Elcomsoft Distributed Password Recovery

Мощная многофункциональная программа для получения доступа к зашифрованным данным. Обеспечивает восстановление паролей к десяткам форматов файлов, документов, ключей и сертификатов на кластерах компьютеров, объединённых в единую распределённую вычислительную сеть.

ELCOMSOFT
PROACTIVE SOFTWARE

Особенности и преимущества

Поддержка более 300 форматов данных
Поддерживает: все версии Microsoft Office, OpenOffice, ZIP/RAR/RAR5, PDF, BitLocker/PGP/TrueCrypt. Общее число поддерживаемых форматов – более 500.

Аппаратное ускорение с использованием потребительских видеокарт
Поддержка видеокарт с графическими акселераторами NVIDIA и AMD

Перебор паролей и атаки по словарю
Гибкие настройки мутаций, создание собственных словарей

Ускорение перебора в 20-200 раз в сравнении с работой на центральном процессоре
Возможность использования до 256 процессоров/ядер (CPU) и до 32 графических чипов (GPU) на один вычислительный узел

Линейное масштабирование до 10,000 рабочих станций

Удалённое развёртывание и управление через консоль
Управление сервером с любой рабочей станции с использованием консоли.
Возможен запуск клиентских и серверных приложений в виде системных сервисов

Поддерживаемые форматы

- Adobe Acrobat9 PDF (SHA256+AES256)
- Apple iWork 09
- Apple iWork 2014
- BitLocker
- BlackBerry backup
- Encypted DMG (AES-128)
- FileVault
- GnuPG 2.0 (secring.gpg)
- Hancell 2010/2014
- IBM Notes
- IKE PSK (HMAC(sha1))
- Keepass
- Keychain
- ZIP (AES128)
- ZIP (AES256)
- ZIP (Classic)
- iTunes Backup
- SHA-1
- SHA-256
- SHA-512

- LM (DES-56)
- MD5
- MS SQL Server 2000
- MS SQL Server 2005
- MS SQL Server 2014
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013/2016
- NTLM (MD4)
- OS X Password
- OpenOffice
- PFX/P12 certificates (with strong encryption)(pbkdf2_sha1(?))
- PFX/P12 certificates (without strong enc-tion)(pbkdf2_sha1(1))
- PGP WDE
- PGP secret key (MD5) (simple1)
- PGP secret key (MD5) (simple2)
- PGP secret key (SHA1) (IteratedSalted1)
- PGP secret key (SHA1) (IteratedSalted2)

- PGPDisk 10.3.0 (.pgd) (AES256)
- PGPDisk 10.3.0 (.pgd) (CAST5)
- PGPDisk 10.3.0 (.pgd) (EME2-AES)
- PGPDisk 10.3.0 (.pgd) (Twofish)
- RAR 3-4
- RAR 5
- Domain Cached Credentials Vista+ (2xMD4 + pbkdf2_sha1(10240))
- Domain Cached Credentials Windows 2000-2003 (2xMD4)
- SQL CE (sdf) v3.0 (MD5+RC4)
- SQL CE (sdf) v3.5 (SHA1+AES128)
- QL CE (sdf) v3.5 Win Mobile 2003-based Pocket PC (SHA1+3DES)
- SQL CE (sdf) v4.0 engine default (SHA512+AES256)
- SQL CE (sdf) v4.0 platform default (SHA256+AES128)
- TrueCrypt: Container AES_RIPEMD160
- TrueCrypt: Container Unkn_Unkn
- TrueCrypt: SimpleDisk AES_RIPEMD160
- TrueCrypt: SimpleDisk Unkn_Unkn
- TrueCrypt: SystemDisk AES_RIPEMD160
- TrueCrypt: SystemDisk Unkn_Unkn
- WPA/WPA2 PSK (pbkdf2_sha1(8192) + HMAC(sha1))

