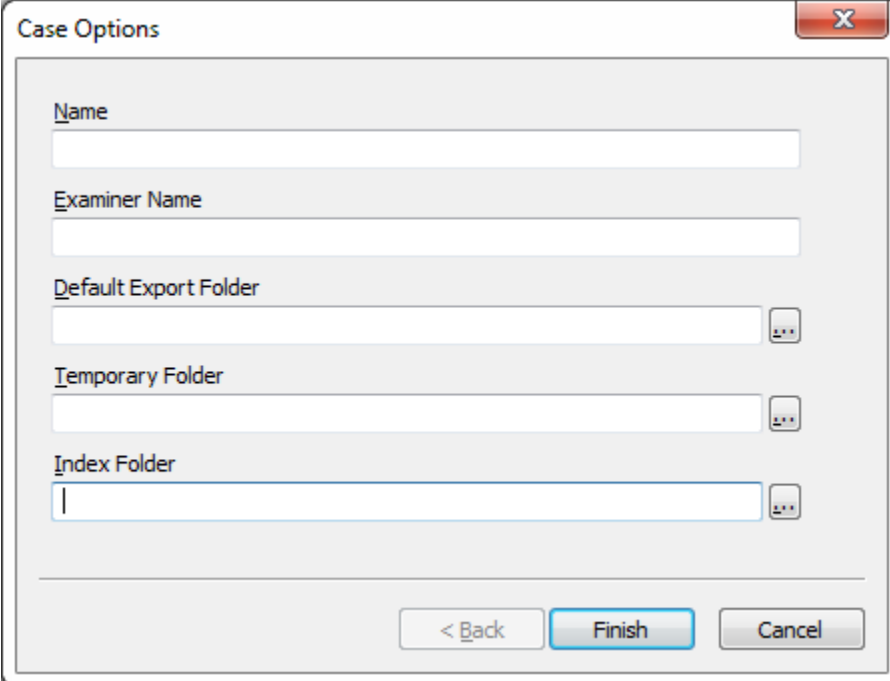


### **Encase Naming Conventions**

#### **EnCase 6.x**

1) When versions EnCase 6.x are initially opened, the following dialogue box will appear:



2) Use the following conventions to fill in each field:

- a) Name - This will be the unique name of the EnCase case file for this particular case. It consists only of the Laboratory Case Number of the evidence acquired or to be acquired into the case.

For example: DSS-16-001234

- b) Examiner Name - This will be the name of the analyst creating the new case file.

For example: "Jim Jackson", "Jane Smith" or "Johnson"

If two or more examiners share the same name they must be uniquely identified.

For example: "Jim Jackson" and "James Jackson"

- c) Default Export Folder - This folder will be named "EnCase Export" and the path to it will be the target drive.

*Approved by Director: Dr. Guy Vallaro*

- d) Temporary Folder - This folder will be named “EnCase Temp” or “EnCase Temporary” and the path to it will be the target drive.
- e) Index Folder - This folder will be named “EnCase Index” and the path to it will be the target drive.

The screenshot shows the 'Options' dialog box in EnCase. The 'Name' field is 'S3\_HD1' and the 'Evidence Number' is '003'. The 'Notes' field contains 'Maxtor 40GB hard drive - Model D740X - Serial #: 256HG43890'. The 'File Segment Size (MB)' is 640. The 'Start Sector' is 0 and the 'Stop Sector' is 1968127. The 'Compression' is set to 'Good (Slower, Smaller)'. The 'Block size (Sectors)' is 64 and the 'Error granularity (Sectors)' is 64. The 'Reader Threads' are 1 and the 'Worker Threads' are 5. The 'Hash Thread' is unchecked. The 'Acquisition MD5' and 'Acquisition SHA1' checkboxes are checked. The 'Output Path' is 'H:\ID-11-123456\S3\_HD1.E01'. The 'Remote acquisition' checkbox is unchecked. The 'Alternate Path' field is empty. The dialog has 'Back', 'Finish', and 'Cancel' buttons at the bottom.

Referring to the screenshot to the left, the following naming conventions are used when acquiring digital media with EnCase 6.x:

1. In the Name field, the naming convention will reflect the Submission # along with the media number based on how many pieces of the particular media type\* there are. For example, if a computer is submitted as Submission #003 and it contains two (2) hard drives, the naming convention would be: S3\_HD1 and S3\_HD2. Meaning;
  - S3 equals Submission #003
  - HD1 equals Hard Drive 1
  - HD2 equals Hard Drive 2
2. The Evidence Number field is the actual 3 digit Laboratory Submission Number.
3. The Notes field contains information about the particular piece of media. For example: Make, Model and Serial Number.
4. The Output Path field is the path to the Staging Drive.
5. Both MD5 and SHA1 acquisition hash boxes should be checked.
6. All other fields may be defined based

upon the examiner's requirements.

