



CTF Stream
CyberTalk Stream

BALKANS
October 21-22, 2021

CRDFGLOBAL



Agenda

Day 1 - 21.10.2021

Time	Description
11.00-11.30	Welcoming remarks
11.30-12.30	Session 1 by Purdue University: <ul style="list-style-type: none">- Disk-based forensics using Linux command line utilities and YARA rules.- Network-based forensics using Wireshark.
12.30-12.45	Coffee-break
12.45-14.00	<ul style="list-style-type: none">- Memory-based forensics using Volatility.- Common encodings and protocols.
14.00-15.00	Lunch break
15.00-16.00	Session 2 by Purdue University: <ul style="list-style-type: none">- Basics of using Ghidra.- Basics of using gdb.- Basics of reading Assembly.
16:00-16.15	Coffee-break
16.15-17.15	<ul style="list-style-type: none">- Deciphering intent and locating malicious code.- Bypasses and inversion of algorithms without source.
17.15-18.00	Team creation, registration, access, and competition environment testing

Day 2 - 22.10.2021

Time	Description
10.00-13.00	CTF game
13.00-14.00	Lunch break
14.00-17.00	CTF game
17.00-18.00	De-briefing, analysis of attacks, results calculation
18.00-18.30	Communication with winning team



This event is a part of CRDF Global's cyber security improvement program in Balkan region, implemented with the support from U.S. Department of State's Office of the Coordinator of U.S. Assistance to Europe and Eurasia.