Rapid Evidence Acquisition Project for Event Reconstruction (REAPER)

Joshua James
Centre for Cybercrime Investigation
University College Dublin
The Goal of REAPER

• To reduce digital crime at the global level
• How: by allowing digital investigators to conduct quality investigations regardless of training or budget
Focus

- Usability
- Automation
- Cost Reduction
History of REAPER

• Started in 2008
• Focused on low cost, highly automatic digital forensic investigations primarily for developing countries
• REAPERlive
  – Specifically for offline automatic media acquisition, processing and analysis
  – Automatic documentation and case management
  – Runs from a bootable external hard drive on suspect system
  – No user input required after boot
Media Acquisition

Verification of collected images

Image acquisition using DD
Sample Technical Log

I: Case Data file Case-2138360924.data created
Wed Jun 17 06:36:30 UTC 2009
I: Using '/media/REAPERsys' looks good for case
I: REAPER_image script started at:
Wed Jun 17 06:36:30 UTC 2009
I: REAPER_image script - v0.1 - 12/5/2009
Wed Jun 17 06:36:30 UTC 2009
P: Hashing drive /dev/hda - SHA256...
I: SHA256 Hash of /dev/hda is:
  e1034911f407badafe413645a0fd694e28768fa17ef92
I: SHA256 Hash of /images/hda-2138360924.dd is:
  e1034911f407badafe413645a0fd694e28768fa17ef92
Drive hash:
  e1034911f407badafe413645a0fd694e28768fa17ef92
File hash

REAPERlive logging started at:
Wed Jun 17 06:36:30 UTC 2009
REAPERControl Script - v0.3 - 25/5/2009
REAPER_detectDrive Script - v0.3 - 17/6/2009
REAPER_setENV Script - v0.2 - 17/5/2009

I: Manually set REAPER drive serial numbers:
I: REAPERsys drive serial: 6RYBXMPA
I: REAPERevi drive serial: 6RYBXDXF
I: REAPER drives detected and mounted...
/dev/sda2 on /media/REAPERsys type ext3 (rw)
/dev/sdb2 on /media/REAPERevi type xfs (rw)
/proc on /media/REAPERsys proc type none (rw,bind)
    none on /media/REAPERsys/proc type devpts (rw)
    /tmp on /media/REAPERsys/tmp type none (rw,bind)
/media/REAPERevi on /media/REAPERsys/evidence type none (rw,bind)
/dev on /media/REAPERsys/dev type none (rw,bind)
    proc on /media/REAPERsys/proc type none (rw,bind)
    none on /media/REAPERsys/dev/pts type devpts (rw)
    /tmp on /media/REAPERsys/tmp type none (rw,bind)
/media/REAPERevi on /media/REAPERsys/evidence type none (rw,bind)

I: Detected suspect drives are:

Disk /dev/hda: 4295 MB, 4295467008 bytes
255 heads, 63 sectors/track, 522 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00010001

<table>
<thead>
<tr>
<th>Device</th>
<th>Boot</th>
<th>Start</th>
<th>End</th>
<th>Blocks</th>
<th>Id</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hda</td>
<td>*</td>
<td>1</td>
<td>521</td>
<td>4184901</td>
<td>7</td>
<td>HPFS/NTFS</td>
</tr>
</tbody>
</table>

--------------------------------------------------------------------------
Evidence Processing

Collected evidence automatically sent to OCFA for processing
(can be started or restarted later)

column "rowsha1.id"
NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "suspendedmeta_pk" for table "suspendedmeta"

CREATE TABLE
CREATE TABLE
CREATE TABLE
CREATE TABLE
CREATE TABLE
CREATE TABLE
CREATE TABLE

Please restart apache for all changes to take effect
I: Starting OCFA case monitor
I: Creating symlink to case conf file in OCFAROOT/etc
ln: creating symbolic link `/usr/local/digiwash/etc/CASE-2138360924.conf’: File exists
P: Processing hda-1346800195.dd...
I: The Source does not appear to match the current computer
I: File id 1346800195 is not equal to session id 2138360924
P: Processing hda-2138360924.dd...
I: Image source looks valid - 2138360924
I: Submitting evidence to OCFA in case Case-2138360924
OCFA
Open Computer Forensics Architecture

