Enhancing Situational Awareness for Tutors of Cybersecurity CtF Games

Karolína Dočkalová, Radek Ošlejšek

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION, YOUTH AND SPORTS

lasaris

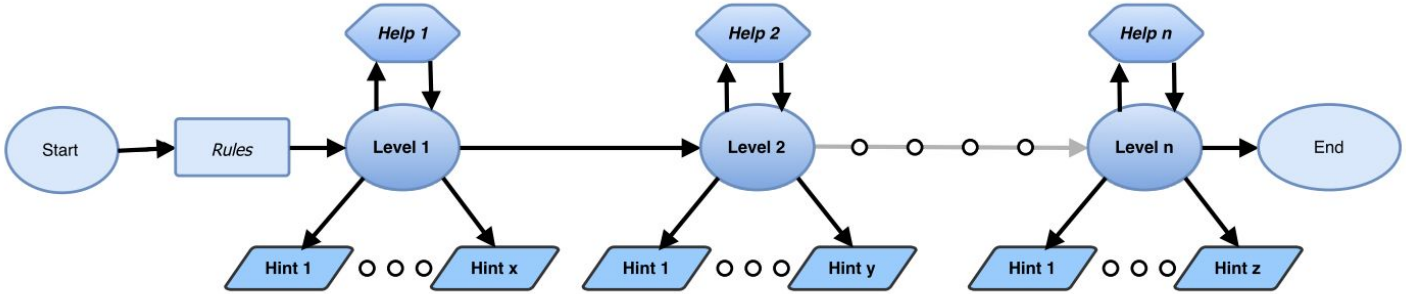
MUNI

KYPO

Capture the Flag Games

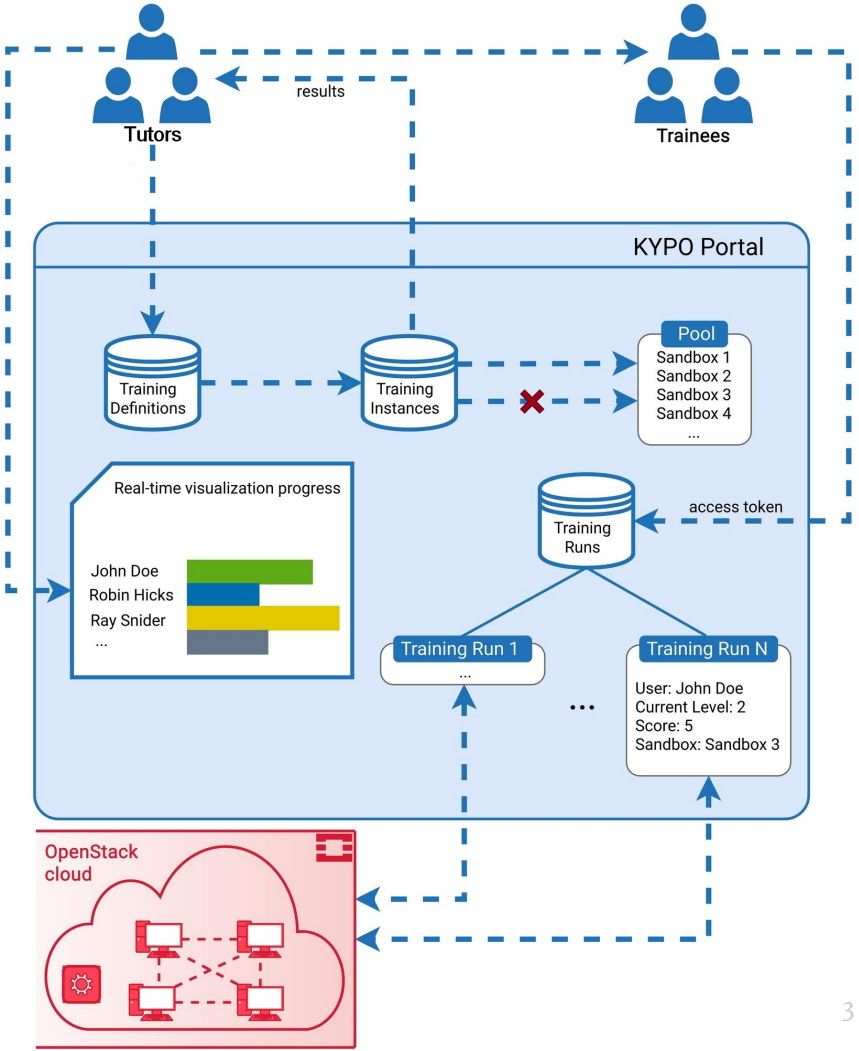
- Our focus – hands-on education-oriented cybersecurity games
- The trainees fulfill individual tasks and receive or lose points according their progress
- A tutor is present to oversee the game and help the trainees

We *visualize the trainees' actions* to give the tutors *insight into the progression* of the training session



KYPO Cyber Range

- Open-source cloud-based simulator of computer networks
- Environment for execution of cybernetic attacks in sandboxes
- One of use cases are the educational CtF games
- The cyber range enables us to collect trainee-specific data regarding individual training runs.



