Hashcat

Hashcat-utils

- /bin/2to2mp2an input.txt output.hccapx [ess0] — gcap to WPA/WPA2
- cl9_to_mkv.bin 8-byte cl9 in.hex 8-byte cl9 out.hex [ess0x5] — mscrlsp to mkv — cl1_to_mkv
- /desktop_to_mkv.pl 8-byte key.in.hex — DES KN to NTLM — desktop_2_mkv
- /keyspacecalc [options] mask — Calculate keyspace with hashcat masks — keyspace

Workload Profiles

Minimal	Low 1
Reasonable	Economic 2
Unresponsive	High 3
Headless	Insane 4

OpenCL Device Types (-D)

CPU	D 1
GPU	D 2
FPGA, DSP, Gen Purpose	D 3

Built in Charsets(7)

abcdefghijklmnopqrstuvwxyz [a-z]	1
ABCDEFGHIJKLMNOPQRSTUVWXYZ [A-Z]	2
0123456789 [0-9]	3
0123456789abcdef [0-9, a-f]	4
0123456789ABCDEF [0-9, A-F]	5
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ [!-/:-@[-`{-~]	6
0x20-0x7f	7
0x00 - 0xff	8

Attack Modes [-a]

Straight	+0
Combination	+1
Brute force	+3
Hybrid Wordlist + Mask	+6
Hybrid Mask + Wordlist	+7
Association	+9

Output

- Enable brain client, activates -S — brain-client
- Define brain client features, see below — brain-client-features
- Brain server host (IP or domain) — brain-host
- Brain server port — brain-port
- Brain server authentication password — brain-password
- Overrides automatically calculated brain session — brain-session
- Allow given sessions only, separated with commas — brain-session-whitelist
- Enable slower (but advanced) candidate generators — slow-candidates
- Enable brain server — brain-server
- Update the brain server during each X seconds (default: 10) — brain-server-timer
- Enable mask increment mode — increment
- Start mask incrementing at X — increment-min
- Stop mask incrementing at X — increment-max
- User defined charset X — custom-charset1 -1
- User defined charset Y — custom-charset2 -2
- User defined charset Z — custom-charset3 -3
- Generate X random rules — generate-rules
- Force min X functions per rule — generate-rules-min
- Force max X functions per rule — generate-rules-func-min
- Pool of rule operators valid for random rule engine — generate-rules-func-set
- Force RNG seed set to X — generate-rules-seed
- Multiply rules applied to each word from wordlists — rules-file-product
- Single rule applied to each word from right wordlist — rule-right
- Single rule applied to each word from left wordlist — rule-left
- Limit X words from the start + skipped words — limit
- Show keyspace base:mod values and quit — keyspace
- Skip X words from the start — skip
- Manual workload tuning, set thread count to X — kernel-threads
- Manually override hashcat vector width to X — backend-vector-width
- Use CPU for device optimizations, disable GPU — optim-disable
- Disable temperature and fanspeed reads and triggers — hwmon-disable
- Abort if temperature reaches X degrees Celsius — hwmon-temp-abort
- Manually override TMTO value for scrypt to X — scrypt-tmto
- Manual workload tuning, set innerloop step size to X — kernel-loops

