
QinetiQ

Unification of Digital Evidence from Disparate Sources

Philip Turner
Digital Investigation Services
QinetiQ, Malvern, UK.
pbturner@qinetiq.com

Digital Forensics … The Problems !

- **Quantity of data**
- **Increasing range of digital devices**
- **Proprietary capture formats/tools for different devices**
- **Entire image has to be available to analysis tool**
- **No real-time support for evidence capture**
- **No multi-processor / distributed system support**

Traditional Evidence Capture

- **Bags**
  - Store items that are considered relevant at time of capture
  - Not everything is captured
- **Tags**
  - Exhibit Reference / Description / Date & Time seized / Name of investigator
  - Continuity – evidence custody transfer
  - Provenance
- **Seals**
  - Tamper detection / prevention

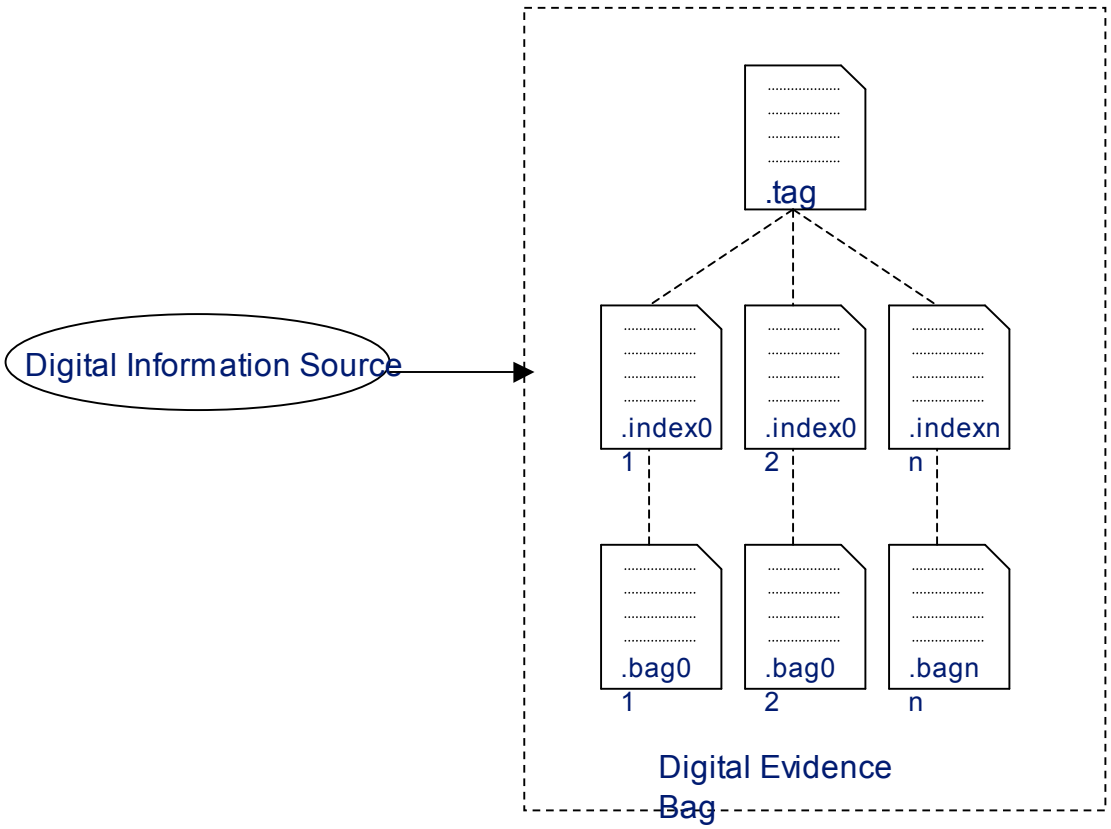
Digital Evidence Capture

- **Capture Everything …. Regardless**
- **Plain ‘dd’ image**
  - No integrity checking
  - No provenance / continuity information
- **Proprietary formats**
  - Limited integrity checking
  - No interoperability between tools
  - Limited provenance information
  - No in-built continuity tracking

Digital Evidence Bags (DEBs) - Aims

- **To provide a simple to use and understandable structure**
- **To provide a flexible structure that is capable of storing information from a disparate range of digital devices**
- **Scaleable and able to hold an ever increasing amount of information**
- **Provide in-built continuity / provenential information**
- **Capable of storing information from static and real-time environments**

DEB Structure (1)



DEB Structure (2)

- **Tag file – plain text**
  - DEB reference identifier
  - Details of information contained in the DEB
  - Name and organisation of person capturing information
  - Date and Time
  - Evidence Unit (EU)
  - Tag Continuity Block (TCB)
  - Index file format definition – meta tags

DEB Structure (3)

- **Index file – text based tab delimited**
  - Details the contents of the corresponding bag
  - Exact format varies depending upon content type of EU
  - May contain details such as filenames, file sizes, timestamp information, make model and S/N of devices
- **Bag file – the information that may be used as evidence**

DEBs – How they work (1)

- **DEB access**
  - Update tag file
    - New TCB appended to tag file – includes application identifier, application description / function, application version information, application hash, EU accessed, processing host identifier
    - New tag seal number calculated

DEBs – How they work (2)

- **Evidence Unit contents**
  - Full bit image data – capture everything regardless
  - Imaging Options – Partial / Selective / Intelligent
    - Real-Time evidence acquisition
    - Time constrained evidence acquisition
    - Particular type of information
    - Customer driven
    - Investigation focussed
    - Forensic triage
    - Covert

DEBs – How they work (3)

- **Evidence Unit processing**
  - Multi-processor / distributed capable
  - Audit trail of DEB access
  - Audit trail of DEB/EU processing tasks

DEBs – Enhancing Best Practice

- **Replicating what is done in the Traditional evidence capture environment in the Digital environment**
- **Audit trail**
  - Learning the successful AND unsuccessful way of performing investigations / finding case relevant information
  - Education

DEB Implementations

- **DEB Viewer**
  - View contents of a DEB
  - Update tag - TCB
- **DEB Application Wrapper**
  - Command line application wrapper
- **Selective imager / data capture**
- **Full media imager**

DEB Benefits

- **Scaleable approach to evidence acquisition**
- **Scaleable approach to forensic processing, allowing for the first time the digital evidence to be processed across multi-processor and distributed systems**
- **Increased evidential material throughput, directing the most applicable techniques at the appropriate types of evidence**
- **Incorporate some of the current evidence capture and analysis methods thus not negating the financial investment in current tools and methods**
- **The ability to process evidence from a diverse range of digital devices**
- **Allow the integration of real-time data acquisition into a sound forensic framework**
- **Permit a selective and/or intelligent data acquisition approach to be implemented as opposed to the current collect everything approach**
- **The ability to automatically create an audit trail of processes carried out on an item of evidence. The metric from which could allow analysis of the most effective way to process digital evidence and be used to educate new practitioners in the best way to undertake a forensic investigation**

Questions ?