CYACOMB FORENSICS

Software Trial Guide

Cyacomb Examiner

CYACOMB FORENSICS

INTRODUCTION

The **Cyacomb Examiner** software trial is designed to demonstrate the effectiveness of Cyacomb's technology in rapidly scanning computers or external storage devices against a collection of known illegal material (Contraband).

To effectively evaluate the results of such a trial, it is vital that the user has complete knowledge and control over the test data used in the trial. To facilitate this, Cyacomb provide a full set of standard test data. It is strongly recommended that this test data is used for the initial software trial to enable the user to fully understand the functionality of the technology. Following this initial trial, Cyacomb can provide additional tools to allow the user to further evaluate the technology with their own test data, upon request.

This document will guide you through using both these methods to effectively evaluate Cyacomb's technology.

CYACOMB'S TECHNOLOGY

Cyacomb's technology offers an alternative automated search for known content which delivers results in seconds or minutes. Original data is processed and used to produce the a **Contraband Filter.**
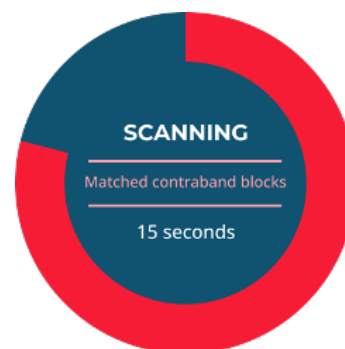

A C**ontraband Filter** is Cyacomb's proprietary alternative to a hash set as used in traditional file hash comparison technology.

When an investigator wishes to analyse a suspect device, **Cyacomb Examiner** is loaded with this **Contraband Filter** and used to scan the device under investigation.

Colour coded scan results are displayed to aid rapid triage decisions.

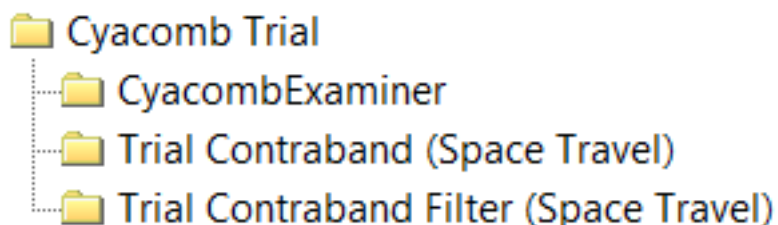# Using the Cyacomb Test Data

WHAT YOU NEED

- **Computer with**
  - Windows 7 or above
  - Administrator privileges

- **Cyacomb Trial Software & Test Data**
  - Cyacomb Examiner Trial Version
  - Cyacomb Trial Contraband
  - Cyacomb Trial Contraband Filter

PREPARING THE TRIAL SOFTWARE & DATA

Extract the provided file 'Cyacomb Trial.zip', which contains the following folders.

CyacombExaminer

Contains the installer for the Cyacomb Examiner application and the User Manual

Trial Contraband (Space Travel)

Contains 146 image and video files (200MB) of royalty-free space travel images that Cyacomb use to represent illegal files (contraband)

Trial Contraband Filter (Space Travel)

Contains a Contraband Filter (Cyacomb Trial.cf) built from the space travel images

SEEDING A DEVICE WITH TRIAL CONTRABAND

Copy the trial Space Travel contraband files to an external storage device such as a USB hard disk drive. Alternatively, if an external storage device is not available, the contraband files can be copied to the same computer that you will install Cyacomb Examiner.

To effectively represent a real-word suspect device, it is recommended to distribute the trial contraband randomly across the device and the folder structure.

Cyacomb Examiner also scans unallocated space and a sample of the trial contraband may be deleted from the test device to demonstrate this.
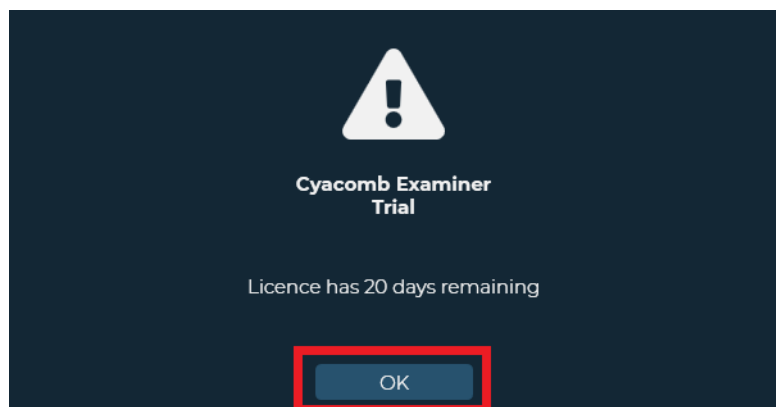
INSTALLING & ACTIVATING TRIAL SOFTWARE

Run the supplied Cyacomb Examiner installer to install the desktop version of Cyacomb Examiner.

