TURKISH NATIONAL POLICE

EMNİYET GENEL MÜDÜRLÜĞÜ

INTERNATIONAL TRAINING CATALOGUE

ULUSLARARASI EĞİTİM KATALOĞU

LE CATALOGUE DE FORMATION INTERNATIONALE

МЕЖДУНАРОДНЫЙ УЧЕБНЫЙ КАТАЛОГ

كتالوج التدريب الدولي

DEPARTMENT OF CYBERCRIME
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

2023

DEPARTMENT OF CYBERCRIME

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

ULUSLARARASI EĞİTİM KATALOĞU

INTERNATIONAL TRAINING CATALOGUE

LE CATALOGUE DE FORMATION INTERNATIONALE

МЕЖДУНАРОДНЫЙ УЧЕБНЫЙ КАТАЛОГ

كتالوج التدريب الدولي

2023

EXPLANATIONS
AÇIKLAMALAR

TRAINING FEE KURS ÜCRETLERİ

The fees of Trainings offered to the police organizations of foreign countries are decided through bilateral agreements. Trainings that are specified in these agreements as free do not incur any fees. However, information on payment and other relevant details about the training can be obtained from the e-mail adress below.

Yabancı Ülke Polis Teşkilatlarına verilebilecek olan eğitimler ikili anlaşmalar çerçevesinde belirlenmektedir. Söz konusu anlaşmalarda eğitimlerin ücretsiz olacağının belirtilmesi şartı ile eğitimler ücretsiz olarak düzenlenebilecektir.

TRAINING CLASSES EĞİTİM SINIFLARI

The classes for trainings will be available to accommodate 20–25 participants to enable a high-quality education. The class designs will be U-shape to allow participants to focus better on training. Classrooms will be equipped with the required technological equipment.

Eğitimlerde kullanılacak sınıflar kaliteli bir eğitime olanak sağlayacak şekilde 20-25 kişiliktir. Sınıflar, öğrenen merkezli eğitime imkan sağlayacak şekilde "U" düzeninde dizayn edilmiş ve her türlü teknolojik ekipmanla desteklenmiştir.

HEALTH AND SAFETY SAĞLIK VE GÜVENLİK

Each participant has to obey the safety rules to be defined by the training centre. The participants are expected to have health insurance prior to their arrival in Turkey.

Her bir katılımcı eğitim merkezinin belirlediği güvenlik kurallarına uymak zorundadır. Katılımcıların Türkiye'ye gelmeden önce sağlık sigortalarını yapmaları beklenir.

TRAINING EĞİTİM

The training centre reserves its right not to issue the certificate due to failure, lack of attendance or misbehaviors as well as to reject the participant/trainee and send him/her back.

Eğitim merkezi başarısızlık, devamsızlık veya uygunsuz davranıştan dolayı sertifika vermeme veya katılımcıyı/kursiyeri geri gönderme hakkını saklı tutar.

CONTACT DETAILS FOR TRAINING REQUESTS EĞİTİM TALEPLERİ İÇİN İLETİŞİM BİLGİLERİ

In order to benefit from training programs in the Catalog, request may be submitted to the respective Turkish Embassies. If there is no Turkish Embassy in your country, request may be submitted to the e-mail address below.

Katalogdaki eğitim programlarından faydalanabilmek için taleplerinizi ülkenizdeki Türkiye Cumhuriyeti Büyük Elçiliklerine iletebilirsiniz. Ülkenizde Türkiye Cumhuriyeti Büyük Elçiliği olmaması halinde ise taleplerinizi aşağıdaki e-posta adresine iletebilirsiniz.

disiliskilerdb@egm.gov.tr

İÇİNDEKİLER / CONTENTS

DİJİTAL DELİLLERE İLK MÜDAHALE VE İMAJ ALMA EĞİTİMİ
TRAINING ON INITIAL INTERVENTION IN DIGITAL EVIDENCE AND IMAGE CAPTURING

AMAÇ

Siber Suçlar birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- Dijital deliller ile ilgili hukuki tanım ve düzenlemeleri söyleyebilecektir.
- Dijital delillere ilk müdahale esaslarını öğrenecektir.

İÇERİK

- Hedefler,Teknik Boyut,Hukuki Boyut
- TD2 Tanıtımı ve Uygulaması
- Write Blocker Ultra Kit
- Helix, FTK İmager, Mac OSX İmaj alma
- Genel Uygulama

KATILIMCILARDA ARANAN ŞARTLAR

- Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Her personel için bilgisayar, İmaj alma yazılımları ve cihazları

PURPOSE

The aim of this training is to improve the knowledge and skills of the personnel working in cybercrime units and to ensure that they act within the framework of the legal rules related to the ethical principles.

TARGET BEHAVIORS

At the end of this course, each personnel:
- will be able to tell the legal definitions and regulations related to digital evidence.
- will learn the first intervention principles of digital evidence.

CONTENT

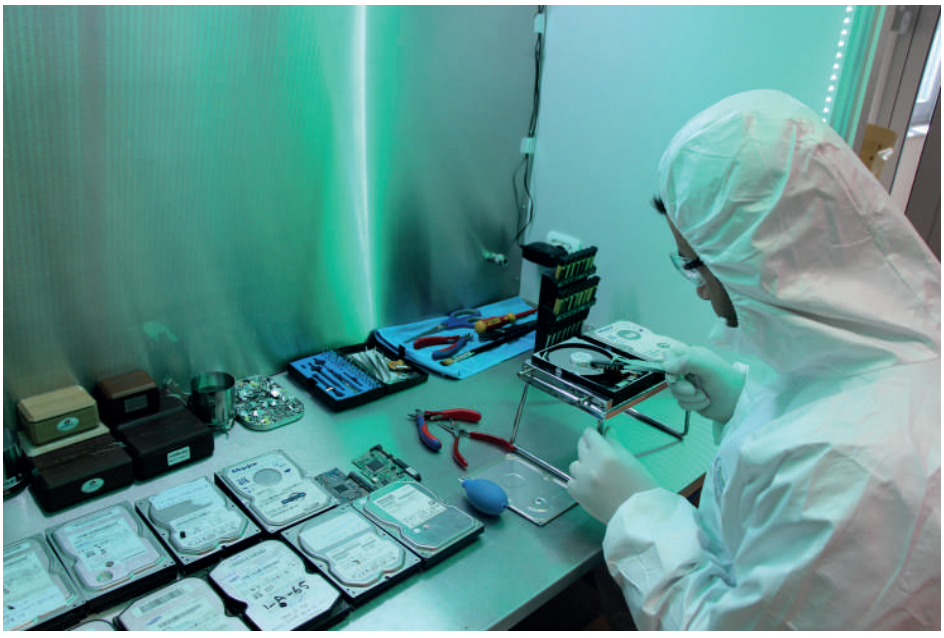
- Objectives, Technical Dimension, Legal Dimension
- TD2 Introduction and Application
- Write Blocker Ultra Kit
- Helix, FTK Imager, Mac OSX Taking Image
- General Application

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in the Cyber Crime Unit.

TOOLS AND MATERIALS

- Computer for every personnel, Image capturing software and devices



İş Günü / Saat Workdays / Hour: 5/30

Eğitici Sayısı Number of Trainers: 3

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION SUR LA PREMIÈRE INTERVENTION SUR PREUVES NUMÉRIQUES ET LA PRISE D'IMAGE
ОБУЧЕНИЕ НАЧАЛЬНОМУ ВМЕШАТЕЛЬСТВУ В ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА И ПРИЕМ ИЗОБРАЖЕНИЙ
التدخل الأولي للأدلة الرقمية والتدريب على أخذ الصور

NO
18-01

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel des unités de lutte contre la cybercriminalité et d'assurer qu'ils peuvent agissent dans le cadre des règles juridiques relatives aux principes éthiques.

RESULTATS EXIGES

A la fin de ce cours,
- On sera capable de dire les définitions légales et les réglementations relatives aux preuves numériques.
- On apprendra les principes de première intervention des preuves numériques

CONTENU

- Objectifs, la dimension technique, la dimension légale
- Introduction et l'application au niveau de TD2
- Kit d'écriture Blocker Ultra
- Acquisition d'images Helix, FTK Image, Mac OSX
- Pratique générale

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans les unités de lutte contre les cybercriminalités

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur pour chaque personnel, logiciel de récupération d'images et périphériques

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях по борьбе с киберпреступностью, и обеспечивать, чтобы они действовали в рамках правовых норм, связанных с этическими принципами.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый сотрудник:
- сможет освоить юридические определения и положения, связанные с цифровыми уликами.
- изучат основы вмешательства в электронные доказательства

СОДЕРЖАНИЕ

- Цели, техническое измерение, юридическое измерение
- Введение и применение TD2
- Блокировщик записи Ultra Kit
- Helix, FTK İmager, Mac OSX Image
- Общая практика

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Быть сотрудником подразделений по борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Для каждого сотрудника компьютер, программное обеспечение и устройства для изображений

الهدف

تطوير معرفة ومهارات العاملين في وحدات مكافحة الجرائم الإلكترونية والتأكد من أنهم يتصرفون في إطار القواعد القانونية المتعلقة بالمبادئ الأخلاقية.

السلوك المستهدف

سيتمكن المشاركون في نهاية هذه الدورة من:
- شرح التعريف القانوني واللوائح المتعلقة بالأدلة الرقمية.
- تعلم مبادئ التدخل الأولي للأدلة الرقمية.

المحتوى

- الأهداف ، البعد الفني ، البعد القانوني
- تعريف وتطبيق TD2
- Write Blocker Ultra Kit
- Helix, FTK İmager, Mac OSX
- Helix, صورةFTK ، الحصول على صورة Mac OSX
- التطبيق العام.

الشروط المطلوب توفرها في المشاركين

- ينبغي أن يكون موظفاً في قسم مكافحة جرائم الإنترنت.

الأدوات والتجهيزات اللازمة

- جهاز كمبيوتر برامج وأجهزة استيراد الصور

Jours / Heures
Рабочих Дней / Часов
المدة
5/30

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
3

Nombre de Coursiere
Количество Участников
عدد المتدربين
15-20

MOBİL CİHAZ İNCELEME EĞİTİMİ
MOBILE DEVICE INVESTIGATION TRAINING

AMAÇ

Siber Suçlar birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- Uluslararası düzeyde kabul edilen yazılımlar vasıtasıyla hukuka uygun olarak alınan adli kopyaların incelenmesini,
- Raporlamayı öğrenecektir.

İÇERİK

- Cep Telefonu Adli İncelemesine Giriş
- Mobil İnceleme Cihazlarının Tanıtımı
- UFED 4PC Kullanımı Mobil Cihazlardan İmaj Alma
- Cellebrite Physical Analyzer ile İnceleme
- XRY İnceleme Yazılımı ile İmaj Alma

KATILIMCILARDA ARANAN ŞARTLAR

- Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Her personel için bilgisayar, Cellebrite ve XRY inceleme kiti

PURPOSE

The aim of this training is to improve the knowledge and skills of the personnel working in cybercrime units and to ensure that they act within the framework of the legal rules related to the ethical principles.

TARGET BEHAVIORS

At the end of this course, each personnel will learn;
- Examination of forensic copies taken in accordance with the law through internationally accepted software,
- Reporting.

CONTENT

- Introduction to Cell Phone Forensic Review
- Introduction of Mobile Investigation Devices
- Using UFED 4PC Image Taking from Mobile Devices
- Investigation with Cellebrite Physical Analyzer
- Image Capture with XRY Review Software

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in the Cyber Crime Unit.

TOOLS AND MATERIALS

- Computer for each personnel, Cellebrite and XRY review kit

İş Günü / Saat Workdays / Hour: 5/30

Eğitici Sayısı Number of Trainers: 3

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION DE RECHERCHE DE L'ÉQUIPEMENT MOBILISE
ТРЕНИНГ ПО ИССЛЕДОВАНИЮ МОБИЛЬНЫХ УСТРОЙСТВ
التدريب على فحص الهاتف الخليوي

NO
18-02

OBJECTIFS

L'objectif de cette formation est d'améliorer les connaissances et les compétences du personnel des unités de lutte contre la cybercriminalité et ils vont examiner ces preuves conformément aux principes juridiques liés et principes éthiques.

RESULTATS EXIGES

À la fin de ce cours,
- Ils peuvent examiner des copies médico-légales prises avec des logiciels acceptés au niveau international conformément à la loi
- Ils peuvent apprendre à signaler ces documents.

CONTENU

- La formation d'introduction à l'examen judiciaire de téléphone portable
- La formation d'Introduction de dispositifs d'examen mobiles
- La formation d'utilisation de l'importation d'images UFED 4PC à partir de périphériques mobiles
- La formation d'examen avec l'analyseur physique avec logiciel Cellebrite
- La formation d'importation d'images avec logiciel XRY Review

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans les unités de lutte contre les cybercriminalités

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur pour chaque personnel, Kit de révision Cellebrite et XRY

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях по борьбе с киберпреступностью, и обеспечивать, чтобы они действовали в рамках правовых норм, связанных с этическими принципами.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый сотрудник:
- сможет изучать криминалистические копии, полученные в соответствии с законодательством с помощью международно признанного программного обеспечения,
- научится отчетности.

СОДЕРЖАНИЕ

- Введение в криминалистическую экспертизу мобильного телефона
- Описание мобильных контрольных устройств
- Получение изображений с мобильных устройств UFED 4PC
- Проверка с физическим анализатором Cellebrite
- Исследование изображений с помощью программного обеспечения XRY Review

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Быть сотрудником подразделений по борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Компьютер для каждого сотрудника, комплект Cellebrite и XRY

الهدف

تطوير معرفة ومهارات العاملين في وحدات مكافحة الجرائم الإلكترونية والتأكد من أنهم يتصرفون في إطار القواعد القانونية المتعلقة بالمبادئ الأخلاقية.

السلوك المستهدف

سيتمكن المشاركون في نهاية هذه الدورة من:
- مراجعة النسخ العدلية المأخوذة وفقًا للقانون من خلال برامج مقبولة دولياً ،
- تعلم كتابة التقرير ،

المحتوى

- مقدمة في الفحص العدلي للهاتف الخليوي
- التعرف على أجهزة فحص الهواتف الخليوية
- استيراد الصور من خلال أجهزة UFED 4PC
- الفحص من خلال Cellebrite
- استيراد الصور من خلال برنامج XRY

الشروط المطلوب توفرها في المشاركين

- ينبغي أن يكون موظفاً في قسم مكافحة جرائم الإنترنت.

الأدوات والتجهيزات اللازمة

- جهاز كمبيوتر. مجموعة فحصCellebrite و XRY.

Jours / Heures
Рабочих Дней / Часов
المدة
5/30

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
3

Nombre de Coursiere
Количество Участников
عدد المتدربين
15-20

SİBER SUÇLAR ARAŞTIRMA EĞİTİMİ
CYBERCRIME RESEARCH TRAINING

AMAÇ

Personellerin açık kaynak araştırmaları ve suç önleme konusunda bilgi ve becerilerinin artırılmasını sağlamak, hukuki kurallar çerçevesinde kalmak suretiyle farkındalık yaratmak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel;
- Bilişim yoluyla işlenen suçların çeşitlerini,
- Suç soruşturmalarında kullanılacak yöntemlerini,
- Suçun önlenmesine yönelik kullanılan teknikleri öğrenecek.