- -m — Hash type — Hash type
- -a — Attack mode — Attack mode
- -V — version — Print version
- -h — help — Print help
- --quiet — Suppress output
- --hex-charset — Assume charset is given in hex
- --hex-salt — Assume salt is given in hex
- --hex-wordlist — Assume wordlist is wordlist are given in hex
- --force — Ignore warnings
- --deprecated-check-disable — Enable deprecated plugins
- --status — Enable automatic update of the status screen
- --status-json — Enable JSON format for status output
- --status-timer — Sets seconds between status screen updates to X
- --stdin-timeout-abort — Abort if there is no activity from stdin for X seconds
- --machine-readable — Display the status view in a machine-readable format
- --keep-guessing — Keep guessing the hash after it has been cracked
- --self-test-disable — Disable self-test functionality on startup
- --loopback — Add new plains to input directory
- --markov-hcstat2 — Specify hcstat2 file to use
- --markov-disable — Disables markov-chains, emulates brute-force
- --markov-classic — Enables classic markov-chains, no per-position
- --markov-inverse — Enables inverse markov-chains, no per-position
- --markov-threshold — Threshold X when to stop accepting new markov-chains
- --runtime — Abort session after X seconds of runtime
- --session — Define specific session name
- --restore — Restore session from --session
- --restore-disable — Do not write restore file
- --restore-file-path — Specific path to restore file, default: session.[name].restore
- --outfile — Define outfile for recovered hash
- --outfile-format — Outfile format to use, separated with commas
- --outfile-autohex-disable — Disable the conversion of $HEX[] from the wordlist
- --outfile-check-timeout — Sets seconds between outfile checks to X
- --wordlist-autohex-disable — Disable the conversion of $HEX[] from the wordlist
- --separator — Separator char for hashlists and outfiles
- --stdout — Do not crack a hash, instead print candidates only
- --show — Compare hashlist with potfile; show cracked hashes
- --left — Compare hashlist with potfile; show uncracked hashes
- --username — Enable ignoring of usernames in hashfile
- --remove — Enable removal of hashes once they are cracked
- --remove-timer — Update input hash file each X seconds
- --potfile-disable — Do not write potfile
- --potfile-path — Specific path to potfile
- --encoding-from — Force internal wordlist encoding from X
- --encoding-to — Force internal wordlist encoding to X
- --debug-mode — Define the debug mode hashcat uses (by using rules)
- --debug-file — Output file for debugging rules
- --induction-dir — Specify the induction directory to use for loopback
- --outfile-check-dir — Specify the outfile directory to monitor for plains
- --logfile-disable — Disable the logfile
- --hccapx-message pair — Load only message pairs from hccapx matching X
- --nonce-error-corrections — The BF cracker tries up to X nonce error corrections
- --keyboard-layout-mapping — Keyboard layout mapping table for special hash modes
- --trunc-print keyfiles — Keyfiles to use, separated with commas
- --veracrypt-keyfiles — Keyfiles to use, separated with commas
- --veracrypt-pim-start — VeraCrypt personal iterations multiplier start
- --veracrypt-pim-stop — VeraCrypt personal iterations multiplier stop
- --benchmark — Run benchmark of selected hash modes
- --benchmark-all — Run benchmark of all hash modes (requires -b)
- --speed-only — Return expected speed of the attack, then quit
- --progress-only — Return ideal progress step size and time to process
- --segment-size — Sets size in MB to cache from the wordfile to X
- --bitmap-max — Sets maximum bits allowed for bitmaps to X
- --bitmap-min — Sets minimum bits allowed for bitmaps to X
- --hook-threads — Sets number of threads for a hook (per compute unit)
- --hash-info — Show information for each hash mode
- --example-hashes — Alias of --hash-info
- --backend-ignore-cuda — Do not try to open CUDA interface on startup
- --backend-ignore-hip — Do not try to open HIP interface on startup
- --backend-ignore-metal — Do not try to open Metal interface on startup
- --backend-ignore-opencl — Do not try to open OpenCL interface on startup
- -I, --backend-info — Show system/environment/backend API info
- -d, --backend-devices — Backend devices to use, separated with commas
- -D, --opencl-device-types — OpenCL device types to use, separated with commas
- -O, --optimized-kernel-enable — Enable optimized kernels (limits password length)
- -M, --multi-hash-mode — Enable multiply kernel launch with processor cycle
- -w, --workload-profile — Enable a specific workload profile, see pool below
- -n, --kernel-accel — Manual workload tuning, set outer-loop step size to X

Rule Debugging Modes

1	Finding-Rule
2	Original-Word
3	Original-WordFinding-Rule
4	Original-WordFinding-RuleProcessed-Word
5	Original-WordFinding-RuleProcessed-WordWordRule

Brain Client Features

1	Send hashed passwords
2	Send attack positions
3	Send hashed passwords and attack positions

Outfile Format

1	hash[:salt]
2	plain
3	hex:plain
4	crack_pos
5	timestamp absolute
6	timestamp relative

Hash Modes

Cryptocurrency Wallet

- 29600 Terra Station Wallet (sha256) - CBC/PKCS7(Specs))
- 28600 Metablock Wallet
- 28200 BitShares v0.x - sha512(sha512_bin(pass))
- 21000 Bitcoin WIF private key (P2PKH), compressed
- 28501 Bitcoin WIF private key (P2WPKH), compressed
- 28502 Bitcoin WIF private key (P2SH-P2WPKH), compressed
- 28503 Bitcoin WIF private key (P2TR), uncompressed
- 28504 Bitcoin WIF private key (P2PKH), compressed
- 28505 Bitcoin WIF private key (P2WPKH), compressed
- 28506 Bitcoin WIF private key (P2SH-P2WPKH), uncompressed
- 11300 Bitcoin/Litecoin wallet.dat
- 16600 Electrum Wallet (Salt Type 1-3)
- 21700 Electrum Wallet (Salt Type 4)
- 21800 Electrum Wallet (Salt Type 5)
- 12700 Blockchain, My Wallet
- 15200 Blockchain, My Wallet, V2
- 18800 Blockchain, My Wallet, Second Password (SHA256)
- 25500 Stargazer Stellar Wallet XLM
- 16300 Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256
- 15600 Ethereum Wallet, PBKDF2-HMAC-SHA256
- 15700 Ethereum Wallet, SCRYPT
- 22700 MultiBit Classic .key (MD5)
- 22900 MultiBit Classic .wallet (scrypt)
- 22700 MultiBit HD (scrypt)
- 26300 Exodus Desktop Wallet (scrypt)

