
QinetiQ

Selective & Intelligent Imaging using Digital Evidence Bags

Philip Turner
Investigations & Security Health Check
QinetiQ, Malvern, UK.
pbturner@qinetiq.com

The Traditional Approach!

- **Capture everything … regardless, then Analyse**
  - Unsophisticated process
  - Start at the beginning … keep going until the end
  - Little or no error handling
- **The problem with this approach**
  - What happens if we only want specific information
  - Increasing capacity of storage media

Selective Imaging – Why do it?

- **Quantity of information**
- **Also…**
  - Forensic Triage
  - Intelligence gathering
  - Legal Requirements
  - E-discovery
  - Incident Response / Live Investigation

Selective / Intelligent Imaging – What is it?

- **Generally associated with the decision NOT to acquire all the possible information during the acquisition process…**
- **Slowly becoming more recognised that partial or selective file copying may be considered – ACPO Good Practice Guide**

Types of Selective Imaging

- **Manual – the investigator selects exactly what is captured**
- **Semi-automatic – the investigator decides on the categories of information to capture**
- **Automatic – selective acquisition in a manner according to pre-configured parameters pertaining to the investigation**

Features of selective imaging (1)

- **Flexibility**
- **Classifying / grouping information**
  - Extension
  - Signature
  - Hash
  - Time
  - Categories – Documents, Pictures, System Files, Configuration Files, Log Files, Encrypted Files, Email Files,

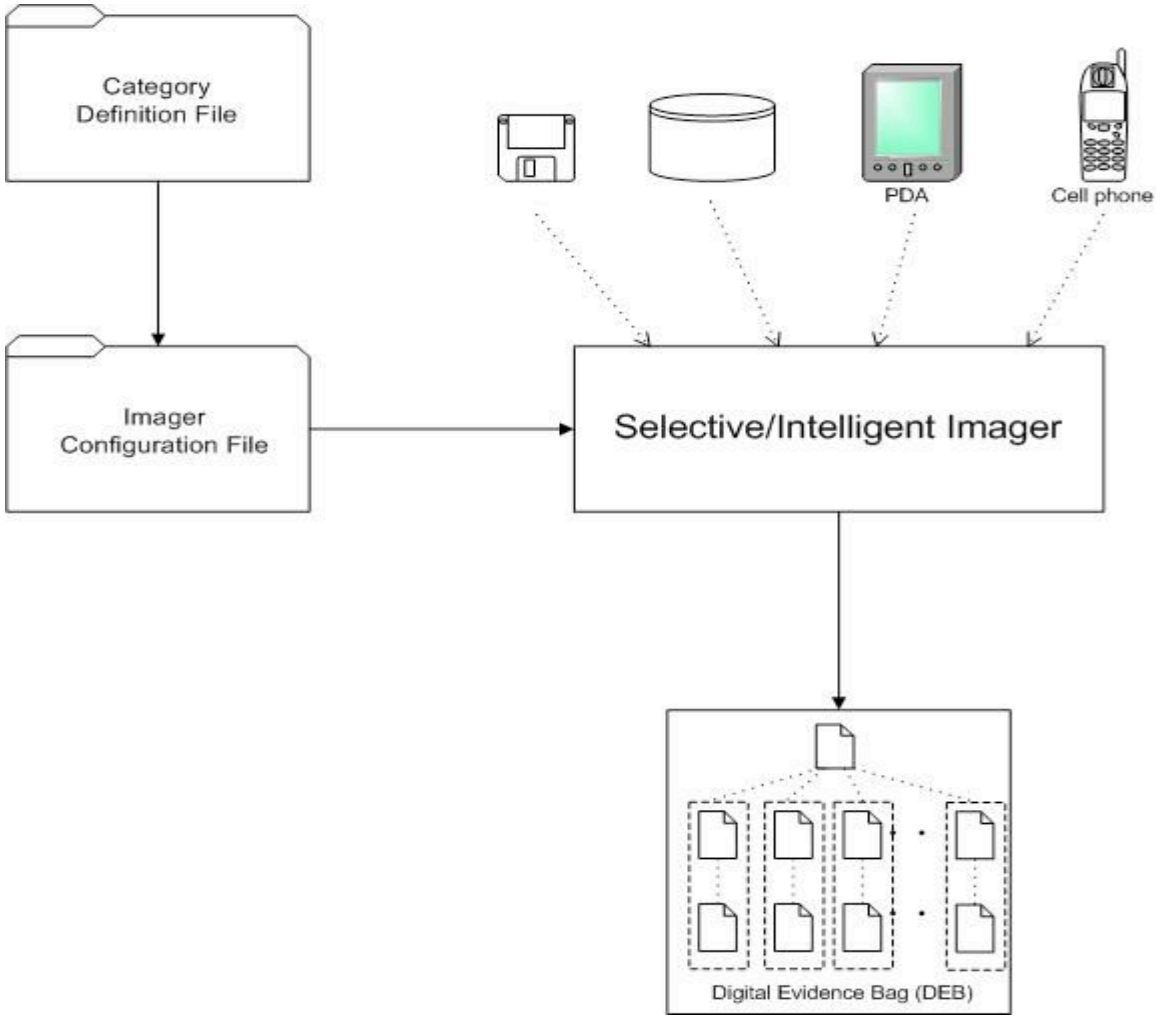
Features of selective imaging (2)

