Selective and Intelligent Imaging Using Digital Evidence Bags

By

Philip Turner

Presented At

The Digital Forensic Research Conference

DFRWS 2006 USA Lafayette, IN (Aug 14th - 16th)

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,

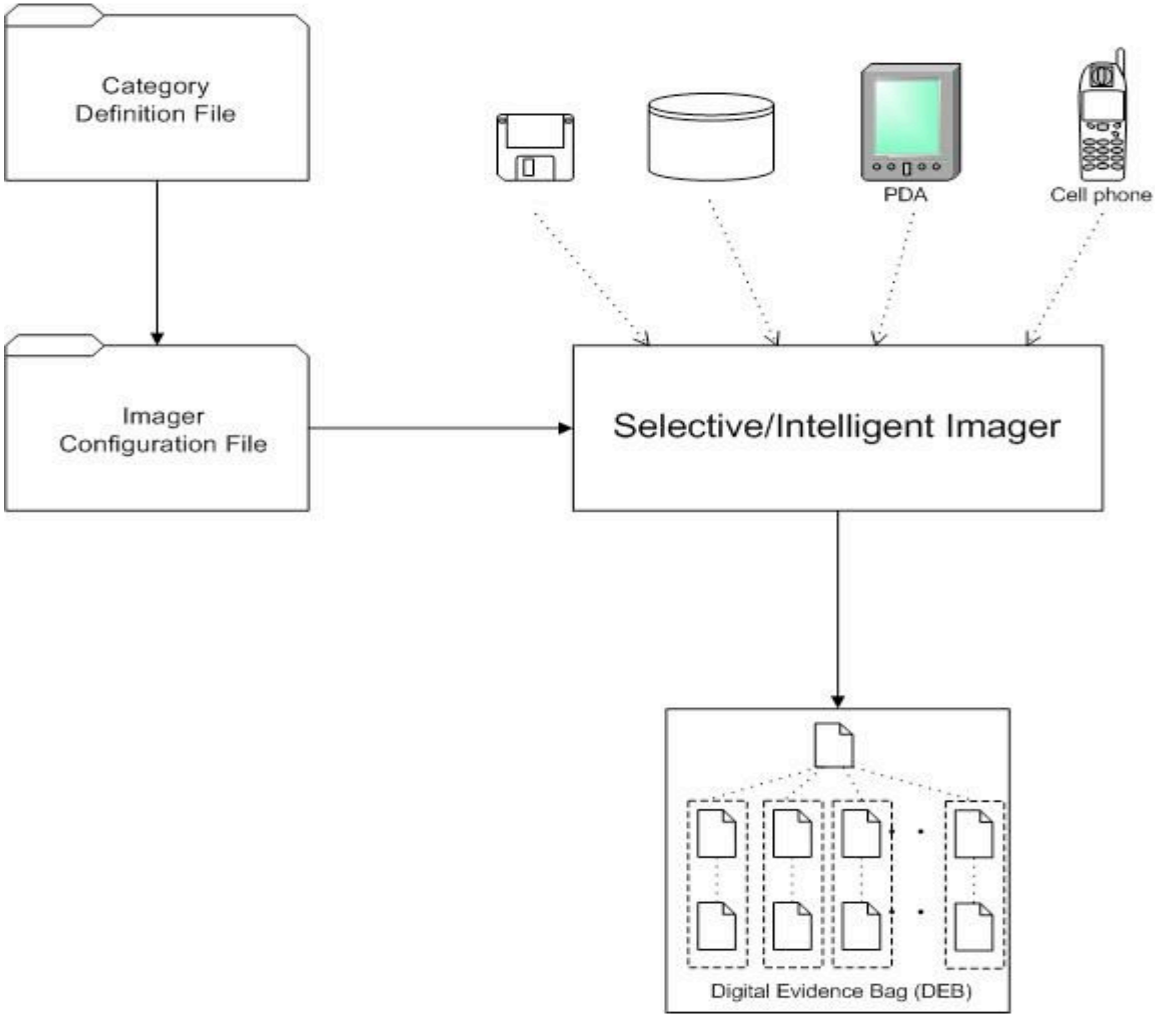
Features of selective imaging (2)