Start the installed version of Cyacomb Examiner and when prompted, select "Start Quick Trial"
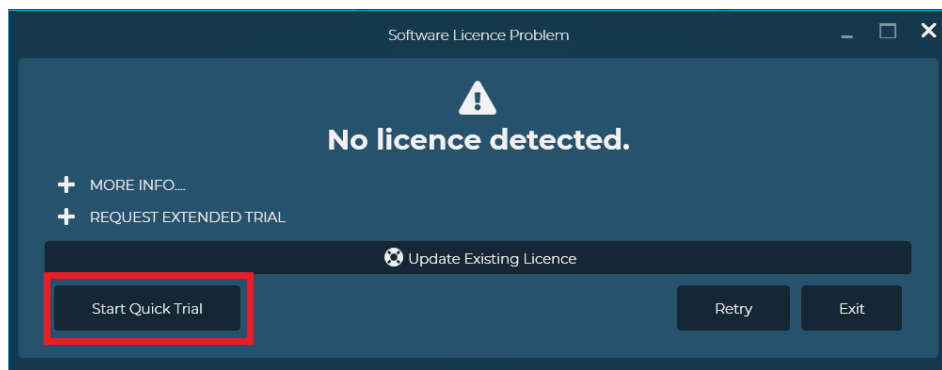
Click "OK" in the serial licence confirmation window

NOTE: Cyacomb Examiner's trial licence is valid for 21 days. Once expired, a new trial cannot be started even if the software is reinstalled. If you wish to extend a trial, please contact your Cyacomb sales advisor directly or email sales@cyacomb.com.
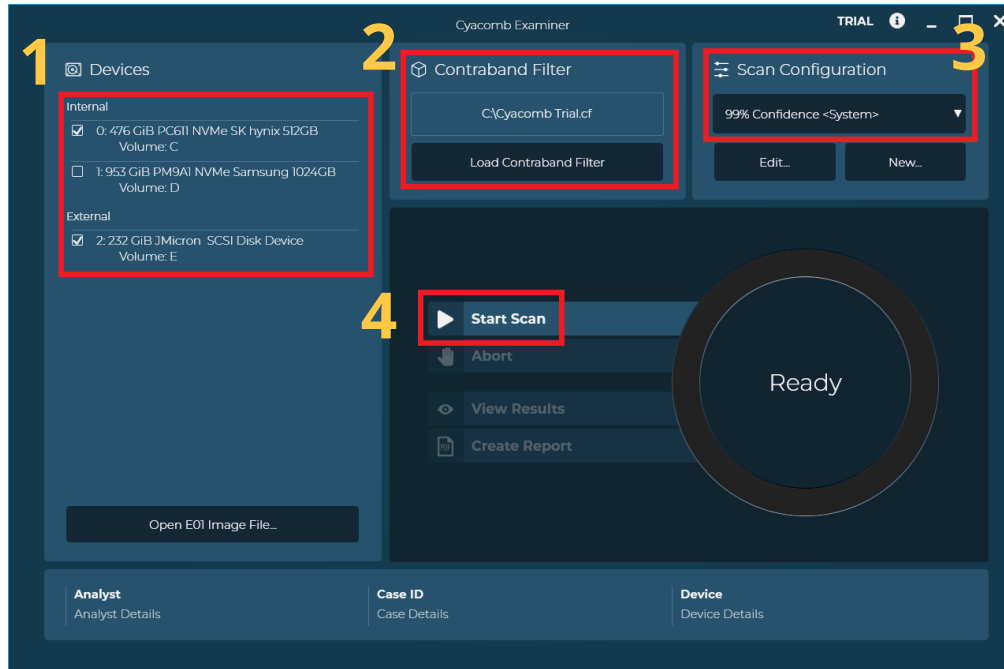
SCANNING THE TEST DEVICE

Start the Cyacomb Examiner trial application and, if the test data has been placed on an external storage device, connect the device to the computer running Cyacomb Examiner.