İÇERİK

- Güvenilir Sanal Devriye, Açık Kaynak Analiz Araçları DeepWeb / Dark Net
- Siber Suçlarla Mücadelede İstihbarat ve Bilgi Toplama Yöntemleri Sosyal Medya Araştırma
- Açık Kaynak Araştırma Raporlama,
- Örnek Vaka

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele Birimlerinde görevli olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Her personel için bilgisayar, internet ve polnet bağlantısı olan eğitim sınıfı bağlantısı

PURPOSE

The aim of this training is to increase the knowledge and skills of personnel about open source research and crime prevention and to raise awareness by staying within the framework of legal rules.

TARGET BEHAVIORS

At the end of this course, each personnel will learn;
- Types of crimes committed by informatics,
- Methods to be used in criminal investigations,
- Techniques used to prevent crime

CONTENT

- Reliable Virtual Patrol, Open Source Analysis Tools DeepWeb / Dark Net
- Intelligence and Information Gathering Methods in Fighting Cybercrime Social Media Research
- Open Source Research Reporting,
- Sample Case

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in the Cyber Crime Unit.

TOOLS AND MATERIALS

- Training classroom with computer, internet and Polnet connection for each personnel

İş Günü / Saat Workdays / Hour 5/34

Eğitici Sayısı Number of Trainers 6

Kursiyer Sayısı Number of Trainees 15-20

FORMATION SUR L'ÊNQUETE SUR LA CYBERCRIMINALITÉ
ТРЕНИНГ ПО ИССЛЕДОВАНИЮ КИБЕРПРЕСТУПНОСТИ
التدريب على البحث في الجرائم الإلكترونية

NO
18-03

OBJECTIFS

L'objectif de cette formation est d'accroître les connaissances et les compétences du personnel en matière de recherche en source ouverte et de prévention du crime et de sensibiliser le public en restant dans le cadre des règles juridiques

RESULTATS EXIGES

À la fin de cette formation les participants doivent être compétent sur ces sujets:

- Types de crimes commis par l'informatique,
- Méthodes à utiliser dans les enquêtes pénales
- Techniques utilisées pour prévenir le crime.

CONTENU

- Les méthodes de Virtual Patrol fiable, Outils d'analyse Open Source DeepWeb / Dark Net
- Les Méthodes de collecte de renseignements et d'informations pour lutter contre la cybercriminalité: recherche sur les médias sociaux
- Rapports de recherche de source ouvert
- La formation d'étude de cas

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans les unités de lutte contre les cybercriminalités

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Connexion de cours de formation avec connexion ordinateur, Internet et polnet pour chaque personnel

ЦЕЛЬ

Повысить знания и навыки персонала об исследованиях открытых источников и предупреждении преступности, а также обеспечить осведомленность, оставаясь в рамках правовых норм.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый сотрудник;

- будет знать виды преступлений, совершаемых информативным путем,
- будет знать методы, которые будут использоваться в уголовных расследованиях,
- изучит методы, используемые для предотвращения преступлений.

СОДЕРЖАНИЕ

- Надежный виртуальный патруль, инструменты анализа с открытым исходным кодом , глубинный веб / тёмная паутина
- Методы разведки и сбора информации в борьбе с киберпреступностью
- Отчет об исследованиях открытого исходного кода,
- Пример происшествия

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Компьютер для каждого сотрудника, учебный класс с подключением к интернету и polnet.

الهدف

زيادة معرفة ومهارات الموظفين في البحث ضمن المصادر المفتوحة ومنع الجرائم وزيادة الوعي من خلال البقاء في إطار القواعد القانونية.

السلوك المستهدف

سيتمكن المشاركون في نهاية هذه الدورة من:

- معرفة أنواع الجرائم المرتكبة من خلال الانترنت ،
- الطرق الواجب استخدامها في التحقيقات الجنائية ،
- تعلم التقنيات المستخدمة لمنع الجريمة.

المحتوى

- دورية افتراضية موثوقة ، أدوات تحليل المصادر المفتوحة DeepWeb / Dark Net
- الاستخبارات وأساليب جمع المعلومات في مجال مكافحة جرائم الإلكترونية. بحوث وسائل التواصل الاجتماعي.
- كتابة تقارير الأبحاث مفتوحة المصدر ،
- دراسة حالة

الشروط المطلوب توفرها في المشاركين

- أن يكون موظفاً في قسم مكافحة الجرائم الالكترونية

الأدوات والتجهيزات اللازمة

- جهاز كمبيوتر قاعة تدريس مجهزة بشبكة انترنت عالية التدفق

Jours / Heures
Рабочих Дней / Часов
المدة
5/34

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
6

Nombre de Coursiere
Количество Участников
عدد المتدربين
15-20

TEMEL ADLİ BİLİŞİM EĞİTİMİ
BASIC FORENSIC INFORMATICS TRAINING

AMAÇ

Siber Suçlar birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- Uluslararası düzeyde kabul edilen yazılımlar vasıtasıyla hukuka uygun olarak alınan adli kopyaların incelenmesini,
- Raporlamayı öğrenecektir.

İÇERİK

- Adli Bilişime Giriş. Dosyalama Sistemleri
- Sayı Dosyalama Sistemleri NTFS Dosya Yapısı
- Boot Süreci, Silinmiş Dosyalar Dosya zamanı, İmaj Türleri, Encase
- Veri Kurtarma, Windows Sitem ve Kullanıcı Klasörleri
- Filtreli Aramalar, İnternet Geçmişi,

KATILIMCILARDA ARANAN ŞARTLAR

- Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Her personel için bilgisayar, FTK ve Encase yazılımları

PURPOSE

The aim of this training is to improve the knowledge and skills of the personnel working in cybercrime units and to ensure that they act within the framework of the legal rules related to the ethical principles.

TARGET BEHAVIORS

At the end of this course, each personnel will learn;
- Examination of forensic copies taken in accordance with the law through internationally accepted software,
- Reporting.

CONTENT

- Introduction to Forensic Cognition Systems
- Numeric Filing Systems NTFS File Structure
- Boot Process, Deleted Files File time, Image Types, Encase
- Data Recovery, Windows System and User Folders
- Filtered Searches, Internet History,

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in the Cyber Crime Unit.

TOOLS AND MATERIALS

- Computer, FTK and Encase software for each personnel

İş Günü / Saat Workdays / Hour: 5/30

Eğitici Sayısı Number of Trainers: 3

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION DE BASE SUR L'INFORMATIQUE JUDICAIRE
БАЗОВЫЙ ТРЕНИНГ ПО КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКЕ
تدريب أساسي حول تكنولوجيا المعلومات العدلية

NO
18-05

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel des unités de lutte contre la cybercriminalité et d'assurer qu'ils agissent dans le cadre des règles juridiques relatives aux principes éthiques.

RESULTATS EXIGES

À la fin de ce cours, chaque participants, ils doivent être compétent sur ces sujets:

- Examen des copies médico-légales prises conformément à la loi avec des logiciels acceptés au niveau international
- Préparation du rapport

CONTENU

Le contenu de ces cours existe ce qui est ceci :

- l'Introduction à l'informatique-légale
- Systèmes de classement des numéros et la structure des fichiers
- Le Processus d'amorçage, fichiers supprimés, types d'image, encas
- La Récupération de données, Windows Mon site et dossiers d'utilisateur
- l'Appels filtrés, histoire d'Internet

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans les unités de lutte contre les cybercriminalités

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Logiciels informatiques, FTK et Encase pour chaque personnel

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях по борьбе с киберпреступностью, и обеспечивать, чтобы они действовали в рамках правовых норм, связанных с этическими принципами.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый сотрудник:

- смогут с помощью международно признанного программного обеспечения изучать криминалистические копии, полученные в соответствии с законодательством,
- научатся отчетности.

СОДЕРЖАНИЕ

- Введение в компьютерную криминалистику. Файловые системы.
- Файловая структура файловой системы NTFS
- Процесс загрузки, время файла удаленных файлов, типы изображений, Encase
- Восстановление данных, сисема Windows и Пользовательские папки
- Отфильтрованные поиски, история интернета,

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Быть сотрудником подразделений по борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Компьютер, для каждого сотрудника, программное обеспечение FTK и Encase

الهدف

تطوير معرفة ومهارات العاملين في وحدات مكافحة الجرائم الإلكترونية والتأكد من أنهم يتصرفون في إطار القواعد القانونية المتعلقة بالمبادئ الأخلاقية

السلوك المستهدف

سيتمكن المشاركون في نهاية هذه الدورة من:

- مراجعة النسخ القضائية المأخوذة وفقًا للقانون من خلال برامج مقبولة دولياً ،
- تعلم كتابة التقرير.

المحتوى

- مدخل إلى تكنولوجيا المعلومات العدلية, أنظمة الملفات
- أنظمة الملفات العددية, نموذج ملفات NTFS
- عملية التمهيد ، الملفات المحذوفة، وقت الملف ، أنواع الصور ، Encase
- استعادة البيانات ، موقع ويندوز ، مجلدات المستخدم،
- المكالمات التي تمت تصفيتها ، تاريخ الإنترنت

الشروط المطلوب توفرها في المشاركين

- أن يكون موظفاً في قسم مكافحة الجرائم الالكترونية

الأدوات والتجهيزات اللازمة

- جهاز كمبيوتر برامج FTK و Encase

Jours / Heures
Рабочих Дней / Часов
المدة
5/30

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
3

Nombre de Coursiere
Количество Участников
عدد المتدربين
15-20

SİBER SALDIRI TEKNİKLERİ EĞİTİMİ
TRAINING ON CYBER ATTACK TECHNIQUES

AMAÇ

Siber Suçlarla Mücadele personelinin, yeteneklerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her katılımcı:
- Bilişim suçları ve teknikleri hakkında bilgi olacaktır.
- Siber saldırı teknikleri ve saldırılara karşı alınacak önlemler hakkında bilgi sahibi olacaktır.

İÇERİK

- Bilişim Suçları ve Yöntemleri
- Güvenlik ve Gizlilik
- OSINT
- Sanallaştırma Teknolojileri
- Temel Linux Komutları
- Temel Linux Hack Araçları
- Sosyal Mühendislik Saldırı ve Korunma Yöntemleri

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Eğitim sırasında kullanılacak araç ve gereçler Başkanlığımızca temin edilecektir.

PURPOSE

To develop the capabilities of the Anti-Cyber Crime personnel and to ensure that they perform their duties in accordance with ethical principles and within the framework of legal rules.

TARGET BEHAVIORS

At the end of this course, each participant:
- Will have information about cyber crimes and techniques.
- Will have information about cyber attack techniques and precautions to be taken against attacks.

CONTENT

- Cybercrimes and Methods
- Security and Privacy
- OSINT
- Virtualization Technologies
- Basic Linux Commands
- Essential Linux Hacking Tools
- Social Engineering Attack and Protection Methods

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Participants must be in charge of the Cyber Crime Units.

TOOLS AND MATERIALS

- The tools and equipment to be used during the training will be provided by our Department.

İş Günü / Saat Workdays / Hour: 5/30

Eğitici Sayısı Number of Trainers: 3

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION SUR LES TECHNIQUES DE CYBERATTAQUE
ТРЕНИНГ ПО МЕТОДАМ КИБЕРАТАК
التدريب على تقنيات الهجوم السيبراني

NO
18-06

OBJECTIFS

L'objectif de cette formation est d'améliorer les compétences du personnel travaillant dans les Unités de lutte contre la cybercriminalité et veiller à ce qu'ils travaillent dans le cadre des règles juridiques, en adhérant aux principes éthiques

RESULTATS EXIGES

- À la fin de ce programme de formation chaque participant aura des informations sur les cybercrimes et les techniques de cybercrime et les techniques de cyber-attaque et les mesures à prendre contre les attaques.

CONTENU

- Cybercrimes et méthodes de cybercrime
- Sécurité et confidentialité
- OSINT
- Technologies de virtualisation
- Commandes Linux de base
- Outils de piratage Linux de base
- Attaque d'ingénierie sociale et méthodes de protection

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans les unités de Lutte contre la cybercriminalité

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Les outils et équipements à utiliser lors de la formation seront fournis par notre Direction.

ЦЕЛЬ

Обеспечить, чтобы сотрудники киберпреступности развивали свои навыки и работали в рамках правовых норм, придерживаясь этических принципов.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Будет осведомлен о киберпреступлениях и методах.
- Будет иметь информацию о методах кибератак и мерах, которые будут приняты против атак.

СОДЕРЖАНИЕ

- Киберпреступления и методы
- Безопасность и конфиденциальность
- Разведка по открытым источникам (РОИ)
- Технология виртуализации
- Базовые команды Linux
- Хакерское программное средство базовой команды Linux
- Методы атаки и защиты социальной инженерии

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Инструменты и оборудование, которые будут использоваться во время обучения, будут предоставлены нашим институтом.

الهدف

التأكد من أن موظفي الجرائم الإلكترونية يطورون مهاراتهم ويعملون في إطار القواعد القانونية، مع الالتزام بالمبادئ الأخلاقية.

السلوك المستهدف

سيتمكن المشاركون في نهاية هذا التدريب من:

- معرفة جرائم وتقنيات الإنترنت.
- معرفة تقنيات الهجوم السيبراني والتدابير الواجب اتخاذها ضد الهجمات.

المحتوى

- الجرائم الإلكترونية وطرقها.
- الأمن والخصوصية.
- OSINT.
- تقنيات المحاكاة الافتراضية.
- أوامر Linux الأساسية.
- أدوات قرصنة Linux الأساسية.
- هجوم الهندسة الاجتماعية وأساليب الحماية.

الشروط المطلوب توفرها في المشاركين

- يجب أن يكون المشارك موظفاً في وحدات مكافحة الجرائم الإلكترونية.

الأدوات والتجهيزات اللازمة

- ستوفر رئاستنا الأدوات والمعدات التي سيتم استخدامها أثناء التدريب.

Jours / Heures Рабочих Дней / Часов المدة	5/30	Nombre D'enseignants Количество Преподавателей عدد المدربين	3	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

DVR CİHAZLARINDAN VERİ KURTARMA EĞİTİMİ
TRAINING ON DATA RECOVERY FROM DVR DEVICES

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- DVR cihazlarının imajlarının alınması ve silinen verilerin kurtarılmasını öğrenecektir.
- DVR cihazlarının log kayıtlarının alınması ve analizini öğrenecektir.

İÇERİK

- Hedefler
- Teknik Boyut
- Hukuki Boyut
- DVR Çalışma Yapısı
- İmaj Alma
- DVR Examiner
- HX Recovery
- DVR Cihazı Üzerinden Veri Alma
- DVR Cihazı Üzerinden Log Alma
- Logların Analizi

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.
- Temel Adli Bilişim Eğitimini almış olmak (FTK, EnCase)
- Dijital Delillere İlk Müdahale ve İmaj Alma Eğitimini almış olmak

ARAÇ, GEREÇ VE MALZEMELER

- Harddisk
- Flash Bellek
- DVR

PURPOSE

The aim is to develop knowledge and skills of the personnel working in units responsible for fighting against cyber crimes, and to enable them to perform their duties within the framework of law and ethical principles.

