UNIL | Université de Lausanne
Ecole des sciences criminelles

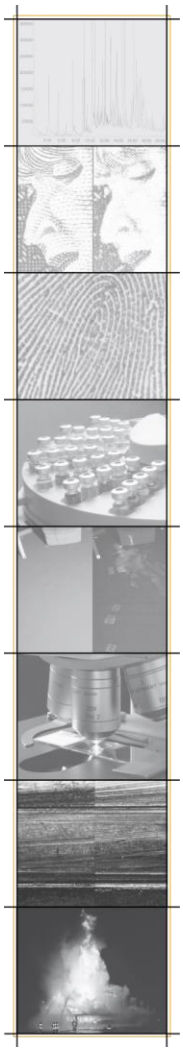
Cours de formation continue – Continuous professional education course :

Malware Forensics I:
Malware techniques and memory forensics

August 26-28th 2015, ESC Lausanne

Course description

Malware and related attack tools play an important role in many of today's digital investigations. In fact, on the one hand malware is used to commit cybercrimes (e.g., financial fraud, identity theft, extortion etc.) as well as for industrial and state-level espionage. On the other hand, malware can be used as an excuse to deny crimes. That is, a suspect may contest digital evidence found on his computer (e.g., incriminating pictures), by claiming that it was planted on his machine by a piece of malware.



Malware forensics is a relatively recent sub-field of digital forensics, whose key objectives are:
(i) the *detection of malware* (i.e., figuring out whether a given system is subverted by malware), and
(ii) *malware analysis* (i.e., what is a malware doing and where is it possibly coming from?)

Malware forensics is often considered to be a complex field, since it requires intimate knowledge of various disciplines of computer science, like operating systems, networking, assembly code, etc.

Course objectives and topics

The objectives of this training are to give an introduction to malware forensics with a particular focus on malware detection using memory forensics techniques on Windows computers. The principal topics covered in the course are:

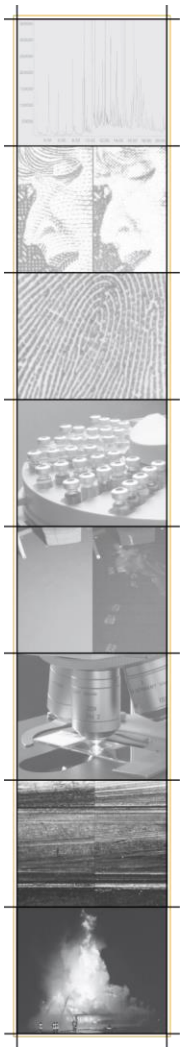
- An overview of the field of malware and malware forensics, to convey the "big picture".
- Typical malware techniques and behaviours (e.g., persistence and root kit techniques, code injections, etc.), which are fundamental for malware detection and analysis.

- Memory acquisition and memory forensics constitute the key part of this course.
  - In particular, we are going to systematically cover what anomalies and suspicious activities induced by malware can be detected using which memory forensics techniques.
  - Thereby we are going to use Volatility, a widely used, highly effective open source memory forensics toolkit, as well as selected commercial tools.
  - We will discuss the main ideas underlying memory forensics techniques, allowing to understand the strengths as well as potential shortcomings of memory forensics.

- Identification of selected important malware families using memory and disk / registry artefacts.

The course consists of theory blocks mixed with substantial hands-on lab work.

At the end of the course, participants will be able to detect typical malware infections and identify common malware behaviours and malware families.



An important aspect of this training is that its objectives are not only to present a collection of tools, but also to develop a conceptual understanding of the field and the related forensic techniques.

Target audience and prerequisites

This training is intended for participants from public administrations and private companies who typically occupy positions such as:

- Digital forensic police officers, digital forensic practitioners
- IT-security specialists, computer scientists

The ESC may ask extra information before accepting a participant. The ESC can refuse any application without having to justify the reason.

The number of participants is limited to 15 participants.

Course participants are expected to have a practical background in IT and / or forensic investigations, and should be proficient using Windows machines. Knowledge of operating system concepts, especially the Windows operating system is a plus, but not a must. All necessary operating system and malware concepts will be (sometimes briefly) introduced. Participants should be interested in learning operating system concepts and technicalities.

Practical information

Dates
From August 26th to 28th 2015 (3 full days)

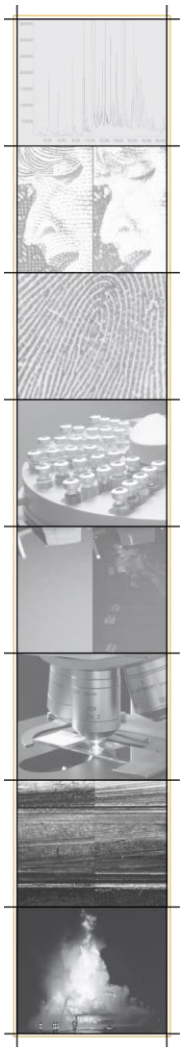
Location
Campus of the University of Lausanne, 1015 Lausanne-Dorigny

Detailed information about the venue and schedule will be sent later to accepted participants.

Language

Spoken:	French (Q&A in French, German or English)
Slides and documentation:	English

Persons in charge of the training
Dr Endre Bangerter, professor, Bern University of Applied Science
Dr David-Olivier Jaquet-Chiffelle, professor, University of Lausanne



Material
Participants are required to bring their own laptop, fulfilling the following requirements:

- The laptop shall either be native Windows machine or have a Windows virtual machine installed (Windows Version 7 or newer)
- Participants shall have sufficient privileges to install software tools on their Windows machines (be it native or virtual)
- USB port
- Wireless or Ethernet networking
- RAM should be at least 4 GB, more is better
- Contemporary CPU
- 30 GB free disk space
- There will be no malware run or installed on the participants systems. However, participants will be given memory images of infected systems. In rare cases, anti-virus might detect infected memory image. Thus, participants shall have the ability to deactivate anti-virus

Registration

Registration information and questions are to be sent to (preferably by e-mail):

ESC secretariat
Batochime, UNIL-Sorge
CH-1015 Lausanne
Tel. +41 21 692 46 00

info.esc@unil.ch

Course cost

- Participants from private companies and other non-governmental organisations: 2'900.- (VAT incl.)
- Participants from police departments and other governmental organisations: 1'800.- (VAT incl.)
- Participants from public education entities: 1'800.- (VAT incl.)

Meals and coffee breaks are not included. Restaurants are available on the campus.