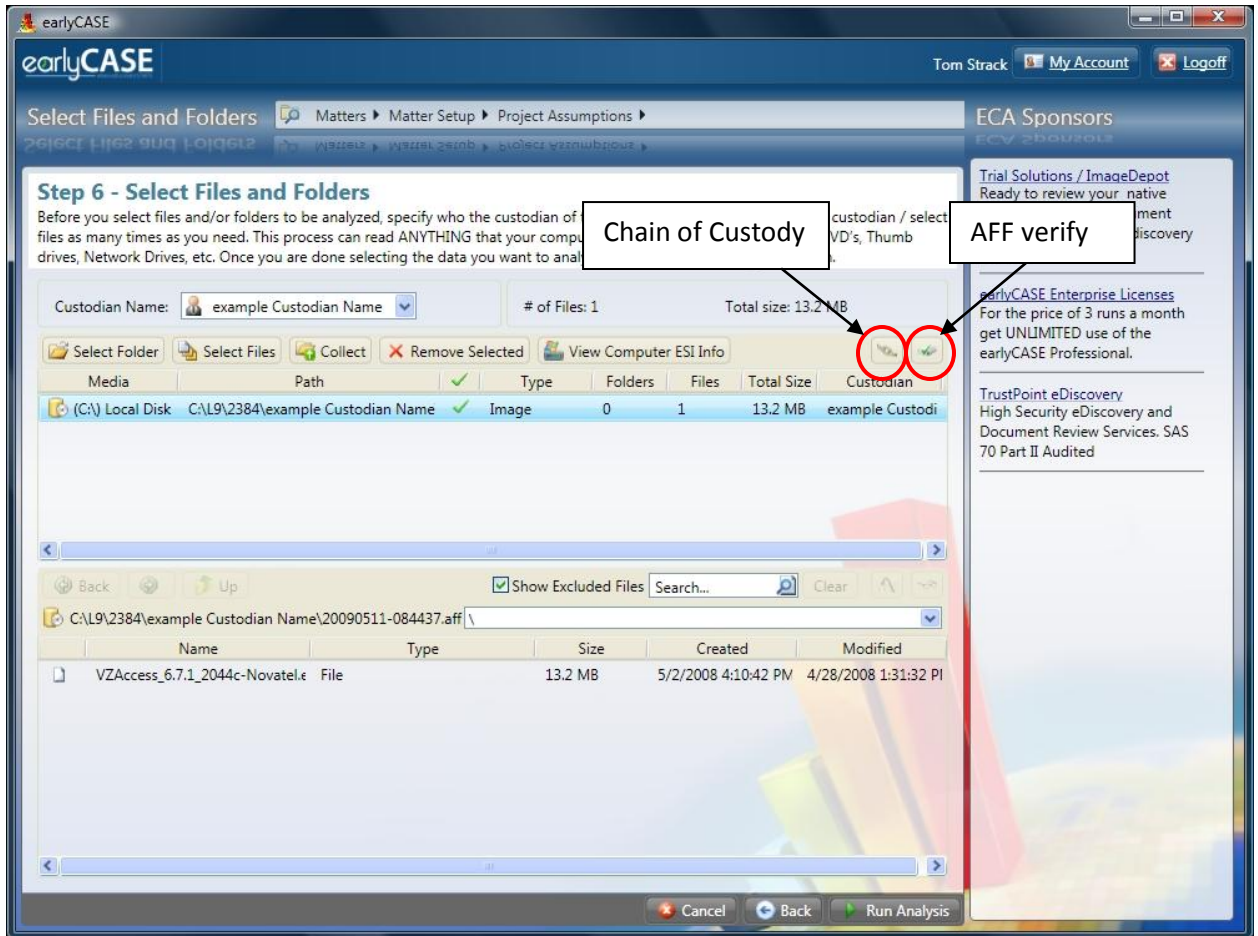
The screenshot shows the 'Collection Details' dialog box with three main sections: Source, Protection, and Target. The Source section includes fields for Custodian (example Custodian Name), checkboxes for Protective Order and Subpoena, Source Drive (PHYSICALDRIVE2 - PS01 USB DISK 2.0 USB Device 243 MB), Source UserID Logon, and Source Password Logon. The Protection section includes Storage Method (Native, Zipped, AFF (Advanced Forensics Format), DD (Low-level Raw Image)), AFF Compression (Zlib, LZMA (slower but more compact), None (faster)), Image Password, and Aff signing Private Key with a Get Key button. The Target section includes Target Drive (C:\, 38.6 GB Free, Map Network Drive), Target Path (C:\L9\2384\example Custodian Name\20090511-084326.aff), Target UserID Logon, Target Password Logon, and User Notes. At the bottom are buttons for Show Password, Cancel, Back, and Collect.

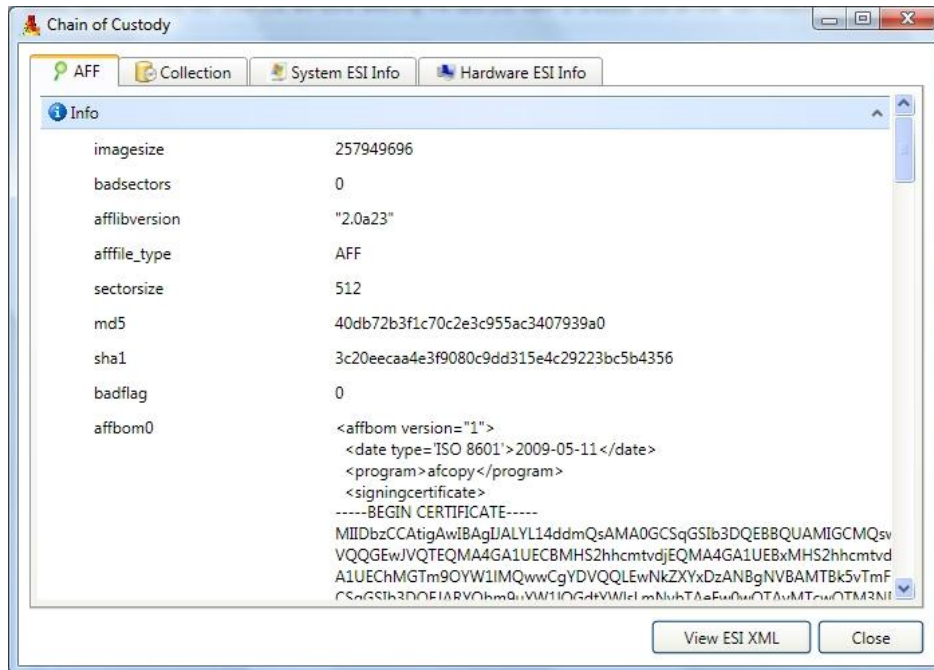
The target section of this screen allows you to specify where (drive) you want to store the images you are creating along with the credentials used to connect to that drive. earlyCASE will check the amount of available space on the target drive and warn you if there is not enough space to contain the image to be created. Keep in mind that a drive image can be AS LARGE AS the source you selected.

Once you have set the options we wish and click on “Collect” you will the image start and the percentage complete will be updated every few seconds. When the image is complete you will see a green check mark. While the image is being created you can go ahead and click on “Run Analysis” and the processing will begin once the image creation has completed. You can also create multiple images at the same time. Be careful if all of the images are being written to the same target location (drive) as this will slow down imaging substantially. If you need to cancel an image is running, click on the image in the upper frame and click on “Remove Selected”, you will be warned that this will stop the imaging process.