TARGET BEHAVIORS

At the end of this training, the participants will:
- Learn to capture the images of DVR devices and recover deleted data.
- Learn to take and analyze log records of DVR devices.

CONTENT

- Targets
- Technical Aspect
- Legal Aspect
- DVR Working Structure
- Image Acquisition
- DVR Examiner Software
- HX Software
- Data Recovery on the DVR Device
- Data Recovery Log on the DVR Device
- Log Analysis

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in Counter Cyber Crimes units.
- Training on Initial Intervention in Digital Evidence and Taking Forensic Copies
- Fundamental Forensic Information Training

TOOLS AND MATERIALS

- HDD
- Flash Drive
- DVR

İş Günü / Saat
Workdays / Hour
5/30

Eğitici Sayısı
Number of Trainers
3

Kursiyer Sayısı
Number of Trainees
8-10

FORMATION SUR LA RÉCUPÉRATION LES DONNÉES PERDUES ET/OU EFFACÉES SUR LES ENREGISTREURS DVR
ТРЕНИНГ ПО ВОССТАНОВЛЕНИЮ ДАННЫХ С ВИДЕОРЕГИСТРАТОРОВ
التدريب انقاذ البيانات من اجهزة DVR

NO
18-07

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans les unités de lutte contre la cybercriminalité et veiller à ce qu'il travaille conformément aux principes éthiques et dans le cadre des règles légales.

RESULTATS EXIGES

À l'issue de cette formation, les participants peuvent

- apprendre comment prendre des images de l'enregistreur DVR et récupérer les données perdues et/ou effacées.
- apprendre obtention des enregistrements et l'analyse des appareils DVR

CONTENU

- Objectifs
- Dimension technique
- Dimension juridique
- Structure de travail de l'enregistreur DVR
- Acquisition d'images
- Examinateur DVR
- Récupération HX
- Réception de données via l'enregistreur DVR
- Obtenir les enregistrements via l'enregistreur DVR
- Analyse des enregistrements

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans des unités de cybercriminalité
- Avoir reçu une formation de base de premiers secours (FTK, EnCase)
- Avoir reçu la formation sur la première intervention aux preuves numériques et l'acquisition d'images

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Disque dur, lecteur flash USB, enregistreur DVR

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях, ответственных за борьбу с киберпреступностью, и дать им возможность выполнять свои обязанности в рамках закона и этических принципов.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Научить захватывать изображения устройств видеорегистраторов и восстанавливать удаленные данные.
- Научить брать и анализировать журнальные записи устройств видеорегистраторов.

СОДЕРЖАНИЕ

- Цели
- Технический аспект
- Правовой аспект
- Рабочая структура видеорегистратора
- Получение изображения
- Осмотрщик видеорегистратора
- HX восстановления
- Восстановление данных на устройстве видеорегистратора
- Восстановление журнальных записей на устройстве видеорегистратора
- Анализ журнальных файлов

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.
- Обучение основам криминалистической информации (FTK, EnCase)
- Обучение первоначальному вмешательству в цифровые улики и получение изображения

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Жёсткий диск
- Флеш-память
- Цифровая видеозапись

الهدف

ان الهدف هو توفير القيام بتأدية الوظيفة ضمن اطار القواعد والشروط القانونية المرتبطة بالمبادئ المؤثرة في وظيفته وتطوير المهارات والقابليات والمعلومات الخاصة بالموظفين المخولين في وحدة محاربة الجرائم الالكترونية.

السلوك المستهدف

وفي نهاية هذه الدورة سيقوم كل موظف:

- سيتعلم تخليص البيانات الممسوحة والحصول على صور اجهزة DVR.
- سيتعلم الحصول على تسجيلا الـ gol والحصول عليها من اجهزة DVR.

المحتوى

- الاهداف
- البعد التقني
- البعد القانوني
- هيكلية عمل DVR
- اخذ الصور
- ممتحن DVR
- مسجل HX
- الحصول على البيانات من على جهاز DVR
- الحصول على Log من على جهاز DVR
- تحليل اللوغارتيمات

الشروط المطلوب توفرها في المشاركين

- يجب ان يكون المشاركين موظفين في وحدات محاربة الجرائم الالكترونية.
- سيكون المشارك قد حصل على تدريب المعلوماتية القضائية الاساسية (EnCase ,FTK).
- سيكون المشترك قد حصل على التدريب الخاص باخذ الصور والمحاربة الاولية للادلة الرقمية.

الأدوات والتجهيزات اللازمة

- القرص الصلب
- ذاكرة فلاش
- DVR

Jours / Heures
Рабочих Дней / Часов
المدة
5/30

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
3

Nombre de Coursiere
Количество Участников
عدد المتدربين
8-10

İLERİ DÜZEY MOBİL UYGULAMA VE TAMİR EĞİTİMİ
ADVANCED TRAINING ON MOBILE APPLICATION AND REPAIR

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:

- Arızası sebebiyle imajı alınamayan mobil cihazlara yazılımsal ve fiziksel müdahalede bulunma ve veri kurtarma tekniklerini öğrenme.

İÇERİK

- Hedefler
- İleri Düzey Müdahale Süreçleri
- İleri Düzey İmaj Alma Yöntemleri
- Mobil İmaj Alma Yöntemlerine Kullanılan Programlar
- Android ve İos Cihazlar Hakkında Bilgi
- Yazılımsal Müdahale Nedir? Hangi Cihazlara Yapılır?
- Yazılımsal Müdahale Adımları
- Root İşlemleri ve Root Dosyalarının Bulunması
- İleri Düzey Yazılımsal İşlem Sonrası İmaj Alma ve İnceleme
- Temel Elektronik Bilgisi
- Telefon Anakartı Üzerindeki Devre Elemanlarının Tanıtılması
- Açılamayan Cihazlara Müdahale Adımları
- Fiziksel Müdahale Hangi Cihazlara Yapılır
- Fiziksel Müdahale Ekipmanlarını ve Kullanımı
- Fiziksel Müdahale Aşamaları
- Ekran Değişimi
- USB Port Değişimi Sıvı Temaslı veya Kısa Devre Yapmış Cihazlara Müdahale
- ISP-JTAG-Chip-off Eğitimi
- Alınan Verilerin Anlamlı Hale Getirilmesi
- Teorik ve Uygulamalı Sınav

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar temel düzeyde mobil cihaz inceleme ve elektronik bilgisine sahip olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- J-Tag, Chip-Off Yazılım Ve Donanımları

PURPOSE

It is to develop knowledge and skills of the personnel working in units responsible for fighting against cyber crimes, and to enable them to perform their duties within the framework of law and ethical principles.

TARGET BEHAVIORS

- At the end of this course, each staff member will: Learn to respond to malfunctioning devices and data recovery techniques.

CONTENT

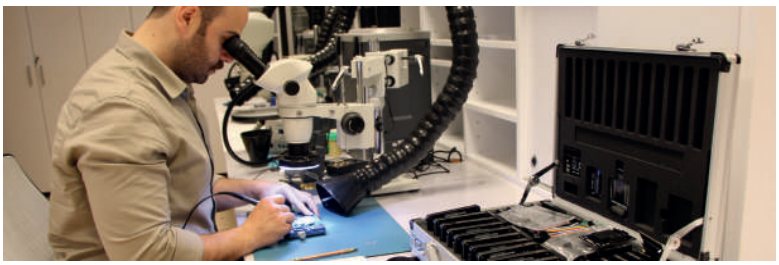
- Target of these course
- Advanced intervention Process
- Advanced Image Acquisition Methods
- Mobile Devices Image Acquisition Software
- Information About Android and İos Mobile Devices
- What is the software intervention? Which devices are suitable for this Procedure
- Software interventions steps
- Root procedure on Android Devices, Finding compatible Root Files
- Image acquiring and examinations after advanced software interventions
- Learning about Electronic Fundamentals
- Learning abut Phone Mainboards Components
- Intervention methods for devices that cannot be opened.
- Which devices are physically interfered with?
- Recognize and learn to use physical response equipment.
- Physical interventions steps
- Screen Replacements
- Usb socket Replacements
- Intervention methods for short circuit devices.
- Learning about ISP- Jtag- Chip Off Process
- Decoding of the data obtained by performing advanced operations.
- Final Exam

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Participants should have a basic knowledge of mobile device analysis and electronics.

TOOLS AND MATERIALS

- J-Tag, Chip-Off Software and Hardware



İş Günü / Saat Workdays / Hour: 10/60

Eğitici Sayısı Number of Trainers: 3

Kursiyer Sayısı Number of Trainees: 10-15

FORMATION SUR LA RÉCUPÉRATION LES DONNÉES PERDUES ET/OU EFFACÉES SUR LES ENREGISTREURS DVR
ТРЕНИНГ ПО ВОССТАНОВЛЕНИЮ ДАННЫХ С ВИДЕОРЕГИСТРАТОРОВ
التدريب على الصيانة وتطبيق المحمول بالمستويات العليا

NO
18-08

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans les unités de lutte contre la cybercriminalité et veiller à ce qu'il travaille conformément aux principes éthiques et dans le cadre des règles légales.

RESULTATS EXIGES

- À l'issue de cette formation de formation, les participants peuvent apprendre les techniques logicielles et physiques d'intervention et de récupération de données pour les appareils mobiles qui ne peuvent pas être imagés en raison de dysfonctionnements

CONTENU

- Objectifs
- Processus d'intervention avancés
- Méthodes d'imagerie avancées
- Programmes utilisés pour les méthodes d'acquisition d'images mobiles
- Informations sur les appareils Android et iOS
- Qu'est-ce que l'intervention logicielle ? À quels appareils s'applique-t-il ?
- Étapes d'intervention logicielle
- Processus Root et la recherche de fichiers Rood
- Acquisition et l'analyse avancées d'images après traitement logiciel
- Connaissances de base en électronique
- Introduction des éléments de circuit sur la carte téléphonique
- Étapes d'intervention en cas d'impossibilité d'ouvrir les appareils
- Sur quels appareils l'intervention physique est effectuée
- Équipement d'intervention physique et son utilisation
- Étapes d'intervention physique
- Changement d'écran
- Changement de port USB
- Comment réagir aux appareils abîmés à cause de contact avec un liquide ou en court-circuit
- Formation sur ISP-JTAG-Chip-off
- Rendre les données reçues significatives
- Examen théorique et pratique

CONDITIONS EXIGES DES PARTICIPANTS

- Les participants doivent avoir une connaissance de base de l'inspection des appareils mobiles et de l'électronique.

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- J-Tag, Chip-Off logiciel

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях, ответственных за борьбу с киберпреступностью, и предоставления им возможности выполнять свои обязанности в рамках закона и этических принципов.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Научится реагировать на неисправные устройства и методы восстановления данных.

СОДЕРЖАНИЕ

- Цели
- Продвинутый Уровень Вмешательства
- Продвинутый Уровень Получения Изображения
- Методы Получения Изображения, Продвинутый Уровень
- Программное обеспечение для получения изображений мобильных устройств
- Информация о мобильных устройствах Android и IOS
- Что такое программное вмешательство? Какие устройства подходят для этой Процедуры
- Этапы вмешательства в программное обеспечение
- Процедура рутирования на устройствах Android, поиск совместимых корневых файлов
- Получение изображений и исследования после передовых программных вмешательств
- Изучение основ электроники
- Знакомство с компонентами материнской платы телефона
- Методы вмешательства для устройств, которые невозможно открыть,
- Какие устройства подвергаются физическому воздействию?
- Знать и учиться использовать оборудование физического реагирования,
- Шаги физического вмешательства,
- Замена экрана
- Замена USB-разъём с контактом жидкости или устройствами короткого замыкания
- Тренинг программному и аппаратному средству «ISP-JTAG-Chip-off»
- Делаем полученные данные значимыми
- Теоретический и практический экзамен

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны иметь базовые знания в области обзора мобильных устройств и электроники.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Программные и аппаратные средства "J-Tag", "Chip-Off"

الهدف

ان الهدف هو توفير القيام بتأدية الوظيفة ضمن اطار القواعد والشروط القانونية المرتبطة بالمبادئ المؤثرة في وظيفته وتطوير المهارات والقابليات والمعلومات الخاصة بالموظفين المخولين في وحدة محاربة الجرائم الالكترونية.

السلوك المستهدف

وفي نهاية هذه الدورة سيقوم كل موظف:

- معرفة تقنيات انقاذ البيانات والتواجد في التدخل الفيزيائي والبرامجياتي للاجهزة المحمولة الذي لم يتم التقاط صورها بسبب العطل.

المحتوى

- الاهداف
- فترات التدخل بالمستويات المتقدمة
- طرق التصوير بالمستويات المتقدمة
- البرامج المستخدمة في ادارة تصوير المحمول
- المعلومات الذي يخص اجهزة آوس واندرويد
- ما هو التدخل البرامجياتي؟ لأي الاجهزة يتم القيام بتنفيذها؟
- خطوات التدخل البرامجياتي
- العثور على ملفات Root ومعاملات Root
- التدقيق والتصوير بعد العمليات البرامجياتية بالمستويات المتقدمة
- المعلومات الالكترونية الاساسية
- تعريف عناصر الدورة الموجودة على البطاقة الرئيسية للهاتف
- خطوات التدخل في الاجهزة الذي المفتوحة
- لأية اجهزة يتم القيام بالتدخل الفيزيائي
- معدات التدخل الفيزيائي واستعمالها
- مراحل التدخل الفيزيائي
- تغيير الشاشة
- التدخل في الاجهزة التي قامت بالدورات القصيرة او ذو تماس سائل تغيير USB Port.
- التدريب على ISP-JTAG-Chip-off
- احضار البيانات المأخوذة وايصالها الى حالة مفهومة
- الامتحانات النظرية والتطبيقية

الشروط المطلوب توفرها في المشاركين

- ان يكون المشاركين اصحاب المعلومات الالكترونية والتدقيق في الاجهزة المحمولة بمستويات أساسية.

الأدوات والتجهيزات اللازمة

- برامجيات J-Tag, Chip-off وتجهيزاتها

Jours / Heures Рабочих Дней / Часов المدة	10/60	Nombre D'enseignants Количество Преподавателей عدد المدربين	3	Nombre de Coursiere Количество Участников عدد المتدربين	10-15

KRİPTO ANALİZ EĞİTİMİ
TRAINING ON CRYPTO ANALYSIS COURSE

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin şifreli disk, alan ve dosyaları tespit edebilmesi ve tespit edilen şifreli içeriklerin çözümlenme yeteneklerinin kazandırılması.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- Şifreli içerikleri tespit edebilecektir.
- Şifreleme algoritmalarını ayırt edebilecektir.
- Şifre çözümlemeye yönelik atak yöntemlerini öğrenecektir.
- Şifre çözümlemeye yönelik hedef odaklı sözlükler oluşturabilecektir.

İÇERİK

- Şifreleme Algoritmaları
- Tamamı Şifreli Diskler
- Şifreli Alanlar
- Şifreli Dosyalar
- Atak Yöntemleri
- Sözlük Oluşturma Yöntemleri
- Genel Uygulama

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

PURPOSE

The aim is improving the Cyber Crime Units 'Staff capability of full disc encryption, encrypted containers encrypted files detection and the abilty to decrpytion of encrypted digital materials.

