Version 15 Octobre 2020

**Introduction à la formation judiciaire sur la cybercriminalité et la preuve électronique**

**Pre-Enquête**

# Contexte et justification

Le cours d’introduction à la formation judiciaire sur la cybercriminalité et la preuve électronique vise à donner les bases mêmes de la connaissance dans ce domaine pour les juges, les magistrats et les procureurs.

The course provides basic concepts on cybercrime and other related topics, such as the international legal framework, the challenges related to electronic evidence and international cooperation, the main elements to conduct a cybercrime investigation. The course is aimed at preparing the ground for more specific courses of the Council of Europe that will follow, such as the Advanced Judicial Course or the Specialized Courses.

Le cours fournit des concepts de base sur la cybercriminalité et d’autres sujets connexes, tels que le cadre juridique international, les défis liés à la preuve électronique et la coopération internationale, les principaux éléments pour mener une enquête sur la cybercriminalité. Le cours vise à préparer le terrain pour des cours plus spécifiques du Conseil de l’Europe qui suivront, tels que le Cours Judiciaire Avancé ou les Cours Spécialisés.

Un formulaire de questions est remis aux participants au début du cours, afin qu’ils aient la possibilité d’écrire leurs questions et préoccupations auxquelles les experts répondront plus tard au cours.

Cela va de pair avec l’étude préliminaire qui se présente sous la forme d’un pré-test (chronométré à 10 minutes) qui donne aux formateurs un aperçu de la mesure dans laquelle les connaissances des participants vont et donne aux formateurs une idée de la façon dont ils vont présenter leur sujet donné.

# Formulaire de questions

Veuillez inscrire dans l’espace ci-dessous jusqu’à trois questions que vous aimeriez que les formateurs abordent pendant le cours.

**Question 1**

**Question 2**

**Question 3**

# Pré-Enquête – Questions

Veuillez répondre aux questions suivantes (OUI ou NON):

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **OUI** | **NON** |
| **1** | Dans un système informatique, l’UCT est l’endroit où les données sont stockées |  |  |
| **2** | Microsoft Office est un système d’exploitation |  |  |
| **3** | 213.43.112.45 est une adresse IP |  |  |
| **4** | Un en-tête de courriel peut fournir une preuve de l’origine du message |  |  |
| **5** | Les médias sociaux sont utilisés par plus de 50 % de la population mondiale |  |  |
| **6** | La Convention de Budapest est le seul traité international sur la cybercriminalité et les preuves électroniques |  |  |
| **7** | 40% des pays dans le monde sont soit parties, soit signataires ou invités à adhérer à la Convention de Budapest |  |  |
| **8** | Le DDoS (attaque par déni de service) est un logiciel malveillant utilisé pour voler des identités numériques |  |  |
| **9** | Un Botnet est un réseau d’ordinateurs compromis utilisé à des fins malveillantes |  |  |
| **10** | Un défacement est une attaque contre un site Web qui modifie l’apparence visuelle du site ou d’une page Web. |  |  |
| **11** | La Convention de Budapest criminalise l’exploitation et les abus sexuels en ligne des enfants |  |  |
| **12** | La diffamation en ligne est une infraction criminelle en vertu de la Convention de Budapest |  |  |
| **13** | Skimming et shimming sont deux formes de logiciels malveillants |  |  |
| **14** | Tous les services fournis sur le Darkweb sont illégaux |  |  |
| **15** | La preuve électronique désigne toute information générée, stockée ou transmise sous forme numérique qui pourrait être plus tard nécessaire pour prouver ou réfuter un fait contesté dans une procédure judiciaire. |  |  |
| **16** | Il est plus difficile de manipuler les preuves électroniques que d’altérer les preuves physiques. |  |  |
| **17** | Tous les appareils électroniques peuvent potentiellement être des sources de preuves électroniques |  |  |
| **18** | La Convention de Budapest fournit des outils pour traiter de la preuve électronique |  |  |
| **19** | La Convention de Budapest ne contient pas de dispositions relatives à la coopération internationale en matière de justice pénale dans le domaine de la cybercriminalité |  |  |
| **20** | Le Deuxième Protocole additionnel remplacera la Convention de Budapest |  |  |
| **21** | Dans le cadre de la Convention de Budapest, Facebook doit être considéré comme un fournisseur de services |  |  |
| **22** | Les données de trafic sont pertinentes pour le contenu de la communication |  |  |
| **23** | L’interception des données de contenu n’est pas autorisée pendant une enquête criminelle |  |  |
| **24** | La cybercriminalité est toujours commise dans le pays de la victime |  |  |
| **25** | Le Point de contact 24/7 est établi obligatoirement dans tous les pays qui sont Parties à la Convention de Budapest |  |  |

# Prê-Enquête– Réponses

Veuillez répondre aux questions suivantes (OUI ou NON):

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **OUI** | **NON** |
| **1** | Dans un système informatique, l’UCT est l’endroit où les données sont stockées |  | X |
| **2** | Microsoft Office est un système d’exploitation |  | X |
| **3** | 213.43.112.45 est une adresse IP | X |  |
| **4** | Un en-tête de courriel peut fournir une preuve de l’origine du message | X |  |
| **5** | Les médias sociaux sont utilisés par plus de 50 % de la population mondiale | X |  |
| **6** | La Convention de Budapest est le seul traité international sur la cybercriminalité et les preuves électroniques | X |  |
| **7** | 40% des pays dans le monde sont soit parties, soit signataires ou invités à adhérer à la Convention de Budapest | X |  |
| **8** | Le DDoS (attaque par déni de service) est un logiciel malveillant utilisé pour voler des identités numériques |  | X |
| **9** | Un Botnet est un réseau d’ordinateurs compromis utilisé à des fins malveillantes | X |  |
| **10** | Un défacement est une attaque contre un site Web qui modifie l’apparence visuelle du site ou d’une page Web. | X |  |
| **11** | La Convention de Budapest criminalise l’exploitation et les abus sexuels en ligne des enfants | X |  |
| **12** | La diffamation en ligne est une infraction criminelle en vertu de la Convention de Budapest |  | X |
| **13** | Skimming et shimming sont deux formes de logiciels malveillants |  | X |
| **14** | Tous les services fournis sur le Darkweb sont illégaux |  | X |
| **15** | La preuve électronique désigne toute information générée, stockée ou transmise sous forme numérique qui pourrait être plus tard nécessaire pour prouver ou réfuter un fait contesté dans une procédure judiciaire. | X |  |
| **16** | Il est plus difficile de manipuler les preuves électroniques que d’altérer les preuves physiques. |  | X |
| **17** | Tous les appareils électroniques peuvent potentiellement être des sources de preuves électroniques | X |  |
| **18** | La Convention de Budapest fournit des outils pour traiter de la preuve électronique | X |  |
| **19** | La Convention de Budapest ne contient pas de dispositions relatives à la coopération internationale en matière de justice pénale dans le domaine de la cybercriminalité |  | X |
| **20** | Le Deuxième Protocole additionnel remplacera la Convention de Budapest |  | X |
| **21** | Dans le cadre de la Convention de Budapest, Facebook doit être considéré comme un fournisseur de services | X |  |
| **22** | Les données de trafic sont pertinentes pour le contenu de la communication |  | X |
| **23** | L’interception des données de contenu n’est pas autorisée pendant une enquête criminelle |  | X |
| **24** | La cybercriminalité est toujours commise dans le pays de la victime |  | X |
| **25** | Le Point de contact 24/7 est établi obligatoirement dans tous les pays qui sont Parties à la Convention de Budapest | X |  |