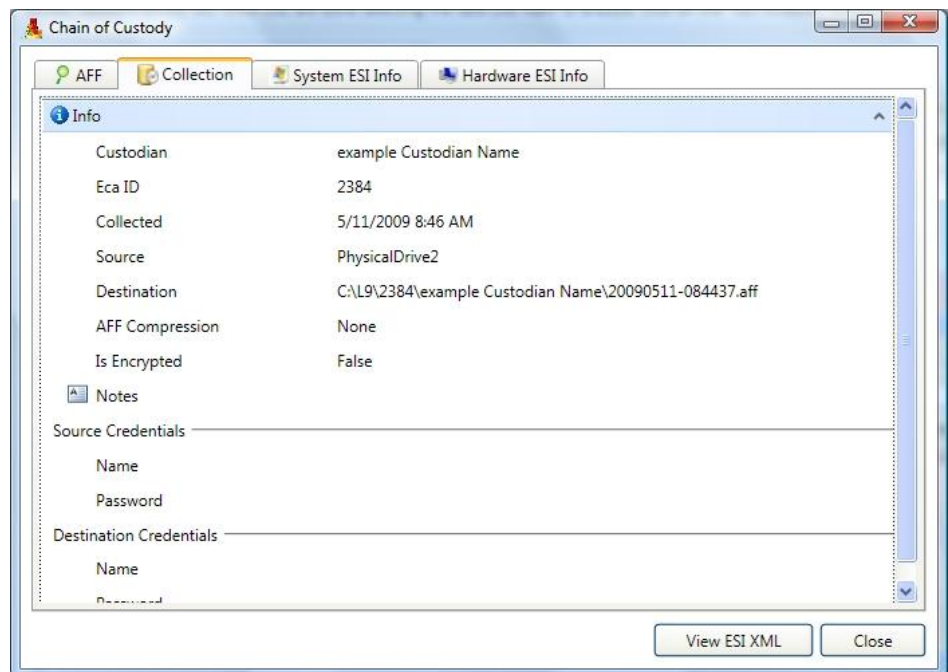
For AFF images that you create you can access the “Chain of Custody” information that is stored in the image directly from earlyCASE by clicking on the image and then clicking on the “Chain of Custody” button. If you need to verify the AFF image (Hashes and Digital Signature) click on the “AFF Verify” button.





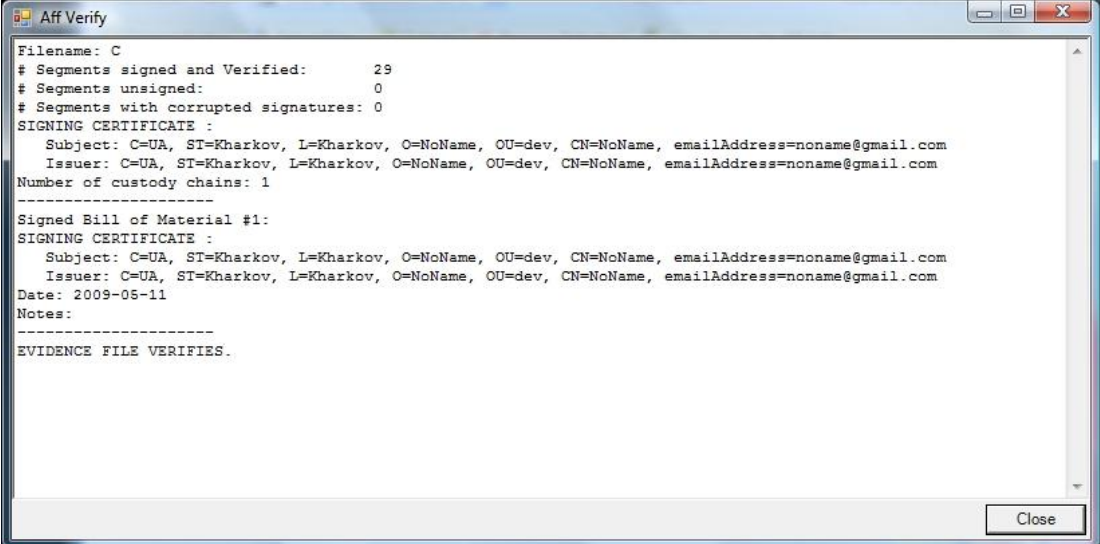
The chain of custody screen is composed of several sections. Information is available on the image itself “AFF” as well as the matter it was collected as a part of “Collection” along with the physical information about the computer it was collected on.

When the Image (AFF or DD) an XML file is created in the same directory as the image itself. The XML file can be viewed outside of earlyCASE. Inside of earlyCASE you can view the XML that is stored inside of the AFF image by clicking on “View ESI XML”. Because XML is portable, it is also very verbose.



Verifying an AFF Image:

The AFF Verify feature will check the hash values stored in the image with recalculated hash values, in addition the AFF verify function will also check to see if the image was signed with a Digital ID and validate all of the segments within the image to insure they are still validly signed and have not been tampered with in any way.



```

Aff Verify
-----
Filename: C
# Segments signed and Verified:      29
# Segments unsigned:                 0
# Segments with corrupted signatures: 0
SIGNING CERTIFICATE :
  Subject: C=UA, ST=Kharkov, L=Kharkov, O=NoName, OU=dev, CN=NoName, emailAddress=noname@gmail.com
  Issuer: C=UA, ST=Kharkov, L=Kharkov, O=NoName, OU=dev, CN=NoName, emailAddress=noname@gmail.com
Number of custody chains: 1
-----
Signed Bill of Material #1:
SIGNING CERTIFICATE :
  Subject: C=UA, ST=Kharkov, L=Kharkov, O=NoName, OU=dev, CN=NoName, emailAddress=noname@gmail.com
  Issuer: C=UA, ST=Kharkov, L=Kharkov, O=NoName, OU=dev, CN=NoName, emailAddress=noname@gmail.com
Date: 2009-05-11
Notes:
-----
EVIDENCE FILE VERIFIES.
-----
Close

```

More on Digitally Signing Images and the Digital ID (Keys) required

Why even sign an image you create in earlyCASE?

Providing a digital ID (key) and signing an image will cause all of the segments to be signed with the key, which in turn provides a much higher level of authenticity to not only the overall image, but every segment within the image. When an image is verified it is checked to see if it was signed with a digital ID, validates the key that signed the image, who owns that digital key, etc. This validation allows you to create image and sign them with your secure key, anyone receiving the image can be 100% assured that the image was truly created by the holder of the key that signed it, and that entire image is trustworthy as having been created by who the image says created it. If you do not have a digital ID there are several steps to get one issued.

Checking to see if you already have a Digital ID on your computer:

Open Internet Explorer and click on "Tools" Then "Internet Options" then click on the "Content" tab and click on the "Certificates" button. You should be on the "Personal" tab, these are your Digital ID's. If you do not have any installed, then of course you don't have any to export for use in signing images with earlyCASE.

Getting a Digital ID for signing email and Image Files:

If you do not already have a .KEY file that authenticates who you are. If possible ask your help desk to issue you a digital ID that is based on your company's digital ID. This will make sure that when you sign an image it is tied to your company as well as you with absolute trustworthiness. If your company does not issue Digital ID's to users - you can get a very simple one here to use within earlyCASE as well in MS Outlook. This process will let you request that a digital ID be issued to your name and email address.

Step 1: Get a FREE Digital ID (the links below are trustworthy sources for a Digital ID)

<http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html> (recommended)

<https://www.thawte.com/secure-email/personal-email-certificates/index.html> (takes longer, does not work in IE 8)

<http://www.ascertia.com/onlineCA/issuer/default.aspx?action=login> (less well known)

Exporting Digital ID's from your computer for use in signing images: *(Note This will change if we change to .CER / CRT X.509 type keys for signing)*

Step 1: Open Internet Explorer goto "Tools" then "Internet Options" then "Content" Now Click on "Certificates" you should be on the "Personal Tab" - Click on the certificate you want to export for signing images in earlyCASE.

Step 2: Click on “Export” then “Next” Select “Yes, Export the private key”

Step 3: Select “Personal Information Exchange – PKCS #12 (.PFX) Check the boxes for “Include all certificates in certification path..” and also check “Enable Strong protection” Then click “next”

Step 4: Do not password this file since you will be using it as a part of the earlyCASE image process.