Instant Messaging Service

- 23100 XMPP SCRAM PBKDF2-SHA1
- 28300 Teamspeak 3 (channel hash)
- 31200 Telegram Desktop >= v2.1.14 PBKDF2-HMAC-SHA1
- 24500 Telegram Desktop >= v2.1.14 PBKDF2-HMAC-SHA512
- 22301 Telegram Mobile App Passcode (SHA256)

Private Key

- 22911 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 1 (DES)
- 22921 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 2 (AES)
- 22931 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 3 (Bcrypt(16))
- 22941 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 4 (Bcrypt(16), AES)
- 22951 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 5 (Bcrypt(16), AES)
- 22961 Web3Jsy (aes-256-ctr)

Framework

- 22911 Ansible Vault (sha256)
- 16900 Ansible Vault (sha256) + Zlib
- 12001 Atlassian (PBKDF2-HMAC-SHA1)
- 19200 Ruby on Rails Restful Authentication
- 30000 Python Werkzeug MD5 (HMAC-MD5 (key = $salt))
- 30001 Python Werkzeug MD5 (HMAC-MD5 (key = $pass))
- 30120 Python Werkzeug SHA256 (HMAC-SHA256 (key = $salt))
- 20300 Python passlib pbkdf2-sha512
- 20301 Python passlib pbkdf2-sha256
- 20400 Python passlib pbkdf2 - sha1
- 15500 JBOSS EAP (SHA-256, base64)

Plaintext

- 99999 Plaintext

One Time Password

- 18100 TOTP (HMAC-SHA1)
- 8000 WBB3 (Woltlab Burning Board)

Forums, CMS, E-Commerce

- 2612 PHPS
- 12500 RAR3-hp
- 7900 Drupal7
- 4521 Redmine
- 4522 PunBB
- 2811 MyBB 1.2+, IPB2+ (Invision Power Board)
- 2611 vBulletin < v3.8.5
- 2711 vBulletin > v3.8.5
- 21600 Web2py
- 21611 Joomla < 2.5.18
- 13900 OpenCart
- 21000 PrestaShop
- 16000 Tripcode
- 7900 Drupal7
- 4521 PunBB
- 2811 MyBB 1.2+, IPB2+ (Invision Power Board)
- 2611 vBulletin < v3.8.5
- 2711 vBulletin > v3.8.5
- 21600 Web2py(sha512(pass) / hex(salt))
- 21611 Joomla(md5(pass) / hex(salt))
- 21700 Berkeley DB(md5(pass) / hex(salt))
- 21800 Joomla(sha256(salt.pass))
- 21900 jTracker
- 22000 WoWSimple
- 22100 Joomla(PBKDF2-SHA512)
- 22600 Digital Ocean

Archive

- 7-Zip 11600
- 12500 RAR3-hp
- 23800 RAR3-p (Compressed)
- 23700 RAR3-p (Uncompressed)
- 13000 RAR5
- 17220 PKZIP (Compressed Multi-File)
- 17200 PKZIP (Compressed)
- 17225 PKZIP (Mixed Multi-File)
- 17230 PKZIP (Mixed Multi-File Checksum Only)
- 17010 PKZIP (Uncompressed)
- 20500 PKZIP Master Key
- 20510 PKZIP Master Key (B-Tree optimization)
- 23001 SecureZIP AES-128
- 23002 SecureZIP AES-192
- 23003 SecureZIP AES-256
- 13600 WinZip
- 18900 Android Backup
- 24700 Stuffit5
- 13200 AxCrypt 1
- 13200 AxCrypt 1 in memory SHA1
- 13400 AxCrypt 2 AES-128
- 23500 AxCrypt 2 AES-256
- 23600 iTunes backup < 10.0
- 14700 iTunes backup < 10.0
- 14800 iTunes backup >= 10.0