NOTE: To maintain forensic integrity, it is highly recommended that when using Cyacomb Examiner in an operational environment, that a write blocker / forensic bridge is placed between the computer running Cyacomb Examiner and the suspect device being scanned.
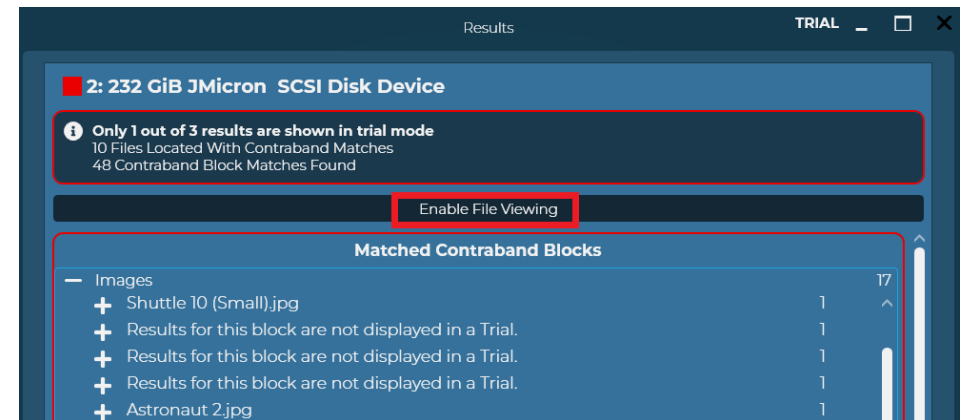
Follow the 4 simple steps below:

1 **Select the attached device(s) to be scanned** (either the attached external device or the computer's own drive)

2 **Load the 'Cyacomb Trial.cf' Contraband Filter from its saved location**

3 **Choose a scan confidence of 99%** (see user manual for further information on scan confidence)

4 **Select 'Start Scan'**

SCAN RESULTS

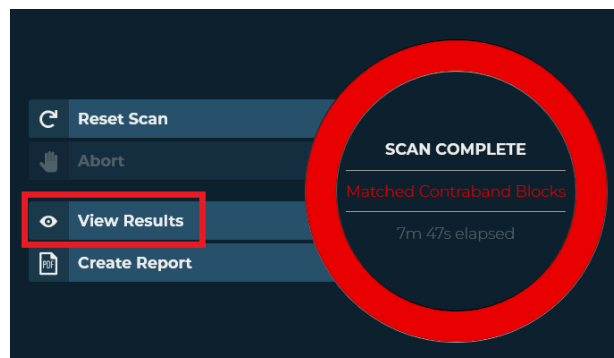Upon completion of the scan, click the "View Results" button.

NOTE: In trial mode, Cyacomb Examiner is restricted to displaying one in every three results

For reasons of operator welfare, the previewing of results is disabled by default in Cyacomb Examiner. To enable previewing of results, click the "Enable File Viewing" button.
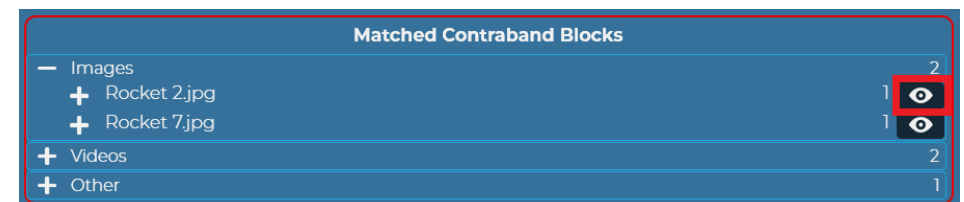

To preview a result, click on the 'eye' button.

Full details on interpreting Cyacomb Examiner's results can be found in the Cyacomb Examiner User Manual.

Using Your Own Test Data

To evaluate Cyacomb Examiner using your own test data you will need **Cyacomb Collector**, Cyacomb's desktop tool for processing contraband and building Contraband Filters, and a Cyacomb Licence Dongle to enable you to run the software. If you do not currently possess Cyacomb Collector, please contact your Cyacomb Sales Representative or email sales@cyacomb.com.