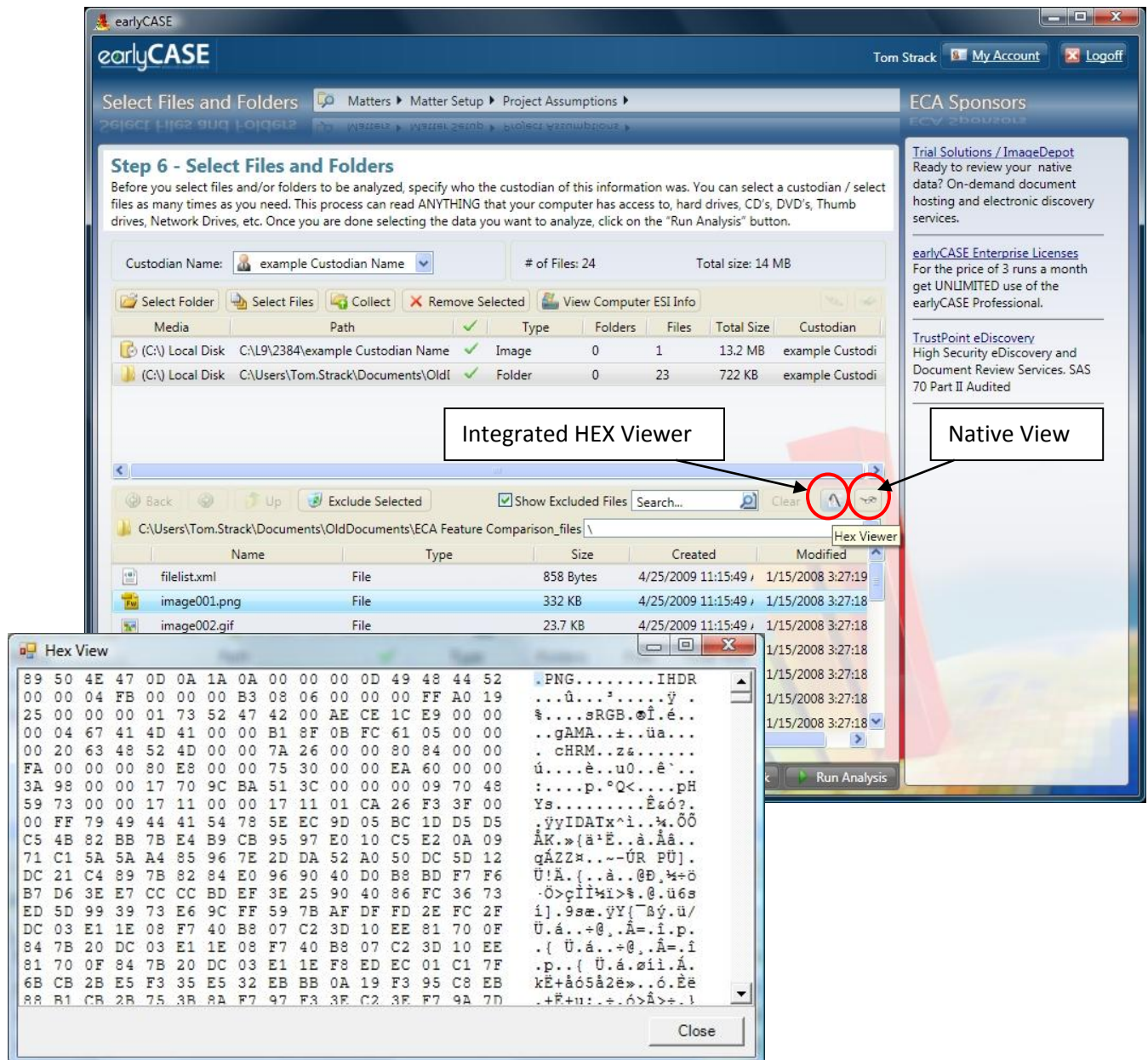
Password protected key files will cause the signing process to fail in earlyCASE

Step 5: Provide the path and filename for the Key file you are exporting – use a .P12 file extension when you provide a name for the key. Put the key in a folder that it will be easy to find it in. FYI: A .PFX and a .P12 key file are the same type just 2 extensions that denote the same type of file.

At this point you have a private key that can be used to sign images in earlyCASE.

Using the Integrated Hex Viewer:

At times you may need to have at the hexadecimal view of a file to understand what the file is. You can do this directly from within earlyCASE by clicking on the file in the lower frame and then click on the Hex viewer button (Crow Bar). In addition to the Hex View there is also a button that will launch a native view of the file you have selected in the lower frame. The view button will launch whatever application the computer you are on has associated with this type of file.



Practical Applications of “Collect”

Here are a few ways in which you can use “Collect” to assist you in preserving, collecting and analyzing ESI in a matter.

1. Making a copy of a disk drive
2. Collecting data from a network share
3. Collecting data from a client machine across the network
4. Collecting data and Analyzing it later from a different machine

Making a copy of a physical disk drive

At times you may be presented a drive that was pulled from a computer or a physical copy of a drive from a computer. Making a forensically sound drive image adds a level of defensibility in that it preserves a documented chain of custody along with adding a means to insure that the data was not changed in any way. The steps that follow will walk you through making a copy of an entire Physical Disk Drive.

Step 1: Attach a physical write blocker to the computer you will be running earlyCASE on if you have one. (RECOMMENDED THAT YOU GET A WRITE BLOCKER IF YOU DO NOT HAVE ONE)

Step 2: Attach the drive you wish to copy to the write blocking device

Step 3: Start the computer and logon

Step 4: Determine where you want to store the image of this drive and verify that sufficient space is available for the image. Remember that images can be the same size as the original source drive.

Step 5: Create or Open the matter that this image will be a part of. Proceed to step 6 within earlyCASE.

Step 6: Specify the custodian and then click on the “Collect” tab

Step 7: Select “Physical Drive” from the “Collection Source Type Screen”

Step 8: In the “Target” section of the collection screen make sure you have selected the target drive you want to store the image on. Use the defaults for “Protection” – AFF image type and ZLib compression

Collecting Data from a Network Share

Data stored on a network share can be collected in several way, you can collect the contents of the folder (and sub folders) or you can take a logical drive image. There are some pros and cons of each approach.

Contents of Folder:

- Easier to look at later, and easier to give others direct access to
- Preserves folder and file metadata
- Can be compress into a zip file and password protected
- No chain of Custody
- Hard to prove that nothing has been changed later in the matter
- Quicker than creating a drive image

Logical Drive Image:

- Stored in a DD or AFF Image
- Creates a chain of custody
- AFF images can be Digitally Signed as well as encrypted
- Easy to prove the files have not been tampered with
- Can be compressed to save space
- Very portable
- Takes longer to create

For the sake of this example we will create a Logical Image of the drive letter that represents the network share we wish to collect. If we did not want to collect the entire drive we could map a drive letter just to the folder we are interested in OR we could use “contents of folder” and collect the data with the folder of interest into a Zip file.

Step 1: Logon to the machine you will be running earlyCASE from and verify that the drive letter and associated network share are accessible.

Step 2: Determine where you want to store the image of this drive and verify that sufficient space is available for the image. Remember that images can be the same size as the original source drive.

Step 3: Create or Open the matter that this image will be a part of. Proceed to step 6 within earlyCASE.

Step 4: Specify the custodian and then click on the “Collect” tab

Step 5: Select “Logical Drive” from the “Collection Source Type Screen”

Step 6: In the “Target” section of the collection screen make sure you have selected the target drive you want to store the image on. Use the defaults for “Protection” – AFF image type and ZLib compression

Collecting data from a client machine across the network

Data stored on a remote computer may be collected remotely if you have access to the disk drive on that computer through either a specific shared drive or thru the administrative share if you know the administrator account information on that machine. This method will create a logical sound copy of the data. Because a network share does not provide low level sector access to a drive a sector image (DD or AFF) cannot be done remotely.

Establishing that you have read access to this drive should be done before you try and use earlyCASE to make a copy of the ESI. To see if you can access the machine you will likely need this information about the source computer / drive you want to collect:

- Machine Name on the Network
- Machines TCP/IP address
- The Drive Letter of the Source Drive you want to collect (i.e. C:\)
- The Credentials to the Administrator account on that machine

Step 1: Lets see if we can reach the machine. The simplest is to open a Command window (command prompt or CMD window) on your machine and ping the computer by its name on the network.

For instance "Ping TomStrack-NB"

if you cannot reach the computer by name, try reaching it by its TCP/IP Address.

