0. Administrivia

Digital Forensics and Cybercrime course

Prof. Zanero

Welcome

In this course, we will analyze:

- Cybercrime: motivations and modus operandi of criminals
- Fraud: patterns and detection mechanisms
- Forensics: analysis of digital evidence
- Ethical elements

Instructors

Prof. Stefano Zanero - @raistolo

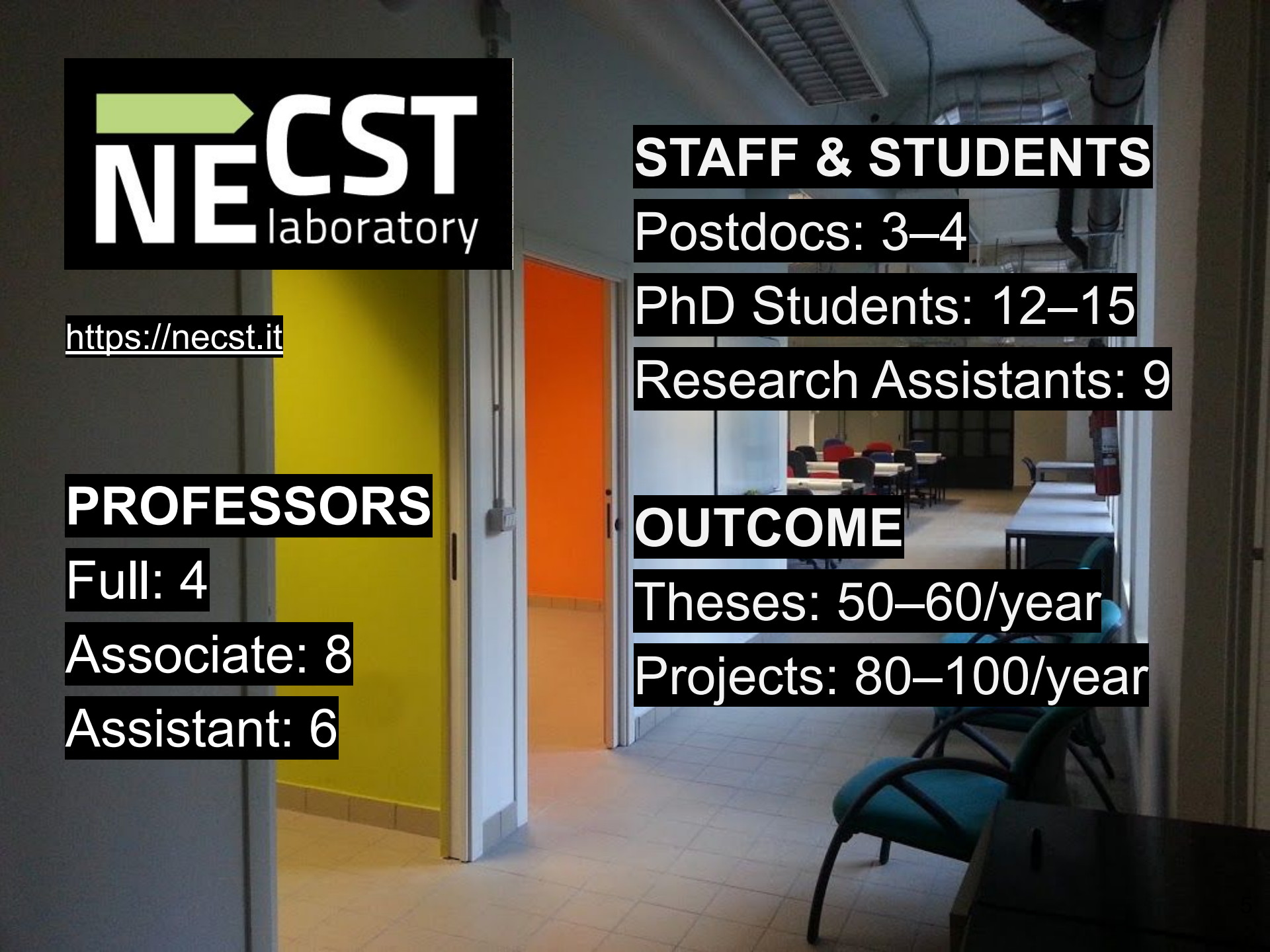
- Email: stefano.zanero@polimi.it
- Phone: 4017
- http://zanero.org

Prof. Michele Carminati

- Email: michele.carminati@polimi.it
- Phone: 3564

What we do as Research Scientists

- Cyber-physical security (automotive, robotics, medical)
- Novel attacks on bleeding-edge technology
- Malicious software (malware) analysis
- Fraud analysis and detection
- Anomaly-based intrusion detection


NECST laboratory
https://necst.it
PROFESSORS
Full: 4
Associate: 8
Assistant: 6
STAFF & STUDENTS
Postdocs: 3–4
PhD Students: 12–15
Research Assistants: 9
OUTCOME
Theses: 50–60/year
Projects: 80–100/year

Course Topics

Summary

1. Cybercrime: threats, modus operandi, underground economy
2. Financially-motivated malware
3. Fraud detection and analysis
4. Digital forensics principles
5. Acquisition, analysis, evaluation and presentation of evidence
6. Ethics elements

\+ ~8 hours in Italian on case studies (not in the exam program, but useful for localizing competence)

Exam Structure

Oral or written test (depending on COVID-19)

- theory and “case” questions (that are still theory)
- First year of the course so we will try to provide a mock exam in advance

Materials

Option 1: Slides + Class/Recordings + [Optional material]

~~**Option 2:** Slides~~ (best way to fail the exam)

Textbooks

- Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Addison-Wesley

Slides (and announcements)

- https://beep.metid.polimi.it/web/188915118/