hashcat - advanced password recovery

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

Simple MD5 Examples:

```
brute force:            hashcat -m 0 -a 3 -o output1.txt hashfile.txt --force
dict attack:            hashcat -m 0 -a 0 -o output2.txt hashfile.txt rockyou.txt --force
hybrid attack:          hashcat -m 0 -a 6 -o output3.txt hashfile.txt rockyou.txt ?d?d --force
combinator attack:      hashcat -m 0 -a 1 -o output4.txt hashfile.txt rockyou.txt rockyou.txt --force
```

- [Options] -

Options Short / Long	Type	Description	Example
-m, --hash-type	Num	Hash-type, see references below	-m 1000
-a, --attack-mode	Num	Attack-mode, see references below	-a 3
-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 words in wordlist are given in hex	
--force		Ignore warnings	
--status		Enable automatic update of the status screen	
--status-timer	Num	Sets seconds between status screen updates to X	--status-timer=1
--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 induct directory	
--markov-hcstat2	File	Specify hcstat2 file to use	--markov-hcstat2=my.hcstat2
--markov-disable		Disables markov-chains, emulates classic brute-force	
--markov-classic		Enables classic markov-chains, no per-position	
-t, --markov-threshold	Num	Threshold X when to stop accepting new markov-chains	-t 50
--runtime	Num	Abort session after X seconds of runtime	--runtime=10
--session	Str	Define specific session name	--session=mysession
--restore		Restore session from --session	
--restore-disable		Do not write restore file	
--restore-file-path	File	Specific path to restore file	--restore-file-path=x.restore
-o, --outfile	File	Define outfile for recovered hash	-o outfile.txt
--outfile-format	Num	Define outfile-format X for recovered hash	--outfile-format=7
--outfile-autohex-disable		Disable the use of $HEX[] in output plains	
--outfile-check-timer	Num	Sets seconds between outfile checks to X	--outfile-check=30
--wordlist-autohex-disable		Disable the conversion of $HEX[] from the wordlist	
-p, --separator	Char	Separator char for hashlists and outfile	-p :
--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	Num	Update input hash file each X seconds	--remove-timer=30
--potfile-disable		Do not write potfile	
--potfile-path	File	Specific path to potfile	--potfile-path=my.pot
--encoding-from	Code	Force internal wordlist encoding from X	--encoding-from=iso-8859-15
--encoding-to	Code	Force internal wordlist encoding to X	--encoding-to=utf-32le
--debug-mode	Num	Defines the debug mode (hybrid only by using rules)	--debug-mode=4
--debug-file	File	Output file for debugging rules	--debug-file=good.log
--induction-dir	Dir	Specify the induction directory to use for loopback	--induction=inducts
--outfile-check-dir	Dir	Specify the outfile directory to monitor for plains	--outfile-check-dir=x
--logfile-disable		Disable the logfile	
--hccapx-message-pair	Num	Load only message pairs from hccapx matching X	--hccapx-message-pair=2
--nonce-error-corrections	Num	The BF size range to replace AP's nonce last bytes	--nonce-error-corrections=16
--truecrypt-keyfiles	File	Keyfiles to use, separated with commas	--truecrypt-key=x.png
--veracrypt-keyfiles	File	Keyfiles to use, separated with commas	--veracrypt-key=x.txt
--veracrypt-pim	Num	VeraCrypt personal iterations multiplier	--veracrypt-pim=1000
-b, --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	
-c, --segment-size	Num	Sets size in MB to cache from the wordfile to X	-c 32
--bitmap-min	Num	Sets minimum bits allowed for bitmaps to X	--bitmap-min=24
--bitmap-max	Num	Sets maximum bits allowed for bitmaps to X	--bitmap-max=24
--cpu-affinity	Str	Locks to CPU devices, separated with commas	--cpu-affinity=1,2,3
--example-hashes		Show an example hash for each hash-mode	
-I, --opencl-info		Show info about detected OpenCL platforms/devices	-I
--opencl-platforms	Str	OpenCL platforms to use, separated with commas	--opencl-platforms=2
-d, --opencl-devices	Str	OpenCL devices to use, separated with commas	-d 1
-D, --opencl-device-types	Str	OpenCL device-types to use, separated with commas	-D 1
--opencl-vector-width	Num	Manually override OpenCL vector-width to X	--opencl-vector=4

