Digitial Forensics XML

SSTIC 2011

Christophe Grenier - grenier@cgsecurity.org

Prior work
Digital Evidence Containers

- raw format/dd format : no metadata
- Expert Witness Format (EWF) aka .E01 : no extensibility
- Digital Evidence Bags" (DEB), Turner, 2005 : no user
- Advanced Forensic Format (AFF), Garfinkel, 2006
- AFF4, Cohen, Garfinkel, and Schatz, 2009 : better than AFF, use a flat RDF schema to store meta-data : storage oriented

Prior work
Windows registry

Windows registry hive files

- Howell, 2009

Unallocated space inside the hive

- Thomassen, 2008;
- Tang, Ding, Xu, and Xu, 2009

No tool currently processes the recorded meta-data

Prior work
File System Metadata Standards

- The Coroner’s Toolkit (Farmer and Venema, 2005) : fields are separated by « | »

  Reused in SleuthKit 2.0
- SleuthKit 3.0 : 11 fields instead of 16, applications reading the output need to be updated
- Electronic Discovery Reference Model (EDRM)

  XML (Socha, 2011) : impossible to describe the location of a file

Prior work
XMLs for Digital Forensics

- XIRAF, an XML Information Retrieval Approach to digital forensics : no tool uses this format
- DEX, Digital Evidence Exchange (Levine and Liberatore, 2009) : a single tool in JAVA uses this format

DFXML

A solution from

Simson Garfinkel - simsong@acm.org

Digital Forensics XML is easy to implement :

- No library needed
- Code available in C, C++, Python

Carvers using DFXML

- Scalpel, Golden Richard
- frag_find, part of afflib, Simson Garfinkel
- PhotoRec, Christophe Grenier

Other tools producing DFXML

- ewfinfo, part of libewf, Joachim Metz

  Can output metadata for EWF disk images in DFXML format.

- md5deep, sha1deep, hashdeep part of md5deep 4 (currently under development), Jesse Kornblum.