Worcester Polytechnic Institute

Department of Computer Science

Lab 2: Windows Acquisition Tools
Module 2

Objectives

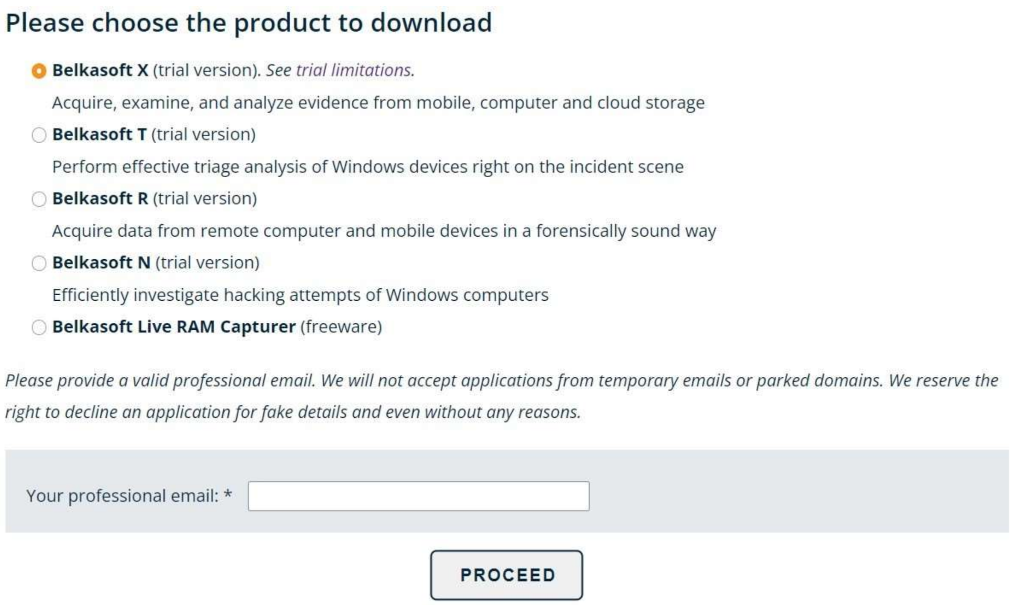
- Perform acquisition using Belkasoft towards a USB drive.

Software Preparation

1. Download and install Belkasoft on your machine. The download page for Belkasoft is: https://belkasoft.com/trial

After filling out your information, you will get an email within one business day with a download link and instructions.

Note: Belkasoft is not free software, the free trial is 30 days.



Please choose the product to download

● **Belkasoft X** (trial version). *See trial limitations.*

Acquire, examine, and analyze evidence from mobile, computer and cloud storage

○ **Belkasoft T** (trial version)

Perform effective triage analysis of Windows devices right on the incident scene

○ **Belkasoft R** (trial version)

Acquire data from remote computer and mobile devices in a forensically sound way

○ **Belkasoft N** (trial version)

Efficiently investigate hacking attempts of Windows computers

○ **Belkasoft Live RAM Capturer** (freeware)

Please provide a valid professional email. We will not accept applications from temporary emails or parked domains. We reserve the right to decline an application for fake details and even without any reasons.

Your professional email: *

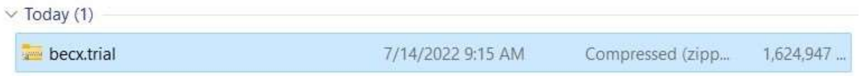
PROCEED

Perform data acquisition using Belkasoft

2. Prepare a USB drive, any size is fine, smaller size one is faster for acquisition. Connect the USB drive to the computer.

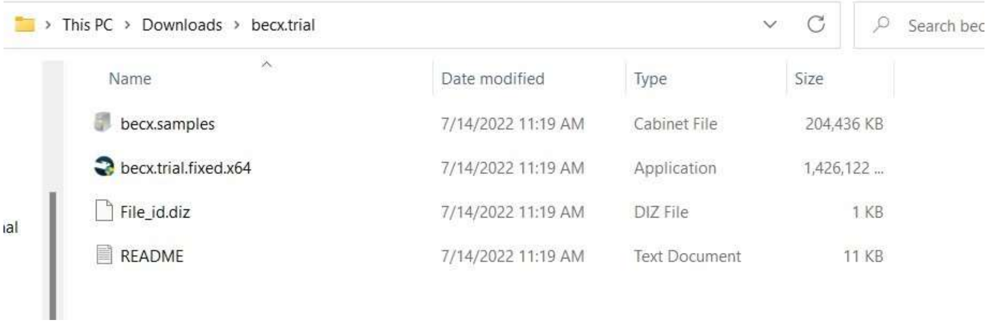
3. Download the Belkasoft folder. Double click “becx.trial.fixed.x64” to install Belkasoft.

Note: Belkasoft is not free software, the free trial is 30 days.



Today (1)

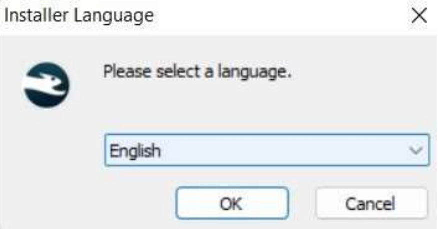
becx.trial 7/14/2022 9:15 AM Compressed (zipp... 1,624,947 ...



This PC > Downloads > becx.trial

Name	Date modified	Type	Size
becx.samples	7/14/2022 11:19 AM	Cabinet File	204,436 KB
becx.trial.fixed.x64	7/14/2022 11:19 AM	Application	1,426,122 ...
File_id.diz	7/14/2022 11:19 AM	DIZ File	1 KB
README	7/14/2022 11:19 AM	Text Document	11 KB

