Réseau des Centres d'Excellence pour l'Afrique

Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC)

Atelier de formation en présentiel sur

Analyse et Investigation de la menace Digital

Du 25 au 29 Juin 2018

PRESENTATION DE LA FORMATION

DESCRIPTION DU COURS

Titre	Analyse et Investigation de la menace Digital
Méthode d'enseignement	En présentiel
Objectifs	Cet atelier de formation donnera les outils nécessaires aux participants afin de mener à bien des investigations sur des traces réseaux dans un contexte de réponse à incident ou d'inforensique, depuis la collecte des données jusqu'à leur analyse et interprétation. Cette formation s'appuie sur les points importants des systèmes Windows que tout investigateur en inforensique se doit de connaître. **Prérequis :** Une connaissance de base de la sécurité des systèmes d'information.
Date	Du 25 au 29 Juin 2018
Durée	5 jours
Date limite d'enregistrement	18 Juin 2018
Frais de formation	500 000 F CFA
Code du cours	**18WS20727AFR-F**

RESULTATS ATTENDUS

Aux termes du séminaire, les auditeurs seront capable de :

- expliquer les fondements de l'analyse inforensique réseau ;
- appréhender les méthodes et les outils d'analyse ;
- mener une investigation de bout en bout.

PUBLIC CIBLE

Cet atelier de formation s'adresse principalement aux profils suivants :

- consultants en sécurité ;
- responsable des Systèmes d'Information ;
- analystes réseau ;
- professionnel de l'IT souhaitant apprendre les concepts vitaux pour mener une investigation inforensique.

FORMATEUR

NOM DU FORMATEUR	CONTACTS
A communiquer ultérieurement	

EVALUATION

Evaluation formative.

AGENDA

Date du 1er jour	Heure de début, Heure de fin	Sujets/Activités
25/06/2018	08:30 - 09:00	Accueil et enregistrement des participants.
	09:00 - 09:30	Cérémonie d'ouverture
	Session du matin (09:30 - 12:45)	**Les fondamentaux de l'inforensique** ▪ Objectif de l'inforensique. ▪ Présentation des cas d'inforensique les plus communs. ▪ Types d'informations stockées électroniquement. ▪ Localisation des preuves électroniquement stockées (ElectronicallyStored Evidence : ESI). ▪ Acquisition et analyse des données volatiles. ▪ Les systèmes de fichiers : généralités. ▪ Rapport de preuves et présentations de celles-ci. ▪ Methodologie inforensique.
	Session de l'après-midi (14:00 - 17:15)	**Acquisition et analyse** ▪ Acquisition des preuves : généralités. ▪ Conservation des preuves. ▪ Méthodes d'acquisition. ▪ Kit de survie de l'expert inforensique. ▪ Outils et technique d'acquisition d'images disques complètes. ▪ Acquisition de données sur le réseau.

		▪ Les outils inforensique graphiques. ▪ Étapes usuelles et outils inforensiques associés. ▪ Acquisition des fichiers supprimés.
Date du 2ième jour	**Heure de début, Heure de fin**	**Sujets/Activités**
26/06/2018	Session du matin (09:00 – 12:15)	**<u>Inforensique Windows : Analyse des Emails et de la base de registres</u> (1)** ▪ Inforensique des Emails. ▪ Emails Microsoft Outlook/Outlook Express/Windows. ▪ Emails des WebMails. ▪ Microsoft Exchange. ▪ Lotus Notes.
	Session de l'après-midi (13:45 - 17:00)	**<u>Inforensique Windows : Analyse des Emails et de la base de registres</u> (2)** ▪ Inforensique en profondeur de la base de registres. ▪ Authentification. ▪ Informations système. ▪ Preuves diverses. ▪ Historique de recherche sous XP et Win7.
Date du 3ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
27/06/2018	Session du matin (09:00 – 12:15)	**<u>Inforensique Windows : Analyse des Emails et de la base de registres</u> (3)** ▪ Accès aux URLs. ▪ Documents récents. ▪ Boites de dialogue 'Ouvrir / Sauvegarder / Exécuter. ▪ Historique de l'exécution d'application. ▪ Éditeur/Création/Version.
	Session de l'après-midi (13:45 - 17:00)	**<u>Inforensique Windows : Analyse des Emails et de la base de registres</u> (4)** ▪ Numéro de série unique. ▪ Lettre du dernier disque. ▪ Nom des volumes. ▪ USB. ▪ Regripper, d'Harlan Carvey. ▪ Registry Viewer, d'Access Data.
Date du 4ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
28/06/2018	Session du matin (09:00 – 12:15)	**<u>Inforensique Windows : Analyse des artefactes et fichiers de journalisation</u>** ▪ Analyse mémoire, mémoire virtuelle et espace non alloué. ▪ Conversations Facebook live, MSN Messenger, Yahoo, AIM, GoogleTalk.