Password Manager

- 60001 Password, sqlite(sha1
- 8200 Password, cloudkeychain
- 5200 Password Safe v3
- 5200 Password Safe v2
- 6800 LastPass + LastPass (sniffed)
- 13400 KeePass 1 (AES/Twofish) and KeePass 2 (AES)
- 13400 KeePass 1 (AES/Twofish) and KeePass 2 (AES) - keyfile only mode
- 29700 Keepass
- 11600 7-Zip
- 15500 JKS Java Key Store
- 15900 Mozilla key3.db
- 26000 Mozilla key4.db
- 26100 Apple Keychain
- 23100 PGP 1.1 - 1.3 (Acrobat 2 - 4)
- 10400 PDF 1.1 - 1.3 (Acrobat 2 - 4), cipher #1
- 10410 PDF 1.1 - 1.3 (Acrobat 2 - 4), cipher #2
- 10420 PDF 1.4 - 1.6 (Acrobat 5 - 8)
- 10500 PDF 1.4 - 1.6 (Acrobat 5 - 8) - user and owner pass
- 25400 PDF 1.7 Level 3 (Acrobat 9)
- 10600 PDF 1.7 Level 8 (Acrobat 10 - 11)
- 10700 MS Office 2007
- 9400 MS Office 2010
- 9500 MS Office 2013
- 9600 MS Office 2016 - SheetProtection
- 25300 MS Office <= 2003 $0/$1, MD5 + RC4
- 9700 MS Office <= 2003 $0/$1, MD5 + RC4, oldemu
- 9710 MS Office <= 2003 $0/$1, MD5 + RC4, cipher #1
- 9810 MS Office <= 2003 $1, SHA1 + RC4, oldemu
- 9720 MS Office <= 2003 $1, SHA1 + RC4, cipher #1
- 9820 MS Office <= 2003 $3/$4, SHA1 + RC4
- 18400 OpenOffice / JOOO 1.2 (SHA-256, AES)
- 18600 OpenOffice / JOOO 3.x (Blowfish)
- 25600 Apple Secure Notes
- 23300 Apple iWork

Network Protocol

- 22000 WPA-PBKDF2-PMK
- 22001 WPA-PMK-PMKID+EAPOL
- 16800 WPA-PBKDF2-PMKID+PMK
- 22000 WPA-PBKDF2-PMK
- 7300 IPMI2 RAKP HMAC-SHA1
- 10200 CRAM-MD5
- 16500 JWT (JSON Web Token)
- 29200 Radmin3
- 19600 Kerberos 5, etype 17, TGS-REP
- 19800 Kerberos 5, etype 17, Pre-Auth
- 28800 Kerberos 5, etype 17, DB
- 19700 Kerberos 5, etype 18, TGS-REP
- 19900 Kerberos 5, etype 18, Pre-Auth
- 28900 Kerberos 5, etype 18, DB
- 7500 Kerberos 5, etype 23, AS-REQ Pre-Auth
- 13100 Kerberos 5, etype 23, TGS-REP
- 18200 Kerberos 5, etype 23, AS-REP
- 5500 NetNTLMv1 / NetNTLMv1+ESS
- 27000 NetNTLMv1 / NetNTLMv1+ESS (NT)
- 5600 NetNTLMv2
- 27100 NetNTLMv2 (NT)
- 29200 Radmin3 Version Greater (Sun4 Sun8 Sparc)
- 4800 iSCSI CHAP authentication, MD5(CHAP)

Network Protocol / Operating System

- 8300 DNSSEC (NSEC3)
- 8500 RACF
- 6300 AIX {smd5}
- 6700 AIX {ssha1}
- 6400 AIX {ssha256}
- 6500 AIX {ssha512}
- 3000 LM
- 19000 QNX /etc/shadow (MD5)
- 19100 QNX /etc/shadow (SHA256)
- 19200 QNX /etc/shadow (SHA512)
- 15300 DPAPI masterkey file v1 (context 1 and 2)
- 15310 DPAPI masterkey file v1 (context 3)
- 15900 DPAPI masterkey file v2 (context 1 and 2)
- 15910 DPAPI masterkey file v2 (context 3)
- 7200 GRUB 2
- 12800 MS-Azure\sync PBKDF2-HMAC-SHA256
- 12400 BSDi Crypt, Extended DES
- 1000 NTLM
- 9900 Radmin2
- 5800 Samsung Android Password/PIN
- 28100 Windows Hello PIN/Password
- 13800 Windows Phone 8+ PIN/password
- 2410 Cisco ASA MD5
- 9200 Cisco-IOS 8 (PBKDF2-SHA256)
- 9300 Cisco-IOS 9 (scrypt)
- 5700 Cisco-IOS type 4 (SHA256)
- 2400 Cisco-PIX MD5
- 8100 Citrix NetScaler (SHA1)
- 22200 Citrix NetScaler (SHA512)
- 1100 Domain Cached Credentials (DCC), MS Cache
- 2100 Domain Cached Credentials 2 (DCC2), MS Cache 2
- 7000 FortiGate (FortiOS)
- 26300 FortiGate(256-FortiOS256)
- 125 ArubaOS
- 501 Juniper IVE
- 22 Juniper NetScreen/SSG (ScreenOS)
- 15100 Juniper/Netbsd md5crypt
- 26500 iPhone passcode (UID key + System Keybag)
- 122 macOS v10.4, macOS v10.5, macOS v10.6
- 1722 macOS v10.7
- 7100 macOS v10.8 - PBKDF2-SHA512
- 1420 Kerberos 5 AES, Windows Server
- 500 md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5)
- 1500 descrypt, DES (Unix), Traditional DES
- 29600 ecryptfs(md5(salt|md5(passwordmap) | salt|sha1(passs)))
- 7400 sha256crypt 5, SHA256 (Unix)
- 1800 sha512crypt 6, SHA512 (Unix)

