ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

RELEASE NOTES
August 2022

Elcomsoft System Recovery

Version 8.30

Elcomsoft System Recovery (ESR) helps forensic experts gain access to protected system accounts and encrypted volumes. Creates portable bootable media. An indispensable tool for digital field triage.

Summary

Elcomsoft System Recovery, a digital field triage tool, is updated to support PIN-protected Windows 10 and Windows 11 accounts with in-place PIN recovery. The update adds LUKS2 support, detects Microsoft Azure accounts, and improves bootable forensic tools with custom filters.

Essential updates

PIN-protected accounts

In Windows 8, Microsoft started steering users to use a PIN code instead of account passwords. Subsequent versions of Windows inherited this ability. By default, PIN codes only contain digits, yet alphanumeric PINs are also possible. Their typical length is 4 or 6 characters, making it possible to break such PIN codes with a simple brute-force attack in almost no time. Elcomsoft System Recovery 8.30 brings the ability to detect PIN-protected accounts and brute-force the PIN code on systems without a Trusted Platform Module (TPM). For digit-only PIN codes, the length of the PIN is detected and displayed.

Update to bootable forensic tools

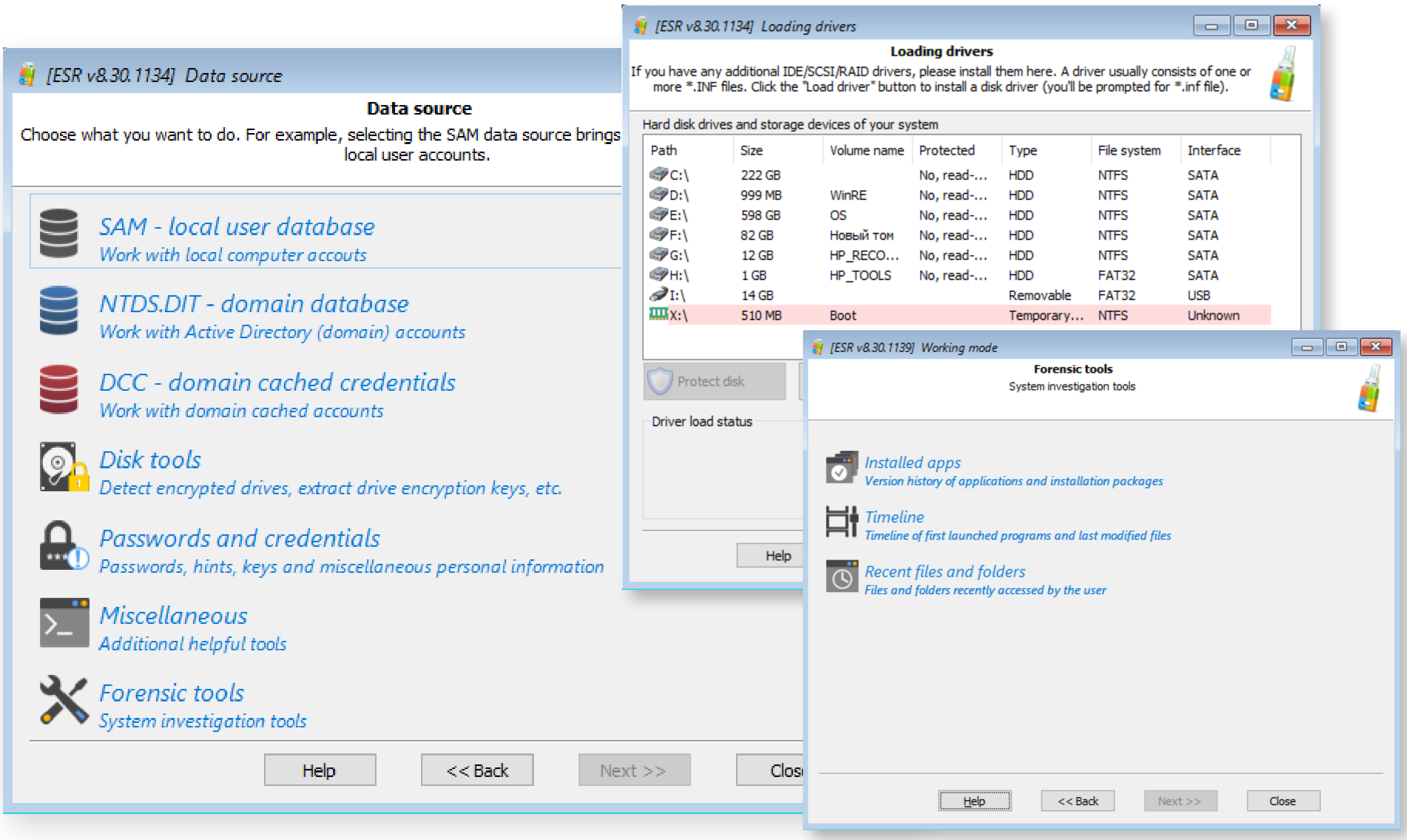
Originally released as a simple tool for resetting Windows users' passwords, Elcomsoft System Recovery is now evolving into a feature-rich bootable forensic toolkit. The tool offers several bootable forensic tools including the timeline, which includes the list of launched apps and past activities laid out in the convenient timeline view, the list of recently accessed files and folders, and the list of installed applications. The new release further improves usability of these tools, adding the ability to filter the results. The filters allow experts to concentrate on what's important while excluding activities with unwanted data such as access to Windows system files.