4. Choose language.

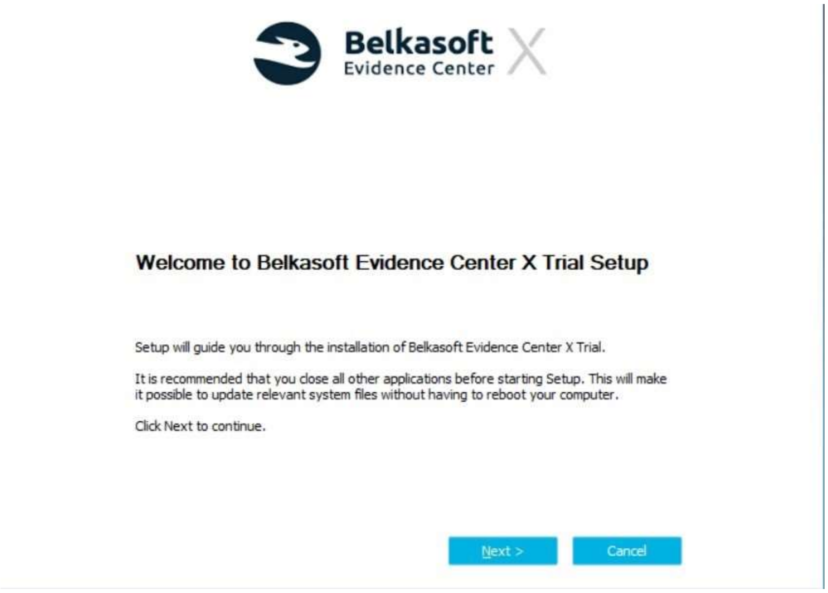


Installer Language

Please select a language.

English

5. Click on “Next” to continue.



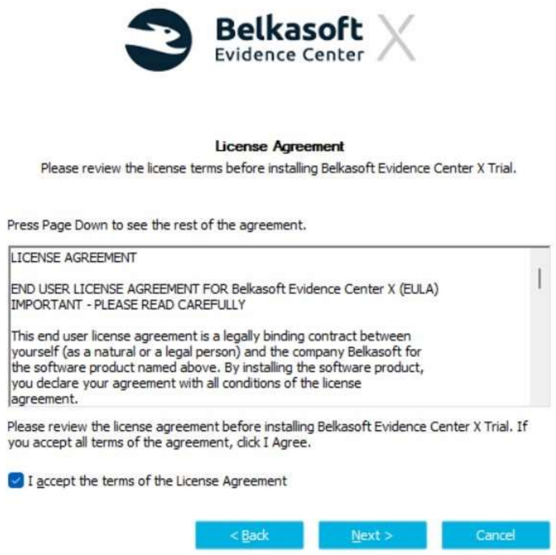
Welcome to Belkasoft Evidence Center X Trial Setup

Setup will guide you through the installation of Belkasoft Evidence Center X Trial.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

6. Check “I agree” then click on “Next” to continue.



License Agreement

Please review the license terms before installing Belkasoft Evidence Center X Trial.

Press Page Down to see the rest of the agreement.

LICENSE AGREEMENT

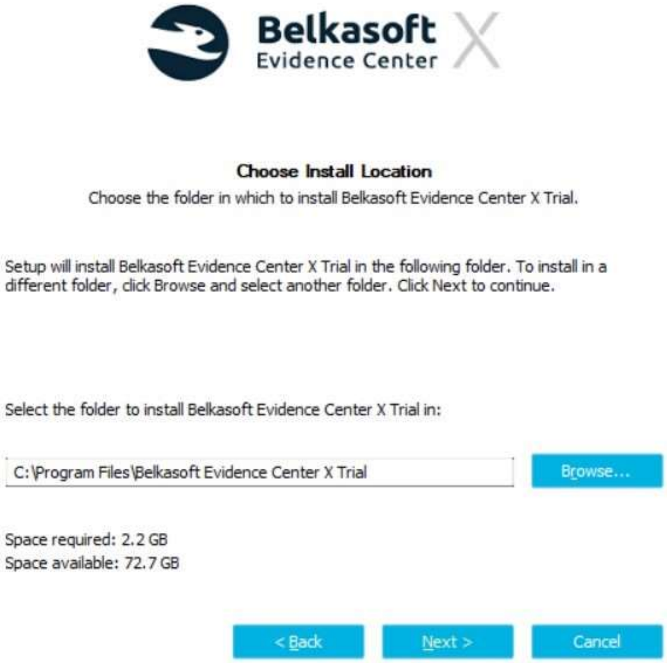
END USER LICENSE AGREEMENT FOR Belkasoft Evidence Center X (EULA)
IMPORTANT - PLEASE READ CAREFULLY

This end user license agreement is a legally binding contract between yourself (as a natural or a legal person) and the company Belkasoft for the software product named above. By installing the software product, you declare your agreement with all conditions of the license agreement.

Please review the license agreement before installing Belkasoft Evidence Center X Trial. If you accept all terms of the agreement, click I Agree.

☑ I accept the terms of the License Agreement

7. Choose the folder to install Belkasoft.



Choose Install Location

Choose the folder in which to install Belkasoft Evidence Center X Trial.

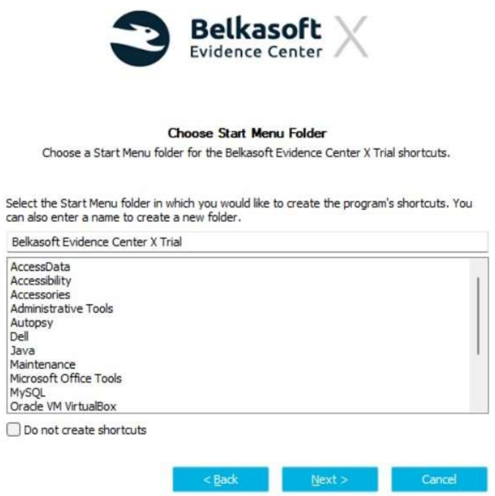
Setup will install Belkasoft Evidence Center X Trial in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Select the folder to install Belkasoft Evidence Center X Trial in:

C:\Program Files\Belkasoft Evidence Center X Trial

Space required: 2.2 GB
Space available: 72.7 GB

8. Click on “Next” to continue.



Choose Start Menu Folder

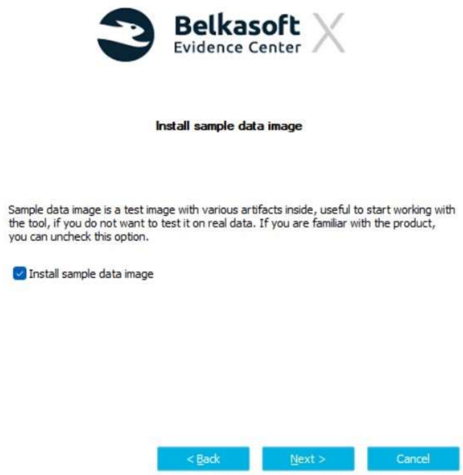
Choose a Start Menu folder for the Belkasoft Evidence Center X Trial shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Belkasoft Evidence Center X Trial

