Using Artificial Intelligence to decrypt Windows passwords

Passcape Software

1 Using Artificial Intelligence to decrypt Windows passwords

The new version of the **Windows Password Recovery** has got a brand-new password recovery Wizard, designed to simplify the process of password recovery as well as to apply some new password lookup technologies. The recovery wizard uses the best and most up-to-date password search algorithms that have been invented over the past few years. It's not just simple words. And that's why:

- The password recovery strength depends on the hardware used.
- To achieve the best result, the program launches different attacks that are optimally matched for searching for different types of passwords.
- The thorough search mode finds more passwords than any similar program.
- The thorough search can generate passwords templates based on found patterns. You can also do it manually in Mask attack options.
- The thorough search mode uses artificial intelligence algorithms to do the job. This is the function that any other similar program lacks.
- No need to go deep into the program's configuration and to investigate different attack settings, the recovery Wizard will do all the 'dirty job' for you.
- And most importantly, the new technology is fully customizable. This means that new versions of Windows Password Recovery can have an even better success rate recovering passwords.
- Besides, unlike some competitive software, which has options (often turned on by default) for sharing found passwords, WPR does not send any data from your computer.

The AI technology has some drawbacks though. It works better only on large lists of password hashes. For example, when decrypting passwords for Active Directory users. Anyway, in a couple of mouse-clicks, you can easily achieve the recovery rate NO ANY OTHER PROGRAM HAS. To show how effective the new algorithms are, we tested and compared similar programs with exactly the same function for recovering passwords using multiple attacks. Shorn of verbiage, the facts are in numbers below.

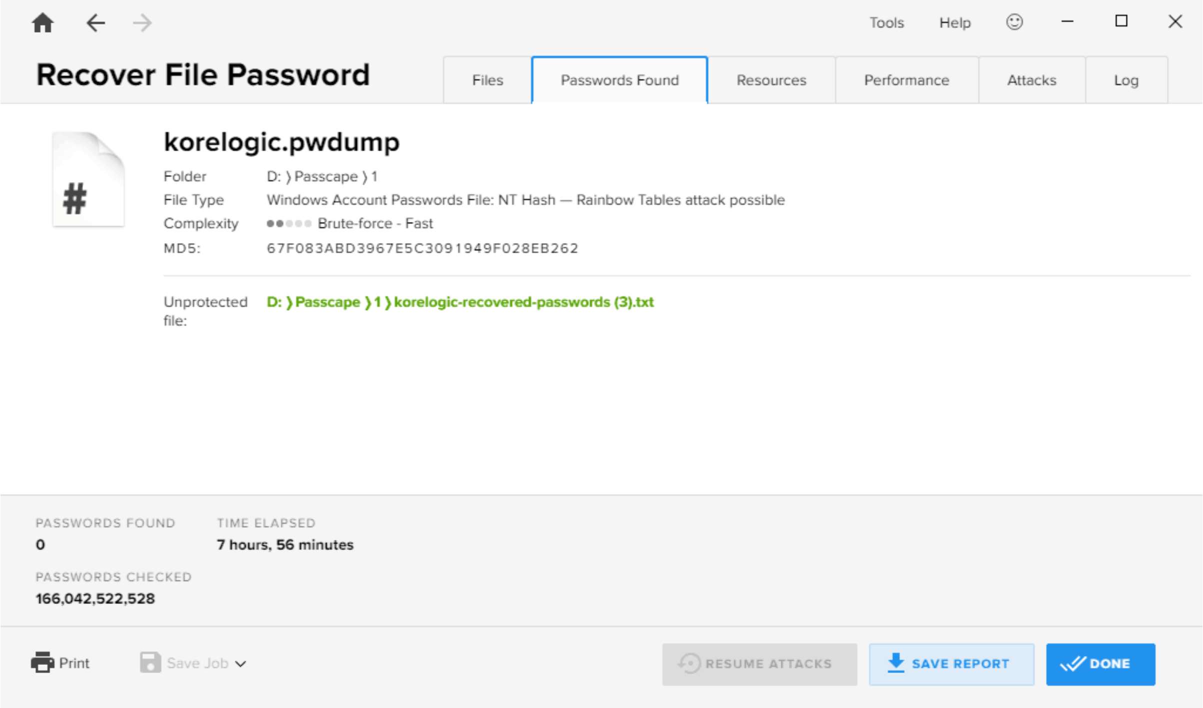
Test PC:
CPU - Intel Core i7-4700K 8 cores, 32 GB RAM
GPU1 - AMD RX 470
GPU2 - NVIDIA GeForce RTX 2060

The list of test hashes that were represented in CoreLogic Crack Me If You Can contest is available for download here. 30823 unique NTLM hashes total.