Ускорение на GPU

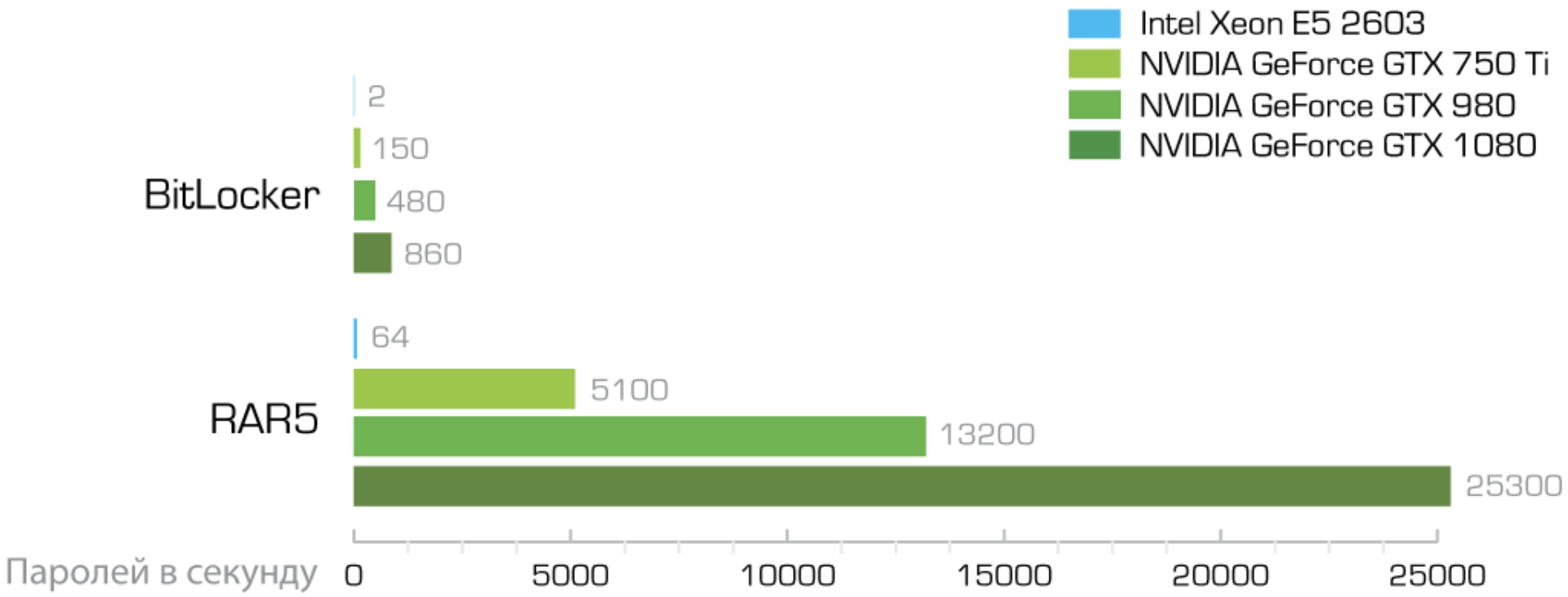
Elcomsoft Distributed Password Recovery использует патентованный способ ускорения процесса перебора паролей, когда в системе присутствует одна или несколько видеокарт NVIDIA или AMD.

Поддерживаются все карты серии NVIDIA GeForce, включая NVIDIA Quadro и Tesla, а также AMD Radeon включая модели серий R2/R4.

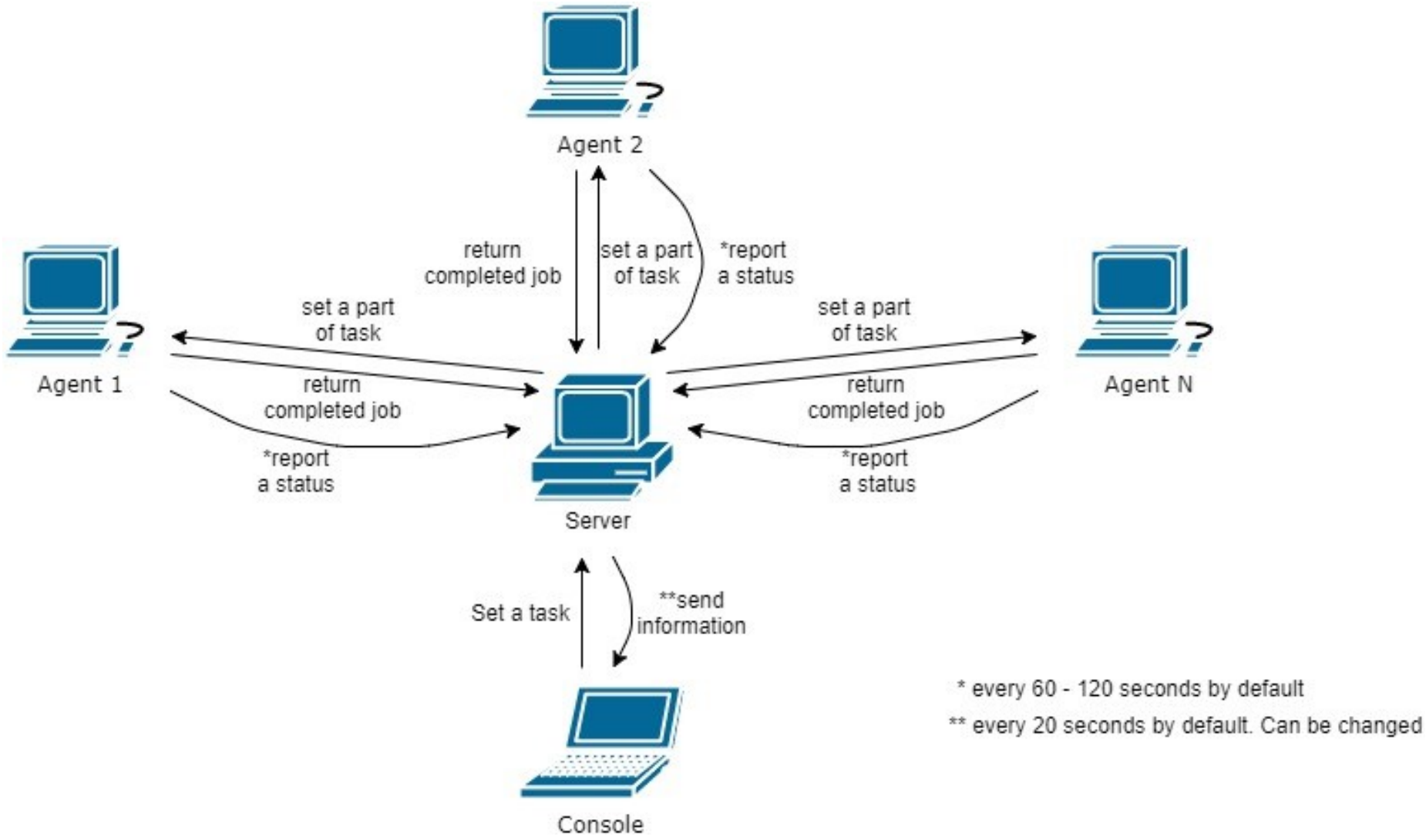
Технология ускорения перекладывает часть сложных вычислений на быстрые и масштабируемые процессоры видеокарт. Скорость расшифровки паролей при использовании GPU вырастает до 50 раз по сравнению с традиционным способом обсчета на ЦПУ.