TARGET BEHAVIORS

At the end of this training, the participants will:
- Gain the abilty to detect the encrypted materials
- Gain the ability to classification of the encryption algorithims
- Gain the abilty to learn how to attack the decrypted materials
- Gain the ability to create efficient dictionaries for password cracking

CONTENT

- Encryption Algorithms
- Full Disk Encryption
- Encrypted Container
- Encrypted Files
- Attack Methods
- Dictionary Creation Methods
- Practices

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in Cyber Crimes units.

İş Günü / Saat Workdays / Hour: 5/30

Eğitici Sayısı Number of Trainers: 3

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION SUR L'ANALYSE CRYPTOGRAPHIQUE
ТРЕНИНГ ПО КРИПТОАНАЛИЗУ
التدريب على تحليل السرية

NO
18-09

OBJECTIFS

L'objectif de cette formation est de permettre au personnel qui travaille dans les unités de lutte contre la cybercriminalité de détecter les disques, zones et fichiers cryptés, et d'acquérir la capacité de déchiffrer les contenus cryptés détectés.

RESULTATS EXIGES

A l'issue de cette formation, les participants auront les capacités de

- détecter le contenu crypté.
- distinguer les algorithmes de chiffrement
- savoir les méthodes d'attaque pour le décryptage.
- créer des dictionnaires ciblés pour l'analyse des mots de passe.

CONTENU

- Algorithmes de chiffrement
- Disques entièrement cryptés
- Champs cryptés
- Fichiers cryptés
- Méthodes d'attaque
- Méthodes de création de dictionnaire
- Travaux pratiques

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans des unités de lutte contre la cybercriminalité

ЦЕЛЬ

Цель состоит в том, чтобы улучшить возможности персонала подразделения по борьбе с киберпреступностью в отношении полного шифрования диска, обнаружения зашифрованных контейнеров, зашифрованных файлов и способности дешифровать зашифрованные материалы.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Получает возможность обнаруживать зашифрованные материалы.
- Получает возможность классификации алгоритмов шифрования информации.
- Получает возможность научиться атаковать расшифрованные материалы.
- Получает возможность создавать эффективные словари для взлома паролей.

СОДЕРЖАНИЕ

- Алгоритм Шифрования Информации
- Полное Шифрование Диска
- Зашифрованный Контейнер
- Зашифрованный Файл
- Методы Атаки
- Методы Создания Словарей
- Общая Практика

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.

الهدف

اكتساب المهارات والقابليات الخاصة بتحليل المحتويات المشفرة والذي تم تثبيتها والذي من الممكن ان يتم من خلالها تثبيت الملفات والمساحات والاقراص المشفرة للموظفين المخولين في وحدات محاربة الجرائم الالكترونية.

السلوك المستهدف

وفي نهاية هذه الدورة سيقوم كل موظف:

- من الممكن ان يتم تثبيت المحتويات المشفرة.
- من الممكن ان يتم تمييز اللوغارتيمات الخاصة بالتشفير.
- سيتم معرفة طرق الهجوم باتجاه حل الشفرة.
- من الممكن ان يتم تشكيل الكلمات المتركزة على الاهداف باتجاه حل الشفرات.

المحتوى

- لوغارتيمات التشفير
- الاقراص المشفرة بشكل كامل
- المساحات المشفرة
- الملفات المشفرة
- ادارة الهجمات
- ادارة تشكيل الكلمات
- التطبيقات العامة

الشروط المطلوب توفرها في المشاركين

- ان يكون المشاركين موظفين في وحدات محاربة الجرائم الالكترونية.

Jours / Heures
Рабочих Дней / Часов
المدة
5/30

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
3

Nombre de Coursiere
Количество Участников
عدد المتدربين
15-20

LOG ANALİZİ EĞİTİMİ
TRAINING ON LOG ANALYSIS

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin Windows ve Linux işletim sistemlerine ait log dosyaları ile çeşitli cihazlara(Modem, web, mail, vb.) ait log dosyaları üzerinde yer alan log satırlarını analiz edebilmesini sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- Windows işletim sistemleri üzerinde log analizi yapabilecektir.
- Linux işletim sistemleri üzerinde log analizi yapabilecektir.
- Web loglarının analizini yapabilecektir.
- İçeriğinde çok sayıda log satırı barındıran günlük dosyaları üzerinde incelemeler yapabilecektir.

İÇERİK

- Windows log dosyaları özellikleri, analizleri ve uygulama
- Linux log dosyaları özellikleri, analizleri ve uygulama
- Web log özellikleri, analizleri ve uygulama
- Çeşitli yazılımlara ait log dosyaları üzerinde analiz yapma
- Genel uygulama

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

PURPOSE

To be able to improve the Cyber Crime Units 'Staff capability of log files analyse on Windows OS, Linux OS and the log lines on the log files of various devices (Modem, web, mail, etc.)

TARGET BEHAVIORS

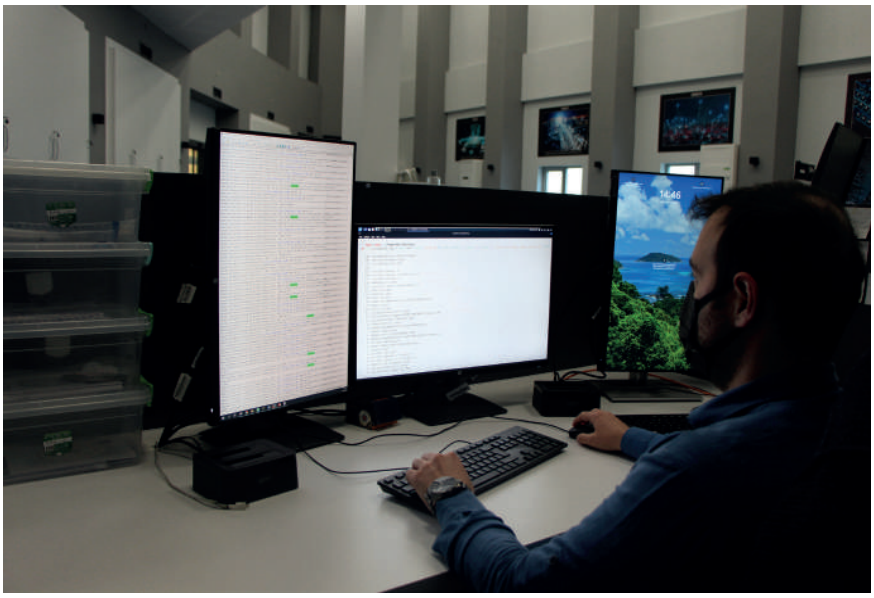
At the end of this training each participant will:
- Gain the capability of log analyse on windows operating system
- Gain the capability log analyse on Linux operating system
- Gain the capability of log analyse on WebLog
- Gain the capability of analysing daily file that include logs

CONTENT

- Windows log files analyse and applications
- Lünux log files analyse and applications
- Web Log properties and applications
- Anlyse on the application log files
- Practices

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in Cyber Crimes units.



İş Günü / Saat Workdays / Hour 5/30

Eğitici Sayısı Number of Trainers 3

Kursiyer Sayısı Number of Trainees 15-20

FORMATION À L'ANALYSE DES JOURNAUX
ТРЕНИНГ ПО АНАЛИЗУ ЖУРНАЛЬНЫХ ФАЙЛОВ
التدريب على تحليل اللوغارتيمات

NO
18-10

OBJECTIFS

L'objectif de cette formation est de permettre au personnel qui travaille dans des unités de lutte contre la cybercriminalite d'analyser les lignes de journal sur les fichiers journaux des systèmes d'exploitation Windows et Linux et les fichiers journaux de divers appareils (Modem, Web, messagerie, etc.).

RESULTATS EXIGES

A l'issue de cette formation, les participants auront les capacités de

- analyser en détail les journaux d'événements des systèmes Windows
- analyser en détail les journaux d'événements des systèmes Linux.
- analyser les journaux Web
- analyser les fichiers journaux contenant de nombreuses lignes de journal.

CONTENU

- Fonctionnalités, l'analyse et l'application des fichiers journaux Windows
- Fonctionnalités, analyse et application des fichiers journaux Linux
- Fonctionnalités, l'analyse et l'application du journal Web
- Analyse sur les fichiers journaux de divers logiciels
- Travaux pratiques

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans des unités de lutte contre la cybercriminalité

ЦЕЛЬ

Улучшить возможности персонала отдела киберпреступности для анализа файлов журнала в ОС Windows, ОС Linux и строк журнала в файлах журнала различных устройств (модем, Интернет, почта и т.д.)

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Получает возможность анализа журнала в операционной системе Windows.
- Получает возможность анализа журнала в операционной системе Linux.
- Получает возможность анализа журналов в электронном журнале (WebLog).
- Получает возможность анализировать ежедневные файлы, включающие много строк журнала.

СОДЕРЖАНИЕ

- Анализ, особенности и применение файлов журналов Windows
- Анализ, особенности и применение файлов журнала Linux
- Анализ, особенности и применение файлов в электронном журнале (WebLog).
- Анализ лог-файлов различного программного обеспечения
- Общая Практика

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.

الهدف

توفير امكانية قيام المشاركين بتحليل سطور اللوغارتيمات الذي يحتل مكانا على ملفات اللوغارتيمات العائدة الى الاجهزة المتعددة (المودم, الموقع الالكتروني, البريد الالكتروني وما شابه) بالاشتراك مع ملفات اللوغاتيمات العائدة الى انظمة تشغيل ويندوز ولينوكس للموظفين المخولين في وحدات محاربة الجرائم الالكترونية.

السلوك المستهدف

وفي نهاية هذه الدورة سيقوم كل موظف:

- من الممكن ان يقوم بتحليل اللوغارتيمات على انظمة التشغيل ويندوز.
- امكانية القيام بتحليل اللوغارتيمات على انظمة التشغيل لينوكس.
- امكانية القيام بتحليل لوغارتيمات المواقع الالكترونية.
- امكانية القيام باجراء التدقيقات على الملفات اليومية التي تقوم بتنمية اسطر اللوغارتيمات باعداد كبيرة في محتوياتها.

المحتوى

- المواصفات, التحليلات والتطبيقات الخاصة بملفات لوغارتيمات الويندوز.
- مواصفات, تحليلات وتطبيقات ملفات لوغارتيمات اللينوكس.
- مواصفات, تحليلات وتطبيقات لوغارتيمات المواقع الالكترونية.
- القيام باجراء التحليلات على ملفات اللوغارتيمات العائدة الى البرامجيات المتعددة.
- التطبيقات العامة

الشروط المطلوب توفرها في المشاركين

- ان يكون المشاركين موظفين في وحدات محاربة الجرائم الالكترونية.

Jours / Heures
Рабочих Дней / Часов
المدة
5/30

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
3

Nombre de Coursiere
Количество Участников
عدد المتدربين
15-20

MOBİL ZARARLI YAZILIM ANALİZ EĞİTİMİ
TRAINING ON MOBILE MALWARE ANALYSIS

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin mobil zararlı yazılımlar üzerinde bilgi ve becerilerinin geliştirilmesi, zararlı yazılımın kabiliyetlerinin belirlenmesi, statik ve dinamik analiz yöntemlerini uygulayarak analiz edilmesini sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- Mobil uygulamalar üzerinde statik analiz yapabilecektir.
- Mobil uygulamalar üzerinde dinamik analiz yapabilecektir.
- Mobil uygulamalar üzerinde kod analizi yapabilecektir.
- Mobil uygulamalar üzerinde network analizi yapabilecektir.

İÇERİK

- Zararlı Mobil Uygulamanın Tespiti
- Statik Analiz Araçları
- Dinamik Analiz Araçları
- Emülatörler
- Kum Havuzları
- Tersine Mühendislik Yöntemleri
- Network Hareketleri
- Genel Uygulama

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

PURPOSE

To be able to improve the Cyber Crime Units 'Staff capability of mobile malware analysis, the applid methods will be static, dynamic, network and code analysis in the lab environment.

TARGET BEHAVIORS

At the end of this training each participant will:
- Gain the capability of static analyse on the mobile application
- Gain the capability of dynamic analyse on the mobile application
- Gain the capability of code analyse on the mobile application
- Gain the capability of network analyse on the mobile application

CONTENT

- Mobile Malware Detection Methods
- Static Analyse Tools
- Dynamic Analyse Tools
- Emulator
- Sandbox
- Reverse Engineering Methods
- Network Analyse
- Practices

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in Cyber Crimes units.

İş Günü / Saat Workdays / Hour 5/30

Eğitici Sayısı Number of Trainers 3

Kursiyer Sayısı Number of Trainees 15-20

FORMATION SUR L'ANALYSE DES LOGICIELS MALVEILLANTS
ТРЕНИНГ ПО АНАЛИЗУ МОБИЛЬНЫХ ВРЕДОНОСНЫХ ПРОГРАММ
التدريب على تحليل البرامجيات المضرة للمحمول

NO
18-11

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans les unités de lutte contre cybercrime sur les logiciels malveillants mobiles, déterminer les capacités du logiciel malveillant et l'analyser en appliquant des méthodes d'analyse statiques et dynamiques.

RESULTATS EXIGES

A l'issue de cette formation, les participants auront les capacités de

- faire des analyses statiques sur des applications mobiles.
- faire des analyses dynamiques sur des applications mobiles.
- faire de l'analyse de code sur des applications mobiles.
- faire des analyses de réseau sur les applications mobiles.

CONTENU

- Détection d'applications mobiles nuisibles
- Outils d'analyse statique
- Outils d'analyse dynamique
- Émulateurs
- Bacs à sable
- Méthodes d'ingénierie inverse (La rétro-ingénierie)
- Mouvements de réseau
- Travaux pratiques

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans des unités de lutte contre la cybercriminalité

ЦЕЛЬ

Цель состоит в том, чтобы развивать знания и навыки по мобильным вредоносным программам сотрудников, работающих в подразделениях по борьбе с киберпреступностью, определять возможности вредоносного ПО и анализировать его с применением методов статического и динамического анализа.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Получает возможность статического анализа в мобильном применении.
- Получает возможность динамического анализа в мобильном применении.
- Получает возможность анализа кода в мобильном применении.
- Получает возможность анализа сетей в мобильном применении.

СОДЕРЖАНИЕ

- Система Выявления Мобильных Вредоносных Программ
- Инструменты Статического Анализа
- Инструменты Динамического Анализа
- Эмуляторы
- Изолированные Среды
- Реверсивный анализ требований
- Анализ Сетей
- Общая Практика

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.

الهدف

توفير امكانية قيام المشاركين بالتحليل من خلال تطبيق انظمة التحليل الديناميكية والاستاتيكية وتحديد فابلية البرامجيات المضرة وتطوير المعلومات والمهارات والقابليات والمعلومات على البرامجيات المضرة المحمولة للموظفين المخولين في وحدات محاربة الجرائم الالكترونية.

السلوك المستهدف

وفي نهاية هذه الدورة سيقوم كل موظف:

- من الممكن ان يقوم بالتحليل الاستاتيكي على تطبيقات المحمول.
- من الممكن ان يقوموا بالتحليل الديناميكي على تطبيقات المحمول.
- من الممكن ان يقوموا بتحليل الرمز على تطبيقات المحمول.
- من الممكن ان يقوموا بتطبيقات تحليل الشبكة على تطبيقات المحمول.