Database Server

- 24600 SQLCipher
- 131 MSSQL (2000)
- 132 MSSQL (2005)
- 1731 MSSQL (2012, 2014)
- 24100 MongoDB ServerKey SCRAM-SHA-1
- 24200 MongoDB ServerKey SCRAM-SHA-256
- 12 PostgreSQL
- 11100 PostgreSQL CRAM (MD5)
- 28600 PostgreSQL SCRAM (SHA-256)
- 3100 Oracle H Type (Oracle 7+)
- 112 Oracle S Type (Oracle 11+)
- 12300 Oracle T Type (Oracle 12+)
- 7401 MySQL A (sha256crypt)
- 11200 MySQL CRAM (SHA1)
- 200 MySQL323
- 300 MySQL4.1/MySQL5
- 8000 Sybase ASE

Enterprise Application Software (EAS)

- 8600 Lotus Notes/Domino 5
- 8700 Lotus Notes/Domino 6
- 9100 Lotus Notes/Domino 8
- 26200 OpenEdge Progress Encode
- 20600 Oracle Transportation Management (SHA256)
- 4711 Huawei sha1(md5(pass).salt)
- 20711 AuthMe sha256

Network Protocol / Enterprise Application Software (EAS)

- 13500 PeopleSoft PS_TOKEN
- 21500 SolarWinds Orion
- 21501 SolarWinds Orion v2
- 24 SolarWinds Serv-U
- 8600 Lotus Notes/Domino 5
- 8700 Lotus Notes/Domino 6
- 9100 Lotus Notes/Domino 8
- 26200 OpenEdge Progress Encode
- 20600 Oracle Transportation Management (SHA256)
- 4711 Huawei sha1(md5(pass).salt)
- 20711 AuthMe sha256

FTP, HTTP, SMTP, LDAP Server

- 11500 CRC32
- 28000 CRC32c(Castagnoli)
- 28001 CRC32c(Intel)
- 18700 Java Object hashCode()
- 25700 MurmurHash
- 27900 MurmurHash3
- 14100 3DES (PT = $salt, key = $pass)
- 14000 DES (PT = $salt, key = $pass)
- 26401 AES-128-ECB NOKEY (PT = $salt, key = $pass)
- 26402 AES-192-ECB NOKEY (PT = $salt, key = $pass)
- 26403 AES-256-ECB NOKEY (PT = $salt, key = $pass)
- 15400 ChaCha20
- 14900 Skip32 (PT = $salt, key = $pass)
- 14901 CAST128 (PT = $salt, key = $pass)
- 11500 CRC32
- 11600 7-Zip
- 12400 BSDi Crypt, Extended DES
- 1500 descrypt, DES (Unix), Traditional DES
- 29000 sha1($salt.sha1($salt.$username).'::'.sha1($salt.$pass))
- 7400 sha256crypt 5, SHA256 (Unix)
- 1800 sha512crypt 6, SHA512 (Unix)

