

**Sujet d'épreuves de la 48<sup>e</sup> Compétition Nationale  
des Métiers**

# **MÉTIER N°54 CYBERSÉCURITÉ**

## **FORENSIC MODULE D ET E**

# TABLE DES MATIERES

<b>TABLE DES MATIERES</b> .....	<b>2</b>
<b>EXPLICATION DU SUJET</b> .....	<b>3</b>
<i>INTRODUCTION</i> .....	<i>3</i>
<i>CONSEILS ET CONSIGNES DANS LE CADRE DE LA REALISATION DU SUJET</i> .....	<i>3</i>
<b>DESCRIPTION DU SUJET</b> .....	<b>4</b>
<i>MODULE D – Analyse Forensique (Ios)</i> .....	<i>4</i>
<i>MODULE E – Analyse Forensique (wINDOWS)</i> .....	<i>4</i>

# EXPLICATION DU SUJET

DUREE TOTALE DE L'ÉPREUVE	4 heures
DIFFUSION DU SUJET	<i>Découvert le jour de la compétition</i>

## PREAMBULE

### INTRODUCTION

La société fictive Wonder Pay, spécialisée dans le paiement numérique et les wallets crypto, s'apprête à lancer ses services sur les marchés.

Peu après le licenciement d'un employé, des anomalies ont été détectées par les équipes de monitoring. Fort heureusement, l'entreprise n'a pas encore effacé le téléphone professionnel de cet employé.

Vous êtes mandaté pour mener une analyse approfondie et déterminer la nature exacte de l'incident.

### CONSEILS ET CONSIGNES DANS LE CADRE DE LA REALISATION DU SUJET

En tant qu'équipe prétendante au titre de champion régional dans votre métier ainsi qu'à la représentation de votre région aux prochaines finales nationales, votre victoire passera inéluctablement par la compréhension des éléments suivants.

Le sujet est rédigé de sorte que les réponses attendues soient sous forme de 'flag' à soumettre directement sur la plateforme dédiées, c'est-à-dire que les réponses seront les mêmes pour tout le monde et aucune variation ne sera possible.

L'objectif ici n'est pas de vous embêter dans votre épreuve mais de vous préparer au mieux à la compétition internationale. Si vous pensez ne pas pouvoir finaliser le sujet, concentrez-vous sur ce que vous maîtrisez. Votre objectif pour la compétition est de capitaliser un maximum de points. Concentrez-vous sur votre réalisation et non celle des autres. On peut parfois être tenté de regarder l'état d'avancement des autres compétiteurs, mais sachez que dans notre métier, dû à son manque de concret visuel, les personnes qui semblent les plus avancées ne sont pas forcément celles qui capitaliseront le maximum de points. Enfin, n'oubliez pas que vous formez une équipe, alors ne vous précipitez pas. Prenez le temps de lire le sujet une première fois dans son intégralité, communiquez avec votre co-équipier et partagez-vous les tâches, optimisez votre temps.

# DESCRIPTION DU SUJET

Cette partie comprends deux modules à réaliser d'une traite en 4 heures :

- Module D – Analyse Forensique Mobile (iOS)
- Module E - Analyse Forensique (Windows)

## MODULE D – ANALYSE FORENSIQUE (IOS)

L'objectif de ce module est de mettre à l'épreuve vos compétences d'investigation numérique sur l'environnement iOS.

Dans ce cadre, votre mission consistera à mener une investigation forensique complète afin de retracer les actions de l'attaquant et de collecter des preuves exploitables.

Les éléments à analyser sont les suivants :

- une image disque du téléphone iOS

## MODULE E – ANALYSE FORENSIQUE (WINDOWS)

L'objectif de ce module est de mettre à l'épreuve vos compétences d'investigation numérique sur l'environnement Windows.

Dans ce cadre, votre mission consistera à mener une investigation forensique complète afin d'identifier les vecteurs d'intrusion, de retracer les actions de l'attaquant et de collecter des preuves exploitables.

Les éléments à analyser sont les suivants :

- un corpus d'e-mails
- un dump mémoire d'un poste Windows