	Passware Kit Forensic 2019: predefined settings*	L0phCrack v 7.1.4: Common password audit**	WPR v12: Recovery Wizard - Thorough search
Elapsed time	7 h 56 m	5 h 59 m	45 m
Password found	2074	2225	15369
Success rate	6.7%	7.2%	49.9%

*This is the only option with a predefined set of attacks

**The next option (Thorough recovery) showed the task would complete in 24 hours. That's too much, so we had to reject it right away.



Recover File Password

korelogic.pwdump

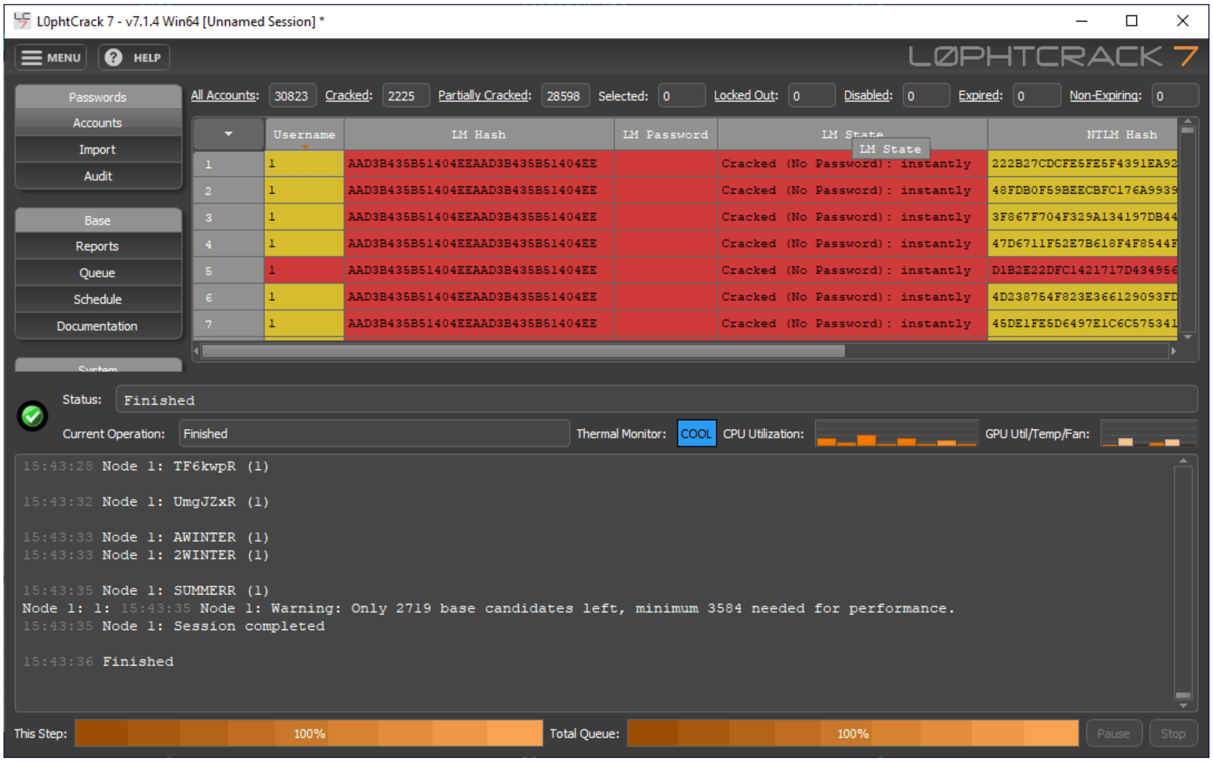
Folder D: ⟩ Passcape ⟩ 1
File Type Windows Account Passwords File: NT Hash — Rainbow Tables attack possible
Complexity ●●●●● Brute-force - Fast
MD5: 67F083ABD3967E5C3091949F028EB262

Unprotected file: D: ⟩ Passcape ⟩ 1 ⟩ korelogic-recovered-passwords (3).txt

PASSWORDS FOUND
0

TIME ELAPSED
7 hours, 56 minutes

PASSWORDS CHECKED
166,042,522,528



All Accounts: 30823 Cracked: 2225 Partially Cracked: 28598 Selected: 0 Locked Out: 0 Disabled: 0 Expired: 0 Non-Expiring: 0

