PB138 — Markups for Cybersecurity

Cybersecurity

NIST Framework

- This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

Markup

XACML: eXtensible Access Control Markup Language

- XACML: eXtensible Access Control Markup Language

Digital forensic

- Digital Forensics XML
- (DFXML) is an XML language used to automate digital forensics processing. DFXML contains information about both the results of forensic processing and the tools used to perform the processing (provenance). Currently there is no Digital Forensics XML standard and there is no fixed schema. There is a draft schema available from NIST.

DFXML

- **DFXML** is a file format designed to capture metadata and provenance information about the operation of software tools in a systematic fashion. The original motivation was to represent the output of digital forensics tools, and specifically the SleuthKit tools. DFXML was expanded to operate with the bulk_extractor digital forensics tool. DFXML was then expanded to cover the output of the tcpflow tool.

Data Carving

- **Data carving**, also known as file carving, is the forensic technique of reassembling files from raw data fragments when no filesystem metadata is available. It is a common procedure when performing data recovery, after a storage device failure, for instance.
- **File carving** is a well known computer forensics term used to describe the identification and extraction of file types from unallocated clusters using file signatures. A file signature, also commonly referred to as a magic number, is a constant numerical or text value used to identify a file format. The object of carving is to identify and extract (carve) the file based on this

signature information alone.

Data Carving Log ML

```
<?xml version="1.0" encoding='UTF-8' ?>
<photorec xmloutputversion="0.3">
<metadata
  xmlns="http://example.org/myapp/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dc="http://purl.org/dc/elements/1.1/">
  <dc:type>Carved Files from Disk Image</dc:type>
  <dc:publisher>CGSecurity.org</dc:publisher>
</metadata>
<!-- Fri Jan 20 11:40:53 2006 -->
<creator>
    <program>photorec</program>
    <version>6.9-WIP</version>
  <build_environment>
      <compiler>GCC 4.4</compiler>
      <compilation_date>Nov 22 2009 13:39:05</compilation_date>
      <library name="ext2fs" version="1.39" />
      <library name="ntfs" version="10:0:0" />
      <library name="ewf" version="20070512" />
      <library name="jpeg"/>
    </build_environment>
    <run_environment>
      <uid>0</uid>
      <username>root</username>
      <working_dir>/User/home/root</working_dir>
      <command_line>photorec image.dd</command_line>
      <os>Linux 2.6.30.9-96.fc11.x86_64 (#1 SMP Wed Nov 4 00:02:04 EST 2009)</os>
      <arch>i386</arch>
    </run_environment>
</creator>
<source>
   <image_filename>/dev/sda</image_filename>
   <sector_size>512</sector_size>
   <device_sectors>251658240</device_sectors>
   <first_sector>0</first_sector>
   <last_sector>251658240</last_sector>
   <device_model>COMPAQ BD009122C6 B016</device_model>
   <device_sn>B3203332    0004</device_sn>
   <acquisition_date>2006-12-01 16:05:47</acquisition_date> <!--GMT-->
</source>
<commands>
  <carve filesystem="ext3" freespaceonly="true" blocksize="1024" />
  <partition type='intel' offset='32256' len='128848986624' />  <!-- in bytes -->
</commands>
<results>
```

```
  <fileobject>
    <filename>recup_dir.3/f7386.ppt</filename>
    <familly>doc</familly>
    <filesize>17408</filesize>
    <digesthash type="md5">id1ad0bf040079b5c8f4b1806b90b2f83</digesthash>
    <byte_runs>
      <run file_offset='0' img_offset='3781632' len='11776'/>
      <run file_offset='11776' img_offset='3793920' len='512' data='false'/>
      <run file_offset='12288' img_offset='3794432' len='4608'/>
    </byte_runs>
  </fileobject>
  <fileobject>
    <filename>DCIM/100CANON/IMG_0016.JPG</filename>
    <filesize>853839</filesize>
    <byte_runs>
      <run file_offset='0' fs_offset='12687872' img_offset='12713984' len='853839'/>
    </byte_runs>
    <digesthash type="md5">dd3852ec13dd160ca134551d68ed2b8d</digesthash>
    <digesthash type="sha1">aa2b9eb89628485e51b5de57edad2487b648e574</digesthash>
  </fileobject>
</results>
<runstats>
  <clock_seconds>15.5</clock_seconds>
  <user_seconds>10.5</user_seconds>
  <system_seconds>0.3</system_seconds>
  <maxrss>1413120</maxrss>
  <reclaims>448</reclaims>
  <pagefaults>0</pagefaults>
  <swaps>0</swaps>
  <inputs>0</inputs>
  <outputs>0</outputs>
  <stop_time>2009-12-19 19:58:16</stop_time> <!--GMT-->
</runstats>
</photorec>
```