```
 -O, --optimized-kernel-enable  |      | Enable optimized kernels (limits password length)    |
 -w, --workload-profile         | Num  | Enable a specific workload profile, see pool below   | -w 3
 -n, --kernel-accel             | Num  | Manual workload tuning, set outerloop step size to X | -n 64
 -u, --kernel-loops             | Num  | Manual workload tuning, set innerloop step size to X | -u 256
     --nvidia-spin-damp         | Num  | Workaround NVIDIAs CPU burning loop bug, in percent  | --nvidia-spin-damp=50
     --gpu-temp-disable         |      | Disable temperature and fanspeed reads and triggers  |
     --gpu-temp-abort           | Num  | Abort if GPU temperature reaches X degrees Celsius   | --gpu-temp-abort=100
     --scrypt-tmto              | Num  | Manually override TMTO value for scrypt to X         | --scrypt-tmto=3
 -s, --skip                     | Num  | Skip X words from the start                          | -s 1000000
 -l, --limit                    | Num  | Limit X words from the start + skipped words         | -l 1000000
     --keyspace                 |      | Show keyspace base:mod values and quit               |
 -j, --rule-left                | Rule | Single rule applied to each word from left wordlist  | -j 'c'
 -k, --rule-right               | Rule | Single rule applied to each word from right wordlist | -k '^-'
 -r, --rules-file               | File | Multiple rules applied to each word from wordlists   | -r rules/best64.rule
 -g, --generate-rules           | Num  | Generate X random rules                              | -g 10000
     --generate-rules-func-min  | Num  | Force min X functions per rule                       |
     --generate-rules-func-max  | Num  | Force max X functions per rule                       |
     --generate-rules-seed      | Num  | Force RNG seed set to X                              |
 -1, --custom-charset1          | CS   | User-defined charset ?1                              | -1 ?l?d?u
 -2, --custom-charset2          | CS   | User-defined charset ?2                              | -2 ?l?d?s
 -3, --custom-charset3          | CS   | User-defined charset ?3                              |
 -4, --custom-charset4          | CS   | User-defined charset ?4                              |
 -i, --increment                |      | Enable mask increment mode                           |
     --increment-min            | Num  | Start mask incrementing at X                         | --increment-min=4
     --increment-max            | Num  | Stop mask incrementing at X                          | --increment-max=8
 -S, --slow-candidates          |      | Enable slower (but advanced) candidate generators    |
     --brain-server             |      | Enable brain server                                  |
 -z, --brain-client             |      | Enable brain client, activates -S                    |
     --brain-client-features    | Num  | Define brain client features, see below              | --brain-client-features=3
     --brain-host               | Str  | Brain server host (IP or domain)                     | --brain-host=127.0.0.1
     --brain-port               | Port | Brain server port                                    | --brain-port=13743
     --brain-password           | Str  | Brain server authentication password                 |
--brain-password=bZfhCvGUSjRq
     --brain-session            | Hex  | Overrides automatically calculated brain session     | --brain-session=0x2ae611db
     --brain-session-whitelist  | Hex  | Allow given sessions only, separated with commas     |
--brain-session-whitelist=0x2ae611db

- [ Hash modes ] -

      # | Name                                               | Category
  ======+==================================================+======================================
    900 | MD4                                                | Raw Hash
      0 | MD5                                                | Raw Hash
   5100 | Half MD5                                           | Raw Hash
    100 | SHA1                                               | Raw Hash
