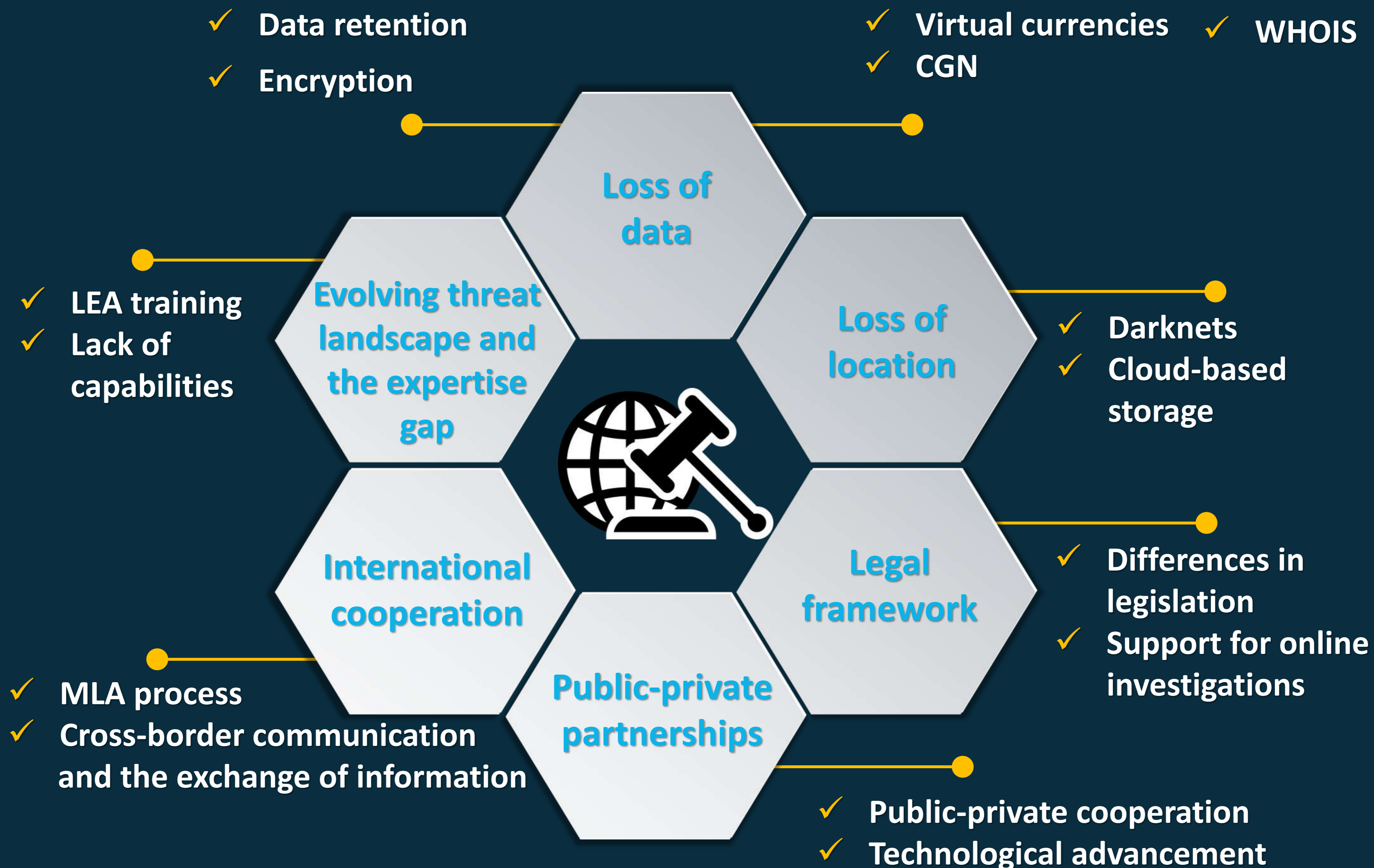


Cyber Capacity Building and Operational Cooperation

- Side Event of the 5th Session of the Ad Hoc Committee -
Date: 12 April, 2-3pm
Venue: Room CR1, VIC