		▪ URLs d'IE8 InPrivate/Recovery. ▪ WebMails de Yahoo, Hotmail, Gmail. ▪ Inforensique des fichiers contenant des preuves sensibles. ▪ Analyse inforensique des journaux d'évènements de Windows.
	Session de l'après-midi (13:45 - 17:00)	**Inforensique Windows : Inforensique du navigateur web** ▪ Inforensique des navigateurs web. ▪ Internet Explorer. ▪ Localisation des fichiers clés de l'inforensique FF2 and FF3. ▪ Web Historian, de Mandiant. ▪ FTK, de FTK. ▪ FoxAnalysis.
Date du 5ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
29/06/2018	Session du matin (09:00 – 12:15)	**Exercices pratiques** Une mise situation d'analyse inforensique clôturera cet atelier de formation. Ce cas pratique final permettant aux participants d'utiliser l'ensemble des outils et méthodes découverts tout au long de la formation afin de construire un rapport inforensique sur un cas d'étude spécialement mis en place.
	Session de l'après-midi (12:15 - 13:30)	Evaluation du séminaire, remise des attestations et clôture de l'atelier.

METHODOLOGIE

Exposés, travaux pratiques et échanges interactifs.

COORDINATION DE LA FORMATION

Point focal ESATIC: Nom : M. Kossonou rodolphe Service de la formation continue,ESATIC Tel. : + 225 21 218 100 Fax : + 225 21 259 656 Email : rodolphe.kossonou@esatic.ci	**Coordinateur AFR UIT:** Nom : Mme Oumou Niang UIT Bureau de Dakar Tel: +221 33 859 70 10 Fax: +221 33 868 63 86 E-mail : oumou.niang@itu.int

INSCRIPTION ET PAYEMENT

Inscription sur le Site d'ITU Académie:
Veuillez noter qu'afin de pouvoir vous inscrire à un cours vous devez au préalable créer un compte sur le portail web d'ITU Académie à l'adresse suivante :
https://academy.itu.int/index.php?option=com_hikashop&view=user&layout=form&Itemid=559&lang=en

Inscription à une formation:

L'inscription et le paiement doivent être fait en ligne sur : https://academy.itu.int/index.php?option=com_joomdle&view=coursecategoryextended&cat_id=:&course_id=1248:analyse-et-investigation-de-la-menace-digital&Itemid=476&lang=en

Si vous avez déjà un compte ou que vous créez un nouveau compte, vous pouvez vous inscrire en ligne pour la formation à l'adresse ci-dessus.

Vous pouvez également vous inscrire en suivant les étapes ci-dessous :

- Allez sur la page d'accueil du site web ITU Académie
- En haut à l'angle, vous trouverez l'option recherche (option search)
- Tapez le nom du cours dans l'espace réservez à cet effet et cliquer sur recherche
- Lorsque le cours apparait, sélectionnez ''book this course' 'et suivez les instructions pour vous inscrire

Paiement

1. Paiement en ligne

Les frais de participation à cette formation sont de **912 USD**. Ce montant prend en compte l'inscription, la documentation, la pause-café et le déjeuner.Il est recommandé de procéder au paiement via le système de paiement en ligne en utilisant le même lien que celui de l'inscription en ligne ci-dessus mentionné.

2. Paiement par virement bancaire

Lorsqu' il n'est pas possible de procéder à un paiement en ligne, un virement bancaire peut être fait sur le compte bancaire de l'IUT indique ci-dessous. Dans ce cas, le participant devra sélectionner, l'option de paiement ''offline'' utilisant le lien ci-dessus mentionné.

Le participant sera ainsi redirigé vers une page ou une facture lui sera émise. Sur cette base, le participant pourra transférer les frais de formation sur le compte bancaire de l'UIT. Une fois le transfert fait, il est IMPERATIF que l'appliquant soumette la preuve de paiement sur le site de l'ITU académie, sous l'onglet ''Offline Invoices'' dans le menu principal. Il est conseillé au participant de notifier la division HCB à l'adresse hcbmail@itu.int après qu'il est soumis sa preuve de paiement en ligne.

La non-soumission des documents mentionnés ci-dessus peut entrainer l'annulation de l'inscription.

Coordonnées bancaires de l'UIT:

Nom et adresse de la Banque :	UBS SWITZERLAND AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Bénéficiaire:	Union Internationale des Télécommunications
Numéro de Compte :	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Montant :	912 USD
Référence du paiement :	CoE-AFR 20727 P.40590.1.04

1. Autres méthodes de paiement

Si pour des raisons de régulations nationales il y a des restrictions ne permettant pas d'utiliser les options de paiement 1 et 2 ci-dessus, veuillez contacter le coordinateur de l'IUT pour plus d'assistance.