   1300 | SHA2-224                                           | Raw Hash
   1400 | SHA2-256                                           | Raw Hash
  10800 | SHA2-384                                           | Raw Hash
   1700 | SHA2-512                                           | Raw Hash
  17300 | SHA3-224                                           | Raw Hash
  17400 | SHA3-256                                           | Raw Hash
  17500 | SHA3-384                                           | Raw Hash
  17600 | SHA3-512                                           | Raw Hash
  17700 | Keccak-224                                         | Raw Hash
  17800 | Keccak-256                                         | Raw Hash
  17900 | Keccak-384                                         | Raw Hash
  18000 | Keccak-512                                         | Raw Hash
    600 | BLAKE2b-512                                        | Raw Hash
  10100 | SipHash                                            | Raw Hash
   6000 | RIPEMD-160                                         | Raw Hash
   6100 | Whirlpool                                          | Raw Hash
   6900 | GOST R 34.11-94                                    | Raw Hash
  11700 | GOST R 34.11-2012 (Streebog) 256-bit               | Raw Hash
  11800 | GOST R 34.11-2012 (Streebog) 512-bit               | Raw Hash
     10 | md5($pass.$salt)                                   | Raw Hash, Salted and/or Iterated
     20 | md5($salt.$pass)                                   | Raw Hash, Salted and/or Iterated
     30 | md5(utf16le($pass).$salt)                          | Raw Hash, Salted and/or Iterated
     40 | md5($salt.utf16le($pass))                          | Raw Hash, Salted and/or Iterated
   3800 | md5($salt.$pass.$salt)                             | Raw Hash, Salted and/or Iterated
   3710 | md5($salt.md5($pass))                              | Raw Hash, Salted and/or Iterated
   4010 | md5($salt.md5($salt.$pass))                        | Raw Hash, Salted and/or Iterated
   4110 | md5($salt.md5($pass.$salt))                        | Raw Hash, Salted and/or Iterated
   2600 | md5(md5($pass))                                    | Raw Hash, Salted and/or Iterated
   3910 | md5(md5($pass).md5($salt))                         | Raw Hash, Salted and/or Iterated
   4300 | md5(strtoupper(md5($pass)))                        | Raw Hash, Salted and/or Iterated
   4400 | md5(sha1($pass))                                   | Raw Hash, Salted and/or Iterated
    110 | sha1($pass.$salt)                                  | Raw Hash, Salted and/or Iterated
    120 | sha1($salt.$pass)                                  | Raw Hash, Salted and/or Iterated
    130 | sha1(utf16le($pass).$salt)                         | Raw Hash, Salted and/or Iterated
    140 | sha1($salt.utf16le($pass))                         | Raw Hash, Salted and/or Iterated
   4500 | sha1(sha1($pass))                                  | Raw Hash, Salted and/or Iterated
```

4520	sha1($salt.sha1($pass))	Raw Hash, Salted and/or Iterated
4700	sha1(md5($pass))	Raw Hash, Salted and/or Iterated
4900	sha1($salt.$pass.$salt)	Raw Hash, Salted and/or Iterated
14400	sha1(CX)	Raw Hash, Salted and/or Iterated
1410	sha256($pass.$salt)	Raw Hash, Salted and/or Iterated
1420	sha256($salt.$pass)	Raw Hash, Salted and/or Iterated
1430	sha256(utf16le($pass).$salt)	Raw Hash, Salted and/or Iterated
1440	sha256($salt.utf16le($pass))	Raw Hash, Salted and/or Iterated
1710	sha512($pass.$salt)	Raw Hash, Salted and/or Iterated
1720	sha512($salt.$pass)	Raw Hash, Salted and/or Iterated
1730	sha512(utf16le($pass).$salt)	Raw Hash, Salted and/or Iterated
1740	sha512($salt.utf16le($pass))	Raw Hash, Salted and/or Iterated
50	HMAC-MD5 (key = $pass)	Raw Hash, Authenticated
60	HMAC-MD5 (key = $salt)	Raw Hash, Authenticated
150	HMAC-SHA1 (key = $pass)	Raw Hash, Authenticated
160	HMAC-SHA1 (key = $salt)	Raw Hash, Authenticated
1450	HMAC-SHA256 (key = $pass)	Raw Hash, Authenticated
1460	HMAC-SHA256 (key = $salt)	Raw Hash, Authenticated
1750	HMAC-SHA512 (key = $pass)	Raw Hash, Authenticated