المحتوى

- تثبيت تطبيقات المحمول المضرة
- وسائط التحليل الاستاتيكي
- وسائط التحليل الديناميكي
- المحاكيات
- الاحواض الرملية
- طرق الهندسة العكسية
- تحركات الشبكات
- التطبيقات العامة

الشروط المطلوب توفرها في المشاركين

- ان يكون المشاركين موظفين في وحدات محاربة الجرائم الالكترونية.

Jours / Heures Рабочих Дней / Часов المدة	5/30	Nombre D'enseignants Количество Преподавателей عدد المدربين	3	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

TEMEL VERİ KURTARMA EĞİTİMİ (HARDDİSK – FLASH BELLEK VE HAFIZA KARTLARI – RAİD VERİ KURTARMA)
BASIC TRAINING ON DATA RECOVERY (HARD DISC, FLASH MEMORY AND MEMORY CARDS-RAID DATA RECOVERY)

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- İmajı alınamayan, yazılımsal ve donanımsal arızalı hard disklerin imajlarının alınması ve veri kurtarılmasını öğrenecektir.
- İmajı alınamayan, yazılımsal ve donanımsal arızalı flash bellek – micro sd – sd kartların imajlarını ve veri kurtarılmasını alınmasını öğrenecektir.
- Raid Veri Kurtarma iş ve işlemlerini öğreneceklerdir

İÇERİK

- Hedefler
- Teknik Boyut
- Hukuki Boyut
- Harddisk Çalışma Yapısı
- PC3000 Express
- Data Extractor
- Hafıza kartı ve Flash Belleklerden Veri Kurtarma
- Donanımsal Müdahale İşlemleri
- PC3000 Raid Kurtarma

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.
- Temel Adli Bilişim Eğitimini almış olmak (FTK, EnCase)
- Dijital Delillere İlk Müdahale ve İmaj Alma Eğitimini almış olmak

ARAÇ, GEREÇ VE MALZEMELER

- Harddisk
- Flash Bellek
- Micro SD ve SD Kart
- Sıcak Hava İstasyonu
- Havya İstasyonu
- Mikroskop
- Lehimleme Malzemeleri (Cımbız Seti, Kablo, Lehim, Flux)

PURPOSE

It is to develop knowledge and skills of the personnel working in units responsible for fighting against cyber crimes, and to enable them to perform their duties within the framework of law and ethical principles.

TARGET BEHAVIORS

At the end of this training each participant will:
- They will learn how to image and recover data of hard disks that cannot be imaged, software and hardware failures.
- Will learn how to retrieve images and data recovery of non-image, software and hardware defective flash memory - micro sd-sd cards.
- RAID Recovery Training

CONTENT

- Targets
- Technical Aspect
- Legal Aspect
- HDD Working Structure
- PC3000 Express Software
- Data Extractor Software
- Monolith and Flash Device Data Recovery Training
- Hardware Intervention Operations
- PC3000 Raid Recovery training

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Working in Cyber Crimes units.
- Training on Initial Intervention in Digital Evidence and Taking Forensic Copies
- Fundamental Forensic Information Training

TOOLS AND MATERIALS

- HDD
- Flash Drive
- Micro Sd and SD Card Hot Air Station
- Soldering Iron Station
- Microscope
- Soldering Materials (Tweezers, Cable, Solder, Flux)

İş Günü / Saat Workdays / Hour: 13/78

Eğitici Sayısı Number of Trainers: 3

Kursiyer Sayısı Number of Trainees: 6-8

FORMATION DE BASE SUR LA RÉCUPÉRATION DE DONNÉES (DISQUE DUR - MÉMOIRE FLASH ET CARTES MÉMOIRE - RÉCUPÉRATION DE DONNÉES RAID)
БАЗОВЫЙ ТРЕНИНГ ПО ВОССТАНОВЛЕНИЮ ДАННЫХ С ЖЕСТКИХ ДИСКОВ, ФЛЭШ-ПАМЯТИ/ ПЛАТА ПАМЯТИ И RAID)
التدريب على تخليص البيانات الاساسية (القرص الصلب- ذاكرة فلاش وبطاقات الذاكرة – تخليص بيانات Raid)

NO
18-12

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans des unités de lutte contre la cybercriminalité et veiller à ce qu'il travaille conformément aux principes éthiques et dans le cadre des règles légales.

RESULTATS EXIGES

A l'issue de la formation, les participants auront les capacités de

- prendre des images et récupérer des données de disques durs qui ne prendre des images de disques durs qui ne peuvent pas être imagés et dont les logiciels et le matériel sont défaillants.
- récupérer des images et des données de mémoire flash – micro sd – cartes sd qui ne peuvent pas être imagées et dont les logiciels et le matériel sont défaillants.
- savoir le logiciel de récupération de données sur RAID et ses operations

CONTENU

- Objectifs
- Dimension technique
- Dimension juridique
- Structure de travail du disque dur
- Récupération de données à partir de cartes mémoire et de lecteurs flash USB.
- Opérations d'intervention matérielle
- Récupération de raid PC3000

CONDITIONS EXIGES DES PARTICIPANTS

- Travailler dans des unités de cybercriminalité
- Avoir reçu la formation de base en informatique médico-légale (FTK, EnCase)
- Avoir reçu la formation sur la première intervention aux preuves numériques et l'acquisition d'images

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Disque dur
- Lecteur Flash USD
- Micro SD et carte SD
- Station d'air chaud
- Les postes à souder
- Microscope
- Matériaux de soudure (jeu de pincettes, câble, soudure, flux)

ЦЕЛЬ

Предназначен для развития знаний и навыков персонала, работающего в подразделениях, ответственных за борьбу с киберпреступностью, и предоставления им возможности выполнять свои обязанности в рамках закона и этических принципов.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Узнает, как создавать образы и восстанавливать данные с жестких дисков, которые не могут быть созданы, а также при сбоях программного и аппаратного обеспечения.
- Узнает, как извлекать изображения и восстанавливать данные неизображенных, программно-аппаратных дефектов флэш-памяти – микро CD – карта CD.
- Обучение восстановлению данных RAID

СОДЕРЖАНИЕ

- Цели
- Технический аспект
- Правовой аспект
- Рабочая структура жесткого диска
- PC3000 Экспресс
- Экстрактор Данных
- Восстановление Данных с Карт Памяти и Флешек
- Операции по вмешательству в оборудование
- Обучение восстановлению PC3000 RAID

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.
- Обучение основам криминалистической информации (FTK, EnCase)
- Обучение первоначальному вмешательству в цифровые улики и получение изображения

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Жесткий диск
- Флеш-Память
- Микро CD – карта CD
- Станция горячего воздуха
- Станция воздуха
- Микроскоп
- Материалы для пайки (пинцет, кабель, припой, флюс)

الهدف

ان الهدف هو توفير القيام بتأدية الوظيفة ضمن اطار القواعد والشروط القانونية المرتبطة بالمبادئ المؤثرة في وظيفته وتطوير المهارات والقابليات والمعلومات الخاصة بالموظفين المخولين في وحدة محاربة الجرائم الالكترونية.

السلوك المستهدف

وفي نهاية هذه الدورة سيقوم كل موظف:

- سيتعلمون طرق تخليص البيانات واتخاذ الصور للاقراص الصلبة العاطلة للتجهيزات والبرامجيات الذي لم يتم تصويره.
- سيتعلمون الحصول على الطرق لتخليص البيانات والصور الخاصة ببطاقات القرص الصلب ds – المايكرو dc – ذاكرة فلاش المعطلة للتجهيزات والبرامجيات الذي لم يتم تصويرها.
- سيتعلمون اعمال ومعاملات تخليص بيانات Raid.

المحتوى

- الاهداف
- البعد التقني
- البعد القانوني
- هيكلية عمل القرص الصلب
- PC3000 Express
- Data Extractor (مستخرج البيانات)
- تخليص البيانات من ذاكرة فلاش وبطاقة الذاكرة
- معاملات التدخل التجهيزاتية
- تخليص PC3000 Raid

الشروط المطلوب توفرها في المشاركين

- ان يكون المشاركين موظفين في وحدات محاربة الجرائم الالكترونية.
- ان يكون المشاركين قد حصلوا على التعليم الخاص بمعلوماتية القضاء الاساسية (FTK, EnCase).
- ان يكون المشاركين قد حصلوا على تدريب التصوير والتدخل الاول للادلة الرقمية.

الأدوات والتجهيزات اللازمة

- القرص الصلب
- ذاكرة فلاش
- المايكرو CD و بطاقة CD
- محطة الهواء الساخن
- محطة لحام الحديد
- المايكروسكوب
- مواد اللحيم(طقم الملقط, الكابل, اللحيم, فلوكس)

Jours / Heures
Рабочих Дней / Часов
المدة
13/78

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
3

Nombre de Coursiere
Количество Участников
عدد المتدربين
6-8

ZARARLI YAZILIM ANALİZ EĞİTİMİ
TRAINING ON MALWARE ANALYSIS

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin zararlı yazılımlar üzerinde bilgi ve becerilerinin geliştirilmesi, zararlı yazılımın kabiliyetlerinin belirlenmesi, statik ve dinamik analiz yöntemlerini uygulayarak analiz edilmesini sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:
- Zararlı yazılımlar üzerinde statik analiz yapabilecektir.
- Zararlı yazılımlar üzerinde dinamik analiz yapabilecektir.
- Zararlı yazılımlar üzerinde kod analizi yapabilecektir.
- Zararlı yazılımlar üzerinde network analizi yapabilecektir.

İÇERİK

- Kötü Amaçlı Yazılım Analizinin Temelleri
- Kötü Amaçlı Yazılım Sınıflandırması
- Kötü Amaçlı Yazılım Algılama Yöntemleri
- Analiz Ortamı Oluşturma (Lab Kurulumu)
- Statik Analiz Yöntemleri
- Statik Analiz Araçları ve Kullanımı
- Dinamik Analiz Yöntemleri
- Dinamik Analiz Araçları ve Kullanımı
- Kötü Amaçlı Yazılım Ağı Analizi
- Tersine Mühendislik Yöntemleri
- Güvenlik Açığı, Exploit ve Exploit Kitleri
- Fidye Yazılımı
- Dosyasız Enfeksiyon Saldırıları
- Çevrimiçi Bankacılık Kötü Amaçlı Yazılım

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcıların temel zararlı yazılım analizi ve programlama bilgisine sahip olmaları gerekmektedir.

PURPOSE

To be able to improve the Cyber Crime Units 'Staff capability of malware analysis, the applid methods will be static, dynamic, network and code analysis in the malware lab environment.

TARGET BEHAVIORS

At the end of this trainig each participant will:
- Gain the capability of static analyse on the malware
- Gain the capability of dynamic analyse on the malware
- Gain the capability of code analyse on the malware
- Gain the capability of network analyse on the malware

CONTENT

- Malware Analysis Fundamentals
- Malware Classification
- Malware Detection Methods
- Creating Analysis Environment (Lab Setup)
- Static Analysis Methods
- Static Analysis Tools and Usage
- Dynamic Analysis Methods
- Dynamic Analysis Tools and Usage
- Malware Network Analysis
- Reverse Engineering Methods
- Vulnerability, Exploit and Exploit Kits
- Ransomware
- Fileless Infection Attacks
- Online Banking Malware

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Participants are required to have basic malware analysis and programming knowledge.

İş Günü / Saat Workdays / Hour 5/30

Eğitici Sayısı Number of Trainers 3

Kursiyer Sayısı Number of Trainees 15-20

FORMATION MALWARE
ТРЕНИНГ ПО АНАЛИЗУ ВРЕДОНОСНЫХ ПРОГРАММ
التدريب على تحليل البرامجيات المضرة

NO
18-13

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans des unités de lutte contre la cybercriminalité sur les logiciels malveillants, déterminer les capacités du logiciel malveillant, l'analyser en appliquant des méthodes d'analyse statique et dynamique.

RESULTATS EXIGES

A l'issue de la formation, les participants auront les capacités de

- faire des analyses statiques sur les logiciels malveillants.
- effectuer une analyse dynamique sur les logiciels malveillants.
- faire des analyses de code sur les logiciels malveillants.
- faire une analyse de réseau sur les logiciels malveillants.

CONTENU

- Fondamentaux de l'analyse des logiciels malveillants
- Classification des logiciels malveillants
- Méthodes de détection des logiciels malveillants
- Création d'un environnement d'analyse (installation de laboratoire)
- Méthodes d'analyse statique
- Outils d'analyse statique et leurs utilisations
- Méthodes d'analyse dynamique
- Outils d'analyse dynamique et leurs utilisations
- Analyse du réseau de logiciels malveillants
- Méthodes d'ingénierie inverse (la rétro-ingénierie)
- Bogue de sécurité, l'exploit ou code d'exploitation, les kits d'exploitation (ou packs d'exploitation)
- Logiciels de rançon, (aussi appelés rançongiciels ou ransomware)
- Attaques par malware sans fichier
- Logiciels malveillants pour les services bancaires en ligne

CONDITIONS EXIGES DES PARTICIPANTS

- avoir des connaissances de base en analyse et programmation des logiciels malveillants.

ЦЕЛЬ

Цель состоит в том, чтобы развивать знания и навыки по мобильным вредоносным программам сотрудников, работающих в подразделениях по борьбе с киберпреступностью, определять возможности вредоносного ПО и анализировать его с применением методов статического и динамического анализа.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Получает возможность статического анализа вредоносного ПО.
- Получает возможность динамического анализа вредоносного ПО.
- Получает возможность анализа кода на вредоносное ПО.
- Получает возможность сетевого анализа вредоносных программ

СОДЕРЖАНИЕ

- Основы анализа вредоносных программ
- Классификация вредоносных программ
- Методы обнаружения вредоносных программ
- Создание среды анализа (лабораторная установка)
- Методы статического анализа
- Инструменты статического анализа и их использование
- Методы динамического анализа
- Инструменты динамического анализа и их использование
- Анализ сетей вредоносных программ
- Реверсивный анализ требований
- Брешь в системе безопасности, вредоносный код, наборы вредоносных кодов,
- Программы-Вымогатели
- Атаки без файлового заражения
- Вредоносное ПО в интернет-банкинге

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны иметь базовый анализ вредоносного ПО и знания в области программирования.

الهدف

توفير امكانية قيام المشاركين بالتحليل من خلال تطبيق انظمة التحليل الديناميكية والاستاتيكية وتحديد فابلية البرامجيات المضرة وتطوير المعلومات والمهارات والقابليات والمعلومات على البرامجيات المضرة المحمولة للموظفين المخولين في وحدات محاربة الجرائم الالكترونية.

السلوك المستهدف

وفي نهاية هذه الدورة سيحصل كل موظف:

- امكانية التحليل الاستاتيكي على البرامجيات المضرة
- امكانية القيام بالتحليل الديناميكي على البرامجيات المضرة
- امكانية القيام بتحليل الرمز على البرامجيات المضرة
- امكانية تحليل الشبكات على البرامجيات المضرة

المحتوى

- أساسات تحاليل البرامجيات لاهداف سيئة
- تصنيف البرامجيات لاهداف سيئة
- طرق استشعار البرامجيات لاهداف سيئة
- تشكيل وسط تحليلي (تأسيس لاب Lab)
- طرق التحليل الاستاتيكية
- وسائط التحليل الاستاتيكي واستعمالها
- طرق التحليل الديناميكي
- وسائط التحليل الديناميكي واستعمالها
- تحليل شبكات البرامجيات لاهداف سيئة
- طرق الهندسة لما يعاكسه
- الثغرات الامنية, Expolit (الطرد) وكتل Expolit (الطرد)
- برامجيات الفدية
- هجمات العدوات بدون ملف
- البرامجيات الخاصة بالاعمال المصرفية اونلاين لاهداف سيئة

الشروط المطلوب توفرها في المشاركين

- يتوجب ان يكون المشاركين اصحاب معلومات في عمل البرامج وتحليل البرامجيات المضرة الاساسية.