Common Challenges in Combatting Cybercrime



Law Enforcement as a Service



Training and Capacity Building



J-CAT & Attachment Scheme



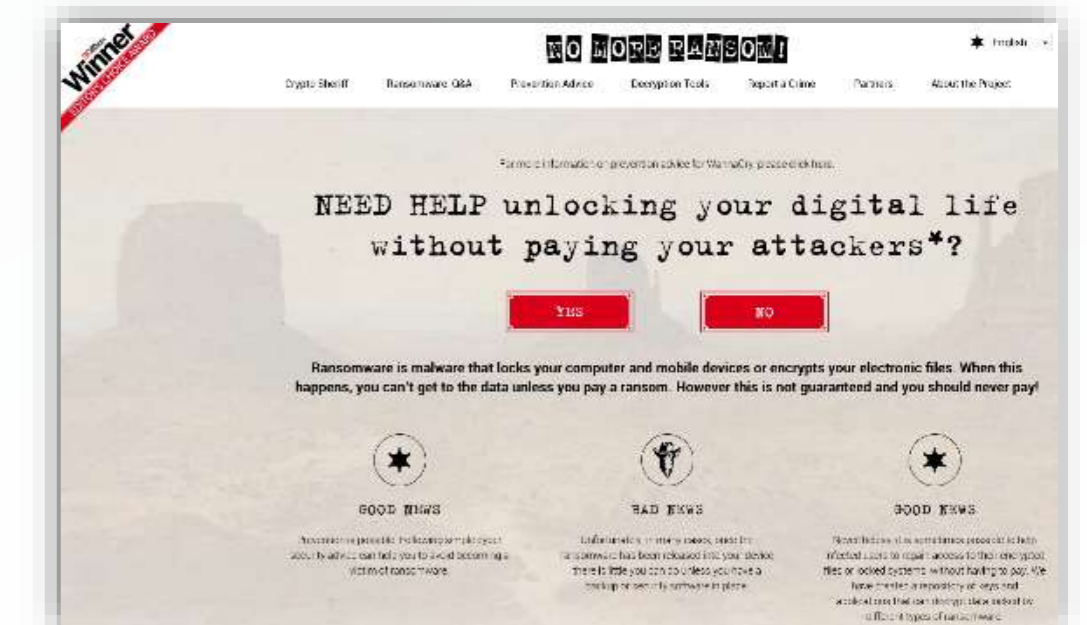
Analytical and Technical Support



On-the-spot Operational Support



Awareness Raising and Sharing of Best Practices



SPACE

Join the 8000+ members of SPACE!



Contact ec3@europol.europa.eu



Exchange expertise & best practices



Consult hundreds of open sources reports



SCAN ME



Find answers to your questions



Network with experts from your field

The SIRIUS Platform on EPE



The SIRIUS project responds to the need of law enforcement and judicial authorities to improve access to electronic evidence during an investigation



> www.europol.europa.eu/sirius

> sirius@europol.europa.eu

The FREETOOL Project



- EU funded project established in 2013
- Set of free cybercrime investigation tools tailored to support LEA
- Tools are developed in partnership with law enforcement, and are freely available to the law enforcement community
- Open Source Intelligence Gathering (OSINT), live data forensics, memory analysis, online resource preservation, network-based evidence triage, intelligent encryption detection, etc.
- 3500+ users from 350 Law Enforcement Agencies spread across 69 countries have signed up so far



- > www.ucd.ie/cci/projects/freetool/
- > <https://thefreetoolproject.eu/>
- > freetool@ucd.ie

