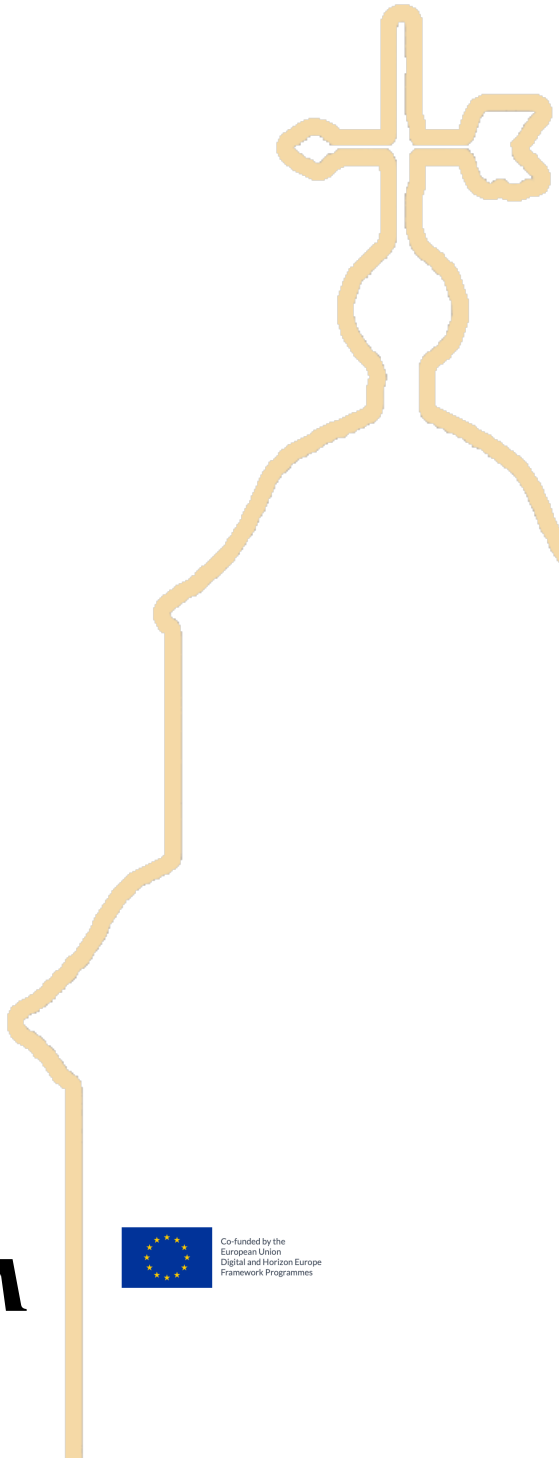
Faculty of Sciences
University of Novi Sad
1969

Dear participant,

We compiled a list of the software that will be used throughout the Summer School. This list can be found here:
https://research.pdmfc.com/wp-content/uploads/2025/07/IPICS25Software.pdf
On the first School Day, there will be a session dedicated to assisting with the setup, if you have any difficulties with the installation, don't worry. The most important would be to have the software downloads in your computer, so we don't waste time waiting for downloads. The installation is usually quick.

Let us know if you have any questions

Best regards,
The IPICS + CSP 2025 Summer School Team



IPICS25 CyberSecPro PDM

Co-funded by the European Union Digital and Horizon Europe Framework Programmes

Faculty of Sciences
University of Novi Sad
1969

IPICS + CSP 2025 Summer School Software Installation Guide

This document outlines the technical requirements and provides download sources and installation instructions for all software and tools required for participants. Please ensure all items are installed and configured before the start of Summer School.

1 - Hardware & Basic Requirements

Laptop Specifications

- Minimum RAM: 8 GB
- Recommended: 16 GB RAM, SSD storage, and at least 50 GB of free disk space

2. Virtualization Requirements

Participants will use both VirtualBox and VMware during the Summer School for running virtual machines.