1760	HMAC-SHA512 (key = $salt)	Raw Hash, Authenticated
14000	DES (PT = $salt, key = $pass)	Raw Cipher, Known-Plaintext attack
14100	3DES (PT = $salt, key = $pass)	Raw Cipher, Known-Plaintext attack
14900	Skip32 (PT = $salt, key = $pass)	Raw Cipher, Known-Plaintext attack
15400	ChaCha20	Raw Cipher, Known-Plaintext attack
400	phpass	Generic KDF
8900	scrypt	Generic KDF
11900	PBKDF2-HMAC-MD5	Generic KDF
12000	PBKDF2-HMAC-SHA1	Generic KDF
10900	PBKDF2-HMAC-SHA256	Generic KDF
12100	PBKDF2-HMAC-SHA512	Generic KDF
23	Skype	Network Protocols
2500	WPA-EAPOL-PBKDF2	Network Protocols
2501	WPA-EAPOL-PMK	Network Protocols
16800	WPA-PMKID-PBKDF2	Network Protocols
16801	WPA-PMKID-PMK	Network Protocols
4800	iSCSI CHAP authentication, MD5(CHAP)	Network Protocols
5300	IKE-PSK MD5	Network Protocols
5400	IKE-PSK SHA1	Network Protocols
5500	NetNTLMv1	Network Protocols
5500	NetNTLMv1+ESS	Network Protocols
5600	NetNTLMv2	Network Protocols
7300	IPMI2 RAKP HMAC-SHA1	Network Protocols
7500	Kerberos 5 AS-REQ Pre-Auth etype 23	Network Protocols
8300	DNSSEC (NSEC3)	Network Protocols
10200	CRAM-MD5	Network Protocols
11100	PostgreSQL CRAM (MD5)	Network Protocols
11200	MySQL CRAM (SHA1)	Network Protocols
11400	SIP digest authentication (MD5)	Network Protocols
13100	Kerberos 5 TGS-REP etype 23	Network Protocols
16100	TACACS+	Network Protocols
16500	JWT (JSON Web Token)	Network Protocols
121	SMF (Simple Machines Forum) > v1.1	Forums, CMS, E-Commerce, Frameworks
400	phpBB3 (MD5)	Forums, CMS, E-Commerce, Frameworks
2611	vBulletin < v3.8.5	Forums, CMS, E-Commerce, Frameworks
2711	vBulletin >= v3.8.5	Forums, CMS, E-Commerce, Frameworks
2811	MyBB 1.2+	Forums, CMS, E-Commerce, Frameworks
2811	IPB2+ (Invision Power Board)	Forums, CMS, E-Commerce, Frameworks
8400	WBB3 (Woltlab Burning Board)	Forums, CMS, E-Commerce, Frameworks
11	Joomla < 2.5.18	Forums, CMS, E-Commerce, Frameworks
400	Joomla >= 2.5.18 (MD5)	Forums, CMS, E-Commerce, Frameworks
400	WordPress (MD5)	Forums, CMS, E-Commerce, Frameworks
2612	PHPS	Forums, CMS, E-Commerce, Frameworks
7900	Drupal7	Forums, CMS, E-Commerce, Frameworks
21	osCommerce	Forums, CMS, E-Commerce, Frameworks
21	xt:Commerce	Forums, CMS, E-Commerce, Frameworks
11000	PrestaShop	Forums, CMS, E-Commerce, Frameworks
124	Django (SHA-1)	Forums, CMS, E-Commerce, Frameworks
10000	Django (PBKDF2-SHA256)	Forums, CMS, E-Commerce, Frameworks
16000	Tripcode	Forums, CMS, E-Commerce, Frameworks
3711	MediaWiki B type	Forums, CMS, E-Commerce, Frameworks
13900	OpenCart	Forums, CMS, E-Commerce, Frameworks
4521	Redmine	Forums, CMS, E-Commerce, Frameworks
4522	PunBB	Forums, CMS, E-Commerce, Frameworks
12001	Atlassian (PBKDF2-HMAC-SHA1)	Forums, CMS, E-Commerce, Frameworks
12	PostgreSQL	Database Server
131	MSSQL (2000)	Database Server
132	MSSQL (2005)	Database Server
1731	MSSQL (2012, 2014)	Database Server
200	MySQL323	Database Server
300	MySQL4.1/MySQL5	Database Server
3100	Oracle H: Type (Oracle 7+)	Database Server

```
  112 | Oracle S: Type (Oracle 11+)                      | Database Server
12300 | Oracle T: Type (Oracle 12+)                      | Database Server
 8000 | Sybase ASE                                       | Database Server
  141 | Episerver 6.x < .NET 4                           | HTTP, SMTP, LDAP Server
 1441 | Episerver 6.x >= .NET 4                          | HTTP, SMTP, LDAP Server
 1600 | Apache $apr1$ MD5, md5apr1, MD5 (APR)            | HTTP, SMTP, LDAP Server
12600 | ColdFusion 10+                                   | HTTP, SMTP, LDAP Server
 1421 | hMailServer                                      | HTTP, SMTP, LDAP Server
  101 | nsldap, SHA-1(Base64), Netscape LDAP SHA         | HTTP, SMTP, LDAP Server
  111 | nsldaps, SSHA-1(Base64), Netscape LDAP SSHA      | HTTP, SMTP, LDAP Server
 1411 | SSHA-256(Base64), LDAP {SSHA256}                 | HTTP, SMTP, LDAP Server
 1711 | SSHA-512(Base64), LDAP {SSHA512}                 | HTTP, SMTP, LDAP Server
16400 | CRAM-MD5 Dovecot                                 | HTTP, SMTP, LDAP Server
15000 | FileZilla Server >= 0.9.55                       | FTP Server
11500 | CRC32                                            | Checksums
