Hands on Post Mortem Forensics Analysis in SUSE® Linux Enterprise Servers
Technical Tutorial
Session Length - 1 hour

Sandro Melo
Teacher in Bandtec College - Brazil
sandro.melo@bandtec.com.br
About me

Sandro Melo - aka CARIOCA - Currently I work at Bandtec College, and also with Advanced Training, Pentest, Response to Security Incidents and Computer Forensic and student/candidate in a Doctorate Program in TIDD/PUC-SP. I was born in the beautiful city of Rio de Janeiro, Brazil. I moved to Sao Paulo where I began my professional career in System Security. Since 1996 I have worked mainly with Linux/FreeBSD and FLOSS (Free/libre and Open Source Software), Network Administration and I am often a guest professor at quite a few universities all over Brazil. I’m a Suse Linux Engineer, LFSA and LPI Level 3 Security.

I take great pride in everything I do, especially with my work in Forensics. I have years of hands-on experience with many of the core technologies and have written many books and articles on security and forensics. When not working or writing, I can be found experimenting with the latest Open Source solutions, installing new versions of the same Operation Systems like Unix, such as Linux, FreeBSD or Mac OS X and also some FLOSS tools because I find it enjoyable. I truly have a deep passion for my work.

Email: sandro.melo@bandtec.com.br
Concept about Computer Forensic
Live Forensics

Memory Forensic

Post Mortem Forensic

Live Forensics

Network Forensic
Why Computer Forensic?
Why Computer Forensic

Because the Computer Forensic skills are not only important to help criminalistics, it is necessary to respond security incidents based on computers.

The Incident response is also a worry for the security of information in corporations nowadays.

There are security standards and norms that define the best practices of security for companies around the world, for instance:

PCI DSS
ISO/IEC 27002
ISO/IEC 27035
Managing incidents effectively involves detective and corrective controls designed to minimize adverse impacts, gather forensic evidence (where applicable) and ‘learn the lessons’ in terms of prompting improvements to the ISMS, especially the implementation of more effective preventive controls.
16.1 Management of information security incidents and improvements
There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.
ISO/IEC 27035

Content: the incident management process is described in five phases closely corresponding to the five phases in the first edition:

Plan and prepare: establish an information security incident management policy, form an Incident Response Team etc.
Detection and reporting: someone has to spot and report “events” that might be or turn into incidents;
Assessment and decision: someone must assess the situation to determine whether it is in fact an incident;
Responses: contain, eradicate, recover from and forensically analyze the incident, where appropriate;
Lessons learnt: make systematic improvements to the organization’s management of information security risks as a consequence of incidents experienced.
A.1.4 Requirements - Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

12.10.3 - Guidance - Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become “polluted” by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation.

10.4 - Guidance - to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach).
As a regards, a PCI Forensic Investigator (PFI)

The requirements are:

The existence of a dedicated forensic investigation practice within your company
Staff with the necessary backgrounds and skills
Experience performing investigations within the financial industry using proven investigative methodologies & tools;
and
Relationships with law enforcement to ensure you can support any resulting criminal investigations
Real Challenges
Real Challenges

• Problems will happen

• The crime organizations are on the Internet

• There are many tools available for offensive security

• Incident Response demand specifics tools, methodology and knowledge

• The Incident Response demands specific skills
Real Challenges

Other hard challenge is to become a Cyber Security Professional also great challenges, in a nutshell:

We already had to learn about security system;

As well as we need to learn about Offensive Security (Pentest)

And currently we need to learn about Response Incident and Computer Forensic too.
Talking about Post Mortem analysis
(Brushing bits, data mining, seeking for Evidence and Artifacts)
Post Mortem Analysis

Evidence of Correlation between Live and Network Forensics → Hard Disk analysis in 5 layers → Timeline creation

File System Analysis → Identification of potential artifacts

Creating the forensic report → Artifact Analysis

Static Analysis ↔ Dynamic Analysis
Post Mortem – Correlations

Correlate Live Forensics

Correlate Net Forensics

Strings and 5-layer Analysis

Correlate Memory Forensics
Initial System Analysis

Several actions can be taken in an attempt to find evidence and artifacts related to Security Incidents under investigation.

