



DFRWS 2004 Observations

**Maciag-Palmer
DFRWS 2004
Linthicum, MD**

Day 1 – Framework for Digital Forensic Science: General Observations

- **We are encouraged that many different groups have been exploring framework models**
 - **There seem to be common features and functions**
 - **Flexibility in process, similar capabilities/phases**
 - **We've seen some good examples of proposed technologies that will support sub-phases or functions in the frameworks**
 - **These will help to concretize research goals by creating well-articulated gaps**
- **Perhaps a guideline for what features frameworks should possess should be our goal, rather than any one particular framework (e.g. CMM)**
 - **Suggest using a framework as a meta-standard for describing what features you should have in your standard (ISO 900x, ISO 17790, etc.)**
 - **Perhaps an RFC process would help us get there from here.**
- **Much of Digital Forensic Investigation lies inside of structure, but may be flexible with respect to process iteration**

Day 1 – Framework for Digital Forensic Science: General Observations

- **However, putting the theory of a framework into practice is still an open issue**
 - **Developing measures of merit for a given framework is a hard problem. So is, validating the framework itself.**
 - **“Try-before-you-buy” is also a difficult thing to do organizationally, as the framework usually drives the organization’s business model**

Day 2 – In-time Forensics: General Observations

- **Challenges to In-time Assessments**
 - **Operations on information take place in an uncontrolled environment**
 - **Difficult to ‘See the elephant’ for what it is.**
 - **Don’t know if all relevant information has been captured pertaining to an investigation or assessment.**
 - **Alternate representations of the ‘ground truth’ need to be sought**
 - **A priori preparation phase is required prior to the complaint**
 - **Dynamic, distributed environments present new challenges for taking system ‘snapshots’**
 - **Capturing the entire environment**
 - **Capturing system state changes during the snapshot process**
 - **Retaining even LARGER amounts of data**
 - **Controlling evidence that is collected**

Day 2 – In-time Forensics: General Observations

- **There doesn't appear to be a paradigm shift in how digital evidence is collected and evaluated compared with what happens now. This applies to:**
 - **Framework**
 - **In-Time**
 - **It's seems a matter of techniques and iteration**

- **Opportunities to leverage, align and integrate digital forensics with intrusion analysis seem promising:**
 - **Indications and Warnings – forensic observables**
 - **HoneyPots/Nets/Wells – opportunities to clearly understand adversarial techniques, with some measurable certainty, so they can be identified and thwarted earlier is a forensic activity.**

- **Research marches on:**
 - **Secure IDS**
 - **Secure Digital Camera**
- **Practitioners are very interested in Quality from different perspectives:**
 - **Triage – quick, accurate early look**
 - **Testing procedure improvements**
 - **Reusing, Sharing information for across forensic domains / communities**
- **“There is certainly more that frameworks to deal with”**

- **Look for :**
 - **Contents posted by the end of next week**
 - **Forums and list servers open for dialog**
 - We will seed some forums with general observations from workgroups
 - Same for the list server DFSci
 - Subscribe on www.dfrws.org
 - **The Report – Mid Sept 04 - draft**
 - **Our job:**
 - Create outline
 - Initial draft
 - **Need your help**
 - Reviewing sections and commenting via forums and list servers

- **Mini-Workshop**
 - **[Jan/Feb?] Live/Remote forensic analysis**
 - **Other suggested topics for a March/April date?**
 - **Suggested format/duration?**
 - **Locations (logistics, draw, relevant attendees availability)**



**Thank you for your time and
efforts in advancing this year's
topic areas!**

**Be sure to use your feedback form for ideas for improvement
and adjustment**

DFRWS Staff