- **Provenance**
  - Unique
  - Unambiguous
  - Concise
  - Repeatable
- **Potentially very complex**

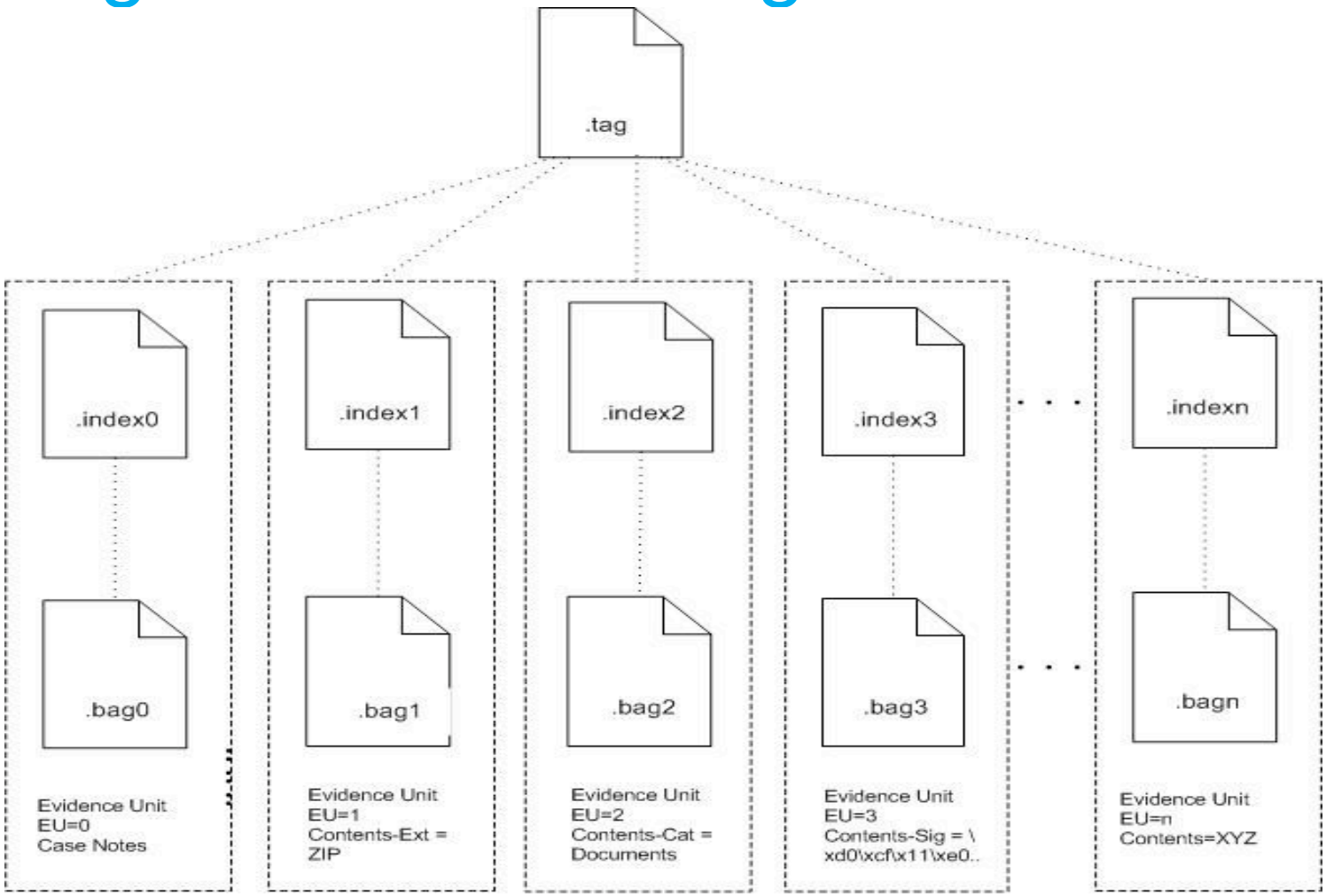
Intelligent Imaging – The next generation

- **Capture the knowledge and experience of domain experts into an intelligent system based on Investigation Types**
- **You have to be able to do selective acquisition first!**
- **How do you know you have captured everything?**