AccessData
Accessibility
Accessories
Administrative Tools
Autopsy
Dell
Java
Maintenance
Microsoft Office Tools
MySQL
Oracle VM VirtualBox

☐ Do not create shortcuts

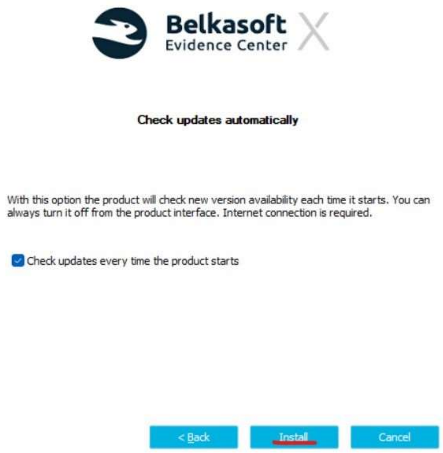


Install sample data image

Sample data image is a test image with various artifacts inside, useful to start working with the tool, if you do not want to test it on real data. If you are familiar with the product, you can uncheck this option.

☑ Install sample data image

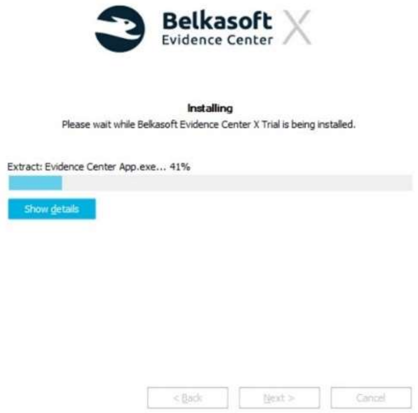
9. Click on “Install” to install.



Check updates automatically

With this option the product will check new version availability each time it starts. You can always turn it off from the product interface. Internet connection is required.

☑ Check updates every time the product starts

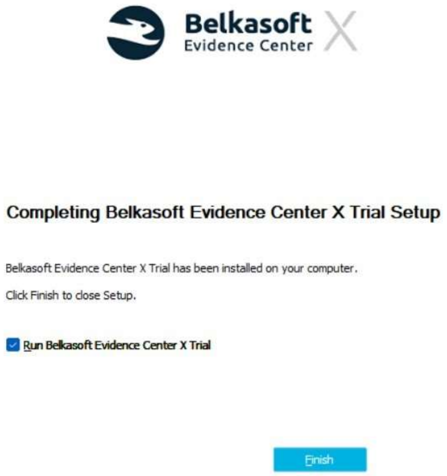


Installing

Please wait while Belkasoft Evidence Center X Trial is being installed.

Extract: Evidence Center App.exe... 41%

10. Click on “Finish” to finish installation.



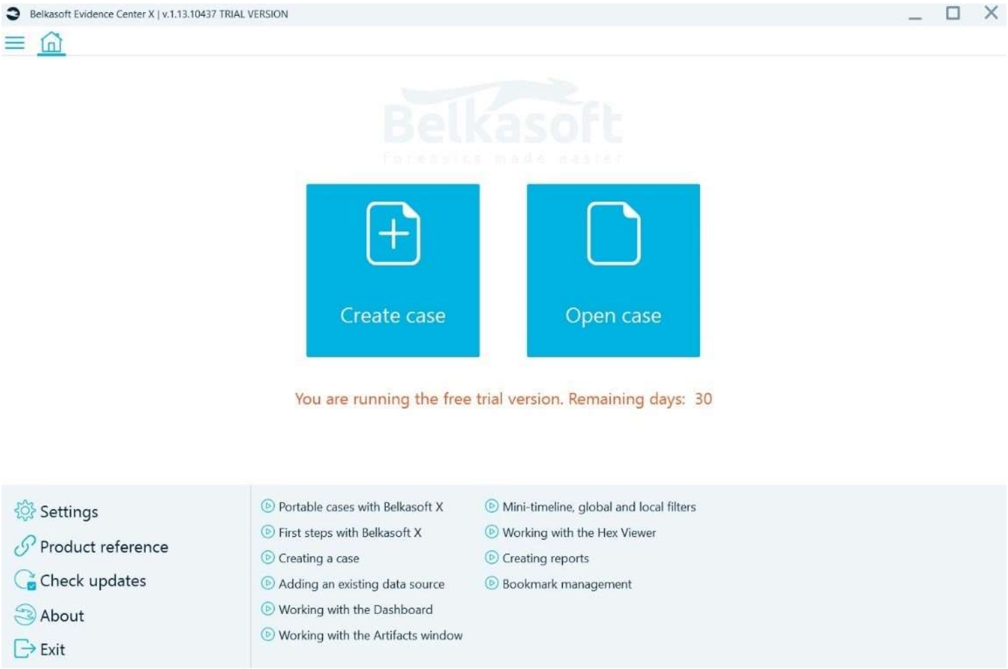
Completing Belkasoft Evidence Center X Trial Setup

Belkasoft Evidence Center X Trial has been installed on your computer.

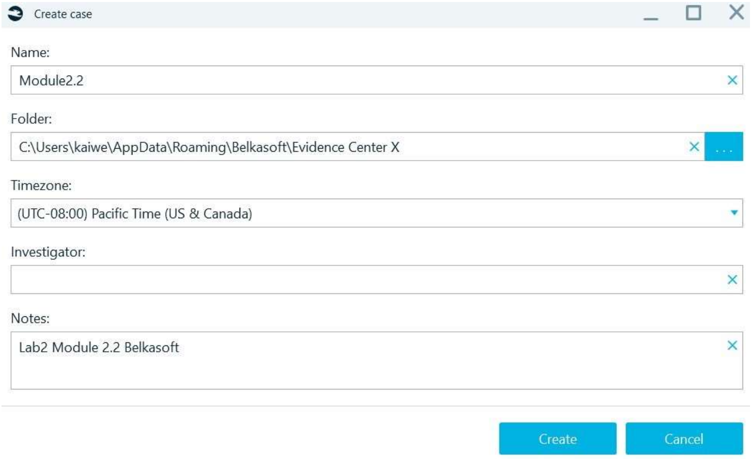
Click Finish to close Setup.

