Contact:
Nataly Koukoushkina
Passware Inc.
+1 (650) 472-3716 ext. 101
media@lostpassword.com

Passware Enables Forensics to Extract Windows, Email and Internet Passwords from Registry of Seized Computers

New version of Passware Kit makes all passwords for Windows accounts, email, websites, and network connections easily available to computer forensics by decrypting the target system's registry files

Mountain View, Calif. (October 11, 2011) – 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 that Passware Kit Forensic v11.1 makes all passwords for Windows accounts, email and websites, easily available to computer forensics by decrypting the target system's registry files.

Passware now makes it possible to instantly recover passwords for email accounts, websites, network, and remote desktop connections on a standalone computer directly from the target system's registry files. In response to customer demands, the latest version of Passware Kit gives computer forensic experts the ability to recover passwords without needing administrator privileges for the target computer. This technical advance in password decryption is a powerful next step in computer forensics.

"Electronic evidence, such as email, internet history and saved websites passwords, plays an important role in cybercrime investigations," said Dmitry Sumin, president, Passware, Inc. "Our software saves considerable, and often critical, investigative time by enabling computer forensics experts with the ability to extract suspect's passwords directly from a copy of registry files taken from the hard drive image, without logging into the target system. This means investigative time is better spent analyzing the data rather than decrypting password protected systems."

In a timely manner, login passwords for Windows users are recoverable from a Security Account Manager (SAM) file. The Security Accounts Manager (SAM) is a registry file in Windows NT/2000/XP/Vista/7 that stores users' passwords in a hashed format (in LM hash and NTLM hash). While a hash function is one-way and ostensibly provides some measure of security for the storage of the passwords, Passware Kit decrypts Windows hashes and recovers the stored passwords.

Other new features of Passware Kit 11.1 include password recovery for 7Zip (*.7Z) archives, hardware acceleration of password recovery with ATI graphic cards, in addition to Nvidia GPUs. This ensures that Passware Kit supports both dominant players in the graphics processors industry to accelerate the time-consuming password recovery processes.

Passware Kit Forensic – a Comprehensive Encrypted Evidence Discovery Solution

Passware Kit Forensic provides immediate password recovery for any protected file detected on a PC or over the network while scanning, revealing hidden and protected data files on a suspect's computer. Passware Kit Forensic, complete with FireWire memory imaging module, is the first and only commercial software that decrypts BitLocker and TrueCrypt hard disks, instantly recovers or bypasses Mac and

Windows login passwords of seized computers, and now can instantly recover passwords from any computer without the need for administrative privileges.

The new version will be first presented in Germany at Forensic Technologies Preview Day 2011, Karlsruhe, October 11-12, 2011, http://bit.ly/ftd11, and later at IT-Forensic Investigator Conference, Bern, Switzerland, October 25, 2011.

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.lostpassword.com/kit-forensic.htm.

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 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.

More information about Passware, Inc. is available at http://www.lostpassword.com/. Passware is a privately held corporation with headquarters in Mountain View, Calif. and a software development and engineering office in Moscow, Russia.

###