For instance "Ping 192.168.2.109"

Step 2: Determine where you want to store the image of this drive and verify that sufficient space is available for the image. Remember that images can be the same size as the original source drive.

Step 3: Create or Open the matter that this image will be a part of. Proceed to step 6 within earlyCASE.

Step 4: Specify the custodian and then click on the "Collect" tab

Step 5: Select "Logical Drive" from the "Collection Source Type Screen"

Step 6: Once you have determined that you physically can communicate with the computer you want to collect data from we need to map a network drive letter to the shared drive. Modern windows machines have a hidden administrative share for local hard drives. For instance the C: drive has a hidden share called C\$

In the map network drive folder window we will type:

\\TomStrack-NB\C\$

If you just want one or more folder from this remote machine use the “Contents of Folder” for the source instead of the logical drive. Logical Drive will get all of the active files that are on the drive you mapped not just a single folder.

Step 6: In the Protection portion of the collect screen you will see that Zipped is set by default. This is the default (and recommended) method of collecting remote data. Because the data is remote taking a few extra precautions to insure its integrity is a good idea.

Step 7: In the “Target” section of the collection screen make sure you have selected the target drive you want to store the image on. Use the defaults for “Protection” – Zipped and No password.

Collecting data and analyzing it later from a different machine

You can run the collect feature to create drive images and then move those drives images to the network, transport them, store them and later include them from a different machine as a part of the matter. Doing this is pretty simple.

Step 1: On the machine that you want to make a copy of a drive from – logon to earlyCASE with the user ID you will be using latter to process the drive you are collecting

Step 2: Create a matter that these drive images will be a part of – OR – open the matter if you already have created one. We will be connecting to this matter as we create images so that all of the chain of custody in the images references the same matter id, etc.

Step 3: You would do the same steps as outlined in “Making a Copy of a Physical Drive” . Once the drive image has been created you close out of the matter and DO NOT PROCESS it. It will be a little less confusing and easier to track if we collect the images and then analyze them from 1 machine.

Step 4: If possible connect the drive(s) containing the drive images to the machine you want to process them on. You can do this in multiple runs, so all of the data does not have to be online when you begin processing. Make sure you keep track of which images you have collected and which have been processed.

Step 5: Specify the custodian and then click on the “SELECT FILE” tab

Step 6: Select image file that you collected previously and want to now process as a part of this matter. Point to the DD, EnCase or AFF image(s) that you wish to process. You can select multiple files by using the standard windows Shift + Click or Ctrl + Click methods of selecting multiple files.

Step 7: In the upper frame you will see the images you selected open up and checked. Once they have been checked you will see a green check mark indicating that they are ready to be processed and you will see “Image” in the type column. If there is problem with an image you will see “Not Supported” in the Type column and a red exclamation mark instead of a green check mark

Example of XML File created (and embedded in AFF Images) when an Image is created:

```
<?xml version="1.0" encoding="utf-8"?>
<ImageInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <MD5>e91c0a439d367b028d488bdf025c136b</MD5>
  <SHA1>04d8b02ef98b6bc3960f9ffcf6cb2fb5d770b34b</SHA1>
  <SHA256>50319dbd8851dfc45b7af9e6346986e4cdc42589b3f4b65672e65820114a4b6a</SHA256>
  <MetaInformation>
    <MetaProperty Name="creator">earlyCASE-Client 2.0.1.30</MetaProperty>
    <MetaProperty Name="acquisition_commandline" />
    <MetaProperty Name="image_gid">4464614e-5e71-44b7-9ceb-ab00ef777454</MetaProperty>
    <MetaProperty Name="acquisition_date">10/26/2009 5:40:08 PM.</MetaProperty>
  </MetaInformation>
  <CollectionInfo>
    <Custodian>phy aff image</Custodian>
    <EcaID>3671</EcaID>
    <Collected>2009-10-26T17:40:10.6217094-04:00</Collected>
    <Time />
    <SourcePath>PhysicalDrive3</SourcePath>
    <DestPath>I:\L9\3671\phy aff image\20091026-100822.aff</DestPath>
    <DestType>Aff</DestType>
    <Compression>ZLib</Compression>
    <Encrypt>>false</Encrypt>
    <Notes />
    <SourceName />
    <SourcePass />
    <DestName />
    <DestPass />
  </CollectionInfo>
  <EsiInfo>
    <HostName>.</HostName>
    <SystemInfo>
      <ComputerInfo>
        <UserName>TomStrack-NB\Tom.Strack</UserName>
        <PrimaryOwnerName>Tom.Strack</PrimaryOwnerName>
        <PCSystemType>Mobile</PCSystemType>
        <SystemType>X86-based PC</SystemType>
        <Description>AT/AT COMPATIBLE</Description>
        <Manufacturer>Dell Inc.</Manufacturer>
        <Model>MXC062 </Model>
        <TotalPhysicalMemory>2144821248</TotalPhysicalMemory>
        <NumberOfProcessors>1</NumberOfProcessors>
        <NumberOfLogicalProcessors>2</NumberOfLogicalProcessors>
        <CurrentTimeZone>-240</CurrentTimeZone>
        <PartOfDomain>>true</PartOfDomain>
        <Domain>earlyCASE.com</Domain>
        <DomainRole>Member_Workstation</DomainRole>
        <DNSHostName>TomStrack-NB</DNSHostName>
      </ComputerInfo>
      <SystemInfo>
        <Manufacturer>Microsoft Corporation</Manufacturer>
        <Name>Microsoft® Windows Vista™ Ultimate </Name>
        <ProductType>Work_Station</ProductType>
        <OSVersion>6.0.6002</OSVersion>
        <OSArchitecture>32-bit</OSArchitecture>
        <BuildNumber>6002</BuildNumber>
        <BuildType>Multiprocessor Free</BuildType>
        <CSDVersion>Service Pack 2</CSDVersion>
        <CSName>TOMSTRACK-NB</CSName>
        <OSLanguage>1033</OSLanguage>
        <OSType>WINNT</OSType>
        <RegisteredUser>Tom.Strack</RegisteredUser>
        <Organization />
        <SerialNumber>89580-OEM-7332132-00141</SerialNumber>
        <CodeSet>1252</CodeSet>
        <CountryCode>1</CountryCode>
        <CurrentTimeZone>-240</CurrentTimeZone>
        <Locale>0409</Locale>
        <InstallDate>2009-04-22T14:26:45</InstallDate>
      </SystemInfo>
    </SystemInfo>
  </EsiInfo>
</ImageInfo>
```

```

<LastBootUpTime>2009-10-26T09:38:18.375199</LastBootUpTime>
<LocalDateTime>2009-10-26T10:08:58.907</LocalDateTime>
<WindowsDirectory>C:\Windows</WindowsDirectory>
<SystemDirectory>C:\Windows\system32</SystemDirectory>
<SystemDrive>C:</SystemDrive>
<BootDevice>\Device\HarddiskVolume2</BootDevice>
<SystemDevice>\Device\HarddiskVolume2</SystemDevice>
</SystemInfo>
<Users>
  <UserItem>
    <FullName />
    <Domain>TOMSTRACK-NB</Domain>
    <Name>Administrator</Name>
    <Description>Built-in account for administering the computer/domain</Description>
    <AccountDisabled>true</AccountDisabled>
    <LocalAccount>true</LocalAccount>
    <SID>S-1-5-21-3352725030-308495448-711787160-500</SID>
  </UserItem>
  <UserItem>
    <FullName>ASP.NET Machine Account</FullName>
    <Domain>TOMSTRACK-NB</Domain>
    <Name>ASPNET</Name>
    <Description>Account used for running the ASP.NET worker process
(aspnet_wp.exe)</Description>
    <AccountDisabled>false</AccountDisabled>
    <LocalAccount>true</LocalAccount>
    <SID>S-1-5-21-3352725030-308495448-711787160-1004</SID>
  </UserItem>
  <UserItem>
    <FullName />
    <Domain>TOMSTRACK-NB</Domain>
    <Name>Guest</Name>
    <Description>Built-in account for guest access to the computer/domain</Description>
    <AccountDisabled>true</AccountDisabled>
    <LocalAccount>true</LocalAccount>
    <SID>S-1-5-21-3352725030-308495448-711787160-501</SID>
  </UserItem>
  <UserItem>
    <FullName />
    <Domain>TOMSTRACK-NB</Domain>
    <Name>Tom.Strack</Name>
    <Description />
    <AccountDisabled>false</AccountDisabled>
    <LocalAccount>true</LocalAccount>
    <SID>S-1-5-21-3352725030-308495448-711787160-1000</SID>
  </UserItem>
  <UserItem>
    <FullName />
    <Domain>EARLYCASE</Domain>
    <Name>Administrator</Name>
    <Description>Built-in account for administering the computer/domain</Description>
    <AccountDisabled>false</AccountDisabled>
    <LocalAccount>false</LocalAccount>
    <SID>S-1-5-21-1818506971-212100732-898978781-500</SID>
  </UserItem>
  <UserItem>
    <FullName />
    <Domain>EARLYCASE</Domain>
    <Name>Guest</Name>
    <Description>Built-in account for guest access to the computer/domain</Description>
    <AccountDisabled>true</AccountDisabled>
    <LocalAccount>false</LocalAccount>
    <SID>S-1-5-21-1818506971-212100732-898978781-501</SID>
  </UserItem>
  <UserItem>
    <FullName />
    <Domain>EARLYCASE</Domain>
    <Name>krbtgt</Name>
    <Description>Key Distribution Center Service Account</Description>
    <AccountDisabled>true</AccountDisabled>
    <LocalAccount>false</LocalAccount>