☑ Run Belkasoft Evidence Center X Trial

11. After installing Belkasoft, click on “Create case” fill out the case information. Then click on “Create” to create a new case.


Belkasoft Evidence Center X | v.1.13.10437 TRIAL VERSION
Belkasoft
Forensics made easier
Create case
Open case
Settings
Product reference
Check updates
About
Exit
Portable cases with Belkasoft X
First steps with Belkasoft X
Creating a case
Adding an existing data source
Working with the Dashboard
Working with the Artifacts window
Mini-timeline, global and local filters
Working with the Hex Viewer
Creating reports
Bookmark management

You are running the free trial version. Remaining days: 30



Name: Module2.2

Folder: C:\Users\kaiwe\AppData\Roaming\Belkasoft\Evidence Center X

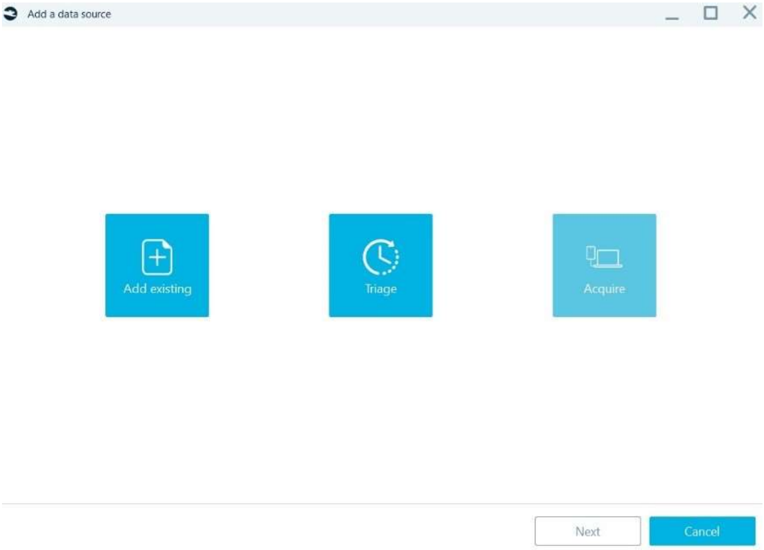
Timezone: (UTC-08:00) Pacific Time (US & Canada)

Investigator:

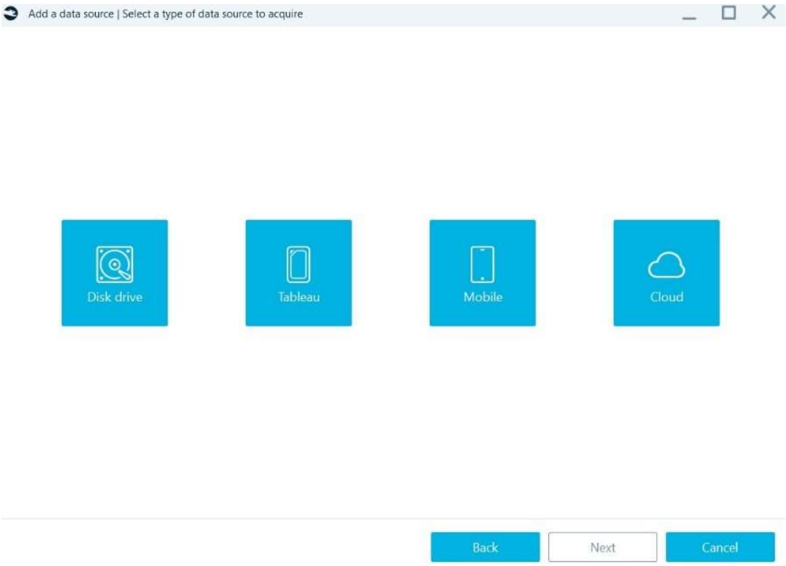
Notes: Lab2 Module 2.2 Belkasoft

12. Then follow the instructions below to acquire data.

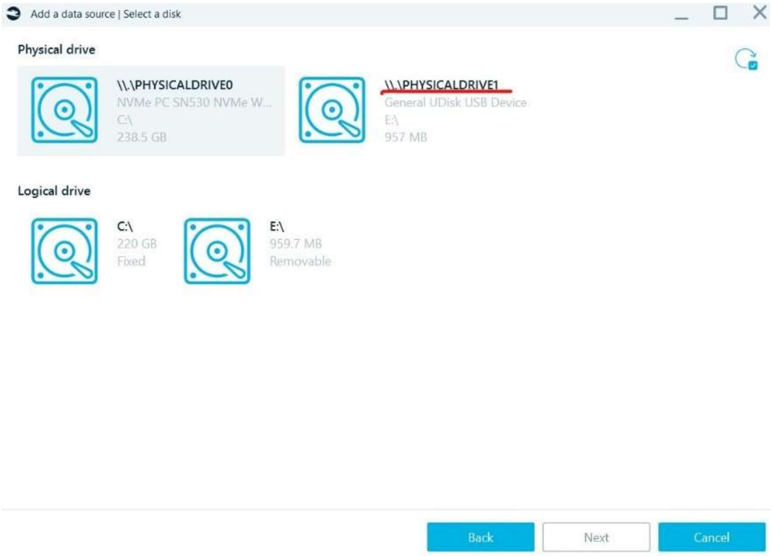
13. Click on “Acquire”.