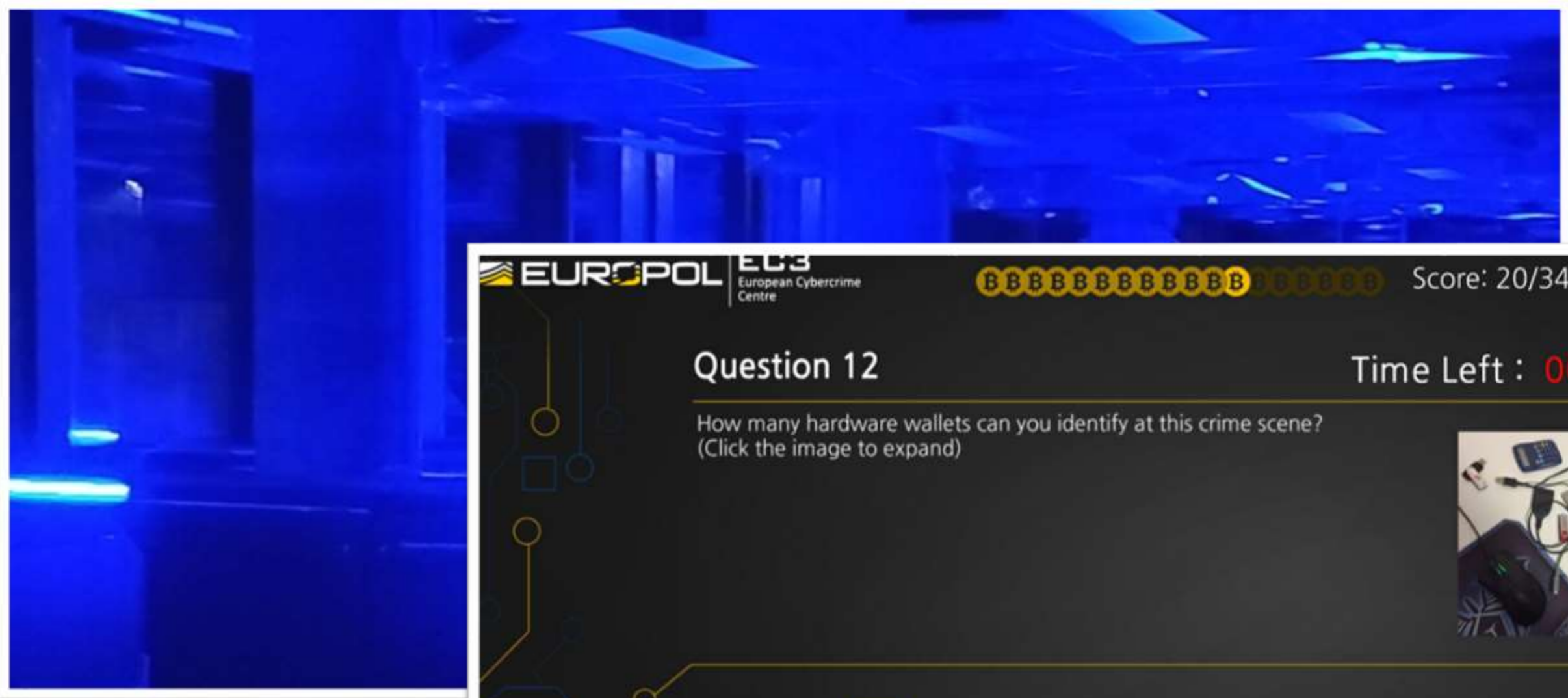
Innovation as a necessity



Innovation as a necessity



Innovation as a necessity




EUROPOL EC3 European Cybercrime Centre

Score: 20/34 01:05.24