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

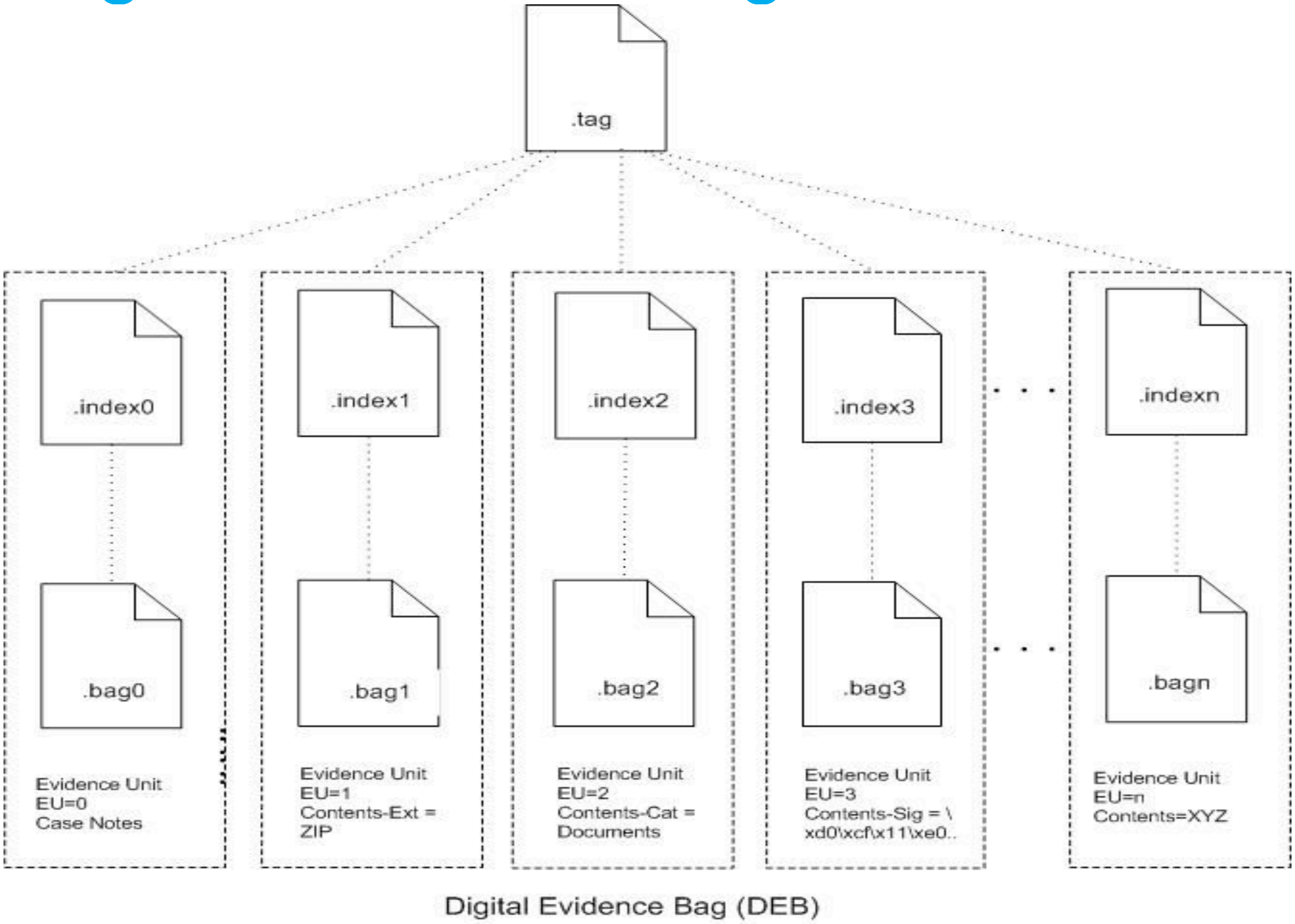
Intelligent Imaging – The next generation

- 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?