14. Click on “Disk Drive”.



15. Choose the physical disk you want to do the data acquisition. In this case is “\\.\PHYSICALDRIVE1”.



Add a data source | Select a disk

Physical drive

\\.\PHYSICALDRIVE0
NVMe PC SN530 NVMe W...
C:\
238.5 GB

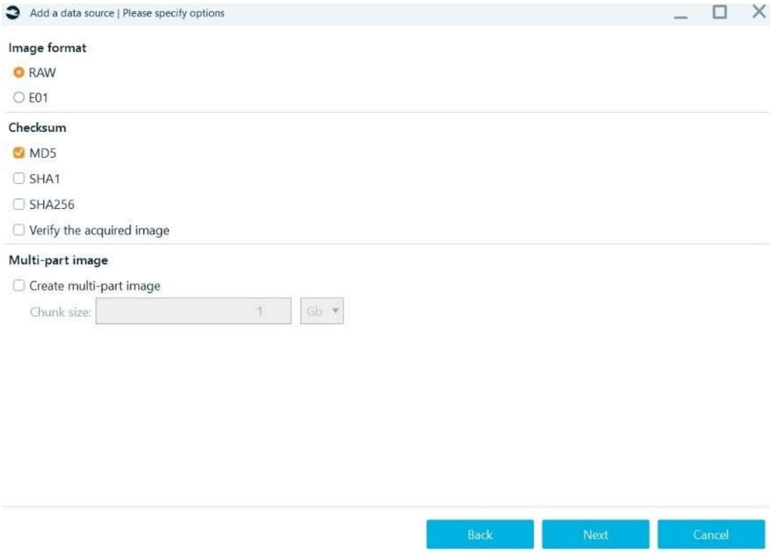
\\.\PHYSICALDRIVE1
General UDisk USB Device
E:\
957 MB

Logical drive

C:\
220 GB
Fixed

E:\
959.7 MB
Removable

16. Check the MD5 box.



Add a data source | Please specify options

Image format

● RAW
○ E01

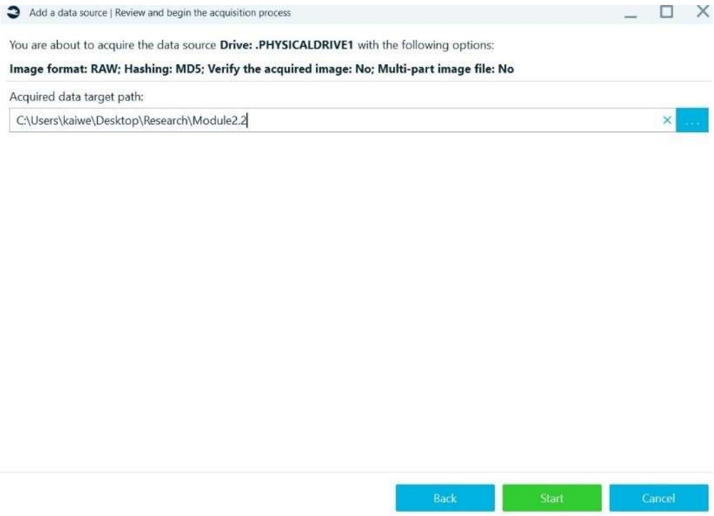
Checksum

☑ MD5
□ SHA1
□ SHA256
□ Verify the acquired image

Multi-part image

□ Create multi-part image
Chunk size: 1 Gb

17. Choose the target path. Then click on “Start”, then acquisition will start automatically.

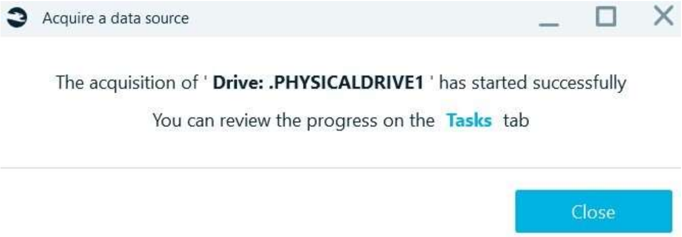

Add a data source | Review and begin the acquisition process

You are about to acquire the data source **Drive: .PHYSICALDRIVE1** with the following options:

Image format: RAW; Hashing: MD5; Verify the acquired image: No; Multi-part image file: No

Acquired data target path:

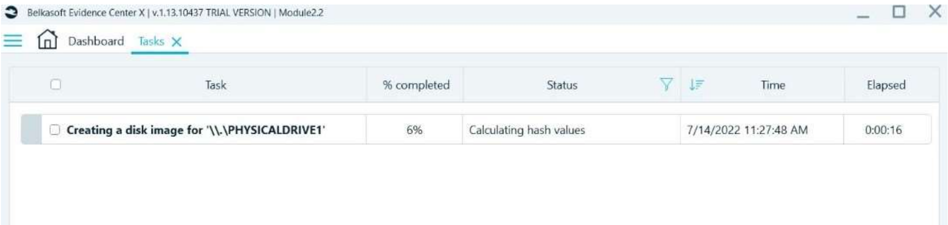
C:\Users\kaiwe\Desktop\Research\Module2.2



The acquisition of ' **Drive: .PHYSICALDRIVE1** ' has started successfully

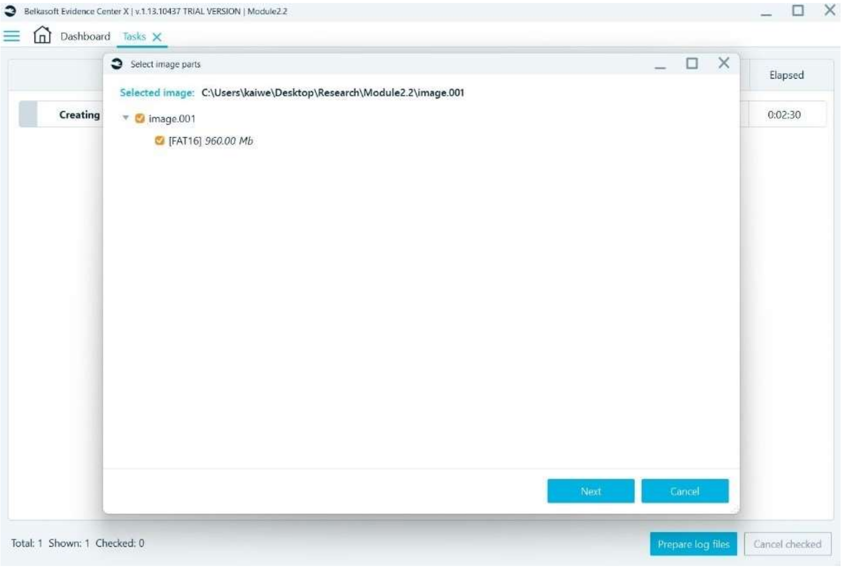
You can review the progress on the **Tasks** tab