KYPO Cyber Range II

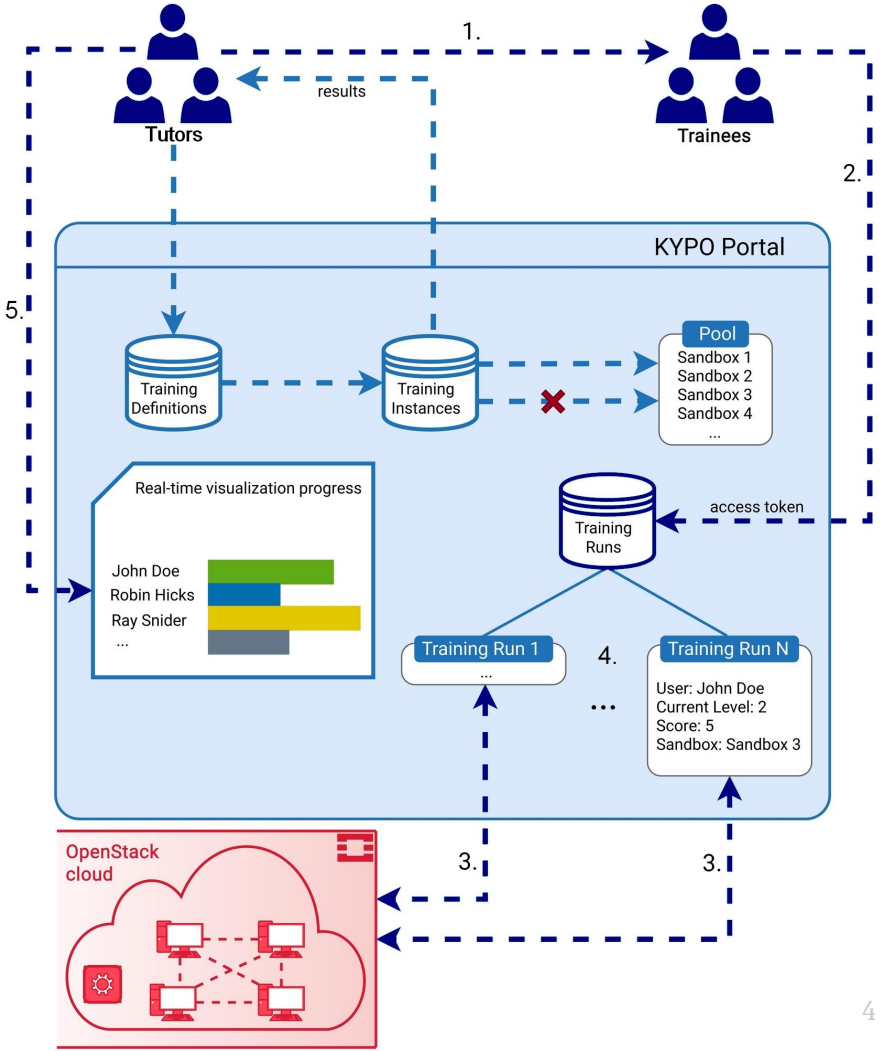
During the training session:

1. + 2. Trainees get access to their training runs

3. Trainees perform actions within the portal to solve their tasks

4. Actions for each training run are logged and and stored (in ElasticSearch DB)

5. **Our aim** - tutors see available data in a visualization tool



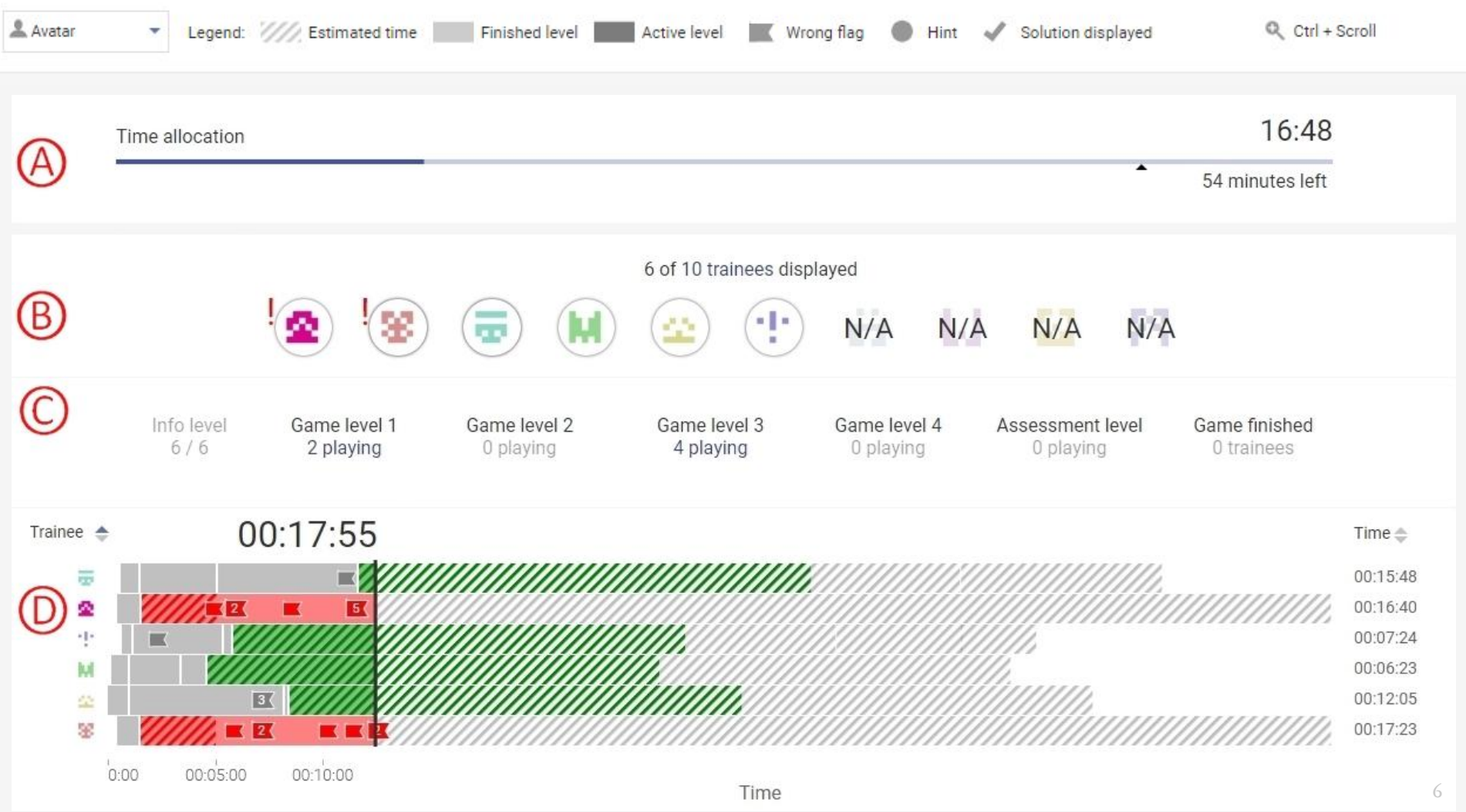
Requirements and design

Our goal was to provide:

- **R1: Training schedule overview** and it's fulfilment or risk of deviation from the schedule
- **R2: Identification of at-risk trainees** which are too slow or struggling with the puzzle (inactive or entering to many wrong flags)

Iterative design, collaboration with domain experts, field observations.

	trainee	**tutor**	game designer
situational awareness	✓	✓	
post-game analysis	✓	✓	✓


Avatar
Legend:
Estimated time
Finished level
Active level
Wrong flag
Hint
Solution displayed
Ctrl + Scroll
A
Time allocation
16:48
54 minutes left
B
6 of 10 trainees displayed
N/A
N/A
N/A
N/A
C
Info level
6 / 6
Game level 1
2 playing
Game level 2
0 playing
Game level 3
4 playing
Game level 4
0 playing
Assessment level
0 playing
Game finished
0 trainees
Trainee
00:17:55
Time
D
00:15:48
00:16:40
00:07:24
00:06:23
00:12:05
00:17:23
0:00
00:05:00
00:10:00
Time
6

Player 4

00:16:36 (~ 6 minutes behind)

in 2. level, Find the Vulnerable SSH Server

Used 3 of 3 hints:

How to find out CVE
9 minutes ago

Name of the SSH lib
11 minutes ago

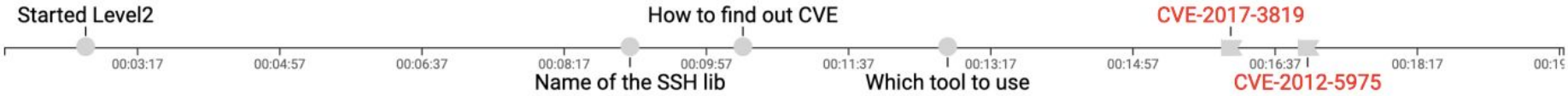
Which tool to use
7 minutes ago

CVE-2018-10933
(correct flag)

CVE-2017-3819
1x
4 minutes ago

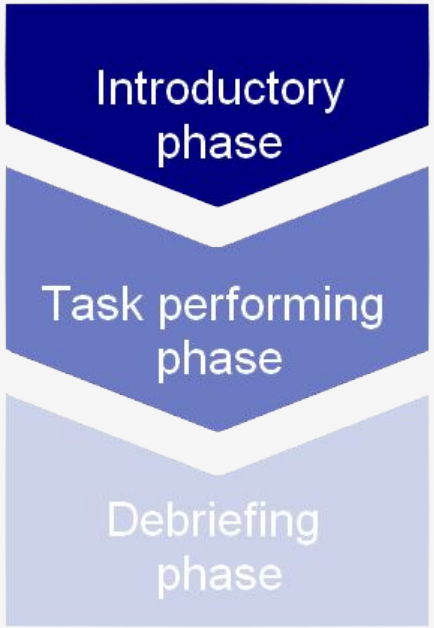
CVE-2012-5975
1x
3 minutes ago

Detailed timeline



Command timeline

Evaluation – Procedure



Two qualitative user studies

- Formative evaluation in person (6 participants)
- Summative evaluation online (8 participants)

The procedure had three phases

Real datasets replayed with timing set 10x faster. The participants observed the session run and gave their inputs regarding two defined tasks.

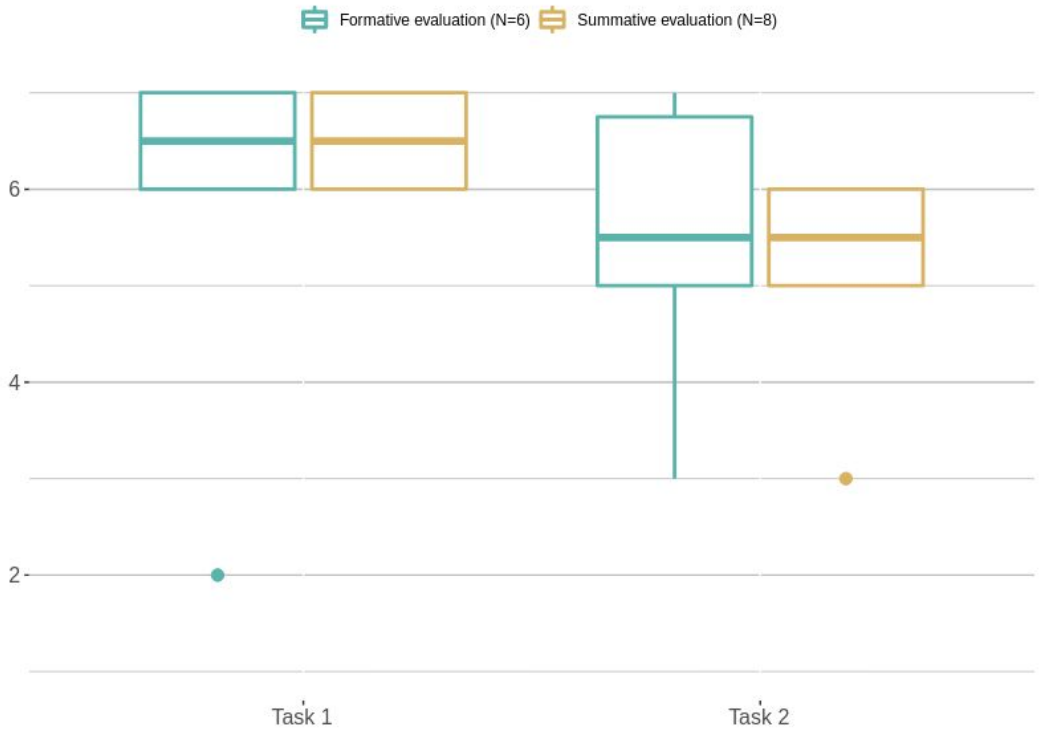
Each session lasted 40-60 minutes

Evaluation II (Single Ease Question)

Usability of the tool?

