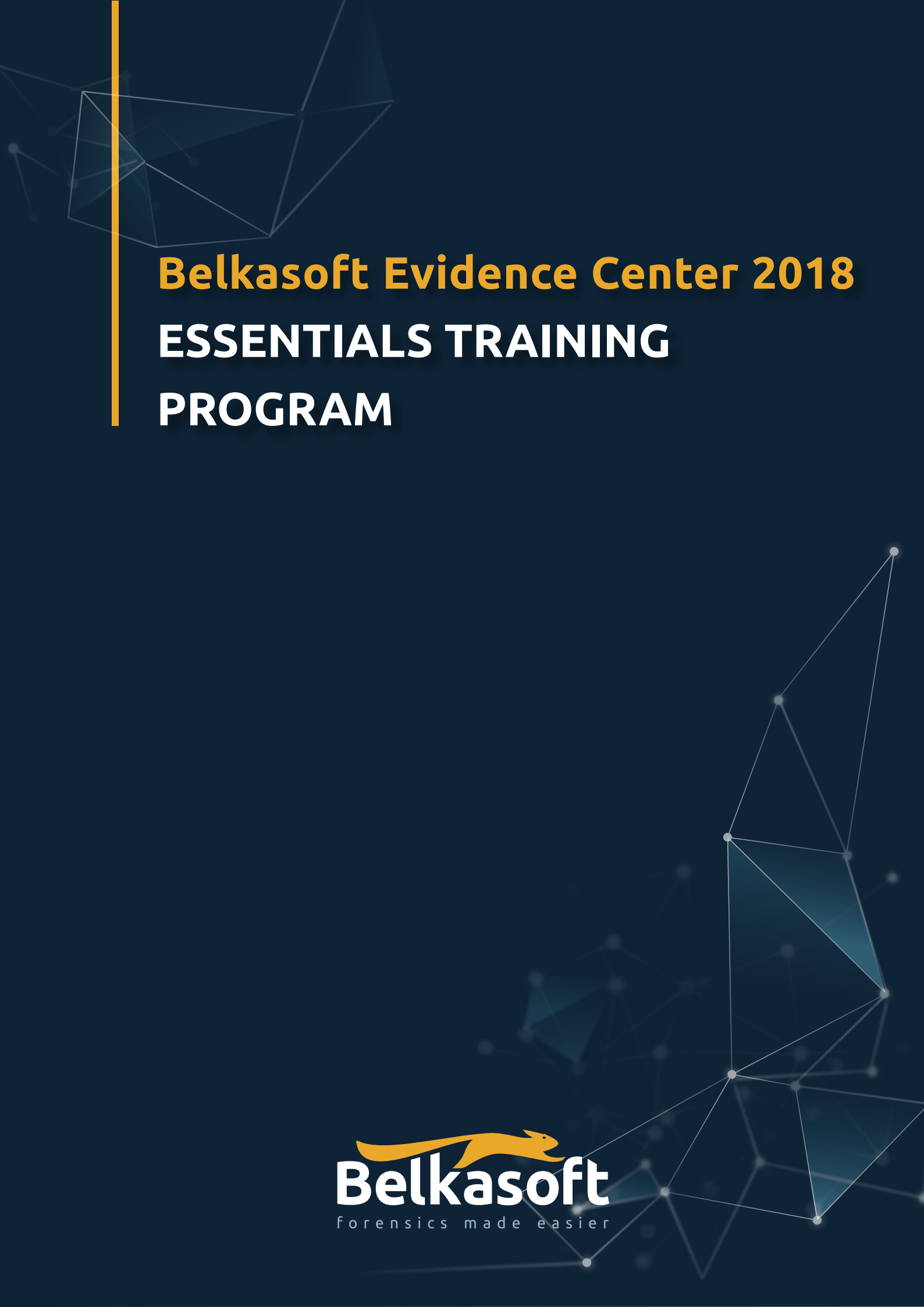
Belkasoft Evidence Center 2018

ESSENTIALS TRAINING PROGRAM



INTRODUCTION

Belkasoft Essentials is intended for investigators of any level of expertise who want to acquire hands-on skills in computer, mobile and cloud investigation and enrich their toolkit with Belkasoft Evidence Center, all-in-one forensic solution.