Knowing the “bad guy's” Modus Operandi helps the Computer Forensic Expert to do his/her job. However, unusual and stealth behavior will always present a challenge.
Initial System Analysis

“Bad guys” who do not have advanced technical knowledge have a Modus Operandi that usually leaves behind evidence of their actions.
Byte Map creation

The creation of an Image String file, as a first step, may allow the identification of relevant information.

# strings -a image.img | tee image.img.strings

The strings command has support only ASCII format, that hhy we need to get other different type of strings, use the srch_strings command:

# srch_strings -a image.img | tee image.img.strings
Strings vs Regex

The use of REGEX when dealing with string files is an essential mechanism. This way, the use of tools like GREP, EGREP, GLARK are useful to extract clues:

```bash
# grep -i\"\.gz\" image.string
# egrep --regexp="\.tgz|\.zip|\.bz2|\.rar|\.c" image.string
# egrep --regexp="[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" image.string
# bulk_extractor -e net -e email -o bulk_output/ image.dd
```
<table>
<thead>
<tr>
<th>Layer</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer</td>
<td>Media (e.g. Hardware identification: size, type, format, vendor)</td>
</tr>
<tr>
<td>Data Layer</td>
<td>Info about the boot sector structure, partitioning, type of file system</td>
</tr>
<tr>
<td>File System Layer</td>
<td>Specific information about files and directories</td>
</tr>
<tr>
<td>Metadata Layer</td>
<td>Information extracted from file Table (e.g. Inode, Fat, MFT)</td>
</tr>
<tr>
<td>File Layer</td>
<td>Analysis of information from Files (Artifact identification)</td>
</tr>
</tbody>
</table>
## The 5 Layers – main tools (Opensuse DFIR)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer</td>
<td>fdisk, sfdisk</td>
</tr>
<tr>
<td>Data Layer</td>
<td>file, testdisk, mmls, mmstat, mmcat, img_cat, img_stat, afflib, afflib-tools, libewf, ewftools, distorm3, aimage, dc3dd, sdd, rdd</td>
</tr>
<tr>
<td>Metadata Layer</td>
<td>ifind, ffind, istat, ils-sleuthkit, fls, icat, mac-robber</td>
</tr>
<tr>
<td>File System Layer</td>
<td>blkcalc, blkcat, blkls, blkstat, find, sorter, sigfind, hfind, chkrootkit, clamav, exiftool, yara, ext4magic, ddrescue, magicrescue, vinetto, pasco, rifiuti, photorec, foremost, scalpel</td>
</tr>
<tr>
<td>File Layer</td>
<td>sporckit / Autopsy</td>
</tr>
</tbody>
</table>
Physical Layer

This is where the Expert should gather and document information about related data storage devices, such as:

Hard disk drives
Removable media
Size, vendor, type...

“P.S.: Information collected to identify the media and also with the goal to give support to the Custody Chain Process”
Data Layer

The preliminary step for this phase of the analysis happens when information is gathered from a storage device, bit by bit.

This is where the integrity of the generated images is assured through the verification of the partition information and the file system structure.

“P.S.: Information collected to identify the media and also with the goal to give support to the Custody Chain Process”
File System Layer: Useful Tools

In this phase the expert should identify informations more specific about the file system.

Common tools to collect info from the File system
This gets journal info from image, (e.g. statistics info about partition)
- Fsstat - Extract informations about as filesystem was structured
- jcat - This shows general info from journaling file system
- Jls - This shows journaling info from structure of file system

“P.S.: Information collected to identify the media and also with the goal to give support to the Custody Chain Process”
Metadata Layer

The metadata analysis information is an extremely important step to give support to search for evidence and other actions in the fifth layer (File Layer). Examples of tool form sleuthkit:

- **fls** - Enables one to consult file and directory information from an image, using metadata.

- **ffind** - Similar to fls but using the specific Inode address.