2.1 VirtualBox

- Purpose: General virtualization
- Download: https://www.virtualbox.org/wiki/Downloads
- Installation:
  - Select your OS (Windows/Linux/macOS)
  - Install both VirtualBox and the Extension Pack (to enable USB, PXE boot, etc.)

2.2 VMware Workstation / Fusion

- Purpose: Required for running the Kali Linux VM
- Download:
  - Windows/Linux: VMware Workstation Player
  - macOS: VMware Fusion Player
- Note: You may need to create a free VMware account to access the player licenses.

3 - Operating Systems

3.1 Kali Linux

- Purpose: Primary penetration testing environment
- Download: https://www.kali.org/get-kali/
- Recommended Options:
  - VMware Image (prebuilt)
  - Live USB or bare-metal installation (optional)

3.2 ParrotOS (Optional)

- Purpose: Alternative security-focused OS
- Download: https://www.parrotsec.org/download/
- Installation Options: ISO for live or install environments

3.3 Metasploitable 2

- Purpose: Intentionally vulnerable VM for exploitation practice
- Download: https://sourceforge.net/projects/metasploitable/
- Instructions: Import .vmdk into VirtualBox or VMware

Co-funded by the European Union Digital and Horizon Europe Framework Programmes

4 - Tools & Software

4.1 Core Network Tools

Tool	Purpose	Installation (Linux)
netdiscover	Network discovery via ARP requests	sudo apt install netdiscover
Nmap	Network scanning/mapping	sudo apt install nmap or nmap.org
Netcat	Network debugging and backdoors	sudo apt install netcat
Wireshark	GUI network traffic analyzer	sudo apt install wireshark or wireshark.org

Note: On some systems, you may need to add your user to the wireshark group to capture packets without sudo.

4.2 Additional Network Tools

- tcpdump – CLI packet analyzer
  sudo apt install tcpdump
- tshark – CLI version of Wireshark
  sudo apt install tshark
- iptables – Linux firewall utility
  Typically preinstalled. Otherwise: sudo apt install iptables

Co-funded by the European Union Digital and Horizon Europe Framework Programmes

5 - Data Protection & Forensics Tools

5.1 CNIL PIA Software

- Purpose: Data Protection Impact Assessment (DPIA)
- Download: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment
- Portable Version: This version can be directly downloaded and launched on your computer with no need to install it locally. It is available for the following operating systems:
    - Windows (32 and 64 bits)
    - Linux (64 bits)
    - Mac OS

5.2 Ghidra

- Purpose: Reverse engineering suite (developed by NSA)
- Download: https://ghidra-sre.org/
- Requirements: Java 11+
  After downloading, unzip and run ghidraRun or ghidraRun.bat.

5.3 PEStudio

- Purpose: Analysis of Windows executable files
- Download: https://www.winitor.com/
- Windows-only: Download and unzip the tool.

5.4 Yara

- Purpose: Malware classification & pattern matching
- Source: https://github.com/VirusTotal/yara
- Installation (Linux):
- sudo apt install yara
- Windows/macOS: Download precompiled binaries from the GitHub releases.

5 - Risk Analysis and Data Anonymization tools

Unfortunately, RM Studio is only in Windows:
RmStudio: https://www.riskmanagementstudio.com/downloads/rmstudio/5810/RmStudio.Setup.5.8.10.exe

Arx, Data Anonymization Tool : https://arx.deidentifier.org/downloads/
Pilar, Risk Analysis: https://www.pilar-tools.com/en/tools/pilar/v74/down.html

Verinice, windows 64 bits (other OS versions will be shown in class):
https://drive.google.com/file/d/1n82P84HVFmRPCkwMbJbSm7Gt0wY0aEvA/view?usp=sharing

Verinice datasets:
https://drive.google.com/file/d/1e6OsJCbJ8j2U7HcmXHSfDdFZuNo4X34e/view?usp=sharing