WHAT YOU NEED

- **Computer with**
  - Windows 7 or above
  - Administrator privileges

- **Cyacomb Trial Software & Test Data**
  - Cyacomb Examiner Trial Version
  - Cyacomb Collector
  - Cyacomb Licence Dongle
  - > 20MB of test contraband

NOTE: The following process details how to build and use a Contraband Filter without the optional categorisation of results. Once familiar with the process, you may wish to refer to the Cyacomb User Manual on how to build a Contraband Filter Set for categorised results

PREPARING YOUR TEST CONTRABAND

As the default contraband target size set in Examiner is 20MB, it is highly recommended that your set of test contraband contains at least 20MB of images / videos.

Place all your test contraband files in a single folder on your computer.
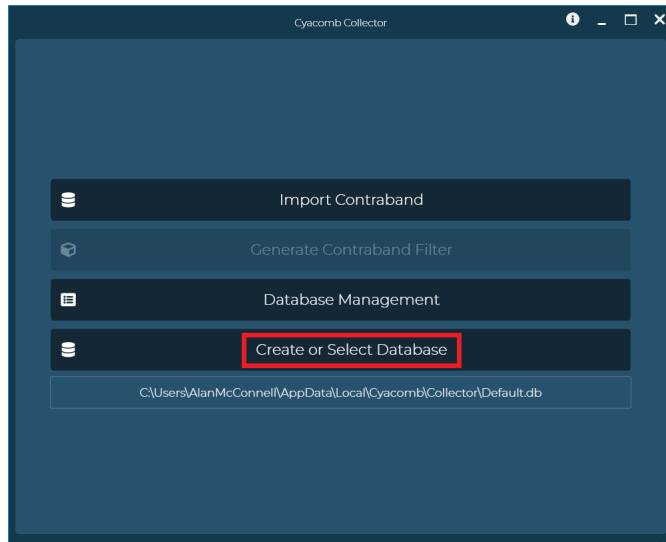
Cyacomb Test Contraband

INSTALLING CYACOMB COLLECTOR

Contraband Filters are built from original data using Cyacomb's data management tool, **Cyacomb Collector**. Each source file is processed by Cyacomb Collector and the collected data stored in Cyan Collector's database. From this database, Contraband Filters can be built.

NOTE: Cyan Collector and its database reside on your own system. No data is ever handled or held by Cyacomb.
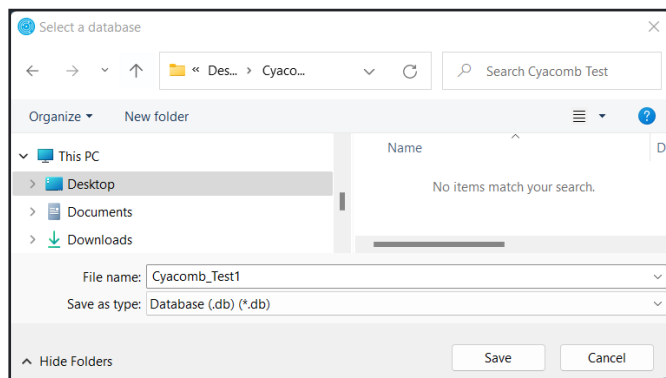
Run the supplied Cyacomb Collector installer to install the software
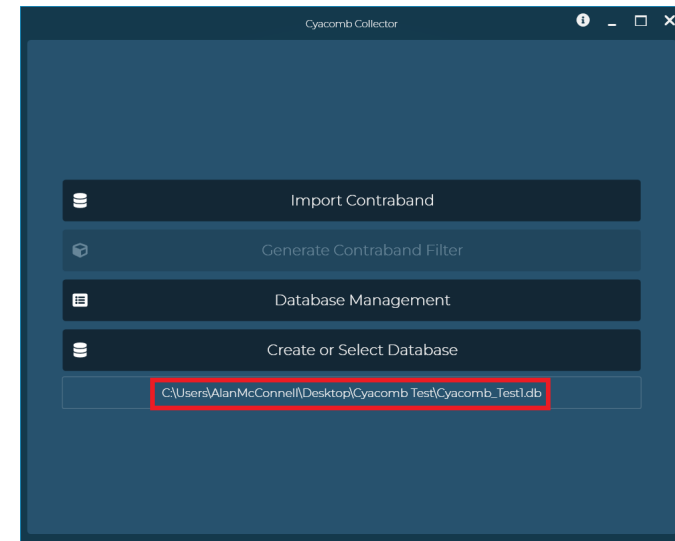
COLLECTING CONTRABAND