Jours / Heures Рабочих Дней / Часов المدة	5/30	Nombre D'enseignants Количество Преподавателей عدد المدربين	3	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

TEMEL NETWORK EĞİTİMİ
BASIC TRAINING ON NETWORK

AMAÇ

Katılımcıların ağ ve ağ güvenliği ürünlerini temel anlamda kullanabilmesi ve bu ürünlerde karşımıza çıkabilecek sorunlarda gerekli birimlerle iletişime geçilmesi.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her katılımcı:
- Ağ cihazları ve yapıları hakkında bilgi sahibi olarak bu sistemlerin nasıl çalıştığını öğrenecek.
- Ağ arıza durumlarının hangi nedenlerden olduğunu tahmin ederek arızaların giderilmesine hakkında bilgi sahibi olacaktır.

İÇERİK

- Ağ kavramı ve ağ topolojileri,
- Ağ cihazları ve ağ kurulumu,
- TCP/IP Modeli,
- OSI Katmanları,
- Switch, Firewall, Router yönetimi

KATILIMCILARDA ARANAN ŞARTLAR

- Orta seviyede bilgisayar bilgisine sahip olmak
- Bilişim teknolojilerini takip etmek

ARAÇ, GEREÇ VE MALZEMELER

- Orta Seviye donanıma sahip kursiyer bilgisayarı

PURPOSE

Participants will basically be able to use network and network security products. Also they will have knowledge about networking.

TARGET BEHAVIORS

End of this course, each participant:
- will learn about network devices and structures and how these systems work.
- will have knowledge about troubleshooting by estimating the causes of Network failures.

CONTENT

- Network concept and network topologies,
- Network devices and network setup,
- TCP/IP Model,
- OSI Layers,
- Switch, Firewall, Router management

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Intermediate level of computer knowledge
- To follow information technologies

TOOLS AND MATERIALS

- Intermediate level trainee computer

İş Günü / Saat Workdays / Hour: 5/30

Eğitici Sayısı Number of Trainers: 1-3

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION DE BASE SUR LES RÉSEAUX INFORMATIQUE
БАЗОВЫЙ ТРЕНИНГ ПО СЕТИ
التدريب على الشبكات الاساسية

NO
18-14

OBJECTIFS

Участники в основном смогут использовать сеть и продукты сетевой безопасности и обращаться в необходимые подразделения в случае возникновения проблем, которые могут возникнуть в этих продуктах.

RESULTATS EXIGES

A l'issue de cette formation, les participants auront les capacités de

- decouvrir le fonctionnement de ces systèmes en ayant des connaissances sur les dispositifs et les structures de réseau.
- disposer d'informations sur le dépannage en estimant les causes des défaillances du réseau

CONTENU

- Concept de réseau et topologies de réseau,
- Périphériques réseau et configuration réseau,
- Modèle TCP/IP,
- Couches du modèle OSI,
- Gestion du commutateur, du pare-feu et du routeur

CONDITIONS EXIGES DES PARTICIPANTS

- Avoir des connaissances informatiques de niveau intermédiaire
- Suivre les technologies de l'information

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur équipé de niveau intermédiaire

ЦЕЛЬ

Цель состоит в том, чтобы развивать знания и навыки по мобильным вредоносным программам сотрудников, работающих в подразделениях по борьбе с киберпреступностью, определять возможности вредоносного ПО и анализировать его с применением методов статического и динамического анализа.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:

- Участники узнают о сетевых устройствах и структурах, а также о том, как эти системы работают.
- Участники получат знания об устранении неполадок путем оценки причин сетевых сбоев.

СОДЕРЖАНИЕ

- Концепция сети и сетевые топологии,
- Сетевые устройства и настройка сети,
- Модель TCP/IP,
- Уровни модели взаимодействия открытых систем,
- Переключатель, межсетевой экран, программа прокладки маршрута

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Владение компьютером, средний уровень
- Следить за информационными технологиями

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Ordinateur équipé de niveau intermédiaire

الهدف

سيقوم المشاركين بتوفير الاتصال مع الوحدات الضرورية في المشاكل الذي من الممكن ان يظهر امامنا في هذه المنتجات وامكانية استعمالها بالمفهوم الاساسي للشبكات ومنتجات أمن الشبكات.

السلوك المستهدف

وفي نهاية هذه الدورة سيحصل كل موظف:

- معرفة كيفية عمل هذه الانظمة مع كونكم صاحب المعلومات فيما يخص اجهزة الشبكات و هيكلياتها,
- سيكونون اصحاب معلومات فيما يخص ازالة العطلات من خلال تخمين كون وضعية عطلات الشبكات لأي سبب.

المحتوى

- مصطلحات الشبكات ومخططات الشبكات,
- اجهزة الشبكات وتركيب الشبكات,
- انماط TCP/IP,
- شبكات OSI,
- طرق المفتاح, جهاز الحماية والراوتر

الشروط المطلوب توفرها في المشاركين

- ان تكون صاحب معلومات في الحاسوب الالي بمستويات متوسطة
- متابعة تقنيات المعلوماتية

الأدوات والتجهيزات اللازمة

- حاسوب الي للمتدربين الذين يمتلكون تجهيزات بمستويات متوسطة

Jours / Heures
Рабочих Дней / Часов
المدة
5/30

Nombre D'enseignants
Количество Преподавателей
عدد المدربين
1-3

Nombre de Coursiere
Количество Участников
عدد المتدربين
15-20

TEMEL SUNUCU SİSTEMLERİ EĞİTİMİ
BASIC SERVER SYSTEMS TRAINING

AMAÇ

Katılımcıların temel sunucu sistemleri ve sistemle entegre çalışabilen ürünler hakkında bilgi sahibi olmaları ve bu ürünleri kendi birimlerinde uygulayabilecek ve kullanabilecek düzeyde bilgi sahibi olmaları

HEDEF DAVRANIŞLAR

Bu kursun sonunda her katılımcı:
- Sunucu sistemleri ve depolama birimleri hakkında bilgi edinecek ve bu sistemlerin nasıl çalıştığını öğrenecek
- Sanallaştırma, DHCP, DNS, LDAP, Radius, Active Directory ve Grup Politikalarını öğrenecek ve uygulayacak

İÇERİK

- Sunucu Sistemleri ve Depolama Birimleri
- Sanallaştırma ve ESXI kurulumu
- Windows Server 2019 Kurulumu
- Active Directory Kurulumu
- DNS-DHCP Kurulumu
- LDAP-Radius Sistemleri
- Active Directory Grup Politikaları ve Uygulamaları

KATILIMCILARDA ARANAN ŞARTLAR

- Temel Network Eğitimini Almış olmaları tavsiye edilir

ARAÇ, GEREÇ VE MALZEMELER

- Bilgisayar (Sanallaştırılabilecek donanımına sahip)

PURPOSE

Participants should have knowledge about basic server systems and products that can work integrated with the system, and have knowledge at a level to be able to implement and use these products in their units.

TARGET BEHAVIORS

At the end of this course, each participant:
- will learn about server systems and storage units and learn how these systems work
- will learn and implement Virtualization, DHCP, DNS, LDAP, Radius, Active Directory and Group Policies

CONTENT

- Server Systems and Storage Units
- Virtualization-ESXI Installation
- Windows Server 2019 Installation
- Active Directory Installation
- DNS -DHCP Installation
- LDAP-Radius Systems
- Active Directory Group Policies and Practices

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Recommended that they have received Basic Network Training

TOOLS AND MATERIALS

- Computer (with a hardware that can be virtualized)

İş Günü / Saat Workdays / Hour 5/35

Eğitici Sayısı Number of Trainers 1-3

Kursiyer Sayısı Number of Trainees 15-20

FORMATION SUR LES SYSTÈMES SERVEUR DE BASE
БАЗОВЫЙ ТРЕНИНГ СЕРВЕРНЫМ СИСТЕМАМ
التدريب على انظمة التقديم الاساسية

NO
18-15

OBJECTIFS

L'objectif de cette formation est de s'assurer que les participants disposent d'informations sur les systèmes de serveur de base et les produits qui peuvent fonctionner de manière intégrée avec le système, et qu'ils ont un niveau de connaissances pour appliquer et utiliser ces produits dans leurs propres unités.

RESULTATS EXIGES

A l'issue de cette formation, les participants
- connaîtront les systèmes de serveurs et les unités de stockage et apprendra comment ces systèmes fonctionnent
- apprendront et mettra en œuvre la virtualisation, DHCP, DNS, LDAP, Radius, Active Directory et les politiques de groupe

CONTENU

- Systèmes de serveurs et unités de stockage
- Virtualisation et l'installation de l'ESXI
- Installation de Windows Server 2019
- Installation d'Active Directory
- Installation DNS-DHCP
- Systèmes LDAP Radius
- Stratégies et les pratiques de groupe Active Directory

CONDITIONS EXIGES DES PARTICIPANTS

- Il est recommandé qu'ils aient suivi la formation de base sur les réseaux informatique

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur (avec le matériel qui peut être virtualisé)

ЦЕЛЬ

Участники должны иметь знания об основных серверных системах и продуктах, которые могут работать интегрированно с системой, и обладать знаниями на уровне, позволяющем внедрить и использовать эти продукты в своих подразделениях.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

В конце этого курса каждый участник:
- Узнает о серверных системах и устройствах хранения и узнает, как эти системы работают.
- Изучит и внедрит виртуализацию, DHCP (протокол динамического конфигурирования хост-машины), DNS (система именования доменов), LDAP (облегчённый протокол доступа к каталогам), RADIUS, служба каталогов Active Directory и групповых политик.

СОДЕРЖАНИЕ

- Серверные системы и устройства хранения
- Установка виртуализации-ESXI
- Установка Windows Server 2019
- Установка Active Directory
- Установка DNS-DHCP
- Системы LDAP-Radius
- Групповые политики и практика Active Directory

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Рекомендуется, чтобы они прошли базовое сетевое обучение.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Компьютер (есть аппаратное обеспечение, которое можно виртуализировать)

الهدف

ان يكون المشاركين اصحاب معلومات بالمستويات الذي من الممكن ان يتم استعمال هذه المنتجات وتطبيقها في وحداتها وان يكونوا اصحاب معلومات فيما يخص المنتجات الذي يمكنه ان يعمل بشكل متكامل مع هذا النظام وانظمة التقديم الاساسية.

السلوك المستهدف

وفي نهاية هذه الدورة سيحصل كل موظف:
- معرفة كيفية عمل هذا النظام والحصول على المعلومات فيما يخص وحدات التخزين وانظمة التقديم.
- سيتم معرفة وتطبيق سياسات المجاميع و DHCP, DNS, LDAP, Radius, Active Directory والافتراضية.

المحتوى

- انظمة التقديم ووحدات التخزين
- تأسيس الافتراضيات وESXI,
- تأسيس ويندوز سيرفر 2019,
- تأسيس الدليل النشط (Active Directory),
- تأسيس DNS-DHCP
- انظمة LDAP-Radius
- سياسات مجموعة الدليل النشط وتطبيقاتها

الشروط المطلوب توفرها في المشاركين

- يتم توصية كونهم قد حصلوا على تدريب الشبكات الاساسية

الأدوات والتجهيزات اللازمة

- الحاسوب الالي (امتلاك التجهيزات الذي من الممكن ان يكون افتراضيا)

Jours / Heures Рабочих Дней / Часов المدة	5/35	Nombre D'enseignants Количество Преподавателей عدد المدربين	1-3	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

ÇEVRİMİÇİ ÇOCUK MÜSTEHCENLİĞİ VE TACİZİ İLE MÜCADELE EĞİTİMİ
TRAINING ON COUNTERING ONLINE CHILD OBSCENITY AND HARRESMENT CRIMES

AMAÇ

Çocuğa Karşı İşlenen Müstehcenlik ve Taciz Suç Soruşturmalarında etkin rol almak ve Çocuk müstehcenliği ve tacizi soruşturma personelinin eksikliklerini geliştirmek.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel Çocuğa Karşı İşlenen Müstehcenlik ve Taciz Suç Soruşturmalarında
- Yaşanan aksaklıkların giderilmesi,
- Mücadele kapsamında kullanılan farklı metodlar ile ilgili bilgi alışverişinin sağlanması,
- Personel verimliğinin artırılması

İÇERİK

- Mevzuat – Tanımlar – Müstehcenlik ve Cinsel Taciz Suçunun İşleniş Şekilleri ve Suç Yöntemleri – Örnek Olay
- Sosyal Medya Platformları Üzerinden Araştırma Yöntemleri –CPS Yazılımı- Bilgi Talebi Yazışmaları
- Çocuk İstismarında Mücadelede Yardımcı Kuruluşlar (NCMEC- NCCEC)- Yurt Dışı Gelen Raporların İncelenmesi ve Dikkat Edilecek Hususlar
- Örnek Dosya İncelemesi - Çocuk İstismarı Suçunun Meydana Geldiği Sitelerin Tespiti ve Yapılan Çalışmalar – Online Oyunlar Üzerinden Meydana Gelen Çocuk İstismarı Suçunun Tespiti
- Mağdur kimlik tespitine yönelik yapılan çalışmalar, ICSE Veri Tabanı
- Soruşturma Süreci ve Planlı Projeli Dosya Hazırlama

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlar Biriminde çalışıyor olmalıdır.
- Katılımcılar ilgili kanunlar hakkında bilgi sahibi olmalı ve siber suç alanında temel seviyede teknik kapasiteye sahip olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- İnternete bağlı yüksek teknolojili bilgisayar, projektör, flash bellek

PURPOSE

To improve personnel investigation skills who works on Crime Against Child Obscenity and Abuse Investigations.

TARGET BEHAVIORS

End of these training, every personnel who take this training will be better on;
- Solving problems which is faced on investigations
- Information exchanges about different investigation methods
- Improve personnel productivity

CONTENT

- Laws – Definitions– Ways of commit child obscenity and abuse crimes – Case Study
- Ways of research on Social Media Platforms – Cps Software – Information Request Methods
- Subsidiaries on combatting Child abuse (NCMEC- NCECC) – Examinations of Foreign Country Reports and things to know
- Study Case –-Detection of web sites where Child abuse crime is commited – Detection of commited child abuse crimes via online games
- Works of victim identification. ICSE Database
- Investigation process and preparing planned project cases

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Participants should be working on Cyber Crime Unit
- Participants should have knowledge about related laws and basic level technical knowledge about combatting Cybercrime

TOOLS AND MATERIALS

- High technology computer with internet connection, Projector, Flash Memory

İş Günü / Saat Workdays / Hour 5/28

Eğitici Sayısı Number of Trainers 4-5

Kursiyer Sayısı Number of Trainees 15-20

FORMATION SUR LA LUTTE CONTRE L'OBSCÉNITÉ DES ENFANT ET L'ABUS SEXUEL SUR MINEUR
ТРЕНИНГ ПО БОРЬБЕ С ОНЛАЙНОВЫМ НЕПРИСТОЙНОСТЬЮ И СЕКСУАЛЬНЫМ НАСИЛИЕМ НАД ДЕТЬМИ
التدريب على مكافحة التحرش بالاطفال ومضايقتهم عبر الانترنت

NO
18-16

OBJECTIFS

L'objectif de cette formation est de veiller à ce que personnel qui travaille dans le domaine des enquêtes sur les crimes contre l'obscénité et la maltraitance des enfants joue un rôle actif dans les enquêtes criminelles sur l'obscénité des enfants et l'abus sexuel sur mineur et élimine ses lacunes.