**Notes:** The screenshot above depicts a version of EnCase 6.x. The same Name, Evidence Number, Notes and Output Path fields exist in previous version of EnCase and should be treated the same.

Both the MD5 and SH1 acquisition boxes are absent in earlier versions of Encase. However, a MD5 hash is automatically generated in the earlier versions.

\* A complete list of abbreviations for the various types of media can be found in SOP-CC-31 – Sub-item Labeling Standards.

## **EnCase 8.x**

1) When versions EnCase 8.x are initially opened, the following dialogue box will appear:

*Approved by Director: Dr. Guy Vallaro*

**Options**

**Templates**

- #1 Basic
- #2 Forensic
- #3 Basic (UK)
- #4 Forensic (UK)
- #5 Flexible
- None

**Case information**

	Name	Value
1	Case Number	<Define Value>
2	Case Date	<Define Value>
3	Examiner Name	<Define Value>
4	Examiner I.D. #	<Define Value>
5	Agency	<Define Value>
6	Description	<Define Value>

**Name and location**

Name:

Full case path:

Base case folder:

**Evidence cache locations**

☐ Use base case folder for primary evidence cache

Primary evidence cache:

Secondary evidence cache:

**Backup settings**

☒ Backup every

Maximum case backup size (GB):

Backup location:

OK Cancel

2) Use the following conventions to fill in each field:

Within Case Information complete the minimum:

- Case Number – DSS-YY-##### Example DSS-19-001234.
- Examiner Name - This will be the name of the analyst creating the new case file.

For example: “Jim Jackson”, “Jane Smith” or “Johnson”

If two or more examiners share the same name they must be uniquely identified.

For example: “Jim Jackson” and “James Jackson”

Name and location:

- c) Name - This will be the unique name of the EnCase case file for this particular case. It consists only of the Laboratory Case Number of the evidence acquired or to be acquired into the case.

For example: DSS-19-001234

- d) Base Case Folder – path where the case file is saved.  
e) Primary evidence cache - path where the data processing elements are saved.  
f) Backup location - path where the backup file for the case is saved.

The following naming conventions are used when acquiring digital media with EnCase 8.x:

1. In the Name field, the naming convention will reflect the Submission # along with the media number based on how many pieces of the particular media type\* there are. For example, if a computer is submitted as Submission #003 and it contains two (2) hard drives, the naming convention would be: S3\_HD1 and S3\_HD2. Meaning;  
-S3 equals Submission #003  
-HD1 equals Hard Drive 1  
-HD2 equals Hard Drive 2
2. The Evidence Number field is the actual 3 digit Laboratory Submission Number.
3. The Notes field contains information about the particular piece of media. For example: Make, Model and Serial Number.
4. The Output Path field is the path to the Staging Drive or Partition.

*Approved by Director: Dr. Guy Vallaro*

Acquire Device 6

Location Format Advanced

Name Evidence Number

Case Number Examiner Name

Notes

☐ Restart Acquisition ☐ Remote acquisition

Output Path

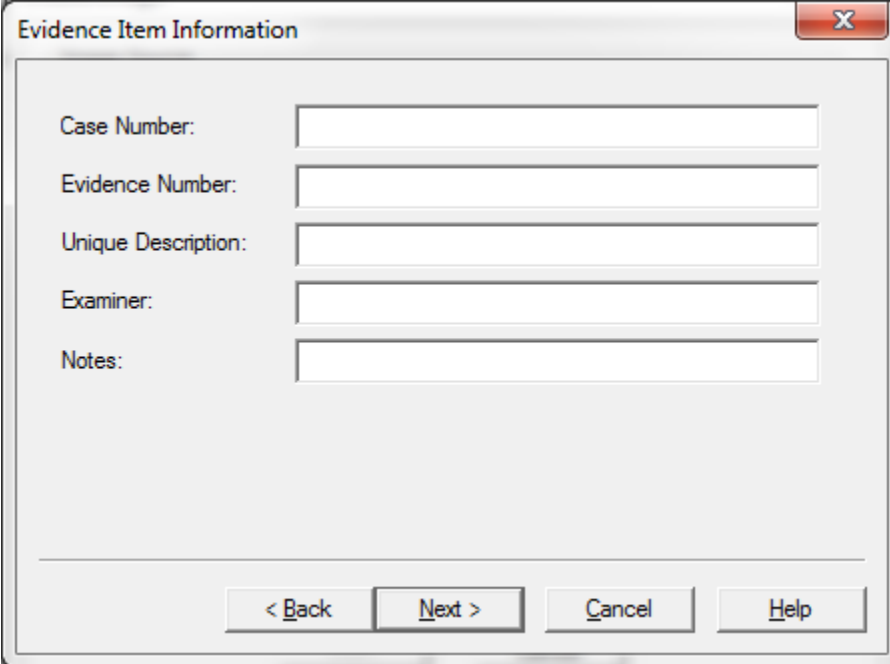
.Ex01

Alternate Path

OK Cancel

**FTK IMAGER 4.x NAMING CONVENTIONS**

- 1) During the process of imaging using FTK Imager 4.x, the following dialogue box will appear:



- 2) Use the following conventions to fill in each field:

- a) Case Number - This will be the unique identifier for the case. It consists only of the Laboratory Case Number of the evidence being acquired.