Insert your Cyacomb Licence Dongle and run the installed Cyacomb Collector, then click on "Create or Select Database".
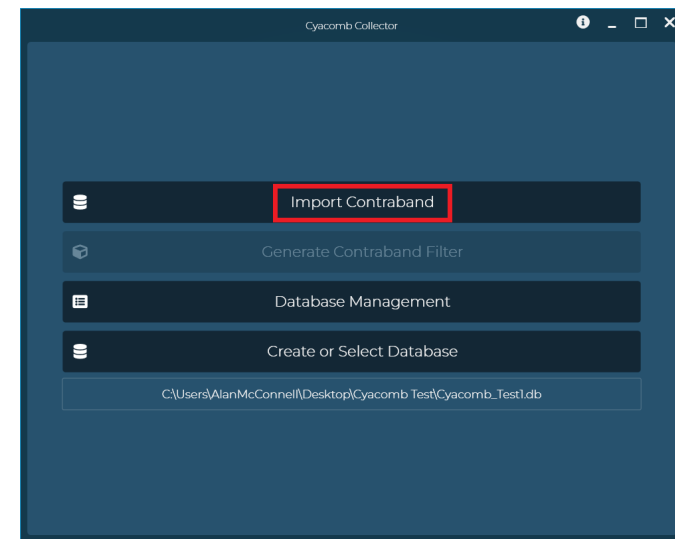

Choose a location and name your database.

Once created, your database will be indicated at the bottom of the UI
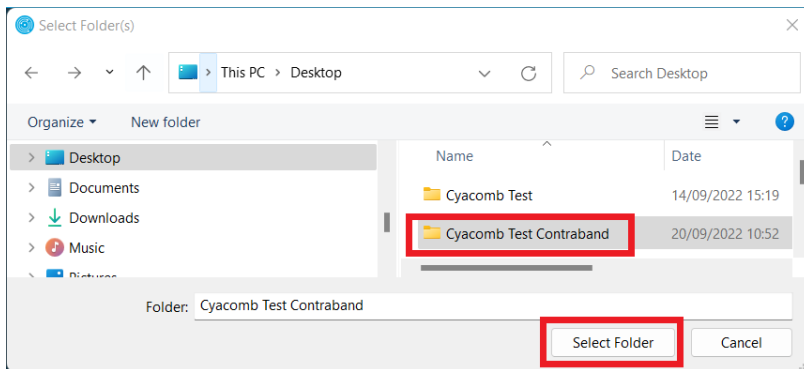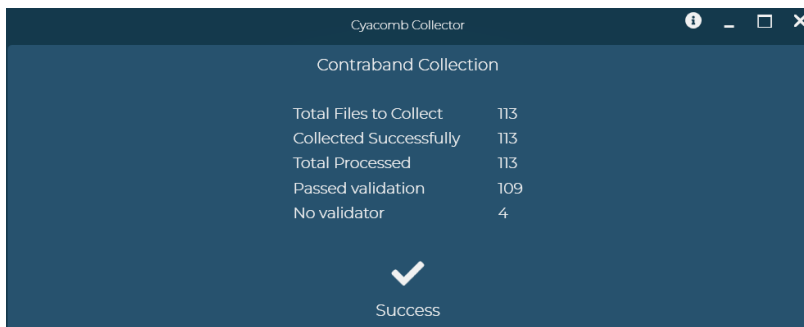

Click "Import Contraband"

Click on the 'folder' icon to browse to your folder of test contraband

Select your folder of contraband and click "Select Folder"

Once all files in your test contraband folder have been collected, a summary will be displayed (please refer to the Cyacomb User Manual for additional descriptions of the collection summary).
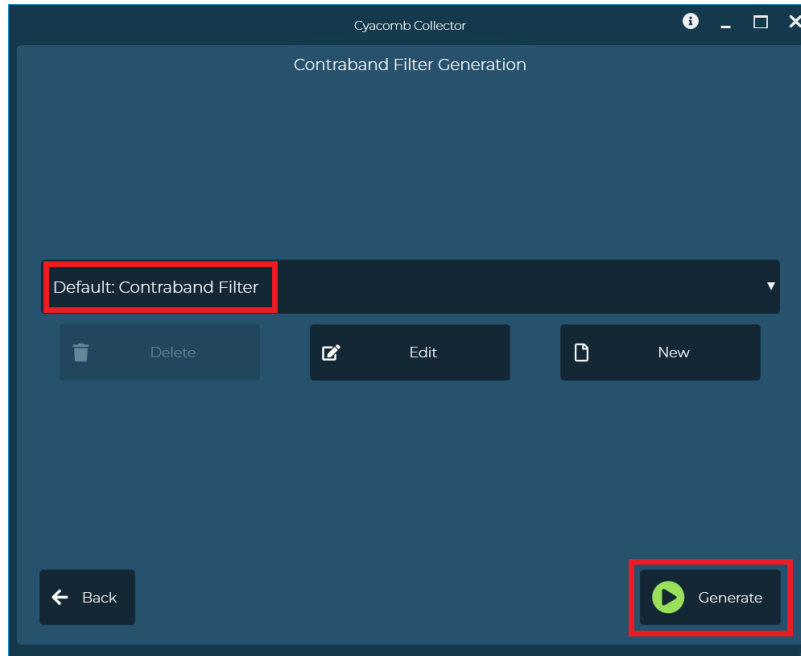

