



Categorizer for Pictures, or C4P, is a combination of forensic EnScripts™ and a standalone Windows Application.

C4P makes it possible to quickly and efficiently classify pictures that have been forensically extracted for review.

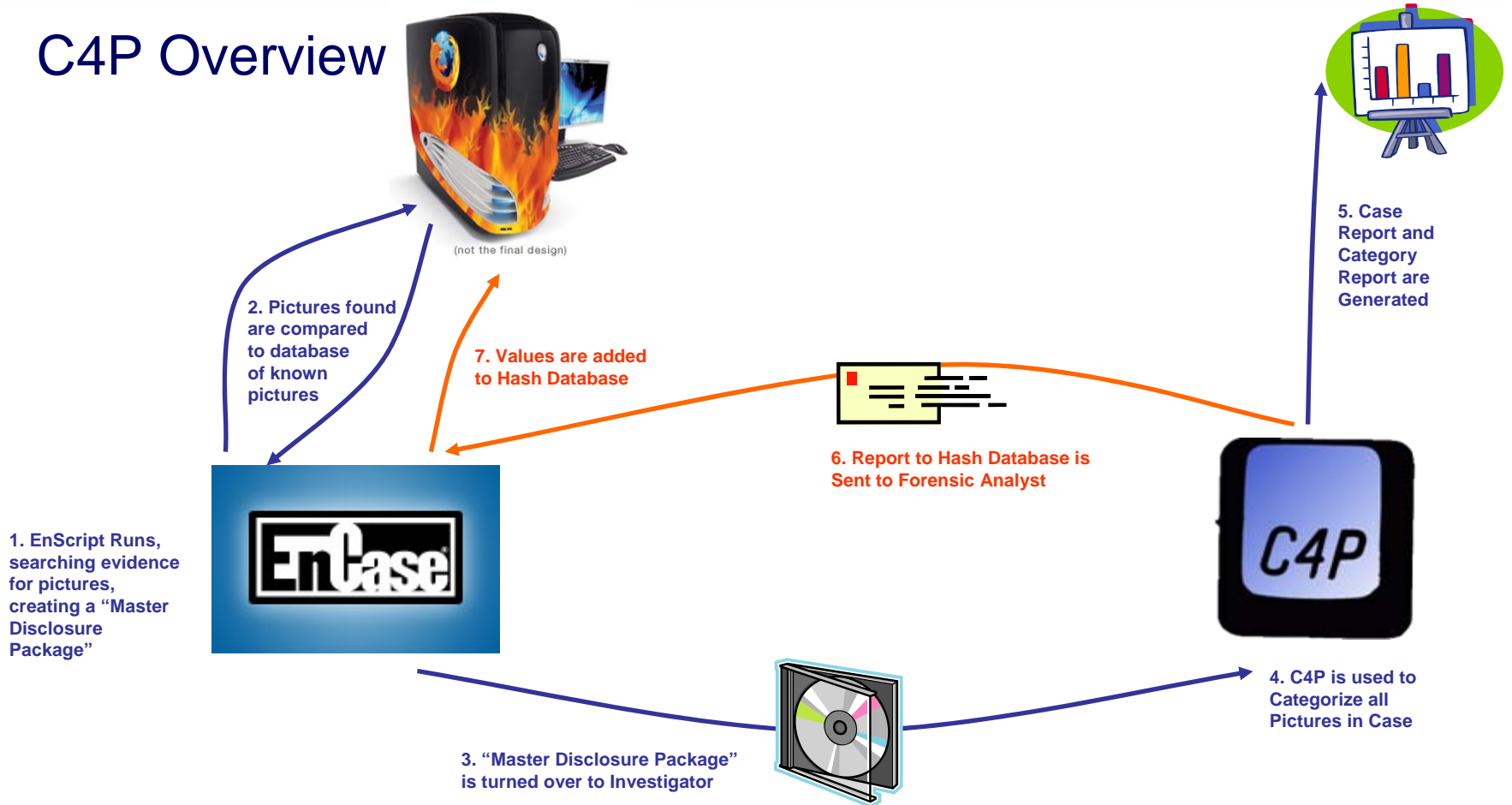
This short slideshow will explain the general concept.