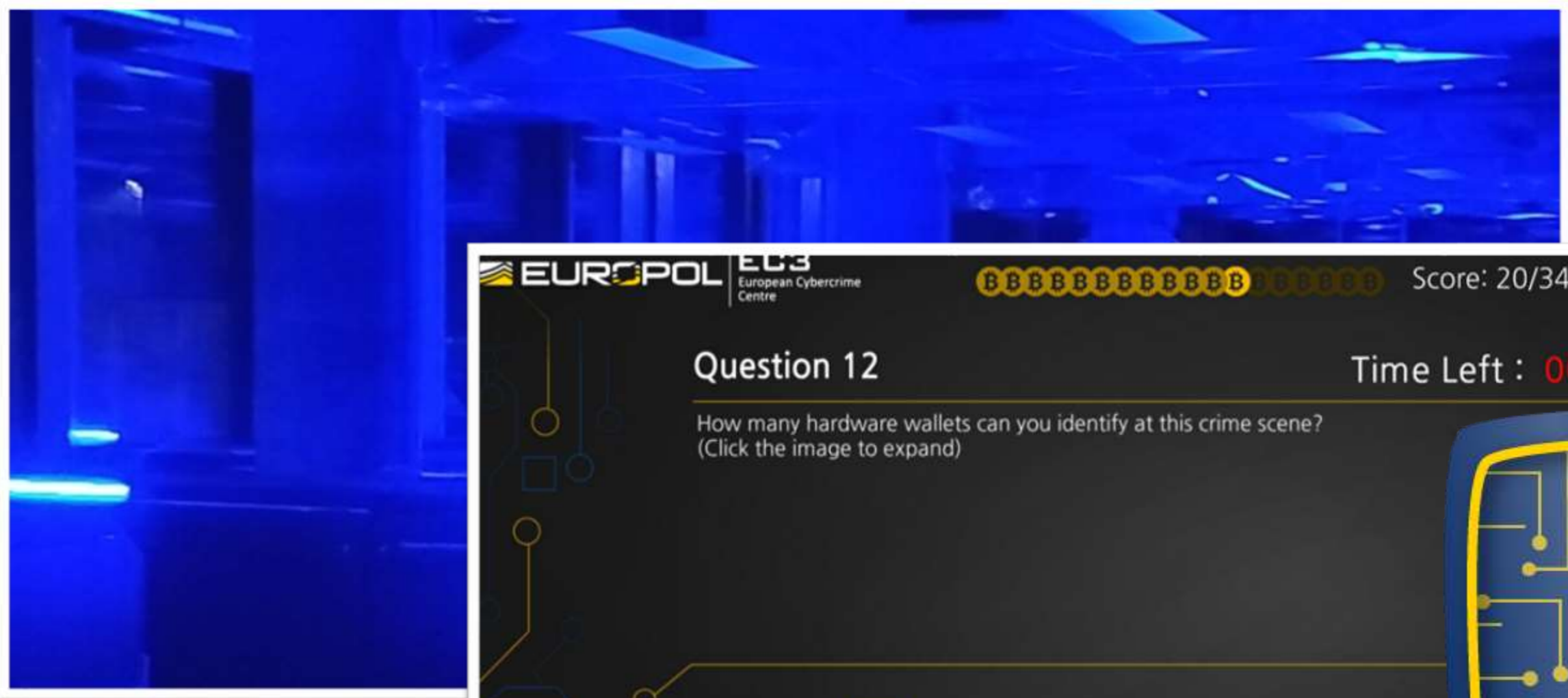
Question 12 Time Left : 00:54.75

How many hardware wallets can you identify at this crime scene?
(Click the image to expand)