18. Click on "Task" tab, you will see the acquisition progress.


Belkasoft Evidence Center X | v.1.13.10437 TRIAL VERSION | Module2.2
Dashboard
Tasks

Task	% completed	Status	Time	Elapsed
□ **Creating a disk image for '\\.\PHYSICALDRIVE1'**	6%	Calculating hash values	7/14/2022 11:27:48 AM	0:00:16

19. After the acquisition is finished, click on the "Next" on the popup window to continue.



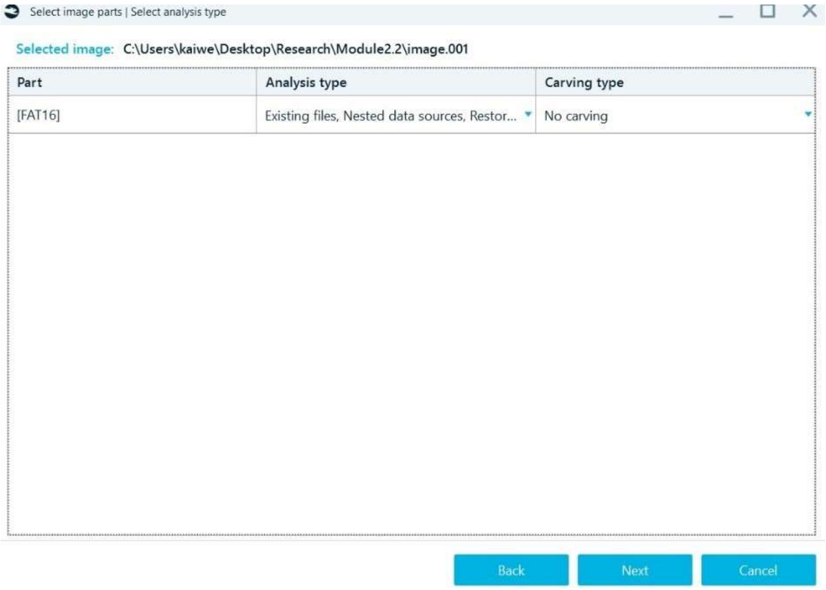
Selected image: C:\Users\kaiwe\Desktop\Research\Module2.2\image.001

☑ image.001

☑ [FAT16] *960.00 Mb*

Total: 1 Shown: 1 Checked: 0

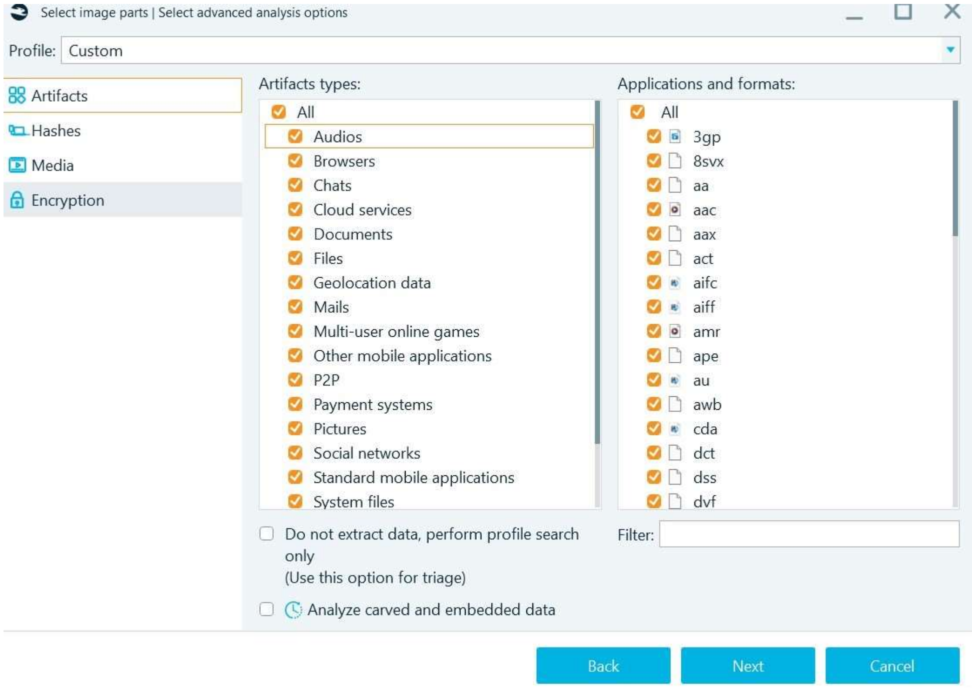
20. Click on "Next" to continue again.



Selected image: C:\Users\kaiwe\Desktop\Research\Module2.2\image.001

Part	Analysis type	Carving type
[FAT16]	Existing files, Nested data sources, Restor...	No carving

21. Keep the original setting and click on "Next" to continue.



Select image parts | Select advanced analysis options

Profile: Custom

- Artifacts
- Hashes
- Media
- Encryption

Artifacts types:

- ☑ All
  - ☑ Audios
  - ☑ Browsers
  - ☑ Chats
  - ☑ Cloud services
  - ☑ Documents
  - ☑ Files
  - ☑ Geolocation data
  - ☑ Mails
  - ☑ Multi-user online games
  - ☑ Other mobile applications
  - ☑ P2P
  - ☑ Payment systems
  - ☑ Pictures
  - ☑ Social networks
  - ☑ Standard mobile applications
  - ☑ System files

Applications and formats:

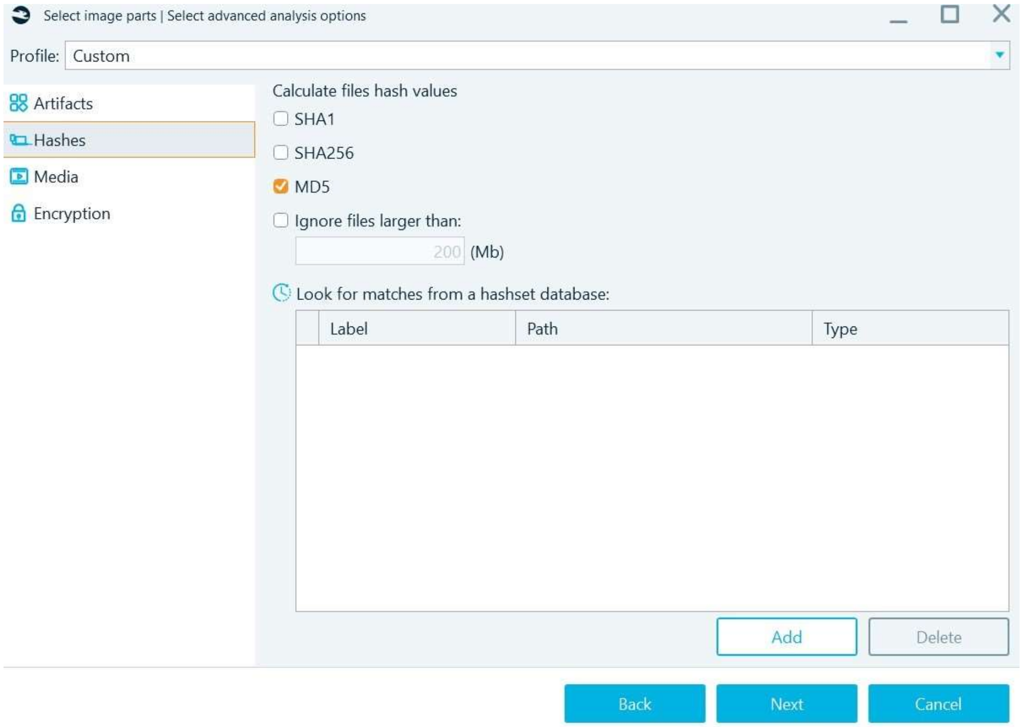
- ☑ All
  - ☑ 3gp
  - ☑ 8svx
  - ☑ aa
  - ☑ aac
  - ☑ aax
  - ☑ act
  - ☑ aifc
  - ☑ aiff
  - ☑ amr
  - ☑ ape
  - ☑ au
  - ☑ awb
  - ☑ cda
  - ☑ dct
  - ☑ dss
  - ☑ dvf

□ Do not extract data, perform profile search only
(Use this option for triage)

Filter:

□ Analyze carved and embedded data

22. Check “MD5”, then click on “Next” to continue.



Select image parts | Select advanced analysis options

Profile: Custom

- Artifacts
- Hashes
- Media
- Encryption

Calculate files hash values

□ SHA1

□ SHA256

☑ MD5

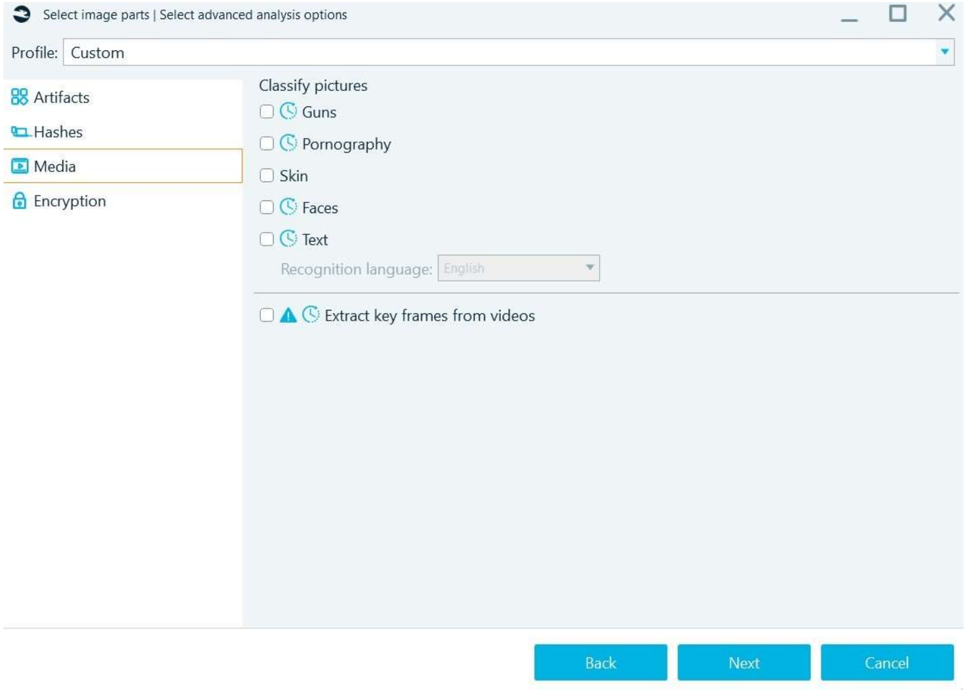
□ Ignore files larger than:

200 (Mb)

Look for matches from a hashset database:

Label	Path	Type

23. Click on “Next” to continue.



Select image parts | Select advanced analysis options

Profile: Custom

Classify pictures

□ Guns

□ Pornography

□ Skin

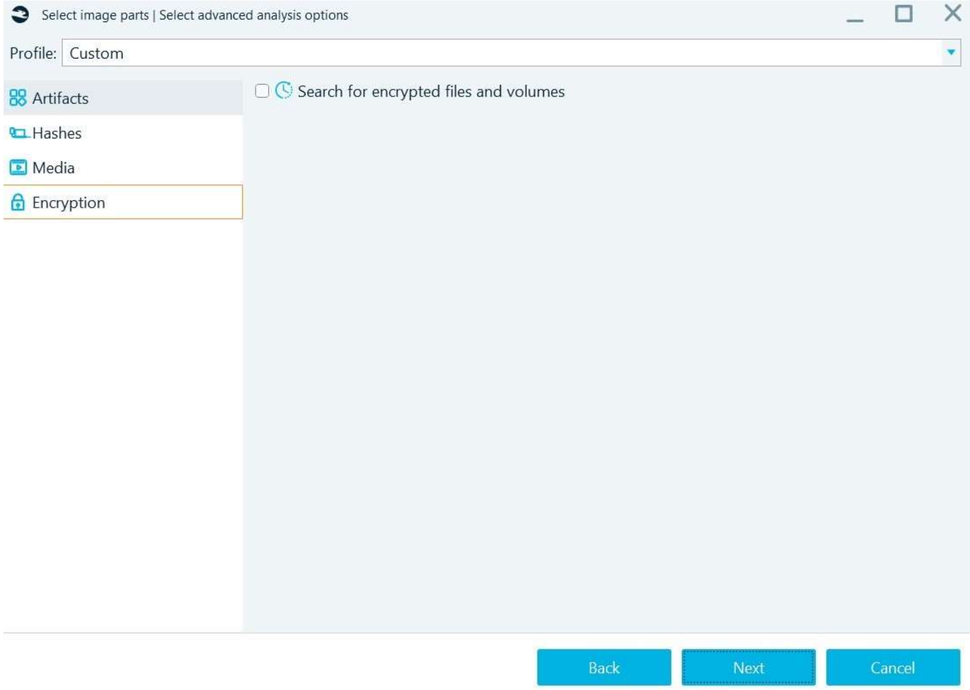
□ Faces

□ Text

Recognition language: English

□ Extract key frames from videos

24. Click on “Next” to continue

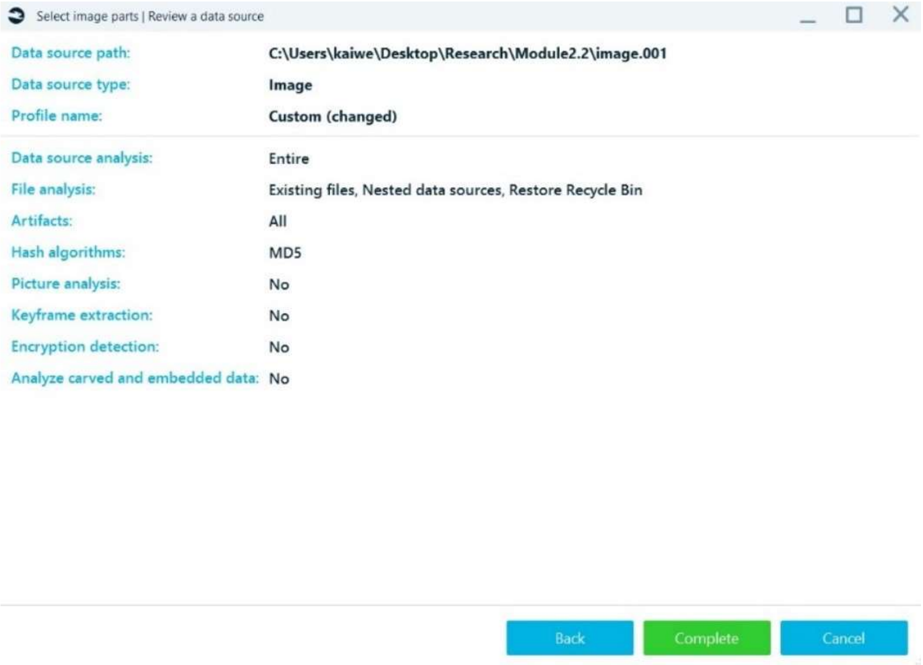


Select image parts | Select advanced analysis options

Profile: Custom

□ Search for encrypted files and volumes

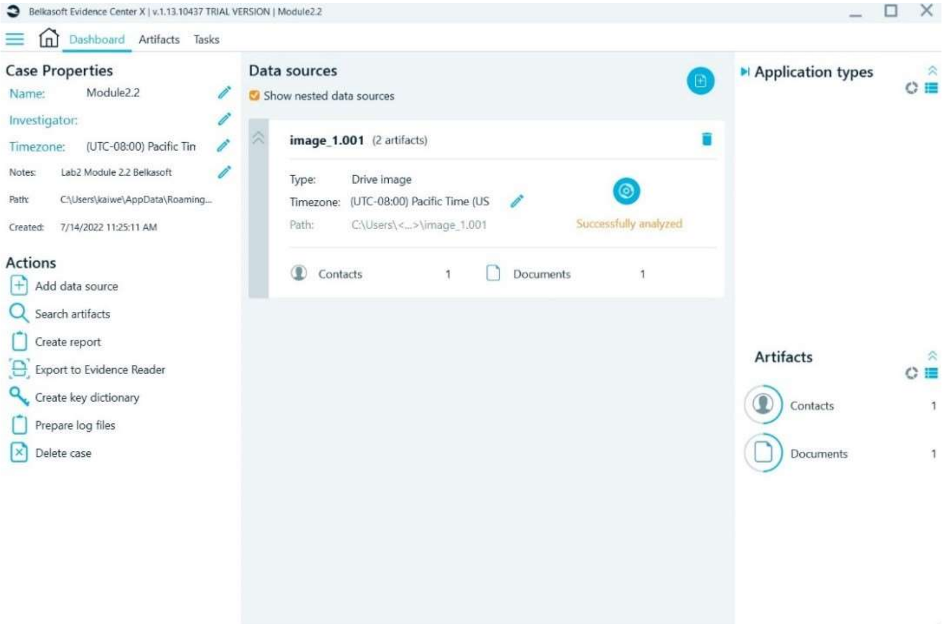
25. Click on “Complete” to finish data acquisition.



Select image parts | Review a data source

Data source path:	C:\Users\kaiwe\Desktop\Research\Module2.2\image.001
Data source type:	Image
Profile name:	Custom (changed)
Data source analysis:	Entire
File analysis:	Existing files, Nested data sources, Restore Recycle Bin
Artifacts:	All
Hash algorithms:	MD5
Picture analysis:	No
Keyframe extraction:	No
Encryption detection:	No
Analyze carved and embedded data:	No

26. Go to the main page, you can see the acquired data. You can also examine the documents using Belkasoft to find the files in your USB drive.



Belkasoft Evidence Center X | v.1.13.10437 TRIAL VERSION | Module2.2

Case Properties

Name: Module2.2
Investigator:
Timezone: (UTC-08:00) Pacific Tin
Notes: Lab2 Module 2.2 Belkasoft
Path: C:\Users\kaiwe\AppData\Roaming...
Created: 7/14/2022 11:25:11 AM

Data sources

☑ Show nested data sources

image_1.001 (2 artifacts)

Type: Drive image
Timezone: (UTC-08:00) Pacific Time (US
Path: C:\Users\<...>\image_1.001

Successfully analyzed

Contacts 1 Documents 1

Artifacts

Contacts 1
Documents 1