

आर्टिफिशियल इंटेलिजेंस से विंडोज पासवर्ड को डिक्रिप्ट करना

© 2019 पास्केप सॉफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)
पास्केप सॉफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

1. आर्टिफिशियल इंटेलिजेंस से विंडोज पासवर्ड को डिक्रिप्ट करना	3
Index	0

आर्टिफिशियल इंटेलिजेंस से विंडोज पासवर्ड को डिक्रिप्ट
करना

1 आर्टिफिशियल इंटेलिजेंस से विंडोज पासवर्ड को डिक्रिप्ट करना

विंडोज पासवर्ड रिकवरी के नए वर्जन को एक नया [पासवर्ड रिकवरी विज़ार्ड](#) मिला है, जिसे पासवर्ड रिकवरी की प्रक्रिया को सरल बनाने के साथ-साथ कुछ नई पासवर्ड लुकअप तकनीकों को लागू करने के लिए डिज़ाइन किया गया है। रिकवरी विज़ार्ड पिछले कुछ वर्षों में आविष्कार किए गए सर्वोत्तम और सबसे अपडेटेड पासवर्ड खोज एल्गोरिदम का उपयोग करता है। यह केवल सरल शब्द नहीं हैं। और यही कारण है:

- पासवर्ड रिकवरी की शक्ति उपयोग किए गए हार्डवेयर पर निर्भर करती है।
- सर्वोत्तम परिणाम प्राप्त करने के लिए, प्रोग्राम अलग-अलग अटैक को लॉन्च करता है जो विभिन्न प्रकार के पासवर्ड की खोज के लिए बेहतर रूप से मेल खाते हैं।
- संपूर्ण सर्च मोड किसी भी समान प्रोग्राम की तुलना में अधिक पासवर्ड ढूंढता है।
- पूरी तरह से खोज पाए गए पैटर्न के आधार पर पासवर्ड टेम्प्लेट उत्पन्न कर सकती है। आप इसे मास्क अटैक विकल्पों में मैनुअल रूप से भी कर सकते हैं।
- संपूर्ण खोज मोड कार्य करने के लिए कृत्रिम बुद्धिमत्ता एल्गोरिदम का उपयोग करता है। यह वह कार्य है जिसका किसी अन्य समान प्रोग्राम में अभाव है।
- कार्यक्रम के विन्यास में गहराई तक जाने की आवश्यकता नहीं है और विभिन्न अटैक सेटिंग्स की जांच करने के लिए, रिकवरी विज़ार्ड आपके लिए सभी 'गंदे काम' करेगा।
- और सबसे महत्वपूर्ण बात यह है कि नई तकनीक पूरी तरह से कस्टमाइजेबल योग्य है। इसका मतलब है कि विंडोज पासवर्ड रिकवरी के नए वर्जनो में पासवर्ड रिकवर करने की सफलता दर और भी बेहतर हो सकती है।
- इसके अलावा, कुछ प्रतिस्पर्धी सॉफ्टवेयर के विपरीत, जिसमें पाए गए पासवर्ड साझा करने के विकल्प (अक्सर डिफॉल्ट रूप से चालू) होते हैं, WPR आपके कंप्यूटर से कोई डेटा नहीं भेजता है।

हालांकि AI तकनीक में कुछ कमियां हैं। यह केवल पासवर्ड हैश की बड़ी सूचियों पर बेहतर काम करता है। उदाहरण के लिए, Active Directory यूजर्स के लिए पासवर्ड डिक्रिप्ट करते समय। वैसे भी, कुछ माउस-क्लिक में, आप आसानी से रिकवरी दर प्राप्त कर सकते हैं जो किसी अन्य कार्यक्रम में नहीं है। यह दिखाने के लिए कि नए एल्गोरिदम कितने प्रभावी हैं, हमने कई अटैक का उपयोग करके पासवर्ड पुनर्प्राप्त करने के लिए समान फंक्शन वाले समान कार्यक्रमों का परीक्षण और तुलना की। शब्दजाल से दूर, तथ्य नीचे संख्या में हैं।

टेस्ट PC:

CPU - Intel Core i7-4700K 8 cores, 32 GB RAM

GPU1 - AMD RX 470

GPU2 - NVIDIA GeForce RTX 2060

कोरलॉजिक क्रैक मी इफ यू कैन कॉन्टेस्ट में प्रदर्शित टेस्ट हैश की सूची [यहां डाउनलोड के लिए](#) उपलब्ध है। 30823 अद्वितीय NTLM हैश कुल।

	Passware Kit Forensic 2019: predefined settings*	L0pHCrack v 7.1.4: Common password audit**	WPR v12: Recovery Wizard - Thorough search
बीता हुआ समय	7 h 56 m	5 h 59 m	45 m
पासवर्ड मिले	2074	2225	15369
सफलता दर	6.7%	7.2%	49.9%

*यह हमलों के पूर्वनिर्धारित सेट के साथ एकमात्र विकल्प है

**अगले विकल्प (पूरी तरह से पुनर्प्राप्ति) ने दिखाया कि कार्य 24 घंटों में पूरा हो जाएगा। यह बहुत अधिक है, इसलिए हमें इसे तुरंत अस्वीकार करना पड़ा।