 3000 | LM                                               | Operating Systems
 1000 | NTLM                                             | Operating Systems
 1100 | Domain Cached Credentials (DCC), MS Cache        | Operating Systems
 2100 | Domain Cached Credentials 2 (DCC2), MS Cache 2   | Operating Systems
15300 | DPAPI masterkey file v1                          | Operating Systems
15900 | DPAPI masterkey file v2                          | Operating Systems
12800 | MS-AzureSync  PBKDF2-HMAC-SHA256                 | Operating Systems
 1500 | descrypt, DES (Unix), Traditional DES            | Operating Systems
12400 | BSDi Crypt, Extended DES                         | Operating Systems
  500 | md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)        | Operating Systems
 3200 | bcrypt $2*$, Blowfish (Unix)                     | Operating Systems
 7400 | sha256crypt $5$, SHA256 (Unix)                   | Operating Systems
 1800 | sha512crypt $6$, SHA512 (Unix)                   | Operating Systems
  122 | macOS v10.4, MacOS v10.5, MacOS v10.6            | Operating Systems
 1722 | macOS v10.7                                      | Operating Systems
 7100 | macOS v10.8+ (PBKDF2-SHA512)                     | Operating Systems
 6300 | AIX {smd5}                                       | Operating Systems
 6700 | AIX {ssha1}                                      | Operating Systems
 6400 | AIX {ssha256}                                    | Operating Systems
 6500 | AIX {ssha512}                                    | Operating Systems
 2400 | Cisco-PIX MD5                                    | Operating Systems
 2410 | Cisco-ASA MD5                                    | Operating Systems
  500 | Cisco-IOS $1$ (MD5)                              | Operating Systems
 5700 | Cisco-IOS type 4 (SHA256)                        | Operating Systems
 9200 | Cisco-IOS $8$ (PBKDF2-SHA256)                    | Operating Systems
 9300 | Cisco-IOS $9$ (scrypt)                           | Operating Systems
   22 | Juniper NetScreen/SSG (ScreenOS)                 | Operating Systems
  501 | Juniper IVE                                      | Operating Systems
15100 | Juniper/NetBSD sha1crypt                         | Operating Systems
 7000 | FortiGate (FortiOS)                              | Operating Systems
 5800 | Samsung Android Password/PIN                     | Operating Systems
13800 | Windows Phone 8+ PIN/password                    | Operating Systems
 8100 | Citrix NetScaler                                 | Operating Systems
 8500 | RACF                                             | Operating Systems
 7200 | GRUB 2                                           | Operating Systems
 9900 | Radmin2                                          | Operating Systems
  125 | ArubaOS                                          | Operating Systems
 7700 | SAP CODVN B (BCODE)                              | Enterprise Application Software (EAS)
 7701 | SAP CODVN B (BCODE) via RFC_READ_TABLE           | Enterprise Application Software (EAS)
 7800 | SAP CODVN F/G (PASSCODE)                         | Enterprise Application Software (EAS)
 7801 | SAP CODVN F/G (PASSCODE) via RFC_READ_TABLE      | Enterprise Application Software (EAS)
10300 | SAP CODVN H (PWDSALTEDHASH) iSSHA-1              | Enterprise Application Software (EAS)
 8600 | Lotus Notes/Domino 5                             | Enterprise Application Software (EAS)
 8700 | Lotus Notes/Domino 6                             | Enterprise Application Software (EAS)
 9100 | Lotus Notes/Domino 8                             | Enterprise Application Software (EAS)
  133 | PeopleSoft                                       | Enterprise Application Software (EAS)
13500 | PeopleSoft PS_TOKEN                              | Enterprise Application Software (EAS)
11600 | 7-Zip                                            | Archives
12500 | RAR3-hp                                          | Archives
13000 | RAR5                                             | Archives
13200 | AxCrypt                                          | Archives