Other relevant action is create of Timeline.

```
# fls -arpm / image.img | mactime -z America/SaoPaulo 2013-01-01 2015-12-31
```
The Final layer is “File Layer”

Firstly, we need to know that this process is very important and very long, because it’s necessary to analyze many types of files and correlate them with Incident information. There many different tools for this phase:

- **dstat** - Shows statistical info from data blocks
- **dls / dcat** - Enables us to list info from allocated, unallocated and slackspace areas
- **dcalc** - Manipulate info from a specific data block
- **sorter** - Enables one to sort the files according to their type.
- **hfind** - Enable one creates and searches and indexed database hash
- **sigfind** - Enables searches for hex and signature at any specified offset
Image Mounting

It's recommended that disk forensic image analysis be a process executed with caution, beginning with a media access preparation known as “mounting”.

The image mounting of the partition with the means of analysis must be accessed as a read-only filesystem, without device file and executable file support.

Example:

```bash
# mount -o loop,noexec,nodev,ro image.img /forensic
```
Recovery and File Carving
Recovery and Data Carving

During File layer analysis, other important action is recovery and data carving (or file carving) of files in non-allocate areas.

**Recovery files** - is process that depend on metadata information for allocate table.

**File carving** - is a process of “recovery” used when we don’t have metadata information available.

In special cases sometime a expert will be able to use advanced file carving techniques to “recue” a type specific of file. This not easy task, depend on of type, fragmentation level, file system.
Useful tools for recovery

**Magicrescue** - together with DLS, this permits the carving of the files

**foremost** - this carving files from their headers and footers.

**Scalpel** - works similar the foremost

**ddrescue** - this carving files from the image of any medium, but is a mode hard. It’s necessary identify file offset address.
File recovery using classic procedure

Attempting to recover a file from an image:

a) Identify the addresses using metadata of unallocated files:

```
# fls -t ext image.img > list.image.txt
```

b) Retrieve content from the list (unallocated files):

```
# cat list.image.txt
```

c) Recover it by using the ICAT command with specific content file by inode (e.g. 4157):

```
# icat image.img 4157 > file.ppt
```
Another way to use FOREMOST is to perform a search for types of file. Examples for images (e.g. jpg, gif, png), for PDF:

```
# foremost -c foremost.conf -t jpeg,png,gif,pdf -v -i image.img -o /carving -T
```

```
# scalpel -c /etc/scalpel/scalpel.conf /dev/loop7 -o /carving
```
Slackspace Extract information

With blkls we can extract all information from image:

```
# blkls -s imagem.img | slackspace.dls
```

In the old version of SleuthKit the command to extract stackspace information from image was dls:

```
# dls -s imagem.img | slackspace.dls
```

After it is possible extract string and use regex to identify clues:

```
# strings -a slackspace > slackspace.dls.strings
```
Physical Layer: Media Information For Chains Custody

Data Layer: Identify Information About Partition Structure And ID Partitions

File System Layer: Identify Information About File System In Use

Meta Data Layer: Identify Information About Files Allocated And Files In Use

Layer: Identify Information Of Artifacts

Layer: Identification Of Malware

Layer: Recovery Of File
The Whole 5-Layer Process

**Physical Layer**
- Media/Images Info

**Data Layer** (2nd)

**Metadata Layer** (4rd)
- String Extracts & Analysis with Regex

**File System Layer** (3rd)
- Artifacts Analysis
- File Carving

**File Layer** (5rd)

**Report**

Start: Copy bit by bit from media to chain of custody
Overall

So, there are many FLOSS tools CLIS (Command Line On Steroids) and also GUI Tools (example: Autopsy, Pyflag, PTK) for the Post Mortem Process, and by combining the 5 Layer Concept with String Extraction it is possible to analyze everything related to an Incident.

Another fact is that the Linux OS is the best choice for Computing Forensics, because it supports many filesystems and you can customize your Forensic Box.

“Every Forensic examiner should Compile his own kernel just like every Jedi builds his own light Saber” - (The Cory Altheide – Google security)
Thank you. Any Questions? Raise your hands, please...
Unpublished Work of SUSE. All Rights Reserved.
This work is an unpublished work and contains confidential, proprietary, and trade secret information of SUSE. Access to this work is restricted to SUSE employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SUSE. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer
This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.