RESULTATS EXIGES

A l'issue de cette formation, les participants
- éliminera les problèmes dans les enquêtes criminelles sur l'obscénité des enfants et l'abus sexuel sur mineur.
- assureront l'échange d'informations sur les différentes méthodes utilisées dans le cadre de la lutte.
- La productivité du personnel sera augmentée

CONTENU

- Législation - Définitions – les façons de commettre des crimes d'obscénité des enfant et l'abus sexuel sur mineur - Étude de cas
- Méthodes de recherche sur les plateformes de médias sociaux - Logiciel CPS - Correspondance des demandes d'informations
- Organisations auxiliaires de lutte contre l'abus sexuel sur mineur (NCMEC-NCCEC) - Examen des rapports de pays étrangers et les considérations
- Exemple d'analyse de fichiers – Détection des sites où se produisent des crimes de l'abus sexuel sur mineur et les études réalisées – Détection des crimes de maltraitance des enfants par le biais de jeux en ligne
- Travaux d'identification des victimes, la base de données ICSE
- Processus d'enquête et la préparation du dossier de projet prévu

CONDITIONS EXIGES DES PARTICIPANTS

- Les participants doivent travailler dans des unités des cybercrimes.
- Les participants doivent avoir des connaissances sur les lois pertinentes et avoir un niveau de capacité technique de base dans le domaine de la cybercriminalité.

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur de technologie haut de gamme connecté à Internet, projecteur, mémoire flash

ЦЕЛЬ

Улучшить навыки проведения расследований персонала, который занимается расследованиями преступлений против детской непристойности и сексуального насилия над детьми.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

По окончании этого курса каждый участник будет участвовать в расследовании случаев преступлений против детской непристойности и сексуального насилия над детьми.
- Устранение возникших проблем,
- Обеспечение обмена информацией о различных методах, используемых в рамках борьбы,
- Иметь информацию о повышении эффективности персонала.

СОДЕРЖАНИЕ

- Законы – Определения – Способы совершения преступлений, связанных с непристойным поведением и сексуальным насилием над детьми – Пример из практики
- Способы исследования платформ социальных сетей – Программное обеспечение CPS – Методы запроса информации
- Дочерние организации по борьбе с сексуальным насилием над детьми (NCMEC-NCECC) – изучение отчетов зарубежных стран и полезные сведения
- Тематическое исследование – Обнаружение веб-сайтов, на которых совершаются преступления, связанные с жестоким обращением с детьми – Обнаружение совершенных преступлений, связанных с сексуальным насилием над детьми, с помощью онлайн-игр.
- Работы по идентификации пострадавших. База данных МКС3)
- Процесс расследования и подготовка запланированных случаев проекта

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.
- Участники должны обладать знаниями о соответствующих законах и базовыми техническими знаниями о борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Высокотехнологичный компьютер с подключением к Интернету, проектор, карта памяти

الهدف

تطوير نقوصات الموظفين في جرائم الاغتصاب واستهجان الاطفال ولعب دور مؤثر في استجواب جرائم الاستهجان والاغتصاب الذي يتم ممارستها تجاه الاطفال.

السلوك المستهدف

التحقيق حول جرائم الاستهجان والاغتصاب الذي يتم ممارسته تجاه الاطفال لكل موظف من الموظفين في نهاية هذه الدورة.
- ازالة التقصيرات الذي تم التعض لها,
- توفير تسويق المعلومات المتعلقة بنظريات مختلفة والمستخدمة ضمن شمولية المحاربة,
- زيادة انتاجية الموظف,

المحتوى

- الموضوعات – التعاريف – الاستهجان والاغتصاب الجنسي, طرق الجرائم واشكال ممارسة الجريمة – الاحداث النموذجية,
- طرق البحث من على منصات التواصل الاجتماعي – برامجيات CPS – برامجيات طلب المعلومات,
- المؤسسات المساعدة في محاربة استغلال الاطفال (NCMEC-NCCEC) – الموضوعات الذي يجب الانتباه اليها والتدقيق في التقارير التي تأتي من خارج القطر,
- التدقيق في الملف النموذجي – الاعمال الذي يتم القيام به وتثبيت المواقع التي تظهر في جرائم استغلال الاطفال – تثبيت جريمة استغلال الاطفال والتي تظهر من على العاب اونلاين,
- الاعمال الذي يتم القيام به باتجاه تثبيت هوية المظلوم, قاعدة بيانات ICSE,
- فترات التحقيق تجهيز الملفات ذات المشاريع المخططة,

الشروط المطلوب توفرها في المشاركين

- ان يكون المشاركين يعملون في وحدة الجرائم الالكترونية,
- ان يكون المشاركين يمتلكون سعة تقنية بمستويات اساسية في مجال الجرائم الالكترونية وان يكونوا اصحاب معلومات فيما يخص القوانين ذات العلاقة.

الأدوات والتجهيزات اللازمة

- الحاسوب الالي ذو تكنولوجيات عالية مرتبطة بالانترنيت, جهز التسقيط, ذاكرة فلاش

Jours / Heures Рабочих Дней / Часов المدة	5/28	Nombre D'enseignants Количество Преподавателей عدد المدربين	4-5	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

ÇEVRİMİÇİ YASA DIŞI BAHİS VE KUMARLA MÜCADELE EĞİTİMİ
TRAINING ON COUNTERING ONLINE ILLEGAL BETTING AND GAMBLING

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:

- Çevrimiçi Yasa Dışı Bahisle Mücadelede daha etkili ve verimli görev yaparak yasa dışı faaliyetlerde kullanılan gelirle ile ilgili soruşturma dosyası oluşturarak el koyma işlemlerinin hukuka uygun bir şekilde gerçekleştirmek.

İÇERİK

- Yasa dışı bahis mevzuat – Tanımlar – Çevrimiçi Yasa Dışı Bahis Suçunun İşleniş Şekilleri – Yasa Dışı Bahis Oynatılma Yöntemleri – Örnek Olay
- Yasa Dışı Bahisle Mücadele kapsamında yapılması gerekenler ve dikkat edilmesi gereken hususlar – Yasa dışı bahisle mücadele kapsamında müşterek çalıştığımız kurumlar ve yazışmalar
- Sosyal Platformlar üzerinde Araştırma Yöntemleri ve Araştırma raporu hazırlama
- IP ve Domain sorgulama araçları – Soruşturma dosyası hazırlama –Tespit edilen Türkiye lokasyonlu sunucuların incelenmesi süreci ve dikkat edilmesi gereken hususlar
- Yasa dışı bahis kapsamında yapılan çalışmalar sonucu tespit edilen şahısların ve şirketlerin mal varlıklarıyla ilgili çalışmalar yapılması ve Suç Gelirleriyle Mücadele kapsamında incelenmesi
- Soruşturma süreci ve planlı projeli dosya hazırlama

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.
- Katılımcılar Siber Suçlarla Mücadele konusunda kanuni bilgiye ve giriş düzeyinde teknik bilgiye sahip olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Yüksek donanımlı ve ihtiyacı karşılayacak internet ağına bağlı bilgisayar, Projeksiyon.

PURPOSE

To develop the knowledge and skills of the personnel working in the Anti-Cyber Crime units and to ensure that they work in accordance with ethical principles and within the framework of legal rules.

TARGET BEHAVIORS

At the end of this course, each staff member:

- To carry out the confiscation proceedings in accordance with the law by creating an investigation file regarding the income used in illegal activities by performing a more effective and efficient task in Combating Online Illegal Betting.

CONTENT

- Illegal betting legislation – Definitions – Online Illegal Gambling Offenses – Illegal Betting Methods – Case Study
- What to do and what to pay attention to within the scope of Fight Against Illegal Betting – Institutions and correspondence with which we work jointly within the scope of combating illegal betting
- Research Methods on Social Platforms and Preparing a Research Report IP and Domain query tools – Investigation file preparation – The process of examining the detected servers located in Turkey and the points to be considered
- Conducting studies on the assets of individuals and companies identified as a result of studies carried out within the scope of illegal betting and examining them within the scope of Combating Proceeds of Crime.
- Investigation process and preparing a planned project file

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Participants must be in charge of the Cyber Crime Units.
- Participants should have legal knowledge and introductory technical knowledge on Combating Cybercrime.

TOOLS AND MATERIALS

- Highly equipped computer for meeting requirements with internet connection and Projection.

İş Günü / Saat Workdays / Hour: 5/26

Eğitici Sayısı Number of Trainers: 4-5

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION SUR LA LUTTE CONTRE LES JEUX D'ARGENT ET DE HASARD ILLÉGAUX
ТРЕНИНГ ПО БОРЬБЕ С ОНЛАЙНОВЫМИ НЕЛЕГАЛЬНЫМИ АЗАРТНЫМИ ИГРАМИ И СТАВКАМИ
التدريب على محاربة الالعاب والمراهنات غير المشروعة عبر الانترنت

NO
18-17

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans les unités de lutte contre la cybercriminalité et veiller à ce qu'il travaille conformément aux principes éthiques et dans le cadre des règles légales.

RESULTATS EXIGES

- À l'issue de cette formation de formation les participants peuvent mener à bien la procédure de confiscation conformément à la loi en créant un dossier d'enquête concernant les revenus utilisés dans des activités illégales en effectuant une tâche plus efficace et efficiente dans la lutte contre les paris illégaux en ligne.

CONTENU

- Législation sur les paris illégaux – Définitions – Délits de jeu illégal en ligne – Étude de cas
- Que faire et à quoi faire attention dans le cadre de lutte contre les paris illégaux – Institutions avec lesquelles nous collaborons dans le cadre de la lutte contre les paris illégaux et les correspondances
- Méthodes de recherche sur les plateformes sociales et la préparation d'un rapport de recherche
- Outils de requête de vérification d'adresse IP et de domaine - Préparation du dossier d'enquête - Le processus d'examen des serveurs détectés situés en Turquie et les points à considérer
- Réaliser des études sur le patrimoine des personnes physiques et morales identifiées à la suite d'études menées dans le cadre des paris illégaux et les examiner dans le cadre de la Lutte contre les produits du crime.
- Processus d'enquête et la préparation du dossier de projet prévu.

CONDITIONS EXIGES DES PARTICIPANTS

- Les participants doivent travailler dans des unités des cybercrimes.
- Les participants doivent avoir des connaissances sur les lois pertinentes et avoir un niveau de capacité technique de base dans le domaine de la cybercriminalité.

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur de technologie haut de gamme connecté à Internet, le projecteur,

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях по борьбе с киберпреступностью, и обеспечивать, чтобы они работали в соответствии с этическими принципами и в рамках правовых норм.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

По окончании курса каждый участник:

- Провести процедуру конфискации в соответствии с законом, создав досье о доходах, использованных в незаконной деятельности, путем выполнения более эффективной и действенной задачи по борьбе с незаконными онлайн-ставками.

СОДЕРЖАНИЕ

- Законодательство о незаконных ставках – Определения – Нарушения, связанные с незаконными азартными играми в Интернете – Незаконные методы заключения пари – Практический пример,
- Что делать и на что обратить внимание в рамках борьбы с незаконными ставками – учреждения и переписка, с которыми мы сотрудничаем в рамках борьбы с незаконными ставками,
- Методы исследования социальных платформ и подготовка отчета об исследовании,
- Инструменты запроса IP и домена – Подготовка файла расследования – Процесс изучения обнаруженных серверов, расположенных в Турции, и моменты, которые необходимо учитывать,
- Проведение исследований активов физических лиц и компаний, выявленных в результате исследований, проведенных в рамках незаконных тотализаторов, и их проверка в рамках борьбы с преступными доходами,
- Процесс расследования и подготовка файла запланированного проекта.

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.
- Участники должны обладать знаниями о соответствующих законах и базовыми техническими знаниями о борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Высокотехнологичный компьютер с подключением к интернету, проектор

الهدف

ان الهدف هو توفير القيام بتأدية الوظيفة ضمن اطار القواعد والشروط القانونية المرتبطة بالمبادئ المؤثرة في وظيفته وتطوير المهارات والقابليات والمعلومات الخاصة بالموظفين المخولين في وحدة محاربة الجرائم الالكترونية.

السلوك المستهدف

ان كل موظف في نتيجة هذه الدورة:

- تحقيق محاربة الرهانات الغير القانونية اونلاين وتطويرها بشكل ملائم لقانون معاملات الحفاظ من خلال تشكيل ملف التحقيق ذات العلاقة بالاشتراك مع الايرادات المستخدمة في الفعاليات والنشاطات خارج القانون من خلال تأدية الوظائف بشكل انتاجي ومؤثر اكثر.

المحتوى

- الموضوعات المتعلقة بالرهانات خارج القانون – التعاريف – اشكال اشتغال الجريمة نتيجة الرهانات خارج القانون اونلاين – طرق تشغيل الموضوعات للرهانات خارج القانون – الاحداث النموذجية
- الموضوعات الذي يتوجب ان يتم الانتباه اليه وضرورات القيام بها ضمن شمولية التدخل في الرهانات خارج القطر – المؤسسات والمكاتبات الذي عملنا فيها بشكل مشترك ضمن شمولية المحاربة مع الرهانات في خارج القطر
- تجهيز تقرير البحث وطرق البحث على المنصات الاجتماعية.
- وسائط الاستعلام عن المجال وIP – تجهيز ملف التحقيق – الموضوعات الذي يتوجب الانتباه اليه وفترات التدقيق في النتائج الذي موقع تركيا والذي تم تثبيته.
- التدقيق ضمن شمولية الحرب مع ايرادات الجريمة والقيام بانجاز الاعمال ذات العلاقة بالموجودات المالية للشركة والاشخاص الذي تم تثبيتهم في نتيجة الاعمال الذي تم انجازها ضمن شمولية الرهان الغير القانوني.
- تجهيز ملف ذو مشروع مخطط وفترات التحقيق.

الشروط المطلوب توفرها في المشاركين

- ان يكون المشتركين موظفين في وحدات المحاربة مع الجرائم الالكترونية,
- ان يكون المشاركين اصحاب معلومات تقنية بمستويات الدخول والمعلومات القانونية في موضوع محاربة الجرائم الالكترونية.

الأدوات والتجهيزات اللازمة

- الحاسوب الالي المرتبط بشبكات الانترنيت الذي يلبي الحاجة وذو تجهيزات عالية, جهاز التسقيط.

