Workshop I: Introduction to ForTrace++: A digital forensics data synthesis framework (*Wolf, Dennis*, Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS))

During this workshop you will be introduced to the open-source data synthesis framework ForTrace++, originally presented on the DFRWS EU 2024. It is used to synthesize holistic and digital forensic relevant data sets in a semi-automated fashion on Windows and Linux VMs. These data sets can be used for, e.g., training of students or the evaluation of digital forensic tools. Instead of generating the data sets manually, the user writes scenarios or uses community defined scenarios that are configurable via YAML files. The aim is to support further applications that can be combined to create more complex scenarios. In the long term, this will enable users to define scenarios by reusing existing 'blocks' and only writing configuration files.

After discussing the general concepts of the ForTrace++, we will explore two simple scenarios, involving the software VeraCrypt, which are demonstrating the Python interface, the configuration files, and the component for semi-random interaction offered by the framework. The latter adds more background noise to the generated data set, to increase its realism. Eventually, we start to examine the data sets for the generated traces.

In order to actively participate on this workshop, please see the information on the public GitLab repository https://gitlab.com/DW0lf/fortrace. It is advised to use a computer running Linux, e.g. Arch, Debian, or Ubuntu, with enough resources to handle one Windows 10 VM with KVM/QEMU as the hypervisor. Nested virtualization is possible as well, if there are enough resources available. Installation instructions for ForTrace++ can be found in the project's readme. For the preparation of both scenarios, including the installation and setup of the Windows 10 VM, there is a readme file in examples/Windows/ForTrace_Workshop/VeraCrypt.