GENERAL INFORMATION

Data of the subject

<table>
<thead>
<tr>
<th>Subject name</th>
<th>Forensic Monitoring, Detection and Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject code</td>
<td>DTC-MCS-524</td>
</tr>
<tr>
<td>Main program</td>
<td>Máster en Ciberseguridad [Primer Curso]</td>
</tr>
<tr>
<td>Involved programs</td>
<td></td>
</tr>
<tr>
<td>Level</td>
<td>Master</td>
</tr>
<tr>
<td>Quarter</td>
<td>Semestral</td>
</tr>
<tr>
<td>Credits</td>
<td>3.0 ECTS</td>
</tr>
<tr>
<td>Type</td>
<td>Obligatoria</td>
</tr>
<tr>
<td>Department</td>
<td>Department of Telematics and Computer Sciencies</td>
</tr>
</tbody>
</table>

Course overview
To familiarize the student with the foundations on which detection tools such as logs and events of Windows and Linux and the analysis of traffic and its dump are based. Establish the bases on the tools for the operation of the monitoring systems, events and information systems (SIEM), the specific approach for intrusion detection (IDS), and understand the correlation mechanisms, generation or import of rules. The specific part of industrial systems will also be covered, both for the inclusion of monitoring with specific tools in industrial networks and for the discovery of specific tools for open sources. The forensic part will include both the forensic understanding related to the judicial field (regulations, preservation of evidence, chain of custody) and the familiarization with the forensic analyst's own tools for computer equipment (memory dump, disk dump, evidence analysis) and extension to mobile devices.

Teacher Information

Teacher

<table>
<thead>
<tr>
<th>Name</th>
<th>Agustín Valencia Gil-Ortega</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Department of Telematics and Computer Sciencies</td>
</tr>
<tr>
<td>EMail</td>
<td><a href="mailto:avalencia@icai.comillas.edu">avalencia@icai.comillas.edu</a></td>
</tr>
</tbody>
</table>

Teacher

<table>
<thead>
<tr>
<th>Name</th>
<th>Antonio Carmona Rosanes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Escuela Técnica Superior de Ingeniería (ICAI)</td>
</tr>
<tr>
<td>EMail</td>
<td><a href="mailto:acarmona@icai.comillas.edu">acarmona@icai.comillas.edu</a></td>
</tr>
</tbody>
</table>

DESCRIPTION OF THE SUBJECT

Contextualization of the subject

Prerequisites
Basic knowledge about Virtual Machines

## Course contents

### Contents

#### Monitoring and Detection

**Monitoring**

- Fundamentals of monitoring
- Event generation: Linux
- Event generation: Windows
- Event generation: Adding sources
- Monitoring traffic

**Detection**

- Detection with IDS
- Detection with YARA and SIGMA
- Repositories

**Correlation**

- Open sources
- External sources
- SIEM correlation

#### Industrial point of view

**Forensic Analysis**

- Fundamentals and first response
- Documentation: Minutes, chain of custody, worksheet
- First response, acquisition and analysis tools
- Analysis of digital evidence
- Advanced techniques. Storage. Low-level analysis

### EVALUATION AND CRITERIA

**Grading**

Evaluation Criteria:

Monitoring (66.6% of the final grade)
60% Lab
40% Final Exam

Forensic Analysis (33.3% of the final grade)

- 50% Lab, Documenting (Mintures, Evicendes, Worksheets) and Expert Report
- 50% Quiz before each class, and Final Exam.

BIBLIOGRAPHY AND RESOURCES

Basic References

**MONITORIZACIÓN:**


Snort: [https://www.snort.org/](https://www.snort.org/)

Yara: [https://virustotal.github.io/yara/](https://virustotal.github.io/yara/)

Sigma: [https://github.com/Neo23x0/sigma](https://github.com/Neo23x0/sigma)

Sysinternals: [https://docs.microsoft.com/en-us/sysinternals/](https://docs.microsoft.com/en-us/sysinternals/)

Ossec: [https://www.ossec.net/](https://www.ossec.net/)

Wireshark: [https://www.wireshark.org/](https://www.wireshark.org/)

Censys: [https://censys.io/](https://censys.io/)

Shodan: [https://www.shodan.io/](https://www.shodan.io/)

MISP: [https://www.misp-project.org/](https://www.misp-project.org/)

**FORENSE:**

SANS: [https://digital-forensics.sans.org/](https://digital-forensics.sans.org/)

Forensic focus: [https://www.forensicfocus.com/](https://www.forensicfocus.com/)

Interpol: [https://www.interpol.int/How-we-work/Innovation](https://www.interpol.int/How-we-work/Innovation)


ENFSI: [http://enfsi.eu/about-enfsi/structure/working-groups/information-technology/](http://enfsi.eu/about-enfsi/structure/working-groups/information-technology/)

XDA developers: [https://www.xda-developers.com/](https://www.xda-developers.com/)

NFI: [https://www.forensischinstituut.nl/](https://www.forensischinstituut.nl/)

Informe de evaluación de herramientas forenses: [https://www.dhs.gov/](https://www.dhs.gov/)

Estándares y metodologías USA: [https://www.nist.gov/](https://www.nist.gov/)

Estándares ISO: [https://www.iso.org/](https://www.iso.org/)

Android: [https://developer.android.com/](https://developer.android.com/)

Autopsy: [https://www.sleuthkit.org/](https://www.sleuthkit.org/)


Nirsoft:

USBdevview: [https://nirsoft.net/utils/usb_devices_view.html](https://nirsoft.net/utils/usb_devices_view.html)
In compliance with current regulations on the **protection of personal data**, we would like to inform you that you may consult the aspects related to privacy and data **that you have accepted on your registration form** by entering this website and clicking on "download"