13300 | AxCrypt in-memory SHA1                           | Archives
13600 | WinZip                                           | Archives
14700 | iTunes backup < 10.0                             | Backup
14800 | iTunes backup >= 10.0                            | Backup
 62XY | TrueCrypt                                        | Full-Disk Encryption (FDE)
   X  | 1 = PBKDF2-HMAC-RIPEMD160                        | Full-Disk Encryption (FDE)
   X  | 2 = PBKDF2-HMAC-SHA512                           | Full-Disk Encryption (FDE)
   X  | 3 = PBKDF2-HMAC-Whirlpool                        | Full-Disk Encryption (FDE)
   X  | 4 = PBKDF2-HMAC-RIPEMD160 + boot-mode            | Full-Disk Encryption (FDE)
    Y | 1 = XTS  512 bit pure AES                        | Full-Disk Encryption (FDE)
    Y | 1 = XTS  512 bit pure Serpent                    | Full-Disk Encryption (FDE)
    Y | 1 = XTS  512 bit pure Twofish                    | Full-Disk Encryption (FDE)
    Y | 2 = XTS 1024 bit pure AES                        | Full-Disk Encryption (FDE)
    Y | 2 = XTS 1024 bit pure Serpent                    | Full-Disk Encryption (FDE)
    Y | 2 = XTS 1024 bit pure Twofish                    | Full-Disk Encryption (FDE)
```

```
      Y | 2 = XTS 1024 bit cascaded AES-Twofish            | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded Serpent-AES            | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded Twofish-Serpent        | Full-Disk Encryption (FDE)
      Y | 3 = XTS 1536 bit all                             | Full-Disk Encryption (FDE)
   8800 | Android FDE <= 4.3                               | Full-Disk Encryption (FDE)
  12900 | Android FDE (Samsung DEK)                        | Full-Disk Encryption (FDE)
  12200 | eCryptfs                                         | Full-Disk Encryption (FDE)
  137XY | VeraCrypt                                        | Full-Disk Encryption (FDE)
     X  | 1 = PBKDF2-HMAC-RIPEMD160                        | Full-Disk Encryption (FDE)
     X  | 2 = PBKDF2-HMAC-SHA512                           | Full-Disk Encryption (FDE)
     X  | 3 = PBKDF2-HMAC-Whirlpool                        | Full-Disk Encryption (FDE)
     X  | 4 = PBKDF2-HMAC-RIPEMD160 + boot-mode            | Full-Disk Encryption (FDE)
     X  | 5 = PBKDF2-HMAC-SHA256                           | Full-Disk Encryption (FDE)
     X  | 6 = PBKDF2-HMAC-SHA256 + boot-mode               | Full-Disk Encryption (FDE)
      Y | 1 = XTS  512 bit pure AES                        | Full-Disk Encryption (FDE)
      Y | 1 = XTS  512 bit pure Serpent                    | Full-Disk Encryption (FDE)
      Y | 1 = XTS  512 bit pure Twofish                    | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit pure AES                        | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit pure Serpent                    | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit pure Twofish                    | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded AES-Twofish            | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded Serpent-AES            | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded Twofish-Serpent        | Full-Disk Encryption (FDE)
      Y | 3 = XTS 1536 bit all                             | Full-Disk Encryption (FDE)
  14600 | LUKS                                             | Full-Disk Encryption (FDE)
  16700 | FileVault 2                                      | Full-Disk Encryption (FDE)
   9700 | MS Office <= 2003 $0/$1, MD5 + RC4               | Documents
   9710 | MS Office <= 2003 $0/$1, MD5 + RC4, collider #1  | Documents
   9720 | MS Office <= 2003 $0/$1, MD5 + RC4, collider #2  | Documents
   9800 | MS Office <= 2003 $3/$4, SHA1 + RC4              | Documents
   9810 | MS Office <= 2003 $3, SHA1 + RC4, collider #1    | Documents
   9820 | MS Office <= 2003 $3, SHA1 + RC4, collider #2    | Documents
   9400 | MS Office 2007                                   | Documents
   9500 | MS Office 2010                                   | Documents
   9600 | MS Office 2013                                   | Documents
  10400 | PDF 1.1 - 1.3 (Acrobat 2 - 4)                    | Documents