```

```

    <SID>S-1-5-21-1818506971-212100732-898978781-502</SID>
  </UserItem>
  <UserItem>
    <FullName>Tom Strack</FullName>
    <Domain>EARLYCASE</Domain>
    <Name>Tom.Strack</Name>
    <Description />
    <AccountDisabled>>false</AccountDisabled>
    <LocalAccount>>false</LocalAccount>
    <SID>S-1-5-21-1818506971-212100732-898978781-1117</SID>
  </UserItem>
  <UserItem>
    <FullName>earlyCASE</FullName>
    <Domain>EARLYCASE</Domain>
    <Name>earlyCASE</Name>
    <Description />
    <AccountDisabled>>false</AccountDisabled>
    <LocalAccount>>false</LocalAccount>
    <SID>S-1-5-21-1818506971-212100732-898978781-1135</SID>
  </UserItem>
  <UserItem>
    <FullName>Field Searcy</FullName>
    <Domain>EARLYCASE</Domain>
    <Name>Field.Searcy</Name>
    <Description />
    <AccountDisabled>>false</AccountDisabled>
    <LocalAccount>>false</LocalAccount>
    <SID>S-1-5-21-1818506971-212100732-898978781-1147</SID>
  </UserItem>
  <UserItem>
    <FullName>Roman Mashta</FullName>
    <Domain>EARLYCASE</Domain>
    <Name>Roman.Mashta</Name>
    <Description />
    <AccountDisabled>>false</AccountDisabled>
    <LocalAccount>>false</LocalAccount>
    <SID>S-1-5-21-1818506971-212100732-898978781-1148</SID>
  </UserItem>
  <UserItem>
    <FullName>Doug Moore</FullName>
    <Domain>EARLYCASE</Domain>
    <Name>NovaOffice</Name>
    <Description />
    <AccountDisabled>>true</AccountDisabled>
    <LocalAccount>>false</LocalAccount>
    <SID>S-1-5-21-1818506971-212100732-898978781-1150</SID>
  </UserItem>
</Users>
</SystemInfo>
<HardwareInfo>
  <Bios>
    <Manufacturer>Dell Inc.</Manufacturer>
    <Name>Phoenix ROM BIOS PLUS Version 1.10 A08</Name>
    <SerialNumber>4LXKRC1</SerialNumber>
    <Version>DELL - 27d7070a</Version>
  </Bios>
  <Processors>
    <ProcessorItem>
      <Architecture>X64</Architecture>
      <ProcessorID>BFEBFBFF000006F2</ProcessorID>
      <CpuSpeed>1833</CpuSpeed>
      <Name>Intel (R) Core (TM) 2 CPU T5600 @ 1.83GHz</Name>
      <Manufacturer>GenuineIntel</Manufacturer>
      <NumberOfCores>2</NumberOfCores>
      <NumberOfLogicalProcessors>2</NumberOfLogicalProcessors>
      <Version>Model 15, Stepping 2</Version>
    </ProcessorItem>
  </Processors>
  <DiskDrives>
    <DiskDriveItem>

```

```

00F3T0 <PNPDeviceID>IDE\DISKWD_C_WD3200BEKT-
11.01A11\5&A3FA7&0&0.0.0.</PNPDeviceID>
<BytesPerSector>512</BytesPerSector>
<InterfaceType>IDE</InterfaceType>
<Manufacturer>(Standard disk drives)</Manufacturer>
<FirmwareRevision>11.01A11</FirmwareRevision>
<SerialNumber>2020202057202d44585730413641353931303037</SerialNumber>
<Index>0</Index>
<MediaType>Fixed hard disk media</MediaType>
<Name>\\.\\PHYSICALDRIVE0</Name>
<SectorsPerTrack>63</SectorsPerTrack>
<TotalCylinders>38913</TotalCylinders>
<TotalSectors>625137345</TotalSectors>
<TotalTracks>9922815</TotalTracks>
<TotalHeads>255</TotalHeads>
<TracksPerCylinder>255</TracksPerCylinder>
<Size>320070320640</Size>
<Partitions>
  <DiskPartitionItem>
    <BlockSize>512</BlockSize>
    <Index>0</Index>
    <NumberOfBlocks>224847</NumberOfBlocks>
    <Size>115121664</Size>
    <StartingOffset>32256</StartingOffset>
    <Bootable>>false</Bootable>
    <PrimaryPartition>>true</PrimaryPartition>
    <BootPartition>>false</BootPartition>
    <Description>Unknown</Description>
    <Name>Disk #0, Partition #0</Name>
  </DiskPartitionItem>
  <DiskPartitionItem>
    <BlockSize>512</BlockSize>
    <Index>0</Index>
    <NumberOfBlocks>535430385</NumberOfBlocks>
    <Size>274140357120</Size>
    <StartingOffset>115153920</StartingOffset>
    <Bootable>>true</Bootable>
    <PrimaryPartition>>true</PrimaryPartition>
    <BootPartition>>true</BootPartition>
    <Description>Installable File System</Description>
    <Name>Disk #0, Partition #1</Name>
  </DiskPartitionItem>
  <DiskPartitionItem>
    <BlockSize>512</BlockSize>
    <Index>0</Index>
    <NumberOfBlocks>87377535</NumberOfBlocks>
    <Size>44737297920</Size>
    <StartingOffset>275333022720</StartingOffset>
    <Bootable>>false</Bootable>
    <PrimaryPartition>>false</PrimaryPartition>
    <BootPartition>>false</BootPartition>
    <Description>Extended Partition</Description>
    <Name>Disk #0, Partition #2</Name>
  </DiskPartitionItem>
</Partitions>
</DiskDriveItem>
<DiskDriveItem>
<PNPDeviceID>SBP2\SEAGATE&ATA_DEVICE_00&LUN0&REV2\00203700071000E0</PNPDeviceID>
<BytesPerSector>512</BytesPerSector>
<InterfaceType>1394</InterfaceType>
<Manufacturer>(Standard disk drives)</Manufacturer>
<FirmwareRevision>120R</FirmwareRevision>
<SerialNumber>00372000e0001007</SerialNumber>
<Index>1</Index>
<MediaType>Fixed hard disk media</MediaType>
<Model>Seagate ATA Device 00 IEEE 1394 SBP2 Device</Model>
<Name>\\.\\PHYSICALDRIVE1</Name>
<SectorsPerTrack>63</SectorsPerTrack>
<TotalCylinders>91201</TotalCylinders>
<TotalSectors>1465144065</TotalSectors>