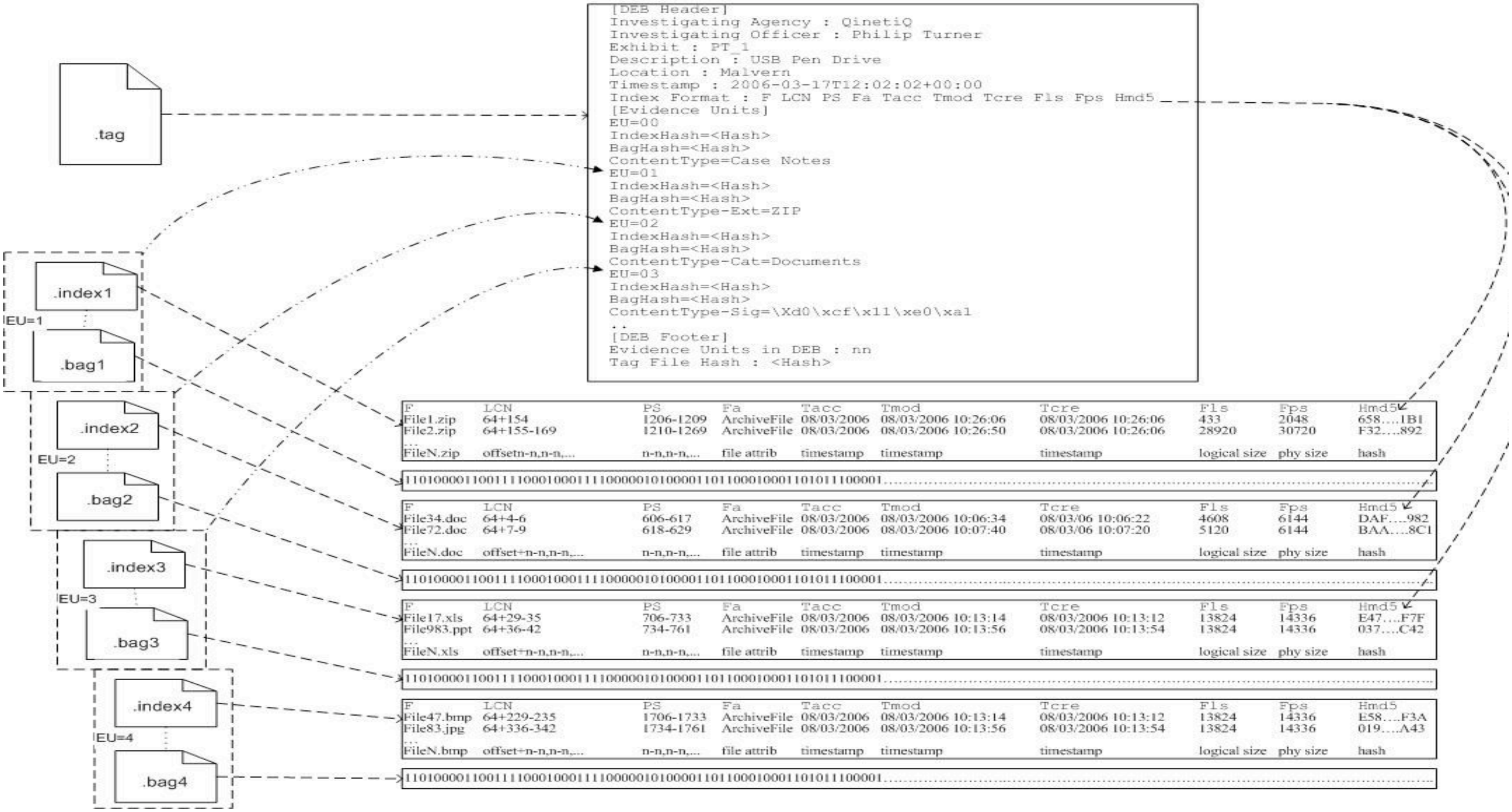
Selective / Intelligent Imager


Category Definition File
PDA
Cell phone
Imager Configuration File
Selective/Intelligent Imager
Digital Evidence Bag (DEB)