  10410 | PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #1       | Documents
  10420 | PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #2       | Documents
  10500 | PDF 1.4 - 1.6 (Acrobat 5 - 8)                    | Documents
  10600 | PDF 1.7 Level 3 (Acrobat 9)                      | Documents
  10700 | PDF 1.7 Level 8 (Acrobat 10 - 11)                | Documents
  16200 | Apple Secure Notes                               | Documents
   9000 | Password Safe v2                                 | Password Managers
   5200 | Password Safe v3                                 | Password Managers
   6800 | LastPass + LastPass sniffed                      | Password Managers
   6600 | 1Password, agilekeychain                         | Password Managers
   8200 | 1Password, cloudkeychain                         | Password Managers
  11300 | Bitcoin/Litecoin wallet.dat                      | Password Managers
  12700 | Blockchain, My Wallet                            | Password Managers
  15200 | Blockchain, My Wallet, V2                        | Password Managers
  16600 | Electrum Wallet (Salt-Type 1-3)                  | Password Managers
  13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES)      | Password Managers
  15500 | JKS Java Key Store Private Keys (SHA1)           | Password Managers
  15600 | Ethereum Wallet, PBKDF2-HMAC-SHA256              | Password Managers
  15700 | Ethereum Wallet, SCRYPT                          | Password Managers
  16300 | Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256     | Password Managers
  16900 | Ansible Vault                                    | Password Managers
  18100 | TOTP (HMAC-SHA1)                                 | One-Time Passwords
  99999 | Plaintext                                        | Plaintext

- [ Brain Client Features ] -

  # | Features
 ===+========
  1 | Send hashed passwords
  2 | Send attack positions
  3 | Send hashed passwords and attack positions

- [ Outfile Formats ] -

  # | Format
 ===+========
  1 | hash[:salt]
  2 | plain
  3 | hash[:salt]:plain
  4 | hex_plain
  5 | hash[:salt]:hex_plain
  6 | plain:hex_plain
  7 | hash[:salt]:plain:hex_plain
  8 | crackpos
  9 | hash[:salt]:crack_pos
```

```
 10 | plain:crack_pos
 11 | hash[:salt]:plain:crack_pos
 12 | hex_plain:crack_pos
 13 | hash[:salt]:hex_plain:crack_pos
 14 | plain:hex_plain:crack_pos
 15 | hash[:salt]:plain:hex_plain:crack_pos

- [ Rule Debugging Modes ] -

  # | Format
 ===+========
  1 | Finding-Rule
  2 | Original-Word
  3 | Original-Word:Finding-Rule
  4 | Original-Word:Finding-Rule:Processed-Word

- [ Attack Modes ] -

  # | Mode
 ===+======
  0 | Straight
  1 | Combination
  3 | Brute-force
  6 | Hybrid Wordlist + Mask
  7 | Hybrid Mask + Wordlist

- [ Built-in Charsets ] -

  ? | Charset
 ===+=========
  l | abcdefghijklmnopqrstuvwxyz
  u | ABCDEFGHIJKLMNOPQRSTUVWXYZ
  d | 0123456789
  h | 0123456789abcdef
  H | 0123456789ABCDEF
  s |  !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
  a | ?l?u?d?s
  b | 0x00 - 0xff

- [ OpenCL Device Types ] -

  # | Device Type
 ===+=============
  1 | CPU
  2 | GPU
  3 | FPGA, DSP, Co-Processor

- [ Workload Profiles ] -

  # | Performance | Runtime | Power Consumption | Desktop Impact
 ===+=============+=========+===================+================
  1 | Low         |   2 ms  | Low               | Minimal
  2 | Default     |  12 ms  | Economic          | Noticeable
  3 | High        |  96 ms  | High              | Unresponsive
  4 | Nightmare   | 480 ms  | Insane            | Headless

- [ Basic Examples ] -

  Attack-          | Hash- |
  Mode             | Type  | Example command
 ==================+=======+==================================================================
  Wordlist         | $P$   | hashcat -a 0 -m 400 example400.hash example.dict
  Wordlist + Rules | MD5   | hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
  Brute-Force      | MD5   | hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a
  Combinator       | MD5   | hashcat -a 1 -m 0 example0.hash example.dict example.dict
```