```

```

<TotalTracks>23256255</TotalTracks>
<TotalHeads>255</TotalHeads>
<TracksPerCylinder>255</TracksPerCylinder>
<Size>750153761280</Size>
<Partitions>
  <DiskPartitionItem>
    <BlockSize>512</BlockSize>
    <Index>1</Index>
    <NumberOfBlocks>1465144002</NumberOfBlocks>
    <Size>750153729024</Size>
    <StartingOffset>32256</StartingOffset>
    <Bootable>>false</Bootable>
    <PrimaryPartition>>true</PrimaryPartition>
    <BootPartition>>false</BootPartition>
    <Description>Installable File System</Description>
    <Name>Disk #1, Partition #0</Name>
  </DiskPartitionItem>
</Partitions>
</DiskDriveItem>
<DiskDriveItem>

```

```

<PNPDeviceID>USBSTOR\DISK&VEN_LEXAR&PROD_JUMPDRIVE&REV_1.20\D303501203080&0</PNPDeviceID>

```

```

  <BytesPerSector>512</BytesPerSector>
  <InterfaceType>USB</InterfaceType>
  <Manufacturer>(Standard disk drives)</Manufacturer>
  <FirmwareRevision>1.20</FirmwareRevision>
  <SerialNumber>&#x1F;</SerialNumber>
  <Index>2</Index>
  <MediaType>Removable Media</MediaType>
  <Model>LEXAR JUMPDRIVE USB Device</Model>
  <Name>\\. \PHYSICALDRIVE2</Name>
  <SectorsPerTrack>63</SectorsPerTrack>
  <TotalCylinders>12</TotalCylinders>
  <TotalSectors>192780</TotalSectors>
  <TotalTracks>3060</TotalTracks>
  <TotalHeads>255</TotalHeads>
  <TracksPerCylinder>255</TracksPerCylinder>
  <Size>98703360</Size>
  <Partitions>
    <DiskPartitionItem>
      <BlockSize>512</BlockSize>
      <Index>2</Index>
      <NumberOfBlocks>193473</NumberOfBlocks>
      <Size>99058176</Size>
      <StartingOffset>32256</StartingOffset>
      <Bootable>>true</Bootable>
      <PrimaryPartition>>true</PrimaryPartition>
      <BootPartition>>true</BootPartition>
      <Description>MS-DOS V4 Huge</Description>
      <Name>Disk #2, Partition #0</Name>
    </DiskPartitionItem>
  </Partitions>
</DiskDriveItem>
<DiskDriveItem>

```

```

<PNPDeviceID>USBSTOR\DISK&VEN_TOSHIBA&PROD_MK1652GSX&REV_\6830000C1D0C&0</PNPDeviceID>

```

```

  <BytesPerSector>512</BytesPerSector>
  <InterfaceType>USB</InterfaceType>
  <Manufacturer>(Standard disk drives)</Manufacturer>
  <FirmwareRevision> </FirmwareRevision>
  <SerialNumber>&#x1F;</SerialNumber>
  <Index>3</Index>
  <MediaType>External hard disk media</MediaType>
  <Model>TOSHIBA MK1652GSX USB Device</Model>
  <Name>\\. \PHYSICALDRIVE3</Name>
  <SectorsPerTrack>63</SectorsPerTrack>
  <TotalCylinders>19457</TotalCylinders>
  <TotalSectors>312576705</TotalSectors>
  <TotalTracks>4961535</TotalTracks>

```

```

<TotalHeads>255</TotalHeads>
<TracksPerCylinder>255</TracksPerCylinder>
<Size>160039272960</Size>
<Partitions>
  <DiskPartitionItem>
    <BlockSize>512</BlockSize>
    <Index>3</Index>
    <NumberOfBlocks>312576642</NumberOfBlocks>
    <Size>160039240704</Size>
    <StartingOffset>32256</StartingOffset>
    <Bootable>>false</Bootable>
    <PrimaryPartition>>true</PrimaryPartition>
    <BootPartition>>false</BootPartition>
    <Description>Installable File System</Description>
    <Name>Disk #3, Partition #0</Name>
  </DiskPartitionItem>
</Partitions>
</DiskDriveItem>
</DiskDrives>
<CdRoms>
  <CDRomDriveItem>
    <PNPDeviceID>IDE\CDROMTSSTCORP DVD+-RW TS-
L632D _____ DE04 _____ \5&amp;3A6BB19F&amp;0&amp;1.0.0</PNPDeviceID>
    <Drive>G:</Drive>
    <VolumeName>Forensic_Images</VolumeName>
    <VolumeSerialNumber>9F69EBEB</VolumeSerialNumber>
    <MediaLoaded>>true</MediaLoaded>
    <Name>TSSTcorp DVD+-RW TS-L632D ATA Device</Name>
    <Size>4093532160</Size>
    <Manufacturer>(Standard CD-ROM drives)</Manufacturer>
  </CDRomDriveItem>
</CdRoms>
<LogicalDisks>
  <LogicalDiskItem>
    <Name>C:</Name>
    <Description>Local Fixed Disk</Description>
    <FileSystem>NTFS</FileSystem>
    <MediaType>Fixed_hard_disk_media</MediaType>
    <DriveType>Local_Disk</DriveType>
    <FreeSpace>127506833408</FreeSpace>
    <Size>274140356608</Size>
    <VolumName />
    <VolumeSerialNumber>54008049</VolumeSerialNumber>
  </LogicalDiskItem>
  <LogicalDiskItem>
    <Name>D:</Name>
    <Description>CD-ROM Disc</Description>
    <MediaType>Removable_media_other_than_floppy</MediaType>
    <DriveType>Compact_Disc</DriveType>
    <FreeSpace>0</FreeSpace>
    <Size>0</Size>
  </LogicalDiskItem>
  <LogicalDiskItem>
    <Name>E:</Name>
    <Description>Removable Disk</Description>
    <FileSystem>FAT</FileSystem>
    <MediaType>NULL_ENUM_VALUE</MediaType>
    <DriveType>Removable_Disk</DriveType>
    <FreeSpace>41291776</FreeSpace>
    <Size>98846720</Size>
    <VolumName>PUBLIC</VolumName>
    <VolumeSerialNumber>421CA32E</VolumeSerialNumber>
  </LogicalDiskItem>
  <LogicalDiskItem>
    <Name>F:</Name>
    <Description>Local Fixed Disk</Description>
    <MediaType>Fixed_hard_disk_media</MediaType>
    <DriveType>Local_Disk</DriveType>
    <FreeSpace>0</FreeSpace>
    <Size>0</Size>
  </LogicalDiskItem>

```

```

<LogicalDiskItem>
  <Name>G:</Name>
  <Description>CD-ROM Disc</Description>
  <FileSystem>CDF5</FileSystem>
  <MediaType>Removable_media_other_than_floppy</MediaType>
  <DriveType>Compact_Disc</DriveType>
  <FreeSpace>0</FreeSpace>
  <Size>4093532160</Size>
  <VolumName>Forensic_Images</VolumName>
  <VolumeSerialNumber>9F69EBEB</VolumeSerialNumber>
</LogicalDiskItem>
<LogicalDiskItem>
  <Name>H:</Name>
  <Description>Local Fixed Disk</Description>
  <FileSystem>NTFS</FileSystem>
  <MediaType>Fixed_hard_disk_media</MediaType>
  <DriveType>Local_Disk</DriveType>
  <FreeSpace>111850123264</FreeSpace>
  <Size>160039239680</Size>
  <VolumName>Test Drive</VolumName>
  <VolumeSerialNumber>4E37B35B</VolumeSerialNumber>
</LogicalDiskItem>
<LogicalDiskItem>
  <Name>I:</Name>
  <Description>Local Fixed Disk</Description>
  <FileSystem>NTFS</FileSystem>
  <MediaType>Fixed_hard_disk_media</MediaType>
  <DriveType>Local_Disk</DriveType>
  <FreeSpace>230260617216</FreeSpace>
  <Size>750153728000</Size>
  <VolumName>LAW50_Images</VolumName>
  <VolumeSerialNumber>5E920A3A</VolumeSerialNumber>
</LogicalDiskItem>
<LogicalDiskItem>
  <Name>R:</Name>
  <Description>Network Connection</Description>
  <FileSystem>NTFS</FileSystem>
  <MediaType>Format_is_unknown</MediaType>
  <DriveType>Network_Drive</DriveType>
  <FreeSpace>127506833408</FreeSpace>
  <Size>274140356608</Size>
  <VolumName />
  <VolumeSerialNumber>54008049</VolumeSerialNumber>
</LogicalDiskItem>
<LogicalDiskItem>
  <Name>S:</Name>
  <Description>Network Connection</Description>
  <FileSystem>NTFS</FileSystem>
  <MediaType>Format_is_unknown</MediaType>
  <DriveType>Network_Drive</DriveType>
  <FreeSpace>9333223424</FreeSpace>
  <Size>145663160320</Size>
  <VolumName />
  <VolumeSerialNumber>A4D63D1D</VolumeSerialNumber>
</LogicalDiskItem>
<LogicalDiskItem>
  <Name>T:</Name>
  <Description>Network Connection</Description>
  <FileSystem>NTFS</FileSystem>
  <MediaType>Format_is_unknown</MediaType>
  <DriveType>Network_Drive</DriveType>
  <FreeSpace>752321576960</FreeSpace>
  <Size>1500068954112</Size>
  <VolumName />
  <VolumeSerialNumber>84C2756B</VolumeSerialNumber>
</LogicalDiskItem>
<LogicalDiskItem>
  <Name>V:</Name>
  <Description>Network Connection</Description>
  <FileSystem>NTFS</FileSystem>
  <MediaType>Format_is_unknown</MediaType>

