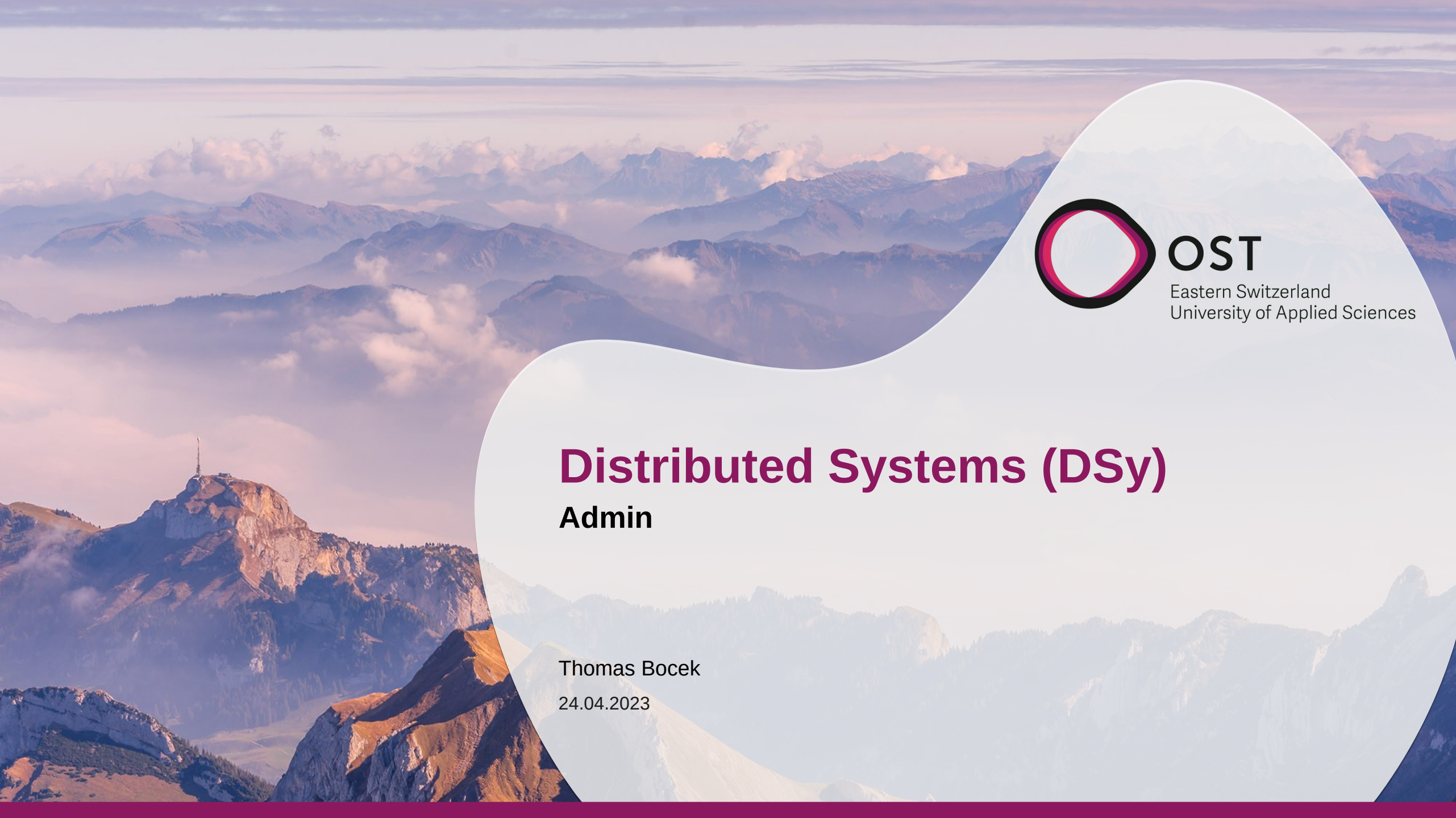

OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems (DSy)

Admin

Thomas Bocek

24.04.2023

Nr	Date	Lecture*	Lecturer
01	21.02.2023	Admin, Introduction / Motivation	Bocek
02	28.02.2023	Introduction / Categorization	Bocek
03	06.03.2023	Monorepos / Polyrepos, Protocols 1	Bocek
-	14.03.2023	-	-
04	21.03.2023	HTTP/3 practical examples, Protocols 2	Bocek
05	28.03.2023	Authentication, Web Architectures	Bocek
06	04.04.2023	Load Balancing	Bocek
-	11.04.2023	-	-
07	18.04.2023	Containers and Vms	Bocek
08	25.04.2023	Deployment, (Docker Swarm, Kubernetes)	Bocek
09	02.05.2023	Distributed Applications: Mastodon, Distributed Applications: Tor	Bocek
10	09.05.2023	Blockchain, Bitcoin	Bocek
11	16.05.2023	Exam preparation, Ethereum Introduction, Smart Contracts	Bocek
12	23.05.2023	Challenge Task Presentations I	you
13	30.05.2023	Challenge Task Presentations II	you
14	06.06.2023	Challenge Task Award Winner Announcement, Q&A	Bocek

* topics may change

Next Lecture

- Exercises on 9.5 only from 10-12, **and 17-19**. Instead talk: “From digital crimes to court in the UK”
  - From 13:00 – 17:00 – 5.002
  - You are all invited to join!

- 13:10 - 14:50
  - Support using relevant real-world examples this session will explore **digital crimes**, from the types of digital devices in use today, their importance in a crime scene and the evidence they could contain relevant data to an investigation. Techniques associated with gathering, preserving and presenting digital evidence from digital devices will also be discussed, highlighting the different approaches that need to be applied to different devices, e.g. a module, **a network router or a smart home device e.g. Amazon Alexa**. This presentation is open to all with an interest in digital investigations.
- 15:10 - 16:50
  - This is a **hands-on practical examination** of two mobile and a Windows device using the latest **industry-standard digital forensic software**. You will explore the **data** that was **recovered** from an **Android** and **Apple** mobile device to **search and identify the relevant data** that could be of evidential value to an investigation, you will explore areas such as the call logs, Internet browsing history, User Account information and other relevant areas. You will undertake the same approach to the Windows device, exploring, identifying and documenting relevant areas of data pertinent to an investigation such as the Windows Registry, Most Recently Used (MRU’s) lists and of course Internet browsing history.