Recover File Password

Files | Passwords Found | Resources | Performance | Attacks | Log

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**

Print | Save Job | RESUME ATTACKS | SAVE REPORT | DONE

L0phtCrack 7 - v7.1.4 Win64 [Unnamed Session]*

MENU | HELP

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

Account	Username	LM Hash	LM Password	IM State	NTLM Hash
1	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	222B27CDCF5E5F4391EA92
2	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	48FDB0F59BEECBFC176A9939
3	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	3F867F704F929A134197DB44
4	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	47D6711F52E7B610F4F0544F
5	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	D1B2E22DFC1421717D434956
6	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	4D238754F823E36E129093FD
7	1	AAD3B435B51404EEAAD3B435B51404EE		Cracked (No Password): instantly	45DE1FE5D6497E1C6C575341

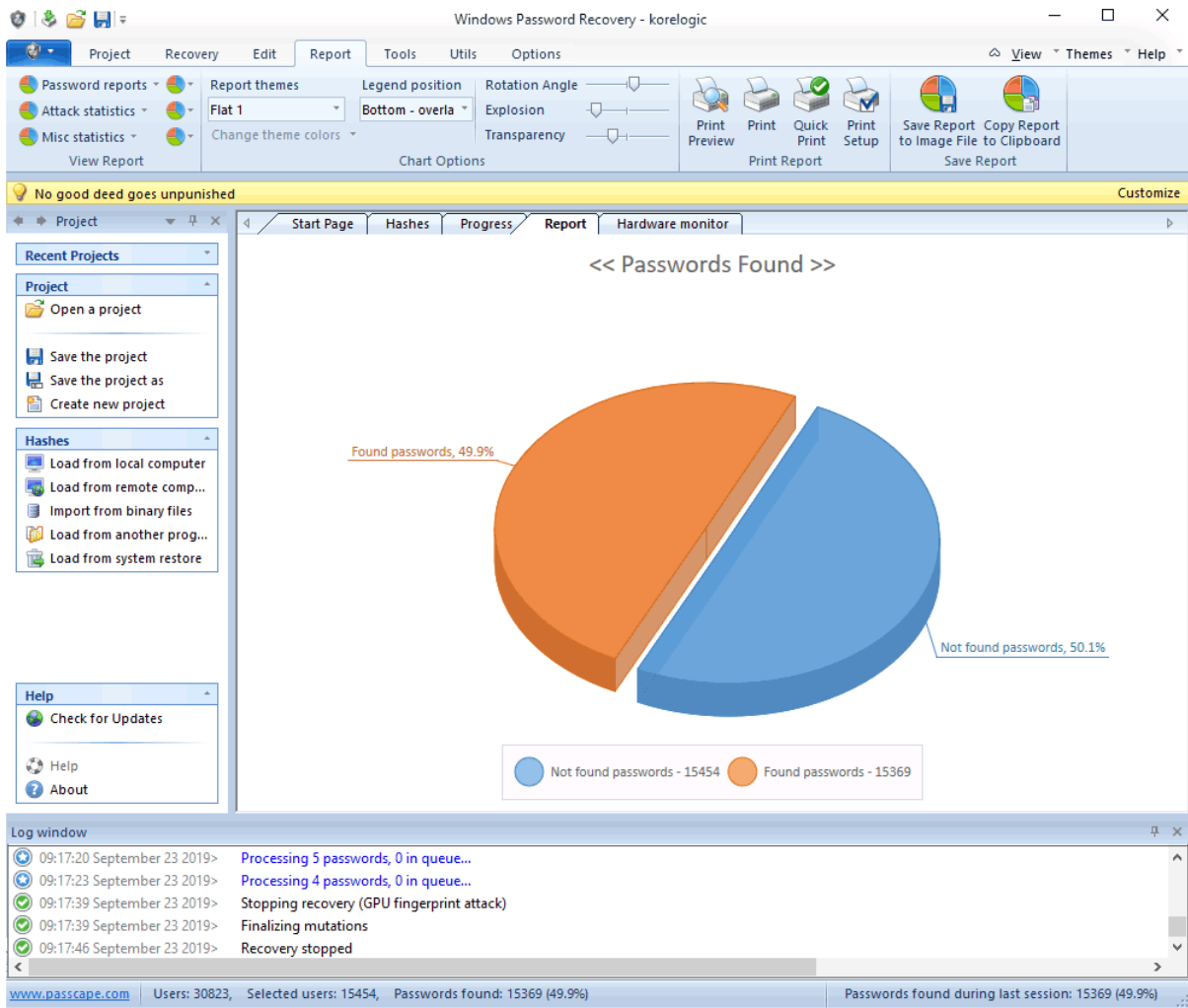
Status: **Finished**

Current Operation: Finished | Thermal Monitor: COOL | CPU Utilization: [Progress Bar] | GPU Util/Temp/Fan: [Progress Bar]

```

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% | Pause | Stop



अब आर्टिफिशियल इंटेलिजेंस के द्वारा सभी गंदे काम करने का समय आ गया है।