Categorizer for Pictures – The Process

Ontario Provincial Police, Electronic Crime Section



C4P Overview





Step 1:

1. EnScript Runs, searching evidence for pictures, creating a "Master Disclosure Package"



The Current Version of C4P is meant to work with the latest version of EnCase v5. There are two ways you can run this script:

- as an actual EnScript, or
- as an EnPack.

An EnPack is a pre-compiled EnScript. Since it has already been compiled, you only have to deal with one file: "C4P.EnPack". However, you cannot see or change the code...

When you run the script you can:

- **Search "Selected Files" Only** – ie: Blue-checked entries
- **Generate Bookmarks** for each hit. Note files will still be copied out
- **Mount Email** – enabling the script to search for picture attachments
- **Populate Picture Library**
- **Run in Debug Mode** – ONLY if you are having troubles
- **Pre-Categorize** the pictures based on data from a Hash Database

Categorizer for Pictures – The Process

Ontario Provincial Police, Electronic Crime Section



Step 2:



2. Pictures found are compared to database of known pictures

1. EnScript Runs, searching evidence for pictures, creating a "Master Disclosure Package"



If you have opted to set up a *C4P Hash Database*, then the EnScript can be set to communicate to it during execution. When a new pictures is found (and validated by the Script), it's *MD5 Hash Checksum* value will be determined.

At this point, the Script would then query the Hash Database to see if there is an existing record for this value. If a record is found, then the C4P EnScript will incorporate the *Category* value found in the Database into the "Master Disclosure Package"

Categorizer for Pictures – The Process

Ontario Provincial Police, Electronic Crime Section



Step 3:

1. EnScript Runs, searching evidence for pictures, creating a "Master Disclosure Package"



2. Pictures found are compared to database of known pictures

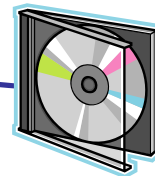


Once the EnScript has completed, the only thing remaining is to copy the data extracted to some sort of portable media. External Hard Drives are the recommended means, although CD/DVD media is also acceptable.

Everything generated by the EnScript is placed under one common folder – identified at the time of Script Execution. This folder structure is called the "Master Disclosure Package".

This package is then turned over to the Investigator for review.

3. "Master Disclosure Package" is turned over to Investigator



Categorizer for Pictures – The Process

Ontario Provincial Police, Electronic Crime Section



Step 4:



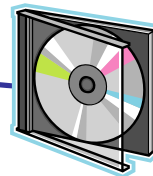
(not the final design)

2. Pictures found are compared to database of known pictures

1. EnScript Runs, searching evidence for pictures, creating a "Master Disclosure Package"



3. "Master Disclosure Package" is turned over to Investigator



4. C4P is used to Categorize all Pictures in Case



The Investigator uses C4P to create a New Case based on the "Master Disclosure Package".

C4P will then exclude duplicate pictures and identify those which have been Pre-categorized. The remaining pictures are "Unchecked" – requiring assessment by the Investigator.

The Investigator uses C4P to categorize all Unchecked pictures.

Categorizer for Pictures – The Process

Ontario Provincial Police, Electronic Crime Section



Step 5:

1. EnScript Runs, searching evidence for pictures, creating a "Master Disclosure Package"



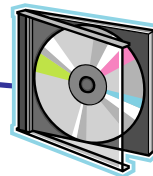
2. Pictures found are compared to database of known pictures



Once the Investigator has finished assessing all pictures in the case, Case Reports and Category Reports can be generated documenting their findings.

C4P also provides some analysis tools that can be applied to the completed investigation.

