

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



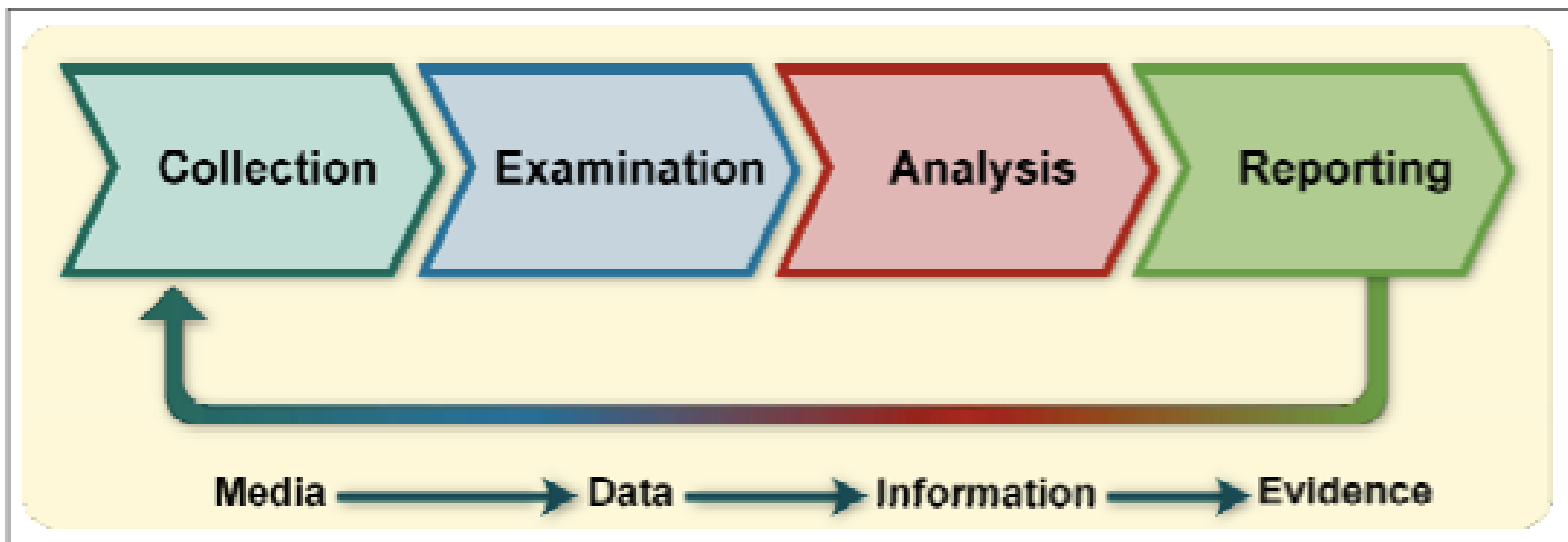
Focus

- Usability
- Automation
- Cost Reduction



History of REAPER

- Started in 2008
- Focused on low cost, highly automatic digital forensic investigations primarily for developing countries





REAPERlive

- 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

```
I: REAPER system drive detected - /dev/sda
P: Mounting REAPER system drive - /dev/sda2
I: Mount successful
I: REAPER evidence drive detected - /dev/sdb
P: Mounting REAPER evidence drive - /dev/sdb2
I: Mount successful
P: Activating swap space at /dev/sdb1
Setting up swap space version 1, size = 1028120 kB
no label, UUID=eceaa81a-40bc-423a-9cd6-e8a6c686c1a4
I: REAPERSys mounted OK
I: REAPERevi mounted OK
P: Setting up environment...
I: Logging directory found
P: Creating log file /logs/Case-3974860963/Case-3974860963.log
I: '/media/REAPERSys' looks good for chroot.
P: Starting the imaging process...
P: Hashing drive /dev/hda - SHA256...
```

```
real    4m8.763s
user    0m36.830s
sys     0m40.095s
I: SHA256 Hash of /dev/hda is:
e1034911f407badafe413645a0fd694e28768fa17ef925b538af0ab3eaf78eb2
P: Imaging /dev/hda to /images/hda-3974860963.dd... (this may take a while)
[13% of 4096Mb] 18176 blocks (568Mb) written. 00:03:06 remaining.
```