Enterprise Application Software (EAS) / Operating System

- 13500 PeopleSoft PS_TOKEN
- 21500 SolarWinds Orion
- 21501 SolarWinds Orion v2
- 24 SolarWinds Serv-U
- 8600 Lotus Notes/Domino 5
- 8700 Lotus Notes/Domino 6
- 9100 Lotus Notes/Domino 8
- 26200 OpenEdge Progress Encode
- 20600 Oracle Transportation Management (SHA256)
- 4711 Huawei sha1(md5(pass).salt)
- 20711 AuthMe sha256
- 8900 scrypt
- 400 phpass
- 16100 TACACS+
- 11400 SIP digest authentication (MD5)
- 13100 Bitcoin/Litecoin mnemonic (BIP39) - checksum
- 26000 Mozilla key3.db - checksum
- 26100 Apple Keychain - checksum
- 15900 Mozilla key4.db - checksum
- 16300 Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256 - checksum
- 15600 Ethereum Wallet, PBKDF2-HMAC-SHA256 - checksum
- 15700 Ethereum Wallet, SCRYPT - checksum
- 22700 MultiBit Classic .key (MD5) - checksum
- 22900 MultiBit Classic .wallet (scrypt) - checksum
- 22700 MultiBit HD (scrypt) - checksum
- 26300 Exodus Desktop Wallet (scrypt) - checksum
- 23100 XMPP SCRAM PBKDF2-SHA1 - channel_binding_flag
- 28300 Teamspeak 3 (channel hash) - channel_name
- 31200 Telegram Desktop >= v2.1.14 PBKDF2-HMAC-SHA1 - checksum
- 24500 Telegram Desktop >= v2.1.14 PBKDF2-HMAC-SHA512 - checksum
- 22301 Telegram Mobile App Passcode (SHA256) - checksum
- 22911 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 1 (DES) - checksum_start
- 22921 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 2 (AES) - checksum_start
- 22931 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 3 (Bcrypt(16)) - checksum_start
- 22941 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 4 (Bcrypt(16), AES) - checksum_start
- 22951 RSA/DSA/ECC/Ed25519 Private Keys (SSH), type 5 (Bcrypt(16), AES) - checksum_start
- 22961 Web3Jsy (aes-256-ctr) - checksum_start
- 22911 Ansible Vault (sha256) - checksum_start
- 16900 Ansible Vault (sha256) + Zlib - checksum_start
- 12001 Atlassian (PBKDF2-HMAC-SHA1) - checksum
- 19200 Ruby on Rails Restful Auth (one round, no sitekey) - checksum
- 30000 Python Werkzeug MD5 (HMAC-MD5 (key = $salt)) - checksum
- 30001 Python Werkzeug MD5 (HMAC-MD5 (key = $pass)) - checksum
- 30120 Python Werkzeug SHA256 (HMAC-SHA256 (key = $salt)) - checksum
- 20300 Python passlib pbkdf2-sha512 - checksum
- 20301 Python passlib pbkdf2-sha256 - checksum
- 20400 Python passlib pbkdf2 - sha1 - checksum
- 15500 JBOSS EAP (SHA-256, base64) - checksum
- 99999 Plaintext - plain
- 18100 TOTP (HMAC-SHA1) - key_hex
- 8000 WBB3 (Woltlab Burning Board) - checksum
- 2612 PHPS - checksum
- 12500 RAR3-hp - checksum
- 23800 RAR3-p (Compressed) - checksum
- 23700 RAR3-p (Uncompressed) - checksum
- 13000 RAR5 - checksum
- 17220 PKZIP (Compressed Multi-File) - checksum
- 17200 PKZIP (Compressed) - checksum
- 17225 PKZIP (Mixed Multi-File) - checksum
- 17230 PKZIP (Mixed Multi-File Checksum Only) - checksum
- 17010 PKZIP (Uncompressed) - checksum
- 20500 PKZIP Master Key - checksum
- 20510 PKZIP Master Key (B-Tree optimization) - checksum
- 23001 SecureZIP AES-128 - checksum
- 23002 SecureZIP AES-192 - checksum
- 23003 SecureZIP AES-256 - checksum
- 13600 WinZip - checksum
- 18900 Android Backup - checksum
- 24700 Stuffit5 - checksum
- 13200 AxCrypt 1 - checksum
- 13200 AxCrypt 1 in memory SHA1 - checksum
- 13400 AxCrypt 2 AES-128 - checksum
- 23500 AxCrypt 2 AES-256 - checksum
- 23600 iTunes backup < 10.0 - checksum
- 14700 iTunes backup < 10.0 - checksum
- 14800 iTunes backup >= 10.0 - checksum
- 60001 Password, sqlite(sha1 - checksum
- 8200 Password, cloudkeychain - checksum
- 5200 Password Safe v3 - checksum
- 5200 Password Safe v2 - checksum
- 6800 LastPass + LastPass (sniffed) - checksum
- 13400 KeePass 1 (AES/Twofish) and KeePass 2 (AES) - checksum
- 13400 KeePass 1 (AES/Twofish) and KeePass 2 (AES) - keyfile only mode - checksum
- 29700 Keepass - checksum
- 11600 7-Zip - checksum
- 15500 JKS Java Key Store - checksum
- 15900 Mozilla key3.db - checksum
- 26000 Mozilla key4.db - checksum
- 26100 Apple Keychain - checksum
- 23100 PGP 1.1 - 1.3 (Acrobat 2 - 4) - checksum
- 10400 PDF 1.1 - 1.3 (Acrobat 2 - 4), cipher #1 - checksum
- 10410 PDF 1.1 - 1.3 (Acrobat 2 - 4), cipher #2 - checksum
- 10420 PDF 1.4 - 1.6 (Acrobat 5 - 8) - checksum
- 10500 PDF 1.4 - 1.6 (Acrobat 5 - 8) - user and owner pass - checksum
- 25400 PDF 1.7 Level 3 (Acrobat 9) - checksum
- 10600 PDF 1.7 Level 8 (Acrobat 10 - 11) - checksum
