# Digital Forensics

## Preamble

**Thibault Debatty**
cylab.be

**Download me...**

# Download me...

https://forensics.pages.cylab.be/

Password: `forensics2025`

# Course organization

# Course organization

Forensics:

- Master Cybersecurity and RMA
- Monday morning
- at RMA
- LtCol Thibault Debatty

Malware Reversal:

- Master Cyber
- Monday afternoon
- at ULB
- Prof Wim Mees

# Cyber Defence Lab and the Royal Military Academy

# Royal Military Academy

Figure 1: RMA from the sky

# Royal Military Academy

- **university**
- responsible for academic, military and physical training
- of all future officers of belgian defense

Research areas:

- Ballistics
- Explosives
- UAV
- Image processing
- **Cyber**
- and many more ...

# Royal Military Academy

Is a military facility

- Access is controled
- Visitors (including external students) must be accompanied
- Photos and videos are NOT allowed

# Why Cyber ?

By law, Belgian Defence is responsible to:

- protect military computers and communication systems
- neutralize cyber attacks and identify the perpetrators
- protect military secrets
- react in case of cyber attack against other computer systems, in case of national crisis

Two main bodies:

- Cyber Force
- Cyber Defence Lab

# Cyber Force

Strengthen the country's cyber capabilities and protect military and critical non-military systems.

- https://www.mil.be/nl/over-defensie/cyber-command/
- https://www.mil.be/fr/a-propos-de-la-defense/cyber-command/

Job offers:

- https://egovselect.be/fr/offres-demploi?locations=defense
- https://egovselect.be/nl/vacatures?locations=defensie

# Cyber Defence Lab

- Cyber Defence Lab of the Royal Military Academy
- https://cylab.be
- A team of 20
- Fighting cyber threats through **research** and **education**

# Cyber Defence Lab

**Education**

- Academic courses at the Royal Military Academy (RMA) and at the Université Libre de Bruxelles (ULB)
- Courses cover topics like Introduction to Networks and Security, Advanced Networks Security, Digital Forensics and Management of Security
- **Coaching sessions for the Cyber Security Challenge** and other Capture-The-Flag competitions
- Supervise **master thesis, internships and PhD students**

# Coaching Cyber Security Challenge

We will organize **coaching sessions in preparation for the Cyber Security Challenge** (and other CTF)

- on Wednesday afternoon
- planning tbc

Info and registration: https://cylab.be/c3

# Cyber Defence Lab

**Research**

12 funded research projects

Topics include:

- Military Cloud
- Intrusion Detection
- Management of Security
- Offensive Security
- Software Supply Chain