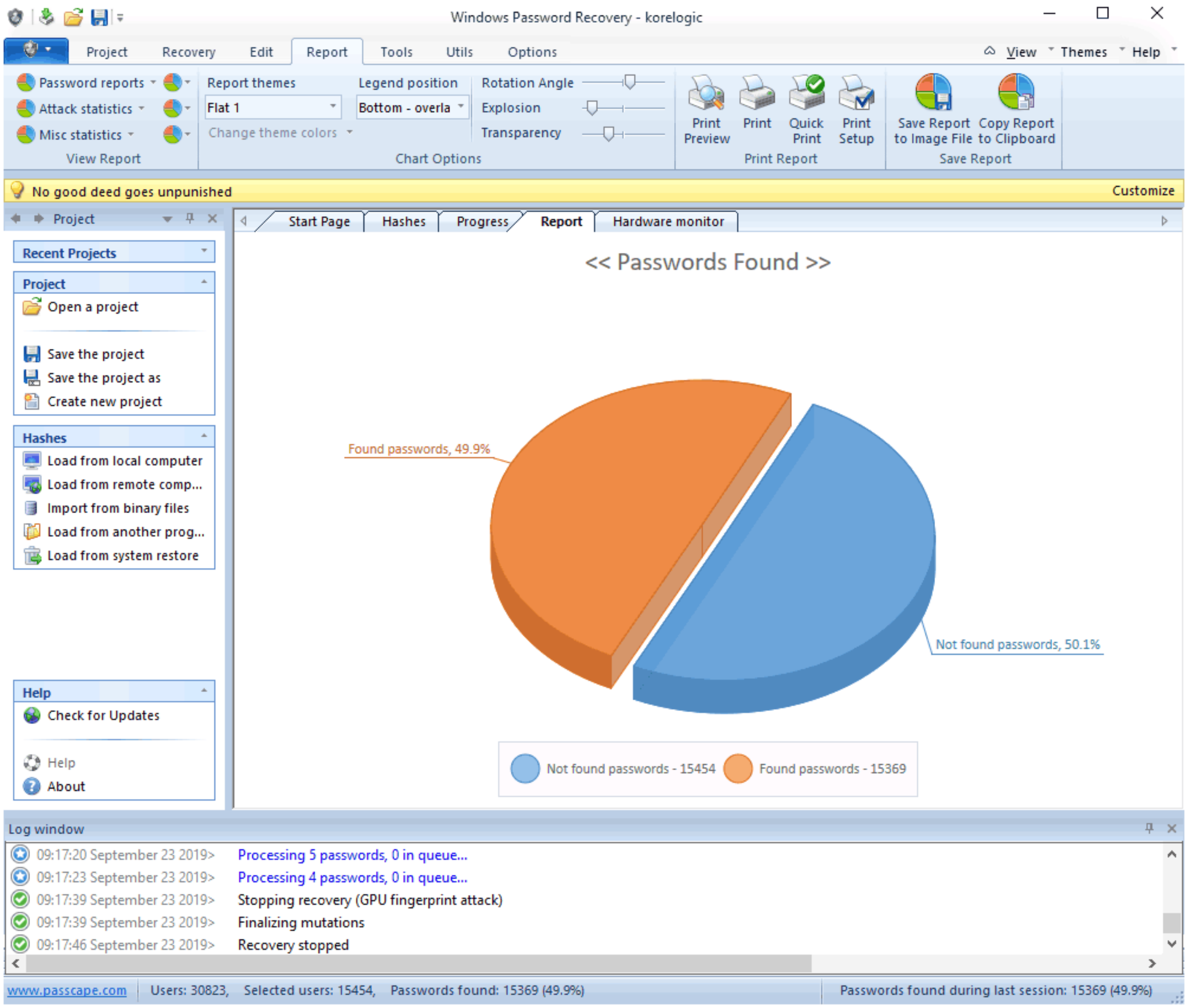
	Username	LM Hash	LM Password	LM State	NTLM Hash
1	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	222B27CDCFE5FE5F4391EA92
2	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	48FDB0F59BEECBFC176A9939
3	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	3F867F704F329A134197DB44
4	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	47D6711F52E7B618F4F8544F
5	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	D1B2E22DFC1421717D434956
6	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	4D238754F823E366129093FD
7	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	45DE1FE5D6497E1C6C575341

Status: Finished

Current Operation: Finished Thermal Monitor: COOL CPU Utilization: GPU Util/Temp/Fan:

```
15:43:28 Node 1: TF6kwpR (1)

15:43:32 Node 1: UmgJZxR (1)

15:43:33 Node 1: AWINTER (1)
15:43:33 Node 1: 2WINTER (1)

15:43:35 Node 1: SUMMERR (1)
Node 1: 1: 15:43:35 Node 1: Warning: Only 2719 base candidates left, minimum 3584 needed for performance.
15:43:35 Node 1: Session completed

15:43:36 Finished
```

This Step: 100% Total Queue: 100%



```
09:17:20 September 23 2019>   Processing 5 passwords, 0 in queue...
09:17:23 September 23 2019>   Processing 4 passwords, 0 in queue...
09:17:39 September 23 2019>   Stopping recovery (GPU fingerprint attack)
09:17:39 September 23 2019>   Finalizing mutations
09:17:46 September 23 2019>   Recovery stopped
```

www.passcape.com | Users: 30823, Selected users: 15454, Passwords found: 15369 (49.9%) | Passwords found during last session: 15369 (49.9%)

Now it's time for Artificial Intelligence to make all the dirty jobs done for you.