```

```

    <DriveType>Network_Drive</DriveType>
    <FreeSpace>152554446848</FreeSpace>
    <Size>1500299264000</Size>
    <VolumName>testdata</VolumName>
    <VolumeSerialNumber>36B7FD4F</VolumeSerialNumber>
  </LogicalDiskItem>
  <LogicalDiskItem>
    <Name>Y:</Name>
    <Description>Network Connection</Description>
    <FileSystem>NTFS</FileSystem>
    <MediaType>Format_is_unknown</MediaType>
    <DriveType>Network_Drive</DriveType>
    <FreeSpace>152554446848</FreeSpace>
    <Size>1500299264000</Size>
    <VolumName>testdata</VolumName>
    <VolumeSerialNumber>36B7FD4F</VolumeSerialNumber>
  </LogicalDiskItem>
  <LogicalDiskItem>
    <Name>Z:</Name>
    <Description>Network Connection</Description>
    <FileSystem>NTFS</FileSystem>
    <MediaType>Format_is_unknown</MediaType>
    <DriveType>Network_Drive</DriveType>
    <FreeSpace>1202962722816</FreeSpace>
    <Size>1500299390976</Size>
    <VolumName>DATA</VolumName>
    <VolumeSerialNumber>ECCDEC61</VolumeSerialNumber>
  </LogicalDiskItem>
</LogicalDisks>
<Shares>
  <ShareItem>
    <Name>ADMIN$</Name>
    <Path>C:\Windows</Path>
  </ShareItem>
  <ShareItem>
    <Name>C$</Name>
    <Path>C:\</Path>
  </ShareItem>
  <ShareItem>
    <Name>G$</Name>
    <Path>G:\</Path>
  </ShareItem>
  <ShareItem>
    <Name>I$</Name>
    <Path>I:\</Path>
  </ShareItem>
  <ShareItem>
    <Name>IPC$</Name>
    <Path />
  </ShareItem>
  <ShareItem>
    <Name>J$</Name>
    <Path>J:\</Path>
  </ShareItem>
  <ShareItem>
    <Name>K$</Name>
    <Path>K:\</Path>
  </ShareItem>
  <ShareItem>
    <Name>L$</Name>
    <Path>L:\</Path>
  </ShareItem>
  <ShareItem>
    <Name>M$</Name>
    <Path>M:\</Path>
  </ShareItem>
  <ShareItem>
    <Name>Tom.Strack</Name>
    <Path>C:\Users\Tom.Strack</Path>
  </ShareItem>
</Shares>

```

```

<NetworkAdapters>
  <NetworkAdapterItem>
    <InterfaceIndex>2</InterfaceIndex>
    <Installed>>true</Installed>
    <Manufacturer>Microsoft</Manufacturer>
    <Name>WAN Miniport (L2TP)</Name>
    <PNPDeviceID>ROOT\MS_L2TPMINIPORT\0000</PNPDeviceID>
    <NetEnabled>>false</NetEnabled>
    <PhysicalAdapter>>false</PhysicalAdapter>
    <NetConnectionStatus>Disconnected</NetConnectionStatus>
  </NetworkAdapterItem>
  <NetworkAdapterItem>
    <AdapterType>Wide Area Network (WAN)</AdapterType>
    <InterfaceIndex>3</InterfaceIndex>
    <Installed>>true</Installed>
    <MACAddress>50:50:54:50:30:30</MACAddress>
    <Manufacturer>Microsoft</Manufacturer>
    <Name>WAN Miniport (PPTP)</Name>
    <PNPDeviceID>ROOT\MS_PPTPMINIPORT\0000</PNPDeviceID>
    <NetEnabled>>false</NetEnabled>
    <PhysicalAdapter>>false</PhysicalAdapter>
    <NetConnectionStatus>Disconnected</NetConnectionStatus>
  </NetworkAdapterItem>
  <NetworkAdapterItem>
    <AdapterType>Wide Area Network (WAN)</AdapterType>
    <InterfaceIndex>4</InterfaceIndex>
    <Installed>>true</Installed>
    <MACAddress>33:50:6F:45:30:30</MACAddress>
    <Manufacturer>Microsoft</Manufacturer>
    <Name>WAN Miniport (PPPOE)</Name>
    <PNPDeviceID>ROOT\MS_PPPOEMINIPORT\0000</PNPDeviceID>
    <NetEnabled>>false</NetEnabled>
    <PhysicalAdapter>>false</PhysicalAdapter>
    <NetConnectionStatus>Disconnected</NetConnectionStatus>
  </NetworkAdapterItem>
  <NetworkAdapterItem>
    <InterfaceIndex>5</InterfaceIndex>
    <Installed>>true</Installed>
    <Manufacturer>Microsoft</Manufacturer>
    <Name>WAN Miniport (IPv6)</Name>
    <PNPDeviceID>ROOT\MS_NDISWANIPV6\0000</PNPDeviceID>
    <NetEnabled>>false</NetEnabled>
    <PhysicalAdapter>>false</PhysicalAdapter>
    <NetConnectionStatus>Disconnected</NetConnectionStatus>
  </NetworkAdapterItem>
  <NetworkAdapterItem>
    <AdapterType>Ethernet 802.3</AdapterType>
    <Guid>{22EF96A3-D638-4DB0-A6CA-924D090961E7}</Guid>
    <InterfaceIndex>8</InterfaceIndex>
    <Installed>>true</Installed>
    <MACAddress>00:18:8B:BE:1E:03</MACAddress>
    <Manufacturer>Broadcom</Manufacturer>
    <Name>Broadcom 440x 10/100 Integrated Controller</Name>
    <NetConnectionID>Local Area Connection</NetConnectionID>
  <PNPDeviceID>PCI\VEN_14E4&amp;DEV_170C&amp;SUBSYS_01D71028&amp;REV_02\4&amp;C61552E&amp;0&amp;00F
0</PNPDeviceID>
    <NetEnabled>>true</NetEnabled>
    <PhysicalAdapter>>true</PhysicalAdapter>
    <NetConnectionStatus>Connected</NetConnectionStatus>
  </NetworkAdapterItem>
  <NetworkAdapterItem>
    <AdapterType>Ethernet 802.3</AdapterType>
    <Guid>{C5931C8B-53A4-4B16-AD5A-8EA2CEE7A735}</Guid>
    <InterfaceIndex>9</InterfaceIndex>
    <Installed>>true</Installed>
    <MACAddress>00:19:D2:C8:9E:CE</MACAddress>
    <Manufacturer>Intel Corporation</Manufacturer>
    <Name>Intel(R) PRO/Wireless 3945ABG Network Connection</Name>
    <NetConnectionID>Wireless Network Connection</NetConnectionID>