Image acquisition using DD

Verification of collected images

```
no label, UUID=eceaa81a-40bc-423a-9cd6-e8a6c686c1a4
I: REAPERSys mounted OK
I: REAPERevi mounted OK
P: Setting up environment...
I: Logging directory found
P: Creating log file /logs/Case-3974860963/Case-3974860963.log
I: '/media/REAPERSys' looks good for chroot.
P: Starting the imaging process...
P: Hashing drive /dev/hda - SHA256...

real    4m8.763s
user    0m36.830s
sys     0m40.095s
I: SHA256 Hash of /dev/hda is:
e1034911f407badafe413645a0fd694e28768fa17ef925b538af0ab3eaf78eb2
P: Imaging /dev/hda to /images/hda-3974860963.dd... (this may take a while)
[99% of 4096Mb] 131072 blocks (4096Mb) written. 00:00:00 remaining.
131087+1 records in
131087+1 records out

real    3m51.524s
user    0m0.592s
sys     0m18.133s
P: Confirming Hash...
```



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 ch
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
Wed Jun 17 06:38:23 UTC 2009
P: Imaging /dev/hda to /images/hda-2138360924.
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: 6RYBXWPA
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)
/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)
/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

Device Boot      Start      End  Blocks  Id System
/dev/hda1  *            1       521   4184901    7  HPFS/NTFS
<----->
```



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  
ey" for table "suspendedmeta"  
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



Open Computer Forensics Architecture

HOME INDEX Overview PPQ

| | |
|---------|--------|
| Case: | test |
| Source: | comp1 |
| Item: | thumb1 |

Evidence browser

test :: comp1 :: thumb1 :: [evidence/output/3_DOS_FAT16](#)

| | |
|--|-------------------------|
| | ROOTDIR |
| | UNALLOC |

Detailed meta information for evidence:

| Job | MetaName | MetaValue |
|-----------|-----------------------------|-----------------------------|
| sleuthkit | stime = 2009-04-22T11:42:27 | etime = 2009-04-22T11:46:48 |
| | accesstime | 2009-04-22T10:15:43:INVALID |