For example: DSS-16-001234

- b) Evidence Number - This will be the unique identifier for that particular piece of media. It can be the Laboratory Submission Number (for example: "001") or a sub-item number of the Laboratory Submission Number (for example: "001-1A").

- c) Unique Description - This field should contain information about the particular piece of media. For example: Make, Model and Serial Number.

- d) Examiner - This will be the name of the analyst acquiring the specific piece of media.

For example: "Jim Jackson", "Jane Smith" or "Johnson"

If two or more examiners share the same name they must be uniquely identified.

*Approved by Director: Dr. Guy Vallaro*

For example: “Jim Jackson” and “James Jackson”

- e) Notes - This field is optional and may contain any information the examiner feels is relevant to the case.

Referring to the screenshot to the left, the following naming conventions are used when acquiring digital media with FTK Imager 4.x:

7. In the Image Destination Folder field change the destination path to the established staging drive.
8. In the Image Filename (Excluding Extension) field, the naming convention will reflect the Submission # along with the media number based on how many pieces of the particular media type\* there are. For example, if a computer is submitted as Submission #003 and it contains two (2) hard drives, the naming convention would be: S3\_HD1 and S3\_HD2. Meaning;
  - S3 equals Submission #003
  - HD1 equals Hard Drive 1
  - HD2 equals Hard Drive 2
9. All other fields may be defined based upon the examiner's requirements.

\* A complete list of abbreviations for the various types of media can be found in SOP-CC-31 – Sub-item Labeling Standards.



**Tableau Forensic Duplicator (TD1) NAMING CONVENTIONS**

- 3) Upon initiation of acquisition using the Tableau Forensic Duplicator, a dialogue box will appear following the menu selection 1. Duplicate Disk, 2. Disk-to-File and Start which will prompt for a case ID, followed by Case Note, Subdir Name and File Base Name. The entries should be made as follows:
- a) Case ID - This will be the unique identifier for the case. It consists only of the Laboratory Case Number of the evidence being acquired.  
For example: DSS-16-001234
  - b) Case Note - This field should contain information about the particular piece of media. For example: Make, Model and Serial Number and the examiners name.
  - c) Subdir Name- leave as default.
  - d) File Base name - will reflect the Submission # along with the media number based on how many pieces of the particular media type\* there are. For example, if a computer is submitted as Submission #003 and it contains two (2) hard drives, the naming convention would be: S3\_HD1 and S3\_HD2. Meaning;  
S3 equals Submission #003  
HD1 equals Hard Drive 1  
HD2 equals Hard Drive 2

\* A complete list of abbreviations for the various types of media can be found in SOP-CC-31 – Sub-item Labeling Standards.

## REQUESTS FOR ANALYSIS

When filling in the fields contained in QR-CC-10 - Laboratory Report Template select from the following list the appropriate request for analysis.

1. Recovery of suspected child pornographic images either in still or video format
2. Recovery of data signifying the distribution of suspected child pornographic images or videos
3. Recovery of data signifying the importation of suspected child pornographic images or videos
4. Recovery of data signifying the production of suspected child pornographic images or videos
5. Recovery of data pertaining to an enticement investigation
6. Recovery of data pertaining to a homicide investigation
7. Recovery of data pertaining to a suicide investigation
8. Recovery of data pertaining to a fraud investigation
9. Recovery of data pertaining to a larceny investigation
10. Recovery of data pertaining to a burglary investigation
11. Recovery of data pertaining to a threatening/harassment investigation
12. Recovery of data pertaining to a financial fraud/counterfeiting investigation
13. Recovery of data pertaining to an e-mail threats/harassment/stalking investigation
14. Recovery of data pertaining to a narcotics investigation
15. Recovery of data pertaining to an identity theft investigation
16. Recovery of data pertaining to a network intrusion investigation
17. Recovery of data pertaining to a domestic violence investigation
18. Recovery of data pertaining to a voyeurism investigation
19. Recovery of cell phone data
20. Recovery of media device data
21. Hard drive restoration
22. Digital media restoration
23. Hard drive sterilization
24. Removable media sterilization

*Approved by Director: Dr. Guy Vallaro*

- 25. Recovery of DVR data
- 26. Imaging/acquisition of media
- 27. Administrative inquiries
- 28. Other - please specify