- 10700 MS Office 2007 - checksum
- 9400 MS Office 2010 - checksum
- 9500 MS Office 2013 - checksum
- 9600 MS Office 2016 - SheetProtection - checksum
- 25300 MS Office <= 2003 $0/$1, MD5 + RC4 - checksum
- 9700 MS Office <= 2003 $0/$1, MD5 + RC4, oldemu - checksum
- 9710 MS Office <= 2003 $1, MD5 + RC4, cipher #1 - checksum
- 9810 MS Office <= 2003 $1, SHA1 + RC4, oldemu - checksum
- 9720 MS Office <= 2003 $1, SHA1 + RC4, cipher #1 - checksum
- 9820 MS Office <= 2003 $3/$4, SHA1 + RC4 - checksum
- 18400 OpenOffice / JOOO 1.2 (SHA-256, AES) - checksum
- 18600 OpenOffice / JOOO 3.x (Blowfish) - checksum
- 25600 Apple Secure Notes - checksum
- 23300 Apple iWork - checksum
- 22000 WPA-PBKDF2-PMK - salt
- 22001 WPA-PMK-PMKID+EAPOL - salt
- 16800 WPA-PBKDF2-PMKID+PMK - salt
- 22000 WPA-PBKDF2-PMK - salt
- 7300 IPMI2 RAKP HMAC-SHA1 - salt
- 10200 CRAM-MD5 - challenge
- 16500 JWT (JSON Web Token) - jwt_b64enc(header).jwt_b64enc(payload)
- 29200 Radmin3 - challenge
- 19600 Kerberos 5, etype 17, TGS-REP - checksum
- 19800 Kerberos 5, etype 17, Pre-Auth - checksum
- 28800 Kerberos 5, etype 17, DB - checksum
- 19700 Kerberos 5, etype 18, TGS-REP - checksum
- 19900 Kerberos 5, etype 18, Pre-Auth - checksum
- 28900 Kerberos 5, etype 18, DB - checksum
- 7500 Kerberos 5, etype 23, AS-REQ Pre-Auth - checksum
- 13100 Kerberos 5, etype 23, TGS-REP - checksum
- 18200 Kerberos 5, etype 23, AS-REP - checksum
- 5500 NetNTLMv1 / NetNTLMv1+ESS - challenge.response
- 27000 NetNTLMv1 / NetNTLMv1+ESS (NT) - challenge.response
- 5600 NetNTLMv2 - challenge.response
- 27100 NetNTLMv2 (NT) - challenge.response
- 29200 Radmin3 Version Greater (Sun4 Sun8 Sparc) - challenge
- 4800 iSCSI CHAP authentication, MD5(CHAP) - challenge
- 8500 RACF - salt
- 6300 AIX {smd5} - salt
- 6700 AIX {ssha1} - salt
- 6400 AIX {ssha256} - salt
- 6500 AIX {ssha512} - salt
- 3000 LM - challenge
- 19000 QNX /etc/shadow (MD5) - salt
- 19100 QNX /etc/shadow (SHA256) - salt
- 19200 QNX /etc/shadow (SHA512) - salt
- 15300 DPAPI masterkey file v1 (context 1 and 2) - salt
- 15310 DPAPI masterkey file v1 (context 3) - salt
- 15900 DPAPI masterkey file v2 (context 1 and 2) - salt
- 15910 DPAPI masterkey file v2 (context 3) - salt
- 7200 GRUB 2 - salt
- 12800 MS-Azure\sync PBKDF2-HMAC-SHA256 - salt
- 12400 BSDi Crypt, Extended DES - salt
- 1000 NTLM - hash
- 9900 Radmin2 - hash
- 5800 Samsung Android Password/PIN - salt
- 28100 Windows Hello PIN/Password - salt
- 13800 Windows Phone 8+ PIN/password - salt
- 2410 Cisco ASA MD5 - salt
- 9200 Cisco-IOS 8 (PBKDF2-SHA256) - salt
- 9300 Cisco-IOS 9 (scrypt) - salt
- 5700 Cisco-IOS type 4 (SHA256) - salt
- 2400 Cisco-PIX MD5 - salt
- 8100 Citrix NetScaler (SHA1) - salt
- 22200 Citrix NetScaler (SHA512) - salt
- 1100 Domain Cached Credentials (DCC), MS Cache - salt
- 2100 Domain Cached Credentials 2 (DCC2), MS Cache 2 - salt
- 7000 FortiGate (FortiOS) - salt
- 26300 FortiGate(256-FortiOS256) - salt
- 125 ArubaOS - salt
- 501 Juniper IVE - salt
- 22 Juniper NetScreen/SSG (ScreenOS) - salt
- 15100 Juniper/Netbsd md5crypt - salt
- 26500 iPhone passcode (UID key + System Keybag) - salt
- 122 macOS v10.4, macOS v10.5, macOS v10.6 - salt
- 1722 macOS v10.7 - salt
- 7100 macOS v10.8 - PBKDF2-SHA512 - salt
- 1420 Kerberos 5 AES, Windows Server - salt
- 500 md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5) - salt
- 1500 descrypt, DES (Unix), Traditional DES - salt
- 29000 sha1($salt.sha1($salt.$username).'::'.sha1($salt.$pass)) - salt
- 7400 sha256crypt 5, SHA256 (Unix) - salt
- 1800 sha512crypt 6, SHA512 (Unix) - salt
- 24600 SQLCipher - salt
- 131 MSSQL (2000) - salt
- 132 MSSQL (2005) - salt
- 1731 MSSQL (2012, 2014) - salt
- 24100 MongoDB ServerKey SCRAM-SHA-1 - salt
- 24200 MongoDB ServerKey SCRAM-SHA-256 - salt
- 12 PostgreSQL - salt
- 11100 PostgreSQL CRAM (MD5) - salt
- 28600 PostgreSQL SCRAM (SHA-256) - salt
- 3100 Oracle H Type (Oracle 7+) - salt
- 112 Oracle S Type (Oracle 11+) - salt
- 12300 Oracle T Type (Oracle 12+) - salt
- 7401 MySQL A (sha256crypt) - salt
- 11200 MySQL CRAM (SHA1) - salt
- 200 MySQL323 - salt
- 300 MySQL4.1/MySQL5 - salt
- 8000 Sybase ASE - salt
- 8600 Lotus Notes/Domino 5 - salt
- 8700 Lotus Notes/Domino 6 - salt
- 9100 Lotus Notes/Domino 8 - salt
- 26200 OpenEdge Progress Encode - salt
- 20600 Oracle Transportation Management (SHA256) - salt
- 4711 Huawei sha1(md5(pass).salt) - salt
- 20711 AuthMe sha256 - salt

