

## 1. Koolituste pakumatus

Pakkuja on valmis läbi viima koolitusi kõikidel teemadel, **välja arvatud Macintosh forensic**. Nimetatud teemal näeme võimalust välisloktori kaasamiseks ja sellest sõltuvalt võib hind nimetatud kursusele olla oluliselt erinev teistest. Kuna käesoleval hetkel ei ole meil kindlaid kokkuleppeid välisloktoriga, siis antud pakumuses Macintosh forensic hinnapakumist välja toodud ei ole.

### 2.1 Muudatused pakutavas

Pakumuses on tehtud muudatused võrreldes koolitusvajaduses kirjeldatuga:

Windows 8 forensic ja Windows 10 forensic on liidetud üheks kursuseks

Vabavaraliste kriminalistika tarkvarade teemad on kaetud teiste pakutavate kursuste raames.

Kõikide pakutavate kursuste programmides on toodud lisainfo eelduste kohta kursusel osaleda soovijatele. Samuti on toodud tehnilised nõuded arvutiklassidele ja vajadusel ka serverile.

Kokkuvõttes tabelis on toodud info kursuste läbiviimise keele kohta ning hinnapakumised kahes variandis. Hinnapakumuses on aluseks võetud:

ühel juhul kursuse hind, kui koolitus toimub TTÜ ruumides ja TTÜ arvutitega, lisatud on

kohvipauside maksumus;

teisel juhul kursuse hind, kui koolitus toimub Tellija ruumides ja Tellija arvutitega ning kohvipausid korraldab Tellija.

Kursus	Keel	Õppematerjal	Päevade arv	TTÜ ruumides	Tellija ruumides
Combined Windows Forensic	Eng	Eng	5	8200€	5900€

## 2. Koolituste läbiviijad

Koolitusi viivad läbi TTÜ Küberkriminalistika ja Küberjulgeoleku Keskuse teadurid ja õppejõud.

Koolitajad on arvestanud Tellija sooviga viia koolitused läbi ajavahemikul 01. oktoober kuni 20. detsember 2016.

## 3. Koolituste programmid

### Combined Windows Forensic

**Course duration: 5 Days**

**Course Availability: October – December 2016**

**Main topics:**

This training on Windows forensics provides the knowledge and skills necessary to analyze Microsoft Windows operating system artifacts, user data, file system mechanics in storage spaces and some commonly used applications like Browsers and social media tools, with a special focus on Windows 8 and Windows 10.

In the first couple of lectures, participants will be briefly introduced to the overall concepts of digital forensics, especially focusing on NTFS file systems and partitioning.

Next, Windows related features like registry hives, event logs and volume shadow copies will be discussed. Participants will also practice OS artifacts saved under locations such as Virtual Hard Disks, Storage Pools, and new values of forensic interest pertaining to user activity on Windows.

Since there is no major difference between Windows 8 and Windows 10 in terms of forensics analysis, major updates will be covered in the related module. During the exercises, both operating systems will be considered if there is a difference between the location and recovery techniques of stored data.

During the last lectures of the course, most frequently used applications like Browsers, Email clients, Twitter, Skype, Office applications will be analyzed to discover user identity and activity related data in order to recover. All of the work will be based on open-source or free tools like SIFT and The Sleuth Kit (TSK) etc. This enables participants to transform learning outcomes into practice right away.

**Course outline:**

Module 1: Introduction

Module 2: Disk and Folder Structures

Module 3: Windows 8 Overview

Module 4: File History and System Restore Points

Module 5: Storage Options

Module 6: Registry & Registry Artifacts

Module 7: Built-in Artifacts

Module 8: Windows 10 Overview

Module 9: Differences Between Windows 8 & Windows 10

Module 10: OneDrive, Office 365 and Office 2016

Module 11: Browser and Social Media Artifacts

Module 12: Exercise and Closing

**Technical Requirements & Prerequisites:**

To obtain the maximum benefit from this course, participants should meet the following requirements: Able to understand course curriculum presented in English

Able to perform basic operations on a personal computer

Have a basic knowledge of computer forensic investigations and acquisition procedures

Be familiar with the Microsoft Windows environment and Windows forensic analysis

Read and understand basic Windows commands and scripts

**Technical Requirements & Prerequisites:**

Students should have access to personal computers (be it their own computers or using lab computers in an appropriate place)

PCs should be capable of running at least 1 virtual machine (Roughly 2 GB or memory and 30 GB of disk space should be allocated)  
High speed Internet access

Vastame meelsasti tekkinud küsimustele või kommentaaridele ning oleme valmis läbi rääkima vastavalt Teie ootustele.

Pakkumuse koostas

Marika Tamm

Projektijuht

TTÜ Avatud ülikooli täienduskoolituskeskus

E-mail: marika.tamm@ttu.ee

Tel: + 372 5145506