**Acceptance clause:** by completing this project the student accepts that he/she is responsible for what he/she will do and that he/she will **not use** these tools outside the virtual one created for that purpose. The student also accepts the legal repercussions that some of these actions may be subject to if these actions are carried out on external sites.

# Project 8: forensics analysis

**Level: 6**

**Difficulty: very high**

**Environment: Linux Machines (VM)**

**Objective: Install and analyze the indicated tools to create a FSA (DO NOT USE outside the virtual network).**

**Task: The student will have to collect information about forensic tools, and configure Router to execute it.**

**Necessary: Start with project 4-5-6-7.**

**sleuthkit**: is a tool for forensics analysis on volume and filesystem data. The Sleuth Kit, also known as TSK, is a collection of UNIX-based command line file and volume system forensic analysis tools. The filesystem tools allow you to examine filesystems of a suspect computer in a non-intrusive fashion. Because the tools do not rely on the operating system to process the filesystems, deleted and hidden content is shown. The volume system (media management) tools allow you to examine the layout of disks and other media. You can also recover deleted files, get information stored in slack spaces, examine filesystems journal, see partitions layout on disks or images etc. But is very important clarify that the TSK acts over the current filesystem only. The Sleuth Kit supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with filesystem analysis tools (TSK supports several filesystems, as NTFS, FAT, exFAT, HFS+, Ext3, Ext4, UFS and YAFFS2)**.**
http://www.sleuthkit.org/sleuthkit/

**Debian Forensics Environment** - essential components. This package provides the core components for a forensics environment. All here available tools are packaged by Debian Security Tools Team. This metapackage includes the most programs to data recovery, rootkit and exploit search, filesystems and memory analysis, image acquisition, volume inspection, special actions over the hardware and many other activities. See also **forensics-all-gui.**

**OpenVAS** (Open Vulnerability Assessment System, originally known as GNessUs) is a software framework of several services and tools offering vulnerability scanning and vulnerability management. https://www.openvas.org/. Download OVA VM.  To download Microsoft Windows OVA machines: https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/ or https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

**Disclaimer:** All materials, links, images, formats, protocols and information used in this document are property of their respective authors, and are shown for educational and non-profit purposes, except those that are assigned under licenses for use or free distribution and/or published for this purpose. (Articles 32-37 of Law 2/2019, Spain)

Any actions and or activities related to the code provided is solely your responsibility. The misuse of the information in this document can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this document/tools to break the law.

The examples, tools, tests or any other activity shown or suggested in this document should NEVER be carried out outside the private network created for this purpose, since criminal and/or punishable responsibility may be incurred.