Version 15 October 2020

**Introductory Judicial Training on Cybercrime and Electronic Evidence**

**Post-Survey**

# Post-Survey – Questions

Please reply to the following questions (YES or NO):

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **YES** | **NO** |
| **1** | In a computer system, the CPU is where data are stored |  |  |
| **2** | Microsoft Office is an operating system |  |  |
| **3** | 213.43.112.45 is an IP address |  |  |
| **4** | An e-mail header can provide evidence of the origin of the message |  |  |
| **5** | Social media are used by more than 50% of the world population |  |  |
| **6** | The Budapest Convention is the only international treaty on cybercrime and electronic evidence |  |  |
| **7** | 40% of countries worldwide are either parties, or signatories or invited to accede to the Budapest Convention |  |  |
| **8** | The DDoS is a malicious software used to steal digital identities |  |  |
| **9** | A botnet is a network of compromised computers used for malicious purposes |  |  |
| **10** | A defacement is an attack on a website that changes the visual appearance of the site or of a webpage |  |  |
| **11** | The Budapest Convention criminalizes the online sexual exploitation and abuse of children |  |  |
| **12** | Online defamation is a criminal offence under the Budapest Convention |  |  |
| **13** | Skimming and shimming are two forms of malware |  |  |
| **14** | All the services provided on the Darkweb are illegal |  |  |
| **15** | Electronic evidence is any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings |  |  |
| **16** | Manipulating electronic evidence is more difficult than tampering with physical evidence |  |  |
| **17** | All electronic devices can potentially be sources of electronic evidence |  |  |
| **18** | The Budapest Convention provides tools to deal with electronic evidence |  |  |
| **19** | The Budapest Convention doesn’t include provisions to address international criminal justice cooperation in the field of cybercrime |  |  |
| **20** | The Second Additional Protocol will replace the Budapest Convention |  |  |
| **21** | In the framework of the Budapest Convention, Facebook is to be considered a service provider |  |  |
| **22** | Traffic data are relevant to the content of the communication |  |  |
| **23** | Interception of content data is not allowed during a criminal investigation |  |  |
| **24** | Cybercrime is always committed within the victim’s country |  |  |
| **25** | The 24/7 Point of Contact is mandatorily established in all countries that are Parties to the Budapest Convention |  |  |