| | changetime | 2009-04-22T10:15:43:INVALID |
| | fsentity-type | reachablenode |
| | inodetype | dir |
| | modificationtime | 2009-04-22T10:15:43:INVALID |
| router | stime = 2009-04-22T11:47:52 | etime = 2009-04-22T11:47:52 |
| dsm | stime = 2009-04-22T11:47:52 | etime = 2009-04-22T11:47:52 |

Open Computer Forensics Architecture

2.0

Keyword Search

Keywords [\(Help\)](#)

Word Search

Submit Query

Searching for: lisp

Found: 5 hits

| nr | score | source | item | ref | metalink | nice | view |
|----|-----------|--------|--------|--|----------------------|----------------------|----------------------|
| 0 | 1 | comp1 | thumb1 | evidence/output/3_DOS_FAT16/ROOTDIR/Programming/lisp/earl/readme.txt | meta | view | nice |
| 1 | 0.239579 | comp1 | thumb1 | evidence/output/3_DOS_FAT16/ROOTDIR/Programming/lisp/earl/earl.lisp | meta | view | nice |
| 2 | 0.214286 | comp1 | thumb1 | evidence/output/3_DOS_FAT16/ROOTDIR/Programming/lisp/earl/slack.lisp | meta | view | nice |
| 3 | 0.214286 | comp1 | thumb1 | evidence/output/3_DOS_FAT16/ROOTDIR/Programming/lisp/earl/slack.lisp | meta | view | nice |
| 4 | 0.0231971 | comp1 | thumb1 | evidence/output/3_DOS_FAT16/UNALLOC/data.unaloc/output1 | meta | view | nice |



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



REAPERdesktop

- 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>



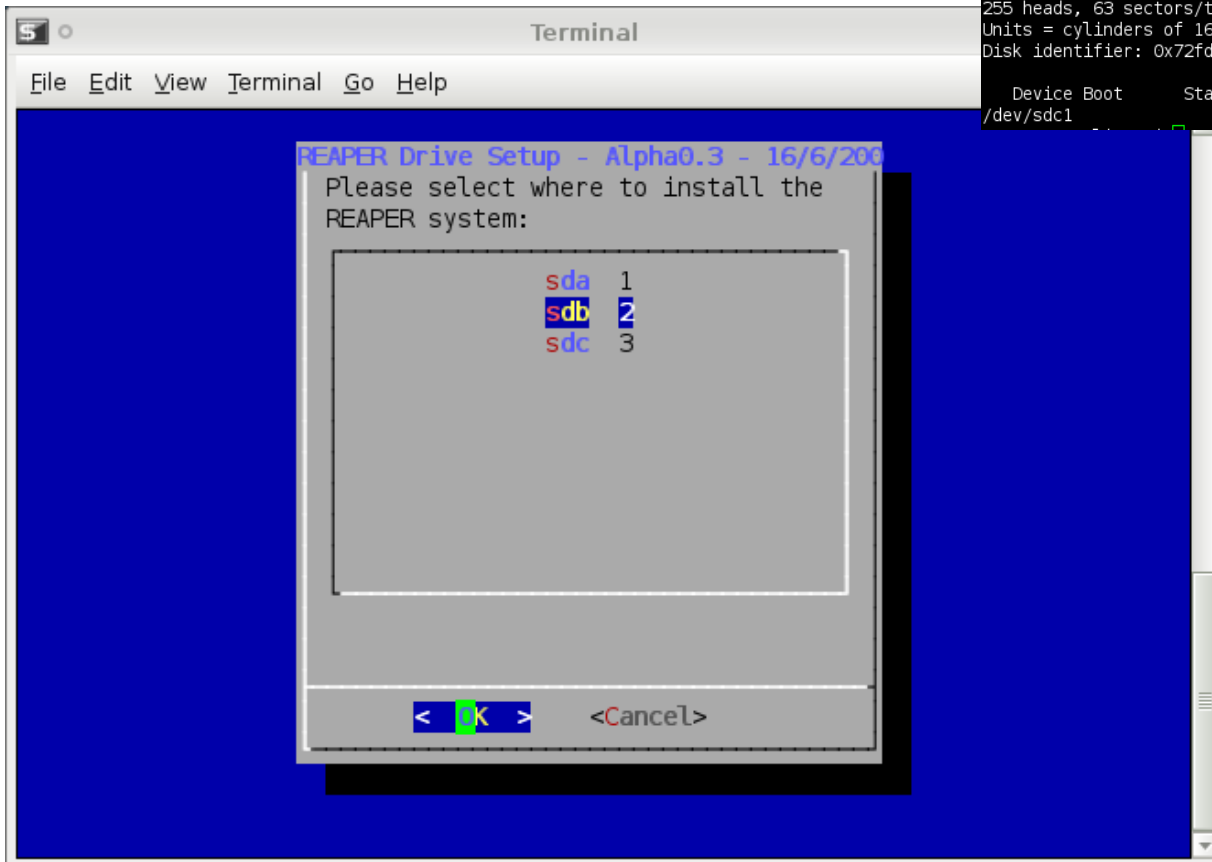
REAPERlive Desktop

The screenshot displays the REAPERlive Desktop environment. The desktop background is dark blue with a large REAPERlive logo in the center. A text box in the center of the desktop reads "Automatically Set up REAPER drives". The desktop contains several icons: "New Volume", "REAPERlive...", "Trash", "Home", and "File System". A terminal window is open in the top right corner, showing the command prompt "user@REAPERlive:~\$" and the command "scrot" being entered. The terminal window title is "Terminal - user@REAPERlive: ~". The system tray at the bottom shows the time "11:39" and several system icons.



Setup REAPER Drives

Investigator selects what drives to install REAPER on