1
3
4
5

Innovation as a necessity



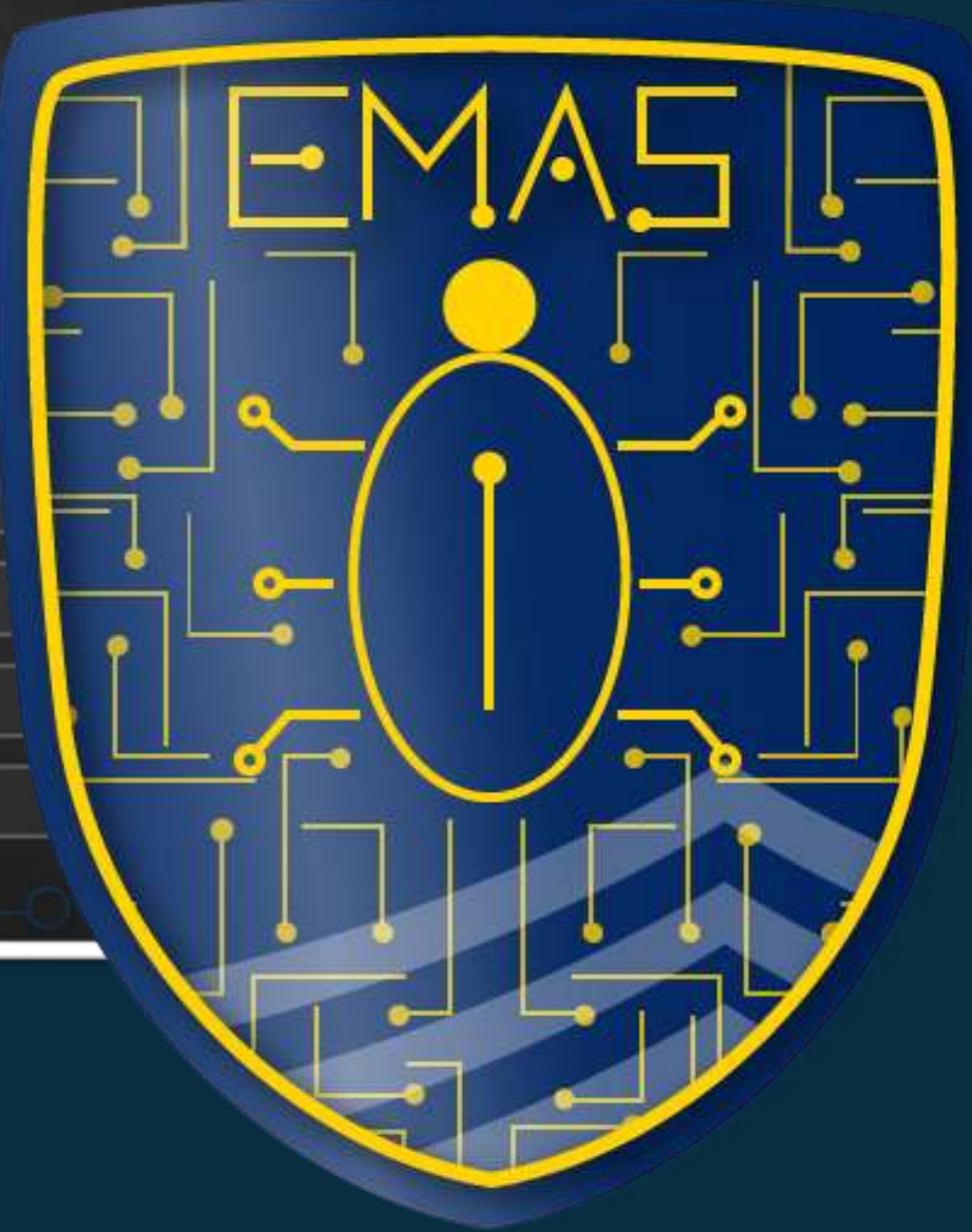
EUROPOL EC3 European Cybercrime Centre

Score: 20/34 01:05.24

Question 12 Time Left : 00:54.75

How many hardware wallets can you identify at this crime scene?
(Click the image to expand)

- 1
- 3
- 4
- 5



Operation DOBO

The image shows the exterior of a building, likely a Europol office, with the word 'EUROPOL' in large, illuminated, blue letters on the facade. The building has a modern, multi-story design with a grid of windows. The scene is captured from a low angle, looking up at the building against a clear sky. The overall color palette is dominated by blue and white tones.

EUROPOL

Op DOBO – Objectives and Results



- ▶ New approach developed by Norway to initiate Long-Distance Child Abuse (LDCA) investigations, leveraging previous and ongoing investigations.
- ▶ Enables investigators to discover networks of seller entities and to investigate persons behind those entities.
- ▶ One such network has been documented using information from two Norwegian and one Swedish investigation.
- ▶ Central person of this network and other accomplices were arrested in the Philippines in September 2022.

Op DOBO – Objectives and Results

- ▶ Planned to extend the investigation to currently unidentified European buyers and Philippine sellers, and ultimately to safeguard the victims involved.
- ▶ As a result of Op DOBO, Slovenia, Austria, France, the Netherlands, and the United Kingdom have started investigations on their own.
- ▶ Europol contributed since August 2021 with the analysis of financial transactions and crosschecks of potential buyers and sellers.
- ▶ Analysis reports have been disseminated to 10+ partner countries (EU and third-party countries).