It is a basic-level course which covers fundamental principles every digital forensic investigator should know. By the successful completion of the course, each participant gets strong skills in Belkasoft Evidence Center, and also deepens their knowledge about techniques behind it and methodology of digital forensic analysis.

In particular the participants will learn how to configure Belkasoft Evidence Center and start the investigation, acquire data from hard drives, smartphones and cloud, add other data sources, analyze most relevant artifacts (including internet evidence, media, registry data etc.) and overcome difficulties working with these types of artifacts. Various analysis options will be considered: extraction of artifacts from existing files, carving, live RAM analysis, hibernation and pagefile analysis.

Every module is accompanied by a set of practical exercises and all related questions will be answered during the training session.

COURSE DETAILS:

LANGUAGE: English

DURATION: 2 days

DELIVERED BY: GoToMeeting or onsite

DAY 1

- Meeting
- Introducing Belkasoft
- What is Belkasoft Evidence Center – introduction of capabilities
- Working with USB dongles
- First steps with Evidence Center
    - Creating case
    - Opening existing case
    - Browsing cases
    - Managing cases
        - *Deleting case manually and from the product*
    - Analyzing Samples folder
    - Product windows: Case Explorer, Task Manager, Item List, Item Properties, File System, viewers
- What is a data source and types of data sources supported by Evidence Center
- Methods to extract evidence from a disk and how a suspect avoids that
- Regular extraction of data:
    - Instant messengers
        - *Important info on Skype and other popular messengers*
        - *Encoding*
    - Working with browsers
        - *Types of information supported*
        - *Browser geolocation data*
        - *Cache preview*

- Working with emails
  - *Copying attachments to folder*
- Working with documents
  - *Preview*
  - *Copying to folder*
  - *Copying embedded files to folder*
- Working with mobile device data
- Working with system files
  - *System Event Logs*
  - *Thumbnails*
  - *Jumplists*
  - *LNK files*
  - *Prefetch*
  - *TOAST notifications*
- Working with pictures
  - *EXIF analysis. EXIF info – important fields*
  - *Face detection*
  - *Text detection*
  - *Skin detection*
  - *Saving in database*
  - *Opening in folder*
  - *Preview*
  - *Filters*
  - *Options*

    - Working with videos
        - *Keyframe extraction options*
    - Timestamps explanation
        - *What time product shows?*
        - *What is UTC and local time?*
        - *How is time conversion performed?*
        - *Points to override timezone: case, data source, profile*
- Bookmarking
    - Where bookmarking works
    - Hotkeys
- Registry analysis. Most forensically important keys. Registry Viewer
- SQLite analysis: Freelists, Journal/WAL, carving. SQLite Viewer
- Geolocation artifacts
    - Types of artifacts having geolocation info
    - Showing on Google Maps Viewer

DAY 2

- Creating reports
  - Creating report from Case Explorer
  - Creating report from Item List
  - Creating report from Search Results
  - Creating report from a bookmark
  - Advanced reporting options
- Search and Search Window. Regular expressions
- Carving
  - Typical use cases
  - Carving a drive and an image
  - Advanced carving options
  - Carving false positives explanations
- Live RAM analysis
  - Analyzing RAM dump in Belkasoft
  - Analyzing hiberfil.sys and pagefile.sys
  - BelkaCarving option and extracting processes
  - Examining processes for artifacts
- Malware detection
  - Detecting suspicious process names
  - Checking processes and files with Virus Total
- Belkasoft Acquisition Tool
  - Acquiring hard drives
  - Acquiring smartphones
  - Downloading cloud data

- Timeline
  - Timeline filters
- File System Explorer
  - File list
  - Copying folders and files recursively
- Hex Viewer
  - Basic features
  - Search
  - Custom carving with Hex Viewer
  - Bookmarking inside HexViewer
  - Type converter
  - Advanced Go To
- Product options
- Working with Belkasoft Evidence Reader
  - Exporting data to Belkasoft Evidence Reader
  - Exploring data and creating reports with Belkasoft Evidence Reader

For more information contact us at
sales@belkasoft.com

Visit belkasoft.com
Try free at https://belkasoft.com/trial
30 days trial

1016 Middle Ave #6, Menlo Park CA 94025, USA
+1 (650) 272-03-84 (USA and Canada)