Jours / Heures Рабочих Дней / Часов المدة	5/26	Nombre D'enseignants Количество Преподавателей عدد المدربين	4-5	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

ÖDEME SİSTEMLERİ VE BİLİŞİM SUÇLARIYLA MÜCADELE EĞİTİMİ
TRAINING ON PAYMENT SYSTEMS AND COUNTER IT CRIMES

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:

- Ödeme Sistemleri ve Bilişim Suçlarıyla Mücadele Mevzuatını, cezai yaptırımlarını, bilgi-belge temini sürecini, suç türlerini, suç yöntemlerini ve bu suçların soruşturma yöntemlerini öğrenecektir.
- Ödeme Sistemleri ve Bilişim Suçlarında örnek olaylar ile öğrendiklerini pekiştirecek olup soruşturma süreçlerini daha etkin kullanabilecektir.

İÇERİK

- Soruşturmaya Giriş
- Ödeme Sistemleri ve Bilişim Suçlarıyla Mücadele Mevzuatı ve Cezai Yaptırımlar
- Bilgi ve Belge Temini
- Suç Türleri ve Yöntemleri
- Soruşturma Aşamaları
- Örnek Olay
- Soruşturma Süreci ve Planlı Projeli Dosya Hazırlama

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Bilgisayar, Kamera, Projeksiyon

PURPOSE

To develop the knowledge and skills of the personnel working in the Counter Cyber Crime units and to ensure that they work in accordance with ethical principles and within the framework of legal rules.

TARGET BEHAVIORS

At the end of this course, each staff member:

- Will learn the Legislation of Payment Systems and IT Crime Combat, criminal sanctions, information-document supply process, types of crime, crime methods and investigation methods of these crimes.
- They will reinforce what they have learned with case studies in Payment Systems and IT Crimes and will be able to use the investigation processes more effectively.

CONTENT

- Introduction to Investigation
- Legislation and Penal Sanctions for Payment
- Systems and Combating Cybercrime
- Information and Documentation
- Types and Methods of Crime
- Investigation Stages
- Case study Investigation Process and Planned Project File Preparation

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Participants should be working in the Cyber Crime units.
- Participants should have knowledge related laws and basic-level technical knowledge in Combating Cybercrime.

TOOLS AND MATERIALS

- Computer, Camera, Projection

İş Günü / Saat Workdays / Hour: 5/27

Eğitici Sayısı Number of Trainers: 4-8

Kursiyer Sayısı Number of Trainees: 15-20

FORMATION SUR LES SYSTÈMES DE PAIEMENT ET LA LUTTE CONTRE LA CYBERCRIMINALITÉ
ОБУЧЕНИЕ ПЛАТЕЖНЫМ СИСТЕМАМ И БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ
التدريب على محاربة الجرائم المعلوماتية وانظمة الدفع

NO
18-18

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans les unités de lutte contre la cybercriminalité et veiller à ce qu'il travaille conformément aux principes éthiques et dans le cadre des règles légales.

RESULTATS EXIGES

À l'issue de cette formation, les participants;

- apprendra la législation sur les systèmes de paiement et la lutte contre la cybercriminalité, les sanctions pénales, le processus de fourniture de documents d'information, les types de délits, les méthodes de délit et les méthodes d'enquête de ces délits.
- renforceront ce qu'il a appris avec des études de cas sur les systèmes de paiement et les délits informatiques et sera en mesure d'utiliser les processus d'enquête plus efficacement.

CONTENU

- Introduction à l'enquête
- Législation et les sanctions pénales pour les systèmes de paiement et la lutte contre la cybercriminalité
- Système de paiement, la législation sur la lutte contre la cybercriminalité et les sanctions pénales
- Fournir des informations et de la documentation
- Types et méthodes de crime
- Étapes de l'enquête
- L'étude de cas et la préparation du dossier de projet prévu

CONDITIONS EXIGES DES PARTICIPANTS

- Les participants doivent travailler dans des unités des cybercrimes.

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur, caméra, projecteur

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях по борьбе с киберпреступностью, и обеспечивать, чтобы они работали в соответствии с этическими принципами и в рамках правовых норм.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

По окончании курса каждый участник:

- Изучит Законодательство о платежных системах и борьбе с киберпреступностью, уголовные санкции, процесс предоставления информации и документов, виды преступлений, способы совершения преступлений и методы расследования этих преступлений,
- Закрепит полученные знания с помощью тематических исследований по платежным системам и преступлениям в сфере информационных технологий и сможет более эффективно использовать процессы расследования.

СОДЕРЖАНИЕ

- Введение в расследование,
- Законодательство и уголовные санкции для платежных систем и борьбы с киберпреступностью,
- Информация и документация,
- Виды и способы преступления,
- Этапы расследования,
- Тематическое исследование,
- Процесс расследования и подготовка файла запланированного проекта.

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Компьютер, Камера, Проектор

الهدف

ان الهدف هو توفير القيام بتأدية الوظيفة ضمن اطار القواعد والشروط القانونية المرتبطة بالمبادئ المؤثرة في وظيفته وتطوير المهارات والقابليات والمعلومات الخاصة بالموظفين المخولين في وحدة محاربة الجرائم الالكترونية.

السلوك المستهدف

ان كل موظف في نتيجة هذه الدورة:

- موضوعات محاربة الجرائم المعلوماتية وانظمة الدفع, العقوبات الجنائية, فترات تأمين المعلومات – الوثائق, انواع الجرائم, ادارة الجرائم ومعرفة طرق التحقيق في هذه الجرائم وطرق الجرائم,
- من الممكن ان يقوم باستعمال انظمة الدفع والجرائم المعلوماتية بشكل مؤثر اكثر لفترات التحقيق حيث تم تعزيزها مع ماتعلموه بالاشتراك مع الاحداث النموذجية

المحتوى

- الدخول الى التحقيق
- العقوبات الجنائية وموضوعات التدخل مع تهم المعلوماتية وانظمة الدفع,
- تأمين المعلومات والوثائق
- انواع الجرائم وطرقها
- ابحاث التحقيق
- الاحداث النموذجية
- تجهيز الملف ذو المشروع المخطط وفترات التحقيق

الشروط المطلوب توفرها في المشاركين

- يجب ان يكون المشاركين موظفين في وحدات محاربة الجرائم الالكترونية.

الأدوات والتجهيزات اللازمة

- الحاسوب الالي , الكاميرا, جهاز التسقيط

Jours / Heures Рабочих Дней / Часов المدة	5/27	Nombre D'enseignants Количество Преподавателей عدد المدربين	4-8	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

SUÇ GELİRLERİYLE MÜCADELE EĞİTİMİ (SİBER)
TRAINING ON COUNTER PROCEEDS OF CRIME (CYBER)

AMAÇ

Siber Suçlarla Mücadele birimlerinde görevli personellerin bilgi ve becerilerinin geliştirilmesi ve görevinde etik ilkelere bağlı, hukuki kurallar çerçevesinde görev yapmasını sağlamak.

HEDEF DAVRANIŞLAR

Bu kursun sonunda her personel:

- Suç Gelirleriyle Mücadelede Daha etkili ve verimli görev yaparak yasa dışı faaliyetlerde kullanılan gelirle ile ilgili soruşturma dosyası oluşturarak el koyma işlemlerinin hukuka uygun bir şekilde gerçekleştirmek.

İÇERİK

- Suç gelirleriyle mücadele mevzuat – tanımlar – aklama suçu
- Aklama suçunun işleniş şekilleri ve yöntemleri – örnek olay
- Suç gelirleriyle mücadele kapsamında müşterek çalıştığımız kurumlardan bilgi talep etme – Suçtan Kaynaklanan Değerlerin Araştırılması
- IP ve Domain sorgulama araçları –Suç Geliri Analiz Araçları – Soruşturma dosyası hazırlama
- Suç gelirleri kapsamında takibi yapılan soruşturma dosyasının hazırlanışı ve düzenlenmesi
- Soruşturma süreci ve planlı projeli dosya hazırlama

KATILIMCILARDA ARANAN ŞARTLAR

- Katılımcılar Siber Suçlarla Mücadele birimlerinde görevli olmalıdır.
- Katılımcılar Siber Suçlarla Mücadele konusunda kanuni bilgiye ve giriş düzeyinde teknik bilgiye sahip olmalıdır.

ARAÇ, GEREÇ VE MALZEMELER

- Yüksek donanımlı ve ihtiyacı karşılayacak internet ağına bağlı bilgisayar, Projeksiyon.

PURPOSE

To develop the knowledge and skills of the personnel working in the Counter Cyber Crime units and to ensure that they work in accordance with ethical principles and within the framework of legal rules.

TARGET BEHAVIORS

At the end of this course, each staff member:

- Fighting Proceeds of Crime To carry out the confiscation proceedings in accordance with the law by creating an investigation file regarding the revenue used in illegal activities by performing a more effective and efficient duty.

CONTENT

- Fight against proceeds of crime legislation – definitions – laundering crime
- Committed forms and methods of money laundering crime – case study
- Requesting information from the institutions we work with within the scope of combating the proceeds of crime – Investigation of Values Arising from Crime
- IP and Domain inquiry tools – Proceeds of Crime Analysis Tools – Investigation file preparation
- Preparation and arrangement of the investigation file followed within the scope of crime revenues
- Investigation process and preparing a planned project file

REQUIRED QUALIFICATIONS FOR PARTICIPANTS

- Participants should be working in the Cyber Crime units.
- Participants should have knowledge related laws and basic-level technical knowledge in Combating Cybercrime.

TOOLS AND MATERIALS

- Highly equipped computer for meeting requirements with internet connection and Projection.

İş Günü / Saat Workdays / Hour 5/27

Eğitici Sayısı Number of Trainers 4-5

Kursiyer Sayısı Number of Trainees 15-20

FORMATION SUR LA LUTTE CONTRE LES PRODUITS DU CRIME (CYBER)
ОБУЧЕНИЕ ПО БОРЬБЕ С ДОХОДАМИ ОТ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ (КИБЕР)
التدريب على محاربة عائدات الجريمة الالكترونية

NO
18-19

OBJECTIFS

L'objectif de cette formation est de développer les connaissances et les compétences du personnel qui travaille dans les unités de lutte contre la cybercriminalité et veiller à ce qu'il travaille conformément aux principes éthiques et dans le cadre des règles légales.

RESULTATS EXIGES

- À l'issue de cette formation, les participants mèneront dans le cadre de la lutte contre les produits du crime, les procédures de confiscation conformément à la loi en créant un dossier d'enquête concernant les revenus utilisés dans des activités illégales, en travaillant de manière plus efficace et efficiente.

CONTENU

- Legistation sur la lutte contre les produits du crime – les définitions – le crime de blanchiment
- Façons et les méthodes de commettre de crime de blanchiment – l'étude de cas
- Demander des informations aux institutions avec lesquelles nous collaborons dans le cadre de la lutte contre les produits du crime – Enquête sur les valeurs découlant du crime
- Outils de requête de vérification d'adresse IP et de domaine - Outils d'analyse des produits de la criminalité – La préparation du dossier d'enquête
- Préparation et l'arrangement du dossier d'enquête suivi dans le cadre des produits du crime
- L'étude de cas et la préparation du dossier de projet prévu

CONDITIONS EXIGES DES PARTICIPANTS

- Les participants doivent travailler dans des unités des cybercrimes.
- Les participants doivent avoir des connaissances sur les lois pertinentes et avoir un niveau de capacité technique de base dans le domaine de la cybercriminalité.

OUTILS ET APPAREILLES EQUIPEMENTS NÉCESSAIRES

- Ordinateur de technologie haut de gamme connecté à Internet, projecteur

ЦЕЛЬ

Развивать знания и навыки персонала, работающего в подразделениях по борьбе с киберпреступностью, и обеспечивать, чтобы они работали в соответствии с этическими принципами и в рамках правовых норм.

ЦЕЛЕВОЕ ПОВЕДЕНИЕ

По окончании курса каждый участник:

- сможет более эффективно и результативно работать в сфере борьбы с преступными доходами, а путем создания досье о расследовании доходов, использованных в незаконной деятельности, обеспечит проведение процессов конфискации в соответствии с законом.

СОДЕРЖАНИЕ

- Законодательство о борьбе с преступными доходами – определения – отмывание денег
- Совершаемые формы и методы отмывания денег – тематическое исследование,
- Запрос информации от учреждений, с которыми мы сотрудничаем, в рамках борьбы с преступными доходами – расследование ценностей, полученных преступным путем.
- Инструменты запроса IP и домена – Инструменты анализа доходов от преступлений – Подготовка файла расследования,
- Подготовка и оформление следственного дела в рамках доходов от преступлений,
- Процесс расследования и подготовка файла запланированного проекта.

ТРЕБОВАНИЯ К УЧАСТНИКАМ

- Участники должны работать в подразделениях по борьбе с киберпреступностью,
- Участники должны обладать знаниями о соответствующих законах и базовыми техническими знаниями о борьбе с киберпреступностью.

ИНСТРУМЕНТЫ, СРЕДСТВА И МАТЕРИАЛЫ

- Высокотехнологичный компьютер с подключением к интернету, проектор

الهدف

ان الهدف هو توفير القيام بتأدية الوظيفة ضمن اطار القواعد والشروط القانونية المرتبطة بالمبادئ المؤثرة في وظيفته وتطوير المهارات والقابليات والمعلومات الخاصة بالموظفين المخولين في وحدة محاربة الجرائم الالكترونية.

السلوك المستهدف

- ان كل موظف في نتيجة هذه الدورة:
- • تحقيقها بشكل ملائم للقانون في عمليات الحيازة من خلال تشكيل ملفات التحقيق ذات العلاقة بالعائدات المستعملة في الفعاليات والنشاطات خارج القانون من خلال القيام باداء وظيفة انتاجية ومؤثرة في محاربة عائدات الجريمة.

المحتوى

- جريمة تبييض – تعريف – موضوعات محاربة عائدات الجريمة
- الاحداث النموذجية – طرق واشكال اشتغال جريمة التبييض
- طلب المعلومات من المؤسسات الذي يعمل فيها بشكل مشترك ضمن شمولية محاربة عائدات الجريمة – اجراء الابحاث على القيم المتولدة من الجريمة
- ادوات الاستعلام عن IP والاستعلام عن المجال- وسائط تحليل عائدات الجريمة – تجهيز ملف التحقيق
- تجهيز وتنظم ملفات التحقيق الذي يتم القيام به من اجل المتابعة ضمن شمولية عائدات الجريمة
- تجهيز الملف ذات المشاريع المخططة وفترات التحقيق

الشروط المطلوب توفرها في المشاركين

- يجب ان يكون المشاركين موظفين في وحدات محاربة الجرائم الالكترونية.
- يجب ان يمتلك المشاركين المعلومات التقنية بمستويات الدخول والمعلومات القانونية في موضوع محاربة الجرائم الالكترونية.

الأدوات والتجهيزات اللازمة

- الحاسوب الالي المرتبط بشبكة الانترنيت الذي سيقوم بتلبية الاحتياجات ويكون ذو تجهيزات مرتفعة, جهاز التسقيط..

Jours / Heures Рабочих Дней / Часов المدة	5/27	Nombre D'enseignants Количество Преподавателей عدد المدربين	4-5	Nombre de Coursiere Количество Участников عدد المتدربين	15-20

DEPARTMENT OF CYBERCRIME

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

İncek Mahallesi Boztepe Sk. No:125 06830 Gölbaşı Ankara/Türkiye

+90 312 462 55 00

+90 312 286 92 06

siber@egm.gov.tr