```
Disk /dev/sdb: 250.0 GB, 250059350016 bytes
240 heads, 63 sectors/track, 32301 cylinders
Units = cylinders of 15120 * 512 = 7741440 bytes
Disk identifier: 0x00093736
```

| Device | Boot | Start | End | Blocks | Id | System |
|-----------|------|-------|-------|------------|----|-----------|
| /dev/sdb1 | | 1 | 32301 | 244195528+ | 7 | HPFS/NTFS |

```
Disk /dev/sdc: 250.0 GB, 250059350016 bytes
255 heads, 63 sectors/track, 30401 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x72fd2eaa
```

| Device | Boot | Start | End | Blocks | Id | System |
|-----------|------|-------|-------|-----------|----|-----------|
| /dev/sdc1 | | 1 | 30401 | 244196001 | 7 | HPFS/NTFS |

Pre-REAPER partition example



Setup REAPER Drives

```
Terminal
File Edit View Terminal Go Help

REAPER Drive Setup - Alpha0.3 - 16/6/2009
Creating swap and evidence partitions...
```

The remaining processes require no user intervention

```
Terminal
v Terminal Go Help

REAPER Drive Setup - Alpha0.3 - 16/6/2009
Building REAPERlive...
This will take a while. Please wait.
```



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](#)

Rapid Evidence Acquisition Project (REAPER)

[Back to profile choice](#)

[Search for Keywords](#)

General Scan:

[Keyword Hits](#) 0

[Hash Hits](#) 36

[Images](#) 15

[Video](#) 0

[Music](#) 0

[Documents](#) 294

[Information \(Log\)](#)



Page 1

[Update Preview Page](#)

.....Items that could not be processed.....

Gallery view



ANT

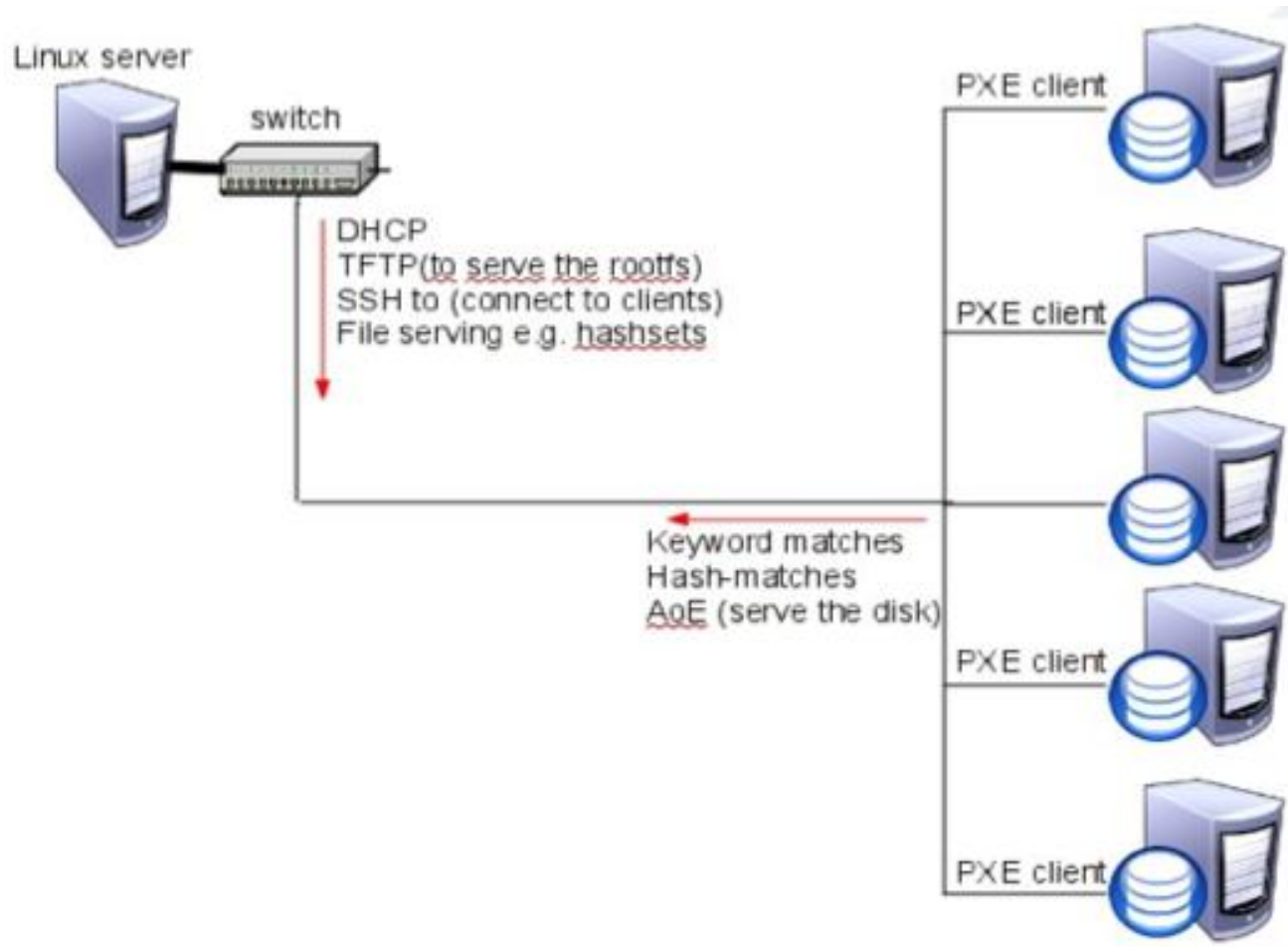
Automated Network Triage

- 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





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: Future

- 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>