• Written by the Dutch National Police Agency

• Processes evidence
  – Disk images or single files
  – Extracts metadata
  – Indexes data
  – Compiles searchable database

• Modular
  – New modules can be written to parse new and different types of data

http://OCFA.sourceforge.net
Media Analysis

- OCFA provides a simple web-based browser and keyword search
Media Analysis

• REAPERview
  – an Automatic Event Reconstruction (AER) project
  – Automatically associates sets of data with user activities
  – Quickly gathers data from various sources to verify findings
  – Gives an overall picture of what a user was doing on the machine
  – Experimental - Still in first stages of development
• REAPERlive Desktop
  - Secure forensic desktop for evidence analysis, reporting and setup of REAPER components
  - Downloaded as ISO or USB image
  - If user already has Debian or Ubuntu, able to download the makeREAPERliveDesktop script
    ▪ Customizable – investigator can add custom tools

http://REAPER.CybercrimeTech.com
Automatically Set up REAPER drives
Setup REAPER Drives

Investigator selects what drives to install REAPER on

Pre-REAPER partition example
Setup REAPER Drives

The remaining processes require no user intervention.
REAPERlive

• Useful for having a non-expert acquire, document and pre-process media
• Still needs expert for analysis
• Useful for eDiscovery
REAPER Preview

• Written with customs officers in mind

• REAPERlive Preview
  – Fast and Simplistic Preview
    • Pictures
    • Movies
    • Documents

• From boot to preview in 3 minutes or less
REAPER Preview

Preview case type profiles

Rapid Evidence Acquisition Project (REAPER)

Please select the type of case:

- General Triage
- Exploitation

Information (Log)

Autoscan Results

Search for Keywords

General Scan:
- Keyword Hits: 0
- Hash Hits: 36
- Images: 15
- Video: 0
- Music: 0
- Documents: 294

Information (Log)

Rapid Evidence Acquisition Project (REAPER)

Back to profile choice

Gallery view

Page 1
Update Preview Page

-------------------items that could not be processed-------------------
ANT
Automated Network Triage

• Developed by Martin Koopmans of the Netherlands Police (Hollands-Midden)

• “A process of sorting computer systems into groups, based on the amount of relevant information or evidence found on these computer systems”

• Client-server based triage using gPXE
ANT

Automated Network Triage

Linux server

switch

DHCP
TFTP (to serve the rootfs)
SSH to (connect to clients)
File serving e.g. hashsets

Keyword matches
Hash-matches
Aoe (serve the disk)

PXE client

PXE client

PXE client

PXE client
REAPER: Observations

• Digital forensic investigations are not only a technical problem
• Difference in the investigation needs of developed and developing countries
• Difference in the investigation needs at national and divisional levels
• How to investigate differs based on case
REAPER Tools

Management
- Needs
- Processes
- Structure

Technology
- Support Management
- Support Investigators
- Well Integrated

Knowledge
- Training
- Decision Matrix
- Law
• REAPER currently being developed to include:
  – Architecture for conducting an organizational needs analysis and process abstraction
  – Open digital forensic investigation and related training.
  – Expert level decision tree to assist non-experts
  – Open ‘framework’ type tools that allow an organization to automate their identified technology-related needs in a software independent manner
Case Study

• Currently evaluating a three-tier investigation process
  – On scene
  – Local Station
  – Forensics Laboratory

• Needs:
  – Expert level knowledge
  – Non-expert level knowledge
For any questions or comments please email: Joshua@CybercrimeTech.com

http://CybercrimeTech.com