# Contact, slides and syllabus

# Contact


- t.debatty@cylab.be
- a.croix@cylab.be

# LinkedIn

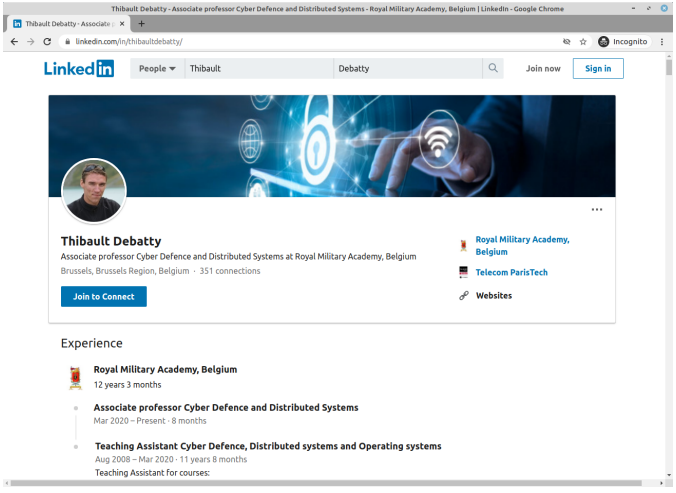


Figure 2: https://www.linkedin.com/in/thibaultdebatty/

# Mailinglist

- https://cylab.be > Resources > Mailinglists > Forensics

# Mailinglist

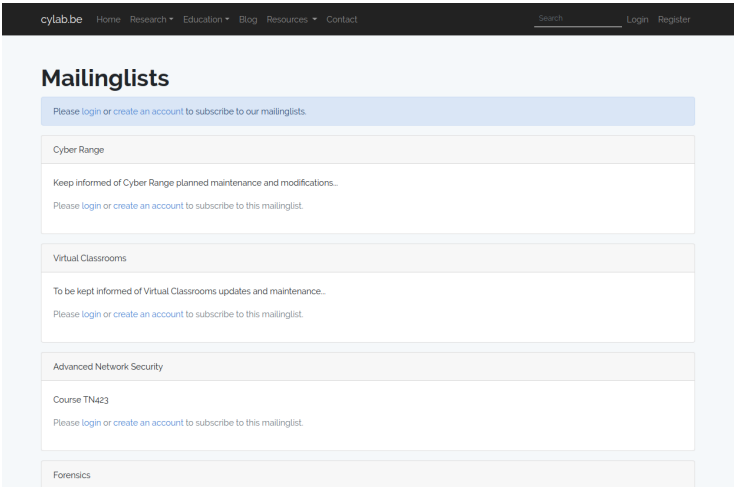


Figure 3: Mailinglist

# Mailinglist

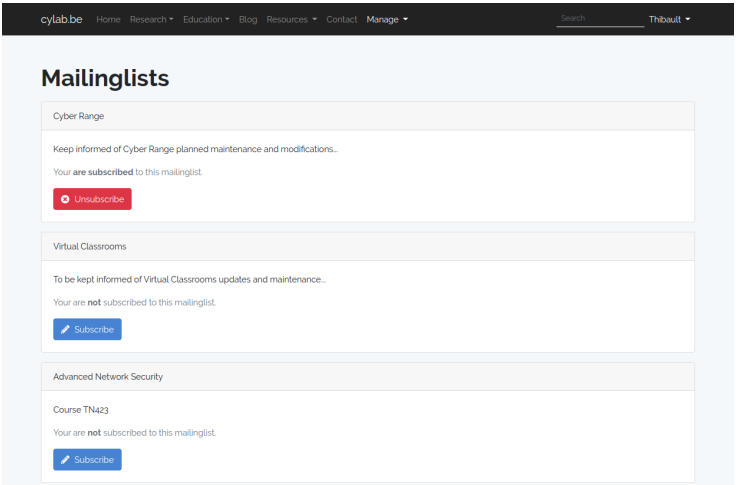


Figure 4: Mailinglist

# Slidess and syllabus

- https://forensics.pages.cylab.be/
- password: `forensics2025`
- will be updated regularly! (check you have the last version)

Syllabus:

- is under construction!

# Course content

# Course content

Topics:

- Disk
- Windows
- Memory
- Network
- Mobile devices

# Course content

This is university course, not a professional training.

We will cover:

- theory of computers and networks
- where is interesting information stored
- how can we retrieve this information (tools)

# Evaluation

- RMA : daily work : written test, theory, closed book
- exam : written test, theory and exercises (on lab computers), closed book

# Evaluation

Example of questions:

- explain what the registry is
- explain how we can show that user logged on a windows computer
- using the provided cheatsheet, extract the name of the last user that logged on this windows computer

# Tentative planning

See `study-guide.pdf`

# Course Requirements

# Course Requirements

- Windows machine
- SIFT workstation
  - Ubuntu 20.04 with preinstalled forensics tools
  - Sleuthkit, RegRipper, volatility etc.
  - https://www.sans.org/tools/sift-workstation/

# SIFT

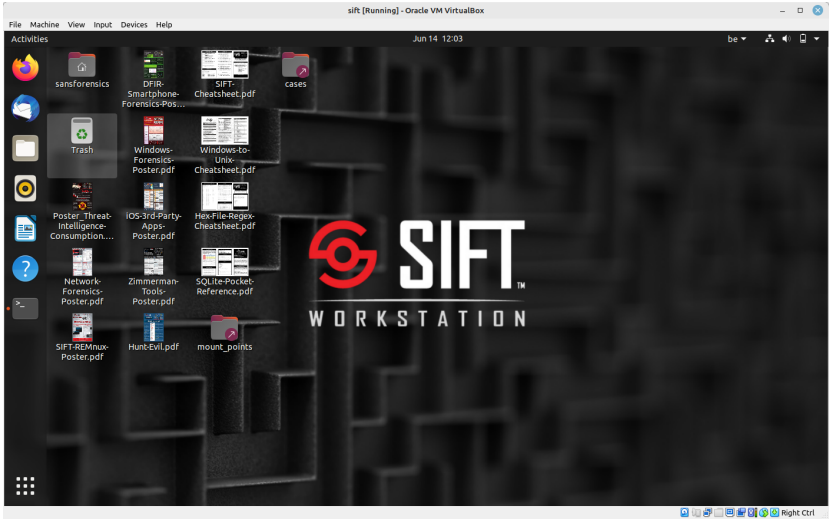


Figure 5: SIFT Workstation

# SIFT

**Exercise**

Download and install the SIFT workstation

# Questions ?