3. "Master Disclosure Package" is turned over to Investigator



4. C4P is used to Categorize all Pictures in Case



5. Case Report and Category Report are Generated

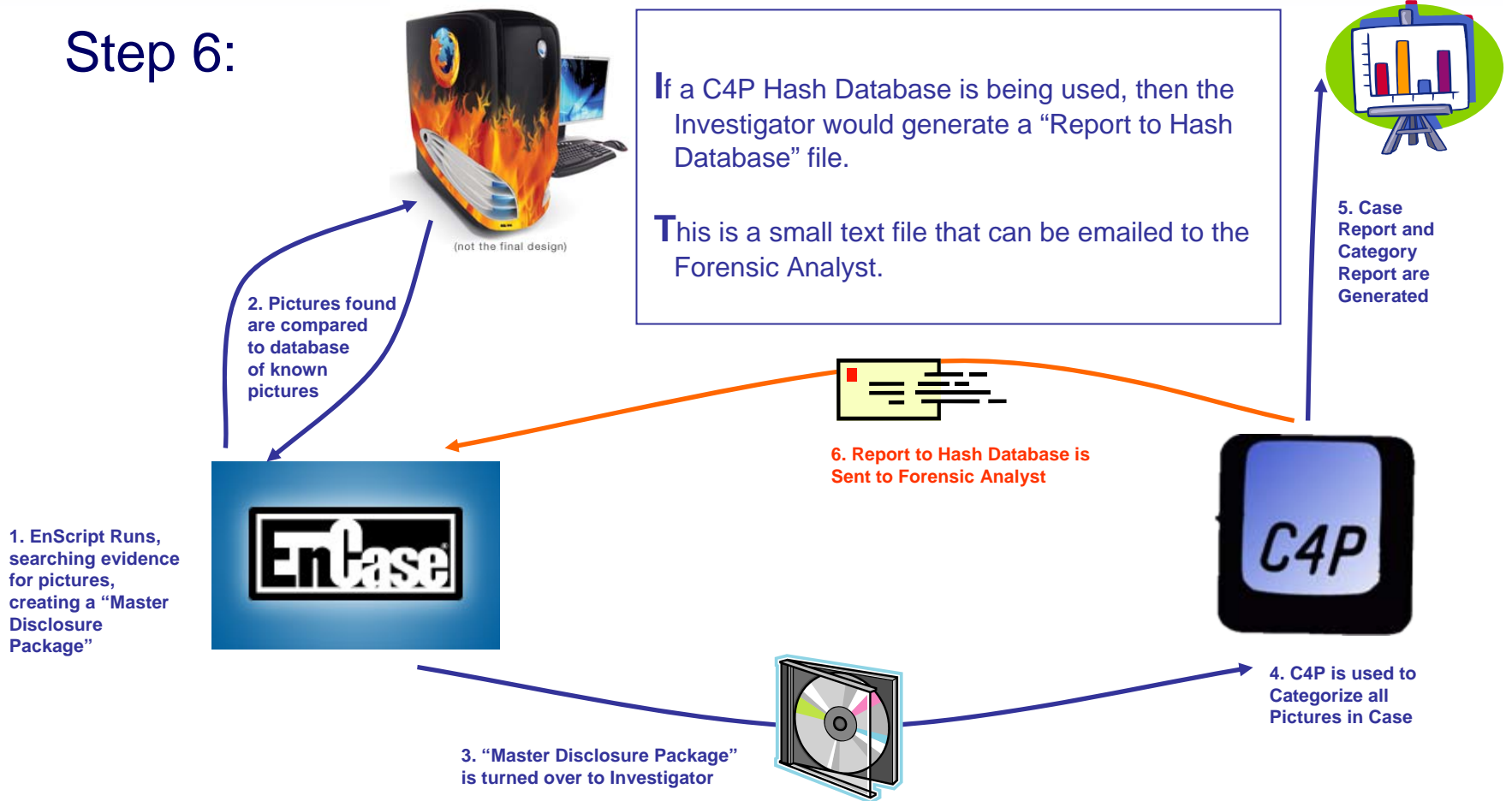


Categorizer for Pictures – The Process

Ontario Provincial Police, Electronic Crime Section



Step 6:

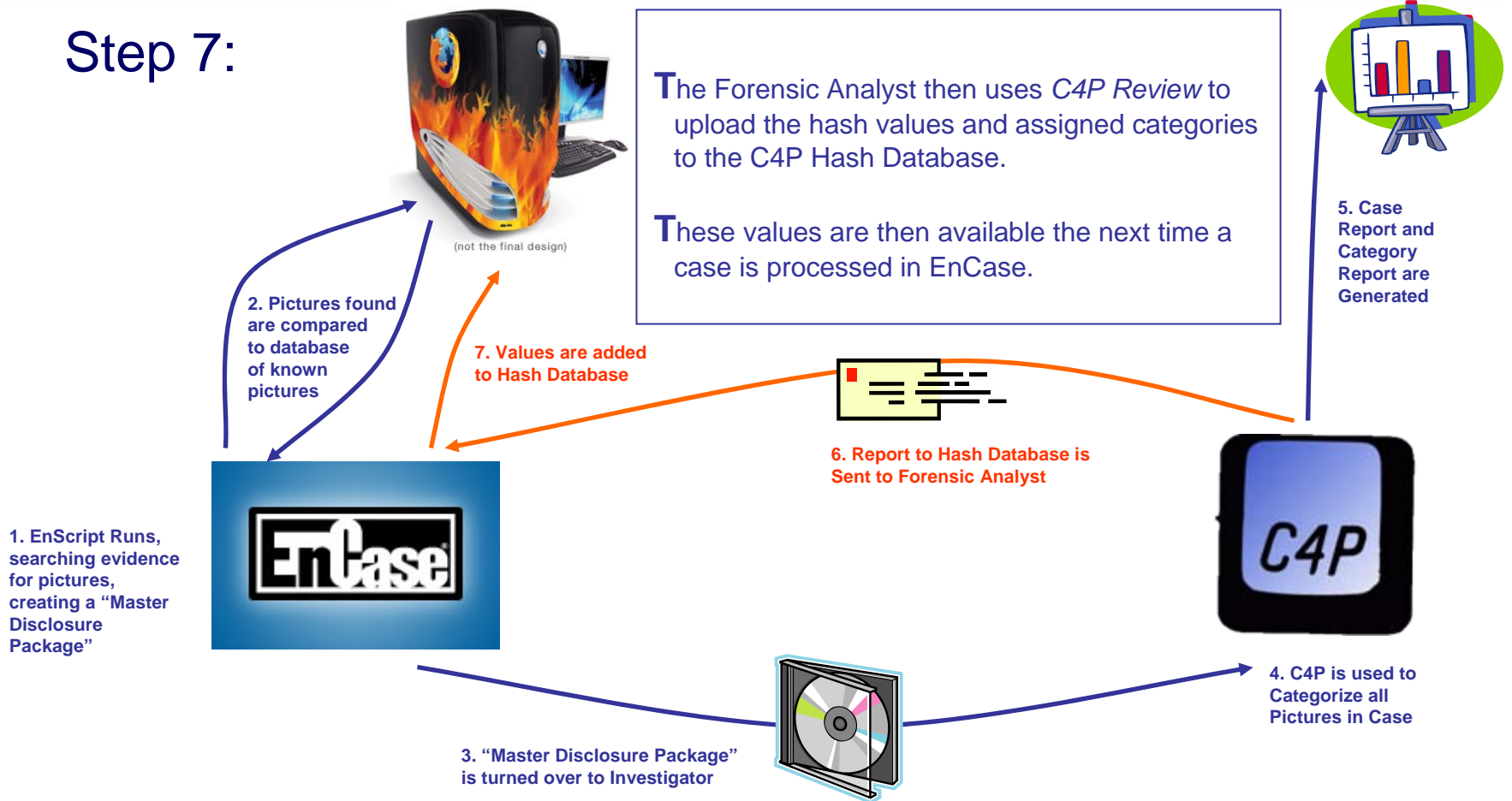


Categorizer for Pictures – The Process

Ontario Provincial Police, Electronic Crime Section



Step 7:





This is the General Overview of how Categorizer for Pictures works. Separate, more detailed, slideshows are also available for the following topics:

C4P EnScript/EnPack:

- Installation
- C4P EnScript: Understanding the Concepts

Categorizer for Pictures v3:

- Installation
- How to Categorize Quickly
- How to Analyze Your Results
- How to Report Your Findings

C4P Hash Database:

- Working with SQL Server
- Working with MySQL
- Installation/Configuration of C4P Review
- Installation/Configuration of C4P Picture Library