BUILDING A CONTRABAND FILTER

To build a Contraband Filter from the collected contraband files, select "Generate Contraband Filter" from the main menu.
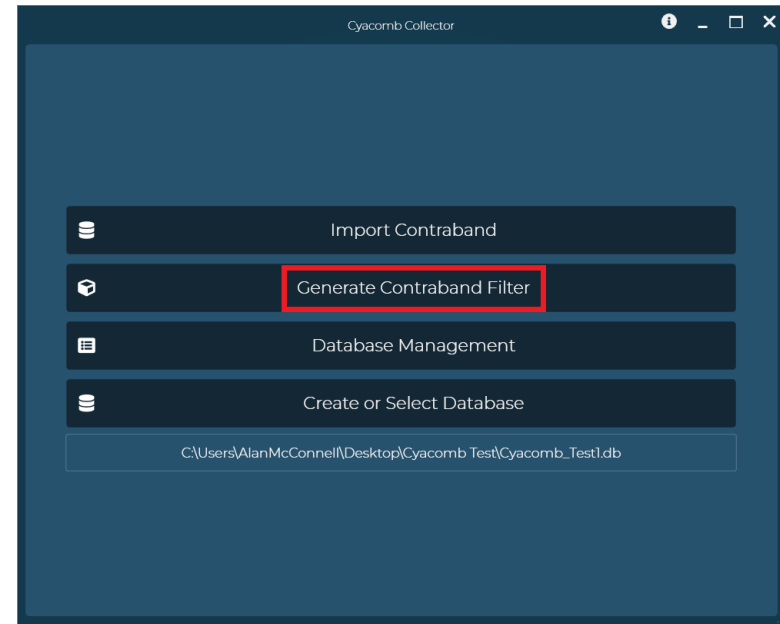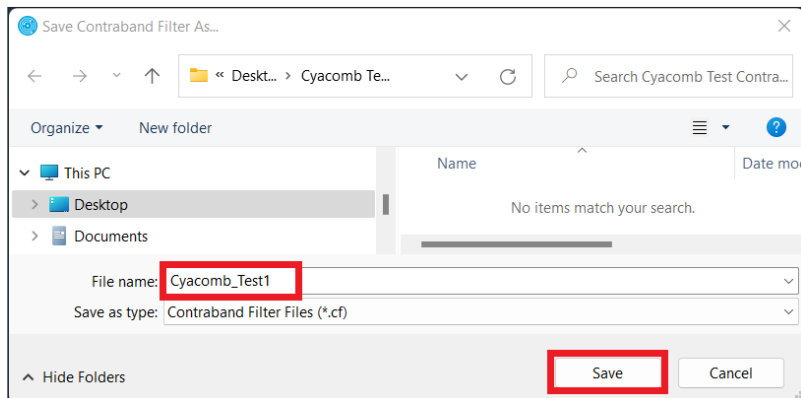

Select "Default Contraband Filter" from the top down menu.

Click "Generate"

Name your Contraband Filter and save it in a desired location.

Upon completion, a summary of the process will be displayed (please refer to the Cyacomb User Manual for additional descriptions of the collection summary).

SCANNING WITH YOUR CONTRABAND FILTER

To test your Contraband Filter, follow the steps described in the section of this guide titled "Using The Cyacomb Test Data", substituting the Cyacomb provided test contraband and Contraband Filter with your own test contraband and the Contraband Filter built from it

TECHNICAL & SALES SUPPORT

For technical support with your Cyacomb software trial, please email:

support@cyacomb.com

For sales support or enquiries please contact your Cyacomb Sales Representative, or email:

sales@cyacomb.com

CYACOMB FORENSICS

cyacomb.com