```

```

<PNPDeviceID>PCI\VEN_8086&amp;DEV_4222&amp;SUBSYS_10208086&amp;REV_02\4&amp;5A01F14&amp;0&amp;00E
1</PNPDeviceID>
  <NetEnabled>>true</NetEnabled>
  <PhysicalAdapter>>true</PhysicalAdapter>
  <NetConnectionStatus>Connected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <InterfaceIndex>6</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>WAN Miniport (IP)</Name>
  <PNPDeviceID>ROOT\MS_NDISWANIP\0000</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>24</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>isatap.{2877A4B1-57BC-4101-A5D4-8E5B46B21182}</Name>
  <PNPDeviceID>ROOT\*ISATAP\0020</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <InterfaceIndex>26</InterfaceIndex>
  <Installed>>true</Installed>
  <Name>Realtek RTL8187 Wireless 802.11b/g 54Mbps USB 2.0 Network Adapter</Name>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <InterfaceIndex>7</InterfaceIndex>
  <Installed>>true</Installed>
  <Name>RAS Async Adapter</Name>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <InterfaceIndex>10</InterfaceIndex>
  <Installed>>true</Installed>
  <Name>ADM851X USB To Fast Ethernet Adapter</Name>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <InterfaceIndex>11</InterfaceIndex>
  <Installed>>true</Installed>
  <Name>ADM851X USB To Fast Ethernet Adapter</Name>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>20</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>Microsoft ISATAP Adapter #2</Name>
  <PNPDeviceID>ROOT\*ISATAP\0005</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>

```

```

<NetworkAdapterItem>
  <InterfaceIndex>13</InterfaceIndex>
  <Installed>>true</Installed>
  <Name>Bluetooth Device (Personal Area Network)</Name>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <InterfaceIndex>14</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>WAN Miniport (SSTP)</Name>
  <PNPDeviceID>ROOT\MS_SSTP\MINIPORT\0000</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <InterfaceIndex>15</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>WAN Miniport (Network Monitor)</Name>
  <PNPDeviceID>ROOT\MS_NDISWANBH\0000</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <AdapterType>Ethernet 802.3</AdapterType>
  <Guid>{2877A4B1-57BC-4101-A5D4-8E5B46B21182}</Guid>
  <InterfaceIndex>17</InterfaceIndex>
  <Installed>>true</Installed>
  <MACAddress>00:19:7D:FE:90:DE</MACAddress>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>Bluetooth Device (Personal Area Network) #2</Name>
  <NetConnectionID>Bluetooth Network Connection 2</NetConnectionID>
  <PNPDeviceID>BTH\MS_BTHPAN\7&amp;1FCBCC43&amp;1&amp;2</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>true</PhysicalAdapter>
  <NetConnectionStatus>MediaDisconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>18</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>Microsoft ISATAP Adapter</Name>
  <PNPDeviceID>ROOT\*ISATAP\0004</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>21</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>isatap. {7E82F04A-C4A7-45C8-BC92-F6988EA41889}</Name>
  <PNPDeviceID>ROOT\*ISATAP\0007</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
<NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>19</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>Microsoft ISATAP Adapter #4</Name>
  <PNPDeviceID>ROOT\*ISATAP\0006</PNPDeviceID>

```

```

    <NetEnabled>>false</NetEnabled>
    <PhysicalAdapter>>false</PhysicalAdapter>
    <NetConnectionStatus>Disconnected</NetConnectionStatus>
  </NetworkAdapterItem>
</NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>27</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>isatap. {2877A4B1-57BC-4101-A5D4-8E5B46B21182}</Name>
  <PNPDeviceID>ROOT\*ISATAP\0021</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
</NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>25</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>isatap.earlyCASE.com</Name>
  <PNPDeviceID>ROOT\*ISATAP\0012</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
</NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>22</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>isatap. {E0F024A7-757A-42FF-A064-A8EDDA2AFAAE}</Name>
  <PNPDeviceID>ROOT\*ISATAP\0022</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
</NetworkAdapterItem>
  <AdapterType>Tunnel</AdapterType>
  <InterfaceIndex>23</InterfaceIndex>
  <Installed>>true</Installed>
  <Manufacturer>Microsoft</Manufacturer>
  <Name>6T04 Adapter</Name>
  <PNPDeviceID>ROOT\*6T04MP\0000</PNPDeviceID>
  <NetEnabled>>false</NetEnabled>
  <PhysicalAdapter>>false</PhysicalAdapter>
  <NetConnectionStatus>Disconnected</NetConnectionStatus>
</NetworkAdapterItem>
</NetworkAdapters>
<NetworkAdapterSettings>
  <NetworkAdapterSettingsItem>
    <Description>Broadcom 440x 10/100 Integrated Controller</Description>
    <InterfaceIndex>8</InterfaceIndex>
    <IPEnabled>>true</IPEnabled>
    <DHCPEnabled>>true</DHCPEnabled>
    <DHCPLeaseExpires>2009-10-27T09:39:04</DHCPLeaseExpires>
    <DHCPLeaseObtained>2009-10-26T09:39:04</DHCPLeaseObtained>
    <DHCPServer>192.168.2.1</DHCPServer>
    <IPAddress_>
      <string>192.168.2.116</string>
      <string>fe80::d0e1:efab:b97c:b081</string>
    </IPAddress_>
    <IPAddress>192.168.2.116; fe80::d0e1:efab:b97c:b081; </IPAddress>
    <DNSHostName>TomStrack-NB</DNSHostName>
    <IPSubnet_>
      <string>255.255.255.0</string>
      <string>64</string>
    </IPSubnet_>
  </NetworkAdapterSettingsItem>
  <NetworkAdapterSettingsItem>
    <Description>Intel (R) PRO/Wireless 3945ABG Network Connection</Description>

```

```

<InterfaceIndex>9</InterfaceIndex>
<IPEnabled>>true</IPEnabled>
<DHCPEnabled>>true</DHCPEnabled>
<DHCPLeaseExpires>2009-10-27T09:39:06</DHCPLeaseExpires>
<DHCPLeaseObtained>2009-10-26T09:39:06</DHCPLeaseObtained>
<DHCPServer>192.168.2.1</DHCPServer>
<IPAddress_>
  <string>192.168.2.118</string>
</IPAddress_>
<IPAddress>192.168.2.118; </IPAddress>
<DNSHostName>TomStrack-NB</DNSHostName>
<IPSubnet_>
  <string>255.255.255.0</string>
</IPSubnet_>
</NetworkAdapterSettingsItem>
</NetworkAdapterSettings>
<PhysicalMemory>
  <PhysicalMemoryItem>
    <Capacity>1073741824</Capacity>
    <Location>DIMM_A</Location>
    <Manufacturer>CE00000000000000</Manufacturer>
    <PartNumber>M4_70T2953CZ3-CE6 </PartNumber>
    <SerialNumber>F1061930</SerialNumber>
    <Speed>667</Speed>
    <MemoryType>DDR</MemoryType>
    <FormFactor>DIMM</FormFactor>
  </PhysicalMemoryItem>
  <PhysicalMemoryItem>
    <Capacity>1073741824</Capacity>
    <Location>DIMM_B</Location>
    <Manufacturer>FFFFFFFFFFFFFFFF</Manufacturer>
    <PartNumber> </PartNumber>
    <SerialNumber>FFFFFFFF</SerialNumber>
    <Speed>0</Speed>
    <MemoryType>DDR</MemoryType>
    <FormFactor>DIMM</FormFactor>
  </PhysicalMemoryItem>
</PhysicalMemory>
</HardwareInfo>
</EsiInfo>
</ImageInfo>

```

New tables in the Microsoft Access Database that are created:

Data_Collection_Tracking – Contains the details related to what and how you created a drive image from within earlyCASE.

DrivelImages – This table contains the minimal information that is contained in any EnCase image files that are processed.

DrimeImagePartitions – This table works in conjunction with the “DrivelImageMetaData” table to handle drive images which have multiple partitions, unallocated space, etc. It holds file system and drive information for each partition in an image.

DrivelImageMetaData -This table holds the information that is populated into the XML embedded in an AFF image. I.e.. the machine, user, OS, etc information about the machine and drive collected.