

Contact:

Nataly Koukoushkina

Passware Inc.

+1 (650) 472-3716 ext. 101

media@lostpassword.com

Passware Proves Windows 10 No More Secure Than Its Predecessors

The password recovery expert releases a decryption solution for Live ID accounts and BitLocker disks on Windows 10, claiming that the process is a matter of minutes

Mountain View, Calif. (October 8, 2015) – [Passware, Inc.](#), a provider of password recovery, decryption, and electronic evidence discovery software for computer forensics, law enforcement organizations, government agencies, and private investigators, announces version 4 of its flagship encrypted electronic evidence discovery product – [Passware Kit Forensic 2015](#). This new release now recovers or bypasses Windows 10 Live ID and BitLocker passwords.

Decryption of BitLocker disk images from Windows 8-10 is now possible within a few minutes via live memory analysis. Passware Kit acquires a live memory image of the encrypted computer over FireWire port and extracts a BitLocker recovery key from it.

By default, this key resides in RAM the moment a computer is turned on and even before getting to the Windows login password prompt. For pre-boot authentication, the BitLocker key gets saved in RAM after entering the BitLocker password or PIN, even if the user logs off their Windows account afterwards.

This recovery key can be used in BitLocker instead of the password to get access to the disk.

In cases when the BitLocker key does not reside in RAM, Passware Kit can launch a brute-force password recovery process to locate the original BitLocker password. While time consuming depending on password settings, recent updates in hardware acceleration and distributed computing options in Passware Kit make it twice as effective as before.

Passware Kit 2015 v.4 also recovers original passwords for Microsoft Live ID accounts in Windows 10. Password recovery is possible from both from Windows registry files (Windows 8-10), and from live memory images (Window 8-8.1) of the target computers.

“With this update, Passware Kit Forensic continues to be the most complete encrypted electronic evidence discovery solution,” said Dmitry Sumin, CEO of Passware. “Now computer investigators can access encrypted evidence on all platforms – Windows, Mac, and in the Cloud.”

Other features of Passware Kit Forensic 2015 v.4 include:

- Dropbox data acquisition
- Automatic updates from Passware Kit Agents
- New Passware Kit Agent for Amazon
- Password recovery for MS Office 2016 documents (both Mac and Windows versions)

Pricing and Availability

Passware Kit Forensic is available directly from [Passware](#) and a network of resellers worldwide. The price is \$995 with one year of free updates. Additional product information and screen shots are available at <http://www.passware.com/pkf>.

About Passware, Inc.

Founded in 1998, Passware, Inc. is the worldwide leading maker of password recovery, decryption, and electronic evidence discovery software. Law enforcement and government agencies, institutions, corporations and private investigators, help desk personnel, and thousands of private consumers rely on Passware software products to ensure data availability in the event of lost passwords. Passware [customers](#) include many Fortune 100 companies and various US federal and state agencies, such as the IRS, US Army, US Department of Defense (DOD), US Department of Justice, US Department of Homeland Security, US Department of Transportation, US Postal Service, US Secret Service, US Senate, and US Supreme Court.

Passware is a privately held corporation with its headquarters in Mountain View, Calif. More information about Passware, Inc. is available at <http://www.passware.com/>.

###