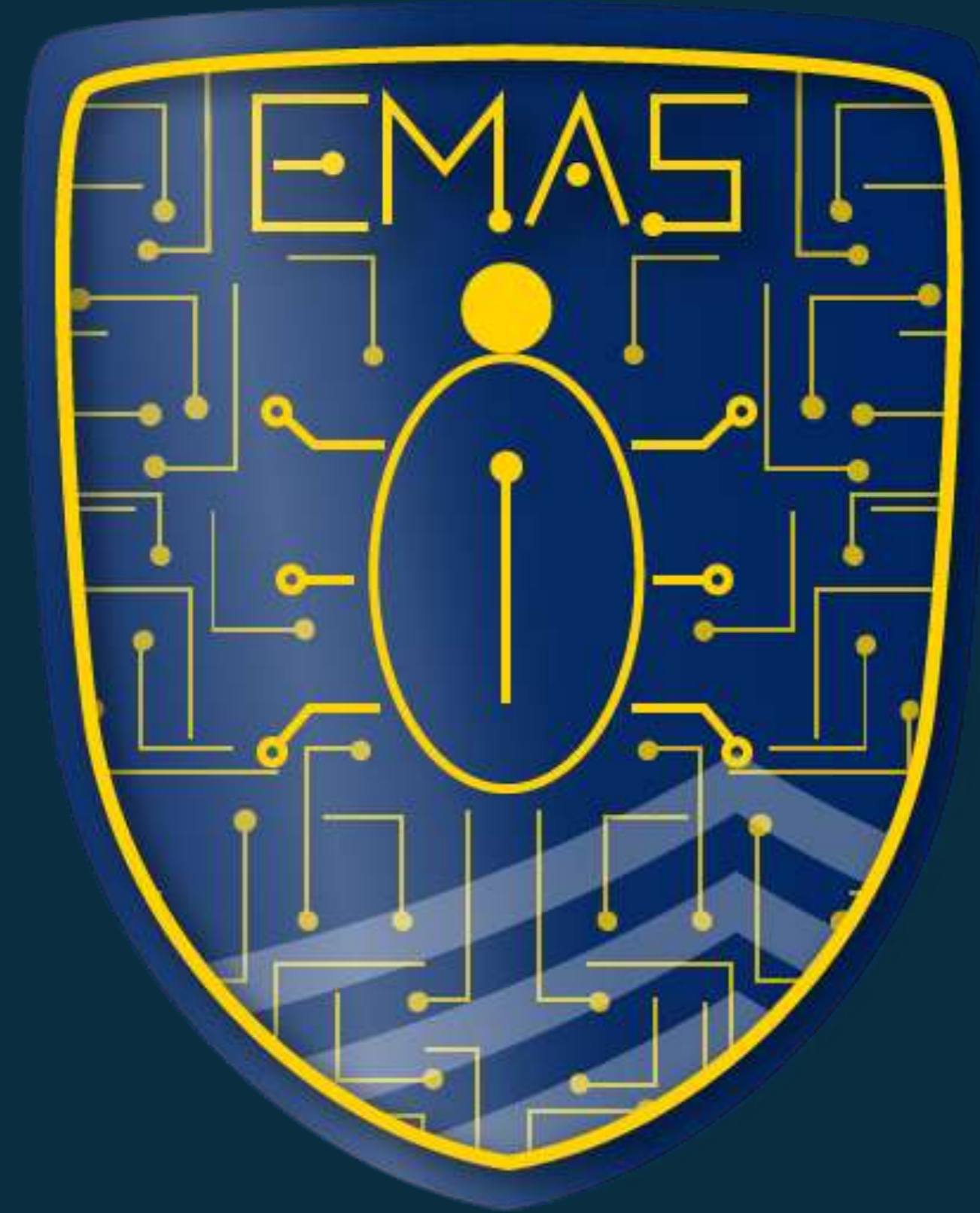


Operation GoldDust

The image shows the exterior of a building, likely a Europol office, with the word 'EUROPOL' in large, illuminated letters on the facade. The scene is captured in a low-angle shot, looking up at the building. The lighting is a cool, blueish-teal color, suggesting dusk or dawn. The building has several windows visible on the left side.

EUROPOL

Europol Malware Analysis Solution



- ▶ Malware samples were analysed through EMAS
- ▶ Confirmed to be Sodinokibi / REvil variants, different from Gandcrab
- ▶ Core similarities identified
- ▶ Results provided to J-CAT countries
- ▶ Network traffic analysed to identify potential C2 servers

Next Steps



**ARE YOU A VICTIM
OF RANSOMWARE?**

DON'T PAY



International Cooperation

“No one country can fight Cybercrime alone”

▶ International Partners

- Romania (Lead)
- France
- Germany
- UK Metropolitan Police
- US FBI
- Canada
- US Secret Service
- Switzerland
- Sweden

▶ International Partners

- South Korea
- Interpol
- Netherlands

▶ Europol – EC3

- J-CAT
- AP Cyborg
- EMAS
- Cyber Intel
- Cryptocurrency Tracing

▶ Industry Partners

- McAfee (NL)
- Bitdefender (RO)
- KPN (NL)

▶ Assistance

- Ukraine
- Russia

Q&A