Full Disk Encryption (FDE)

- 12900 Android FDE (Samsung DEK)
- 8800 Android FDE <= 4.3
- 18300 Apple File System (APFS)
- 14600 LUKS v1 (PBKDF2-SHA1)
- 29921 LUKS v1 (PBKDF2-SHA1 + Serpent)
- 29922 LUKS v1 (PBKDF2-SHA1 + Twofish)
- 29923 LUKS v1 (PBKDF2-SHA1 + AES)
- 29924 LUKS v1 (PBKDF2-SHA512)
- 29931 LUKS v1 (PBKDF2-SHA512 + Serpent)
- 29932 LUKS v1 (PBKDF2-SHA512 + Twofish)
- 29933 LUKS v1 (PBKDF2-SHA512 + AES)
- 29934 LUKS v2 (PBKDF2 - SHA512 - AES)
- 13711 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 512 bit (legacy)
- 13712 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 1024 bit (legacy)
- 13713 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 1536 bit (legacy)
- 13741 VeraCrypt PBKDF2-HMAC + XTS 512 bit + boot-mode (legacy)
- 13742 VeraCrypt PBKDF2-HMAC + XTS 1024 bit + boot-mode (legacy)
- 13743 VeraCrypt PBKDF2-HMAC + XTS 1536 bit + boot-mode (legacy)
- 29411 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 512 bit (legacy)
- 29412 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 1024 bit (legacy)
- 29413 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 1536 bit (legacy)
- 29441 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 512 bit + boot-mode
- 29442 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 1024 bit + boot-mode
- 29443 VeraCrypt PBKDF2-HMAC-SHA512 + XTS 1536 bit + boot-mode
- 13751 VeraCrypt SHA256 + XTS 512 bit (legacy)
- 13752 VeraCrypt SHA256 + XTS 1024 bit (legacy)
- 13753 VeraCrypt SHA256 + XTS 1536 bit (legacy)
- 13761 VeraCrypt SHA256 + XTS 512 bit + boot-mode (legacy)
- 13762 VeraCrypt SHA256 + XTS 1024 bit + boot-mode (legacy)
- 13763 VeraCrypt SHA256 + XTS 1536 bit + boot-mode (legacy)
- 29451 VeraCrypt SHA256 + XTS 512 bit (legacy)
- 29452 VeraCrypt SHA256 + XTS 1024 bit (legacy)
- 29453 VeraCrypt SHA256 + XTS 1536 bit (legacy)
- 29461 VeraCrypt SHA256 + XTS 512 bit + boot-mode
- 29462 VeraCrypt SHA256 + XTS 1024 bit + boot-mode
- 29463 VeraCrypt SHA256 + XTS 1536 bit + boot-mode
- 13721 VeraCrypt SHA512 + XTS 512 bit (legacy)
- 13722 VeraCrypt SHA512