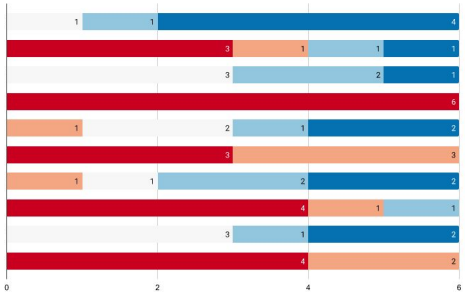
Task 1: Identify trainees in trouble, make an assumption of their cause, and conceive your reaction. (6.5)

T2: Identify problems that can influence the overall training session duration. What is their cause, and what would be your reaction? (5.5)

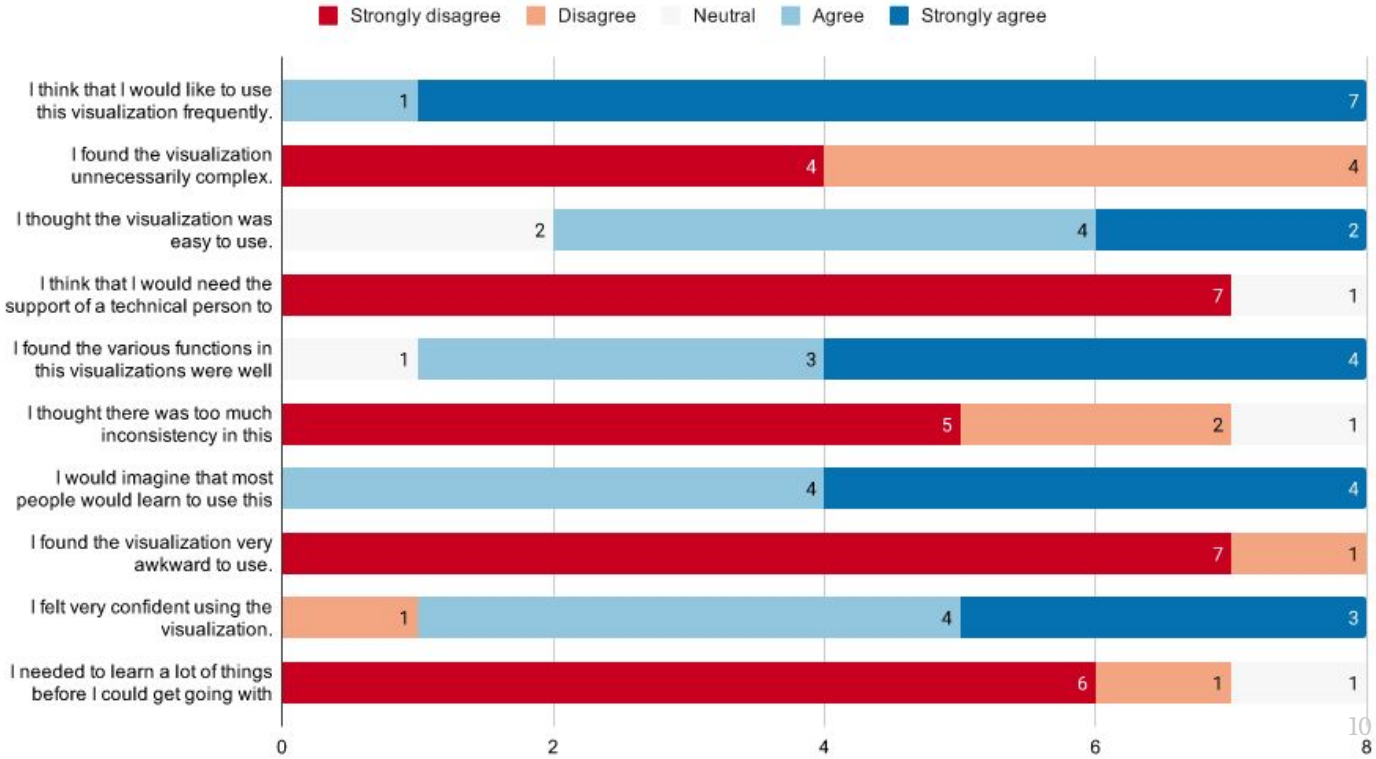


Evaluation III (System Usability Scale)

Formative (79.2)



Summative (87.8)



Outcomes

Insights on the use of notifications, filters and summaries in the workflow

Design recommendations on future tools:

- Intuitiveness over complexity during the training session
- Notifications and identification of notable events
- Simple sorting and filtering, to allow the tutors to quickly focus on a particular issue

Designed for on-site training. Proved very **useful for sessions held remotely** as well.

Thank you for your attention!