Digital Evidence Bag structure



DEB contents



```
[DEB Header]
Investigating Agency : QinetiQ
Investigating Officer : Philip Turner
Exhibit : PT_1
Description : USB Pen Drive
Location : Malvern
Timestamp : 2006-03-17T12:02:02+00:00
Index Format : F LCN PS Fa Tacc Tmod Tcre Fls Fps Hmd5
[Evidence Units]
EU=00
IndexHash=<Hash>
BagHash=<Hash>
ContentType=Case Notes
EU=01
IndexHash=<Hash>
BagHash=<Hash>
ContentType-Ext=ZIP
EU=02
IndexHash=<Hash>
BagHash=<Hash>
ContentType-Cat=Documents
EU=03
IndexHash=<Hash>
BagHash=<Hash>
ContentType-Sig=\Xd0\xcf\x11\xe0\xa1
..
[DEB Footer]
Evidence Units in DEB : nn
Tag File Hash : <Hash>
```

F	LCN	PS	Fa	Tacc	Tmod	Tcre	Fls	Fps	Hmd5
File1.zip	64+154	1206-1209	ArchiveFile	08/03/2006	08/03/2006 10:26:06	08/03/2006 10:26:06	433	2048	658….1B1
File2.zip	64+155-169	1210-1269	ArchiveFile	08/03/2006	08/03/2006 10:26:50	08/03/2006 10:26:06	28920	30720	F32….892
…									
FileN.zip	offsetn-n,n-n,…	n-n,n-n,…	file attrib	timestamp	timestamp	timestamp	logical size	phy size	hash

```
110100001100111100010001111000001010000110110001000110101110000 1……
```

F	LCN	PS	Fa	Tacc	Tmod	Tcre	Fls	Fps	Hmd5
File34.doc	64+4-6	606-617	ArchiveFile	08/03/2006	08/03/2006 10:06:34	08/03/06 10:06:22	4608	6144	DAF….982
File72.doc	64+7-9	618-629	ArchiveFile	08/03/2006	08/03/2006 10:07:40	08/03/06 10:07:20	5120	6144	BAA….8C1
…									
FileN.doc	offset+n-n,n-n,…	n-n,n-n,…	file attrib	timestamp	timestamp	timestamp	logical size	phy size	hash

```
1101000011001111000100011110000010100001101100010001101011100001……
```

F	LCN	PS	Fa	Tacc	Tmod	Tcre	Fls	Fps	Hmd5
File17.xls	64+29-35	706-733	ArchiveFile	08/03/2006	08/03/2006 10:13:14	08/03/2006 10:13:12	13824	14336	E47….F7F
File983.ppt	64+36-42	734-761	ArchiveFile	08/03/2006	08/03/2006 10:13:56	08/03/2006 10:13:54	13824	14336	037….C42
…									
FileN.xls	offset+n-n,n-n,…	n-n,n-n,…	file attrib	timestamp	timestamp	timestamp	logical size	phy size	hash

```
1101000011001111000100011110000010100001101100010001101011100001……
```

F	LCN	PS	Fa	Tacc	Tmod	Tcre	Fls	Fps	Hmd5
File47.bmp	64+229-235	1706-1733	ArchiveFile	08/03/2006	08/03/2006 10:13:14	08/03/2006 10:13:12	13824	14336	E58….F3A
File83.jpg	64+336-342	1734-1761	ArchiveFile	08/03/2006	08/03/2006 10:13:56	08/03/2006 10:13:54	13824	14336	019….A43
…									
FileN.bmp	offset+n-n,n-n,…	n-n,n-n,…	file attrib	timestamp	timestamp	timestamp	logical size	phy size	hash

```
1101000011001111000100011110000010100001101100010001101011100001……
```

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