Support for LUKS 2 encryption

The update can now detect disks encrypted with LUKS2 and extract encryption metadata for subsequent attacks. An updated version of Elcomsoft Distributed Password Recovery will be required to run an attack on a LUKS2 volume.

ESR 8.30 change log:

- Azure Active Directory: account type detection
- PIN-protected accounts (local, local Microsoft, Azure Active Directory)
  - ⌘ In-place recovery of simple PIN codes (up to 6 digits)
  - ⌘ Metadata extraction for offline attacks (an updated version of Elcomsoft Distributed Password Recovery required)
- Forensic Tools (installed apps, timeline, recent files and folders): added filters
- LUKS2 encryption:
  - ⌘ Detection of encrypted disks
  - ⌘ Metadata extraction (an updated version of Elcomsoft Distributed Password Recovery required)



[ESR v8.30.1134] Data source

Data source

Choose what you want to do. For example, selecting the SAM data source brings local user accounts.

SAM - local user database — *Work with local computer accouts*

NTDS.DIT - domain database — *Work with Active Directory (domain) accounts*

DCC - domain cached credentials — *Work with domain cached accounts*

Disk tools — *Detect encrypted drives, extract drive encryption keys, etc.*

Passwords and credentials — *Passwords, hints, keys and miscellaneous personal information*

Miscellaneous — *Additional helpful tools*

Forensic tools — *System investigation tools*

[ESR v8.30.1134] Loading drivers

Loading drivers

If you have any additional IDE/SCSI/RAID drivers, please install them here. A driver usually consists of one or more *.INF files. Click the "Load driver" button to install a disk driver (you'll be prompted for *.inf file).

Hard disk drives and storage devices of your system

Path	Size	Volume name	Protected	Type	File system	Interface
C:\	222 GB		No, read-...	HDD	NTFS	SATA
D:\	999 MB	WinRE	No, read-...	HDD	NTFS	SATA
E:\	598 GB	OS	No, read-...	HDD	NTFS	SATA
F:\	82 GB	Новый том	No, read-...	HDD	NTFS	SATA
G:\	12 GB	HP_RECO...	No, read-...	HDD	NTFS	SATA
H:\	1 GB	HP_TOOLS	No, read-...	HDD	FAT32	SATA
I:\	14 GB			Removable	FAT32	USB
X:\	510 MB	Boot		Temporary...	NTFS	Unknown

Driver load status

[ESR v8.30.1139] Working mode

Forensic tools

System investigation tools

Installed apps — *Version history of applications and installation packages*

Timeline — *Timeline of first launched programs and last modified files*

Recent files and folders — *Files and folders recently accessed by the user*

Steps to renew

1. All active users of Elcomsoft System Recovery are invited to obtain the new version from our website by entering product registration key in the online form https://www.elcomsoft.com/key.html.
2. Users having an expired licenses are welcome to renew their license at corresponding cost that is available after entering registration key in the online form: https://www.elcomsoft.com/key.html.

Contact us at sales@elcomsoft.com for any further questions on updating and license renewing.