Selective / Intelligent Imager

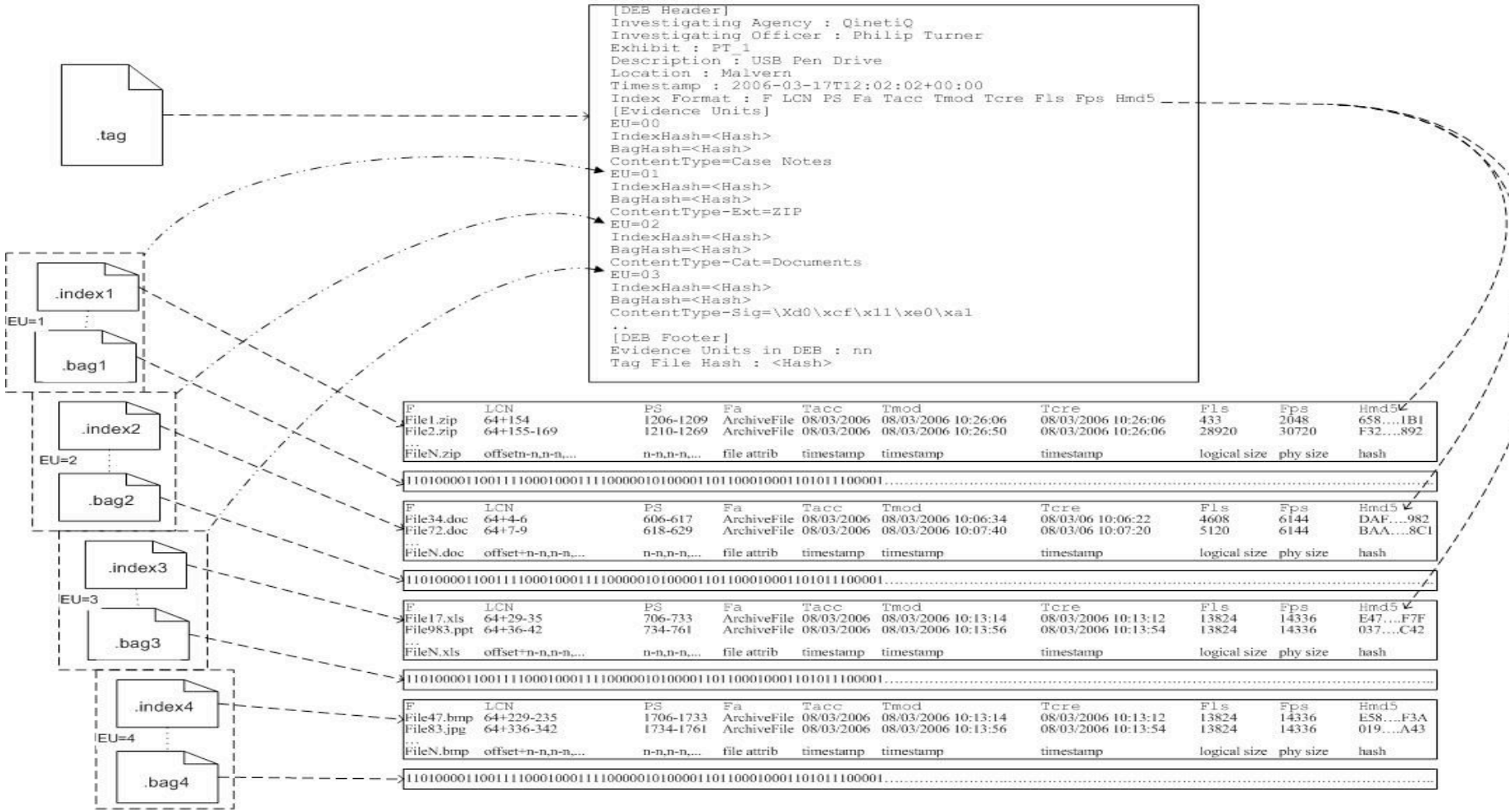


Digital Evidence Bag structure



Digital Evidence Bag (DEB)

DEB contents



Selective/ Intelligent Imaging

- **Testing – the ‘Ultimate’ test**
- **Comprehensive Imaging**
- **A ‘proportional’ approach to acquisition**

Summary

- **An alternative to bit stream imaging**
  - The ability to capture selected information in a forensically sound manner
  - The container is important – must be able to deal with multiple levels of provenential information
- **More acquisition options**
  - File extension
  - File signature
  - Hash
  - Categories – Pictures, Documents, Email…
- **Analysis flexibility**

Questions ???

Philip Turner
Investigations & Security Health Check
QinetiQ, Malvern, UK.
pbturner@qinetiq.com