Collecting a kernel or full Windows memory dump using LiveKD

534 views Last Updated: 8/9/2023 Article Number: 000006972

For Businesses For Individuals For Service providers

Introduction

Investigation and troubleshooting of certain technical issues requires collecting a kernel or a full Windows memory dump.

When the entire Windows operating system crashes, also known as a "blue screen" error, or "BSOD", the article https://kb.acronis.com/content/17639 should be used.

The present article applies to cases when the operating system neither crashes nor freezes.

The article guides step-by-step how to collect a kernel or full Windows memory dump using LiveKD (https://docs.microsoft.com/en-us/sysinternals/downloads/livekd). The main advantage of using LiveKD over other methods is that it does not require system shut down or reboot.

Pre-requisites

As a final result you will have a file with .dmp file name extension. Before proceeding, make sure you have enough disk space to accomodate the file, either on the system or a non-system disk:

A **kernel** memory dump can take up to several GBs of disk space.

A **full** memory dump requires disk space equal to the amount of the installed physical RAM.

Description

1. Download and run Windows SDK installer from https://go.microsoft.com/fwlink/?linkid=864422
2. Click "Next" and "Accept" buttons in the installation wizard until reaching features selection screen