Достигнутые скорости

Подключив одну или несколько бюджетных видеокарт NVIDIA или AMD, можно создать систему с отличным соотношением "цена/производительность", недоступным ни на каком другом аппаратном обеспечении.

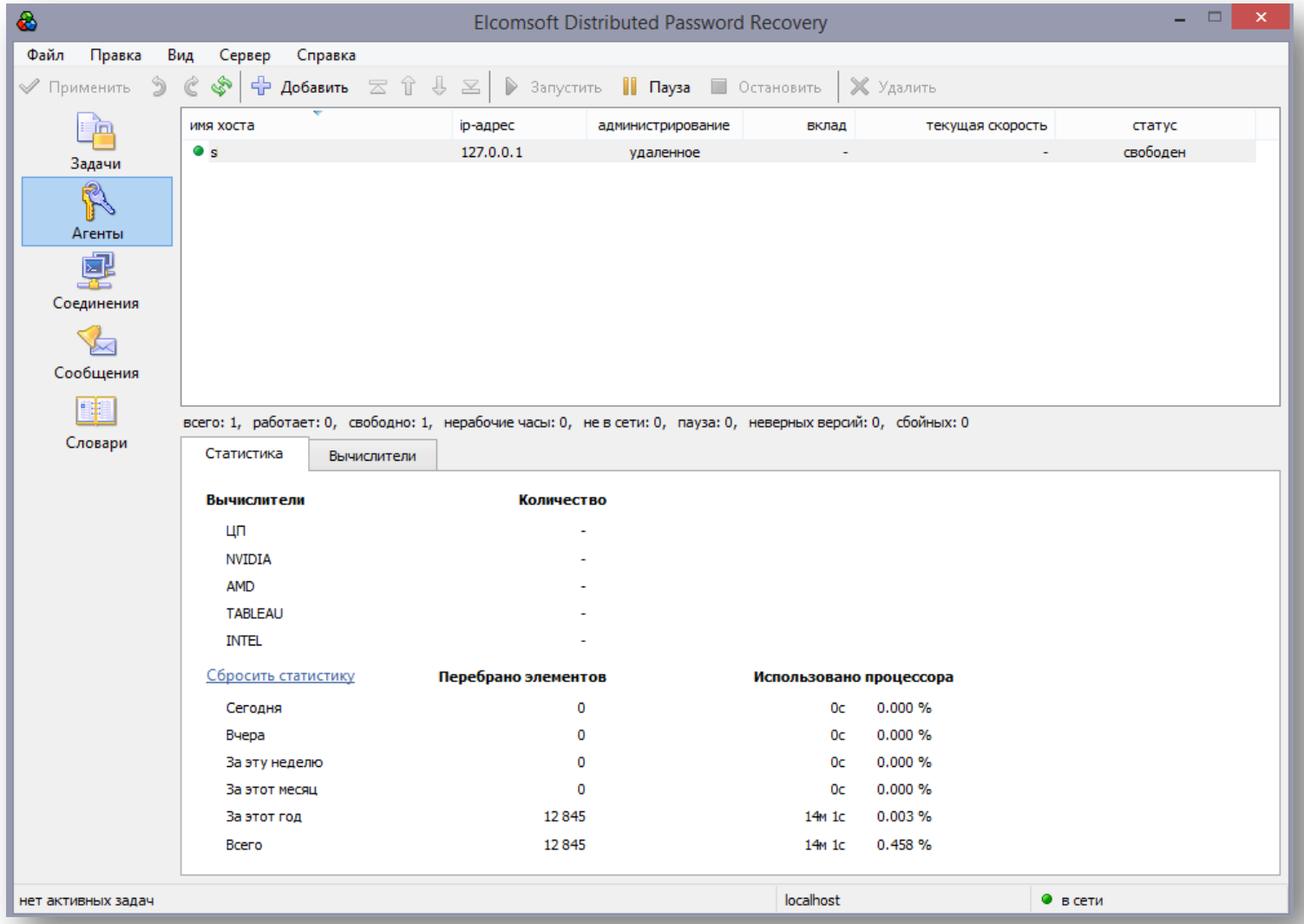


Архитектура программы

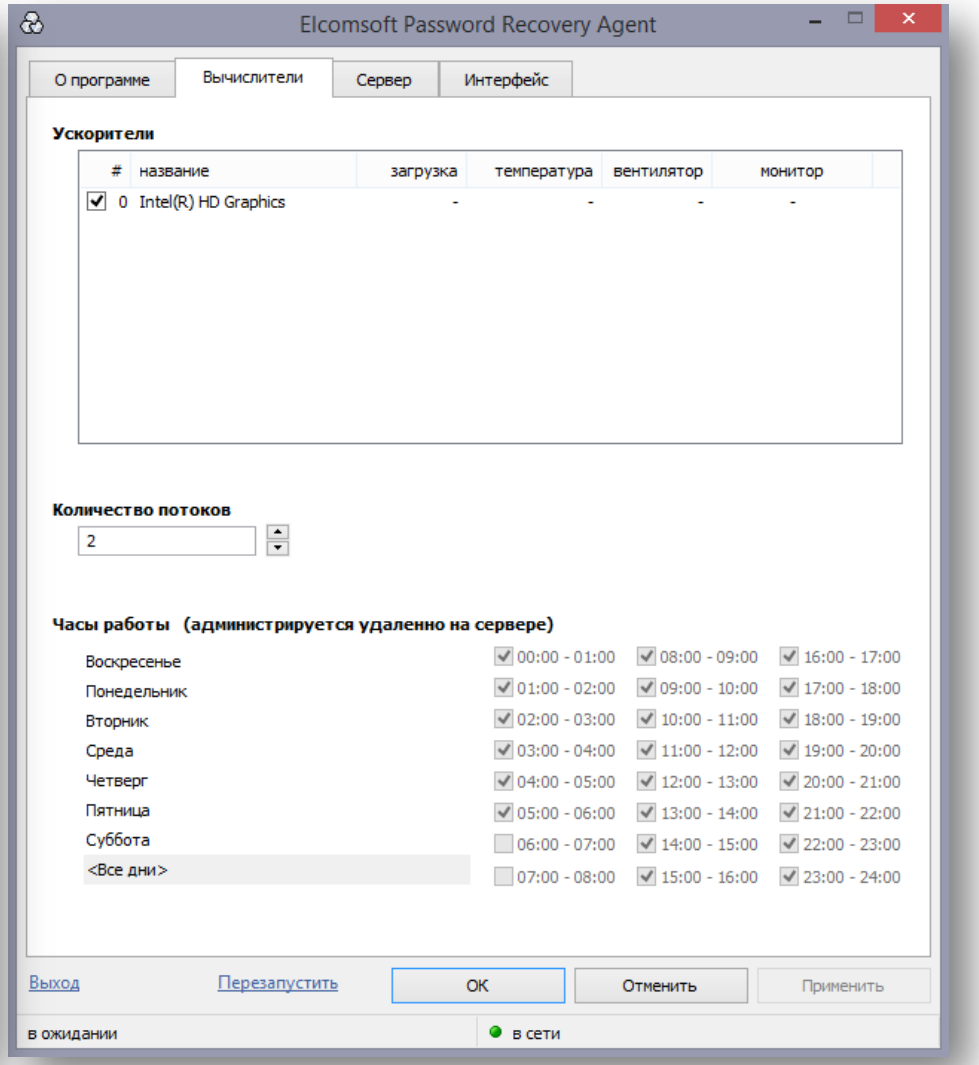


Архитектура программы

Сервер + Консоль



Агент



Интерфейс

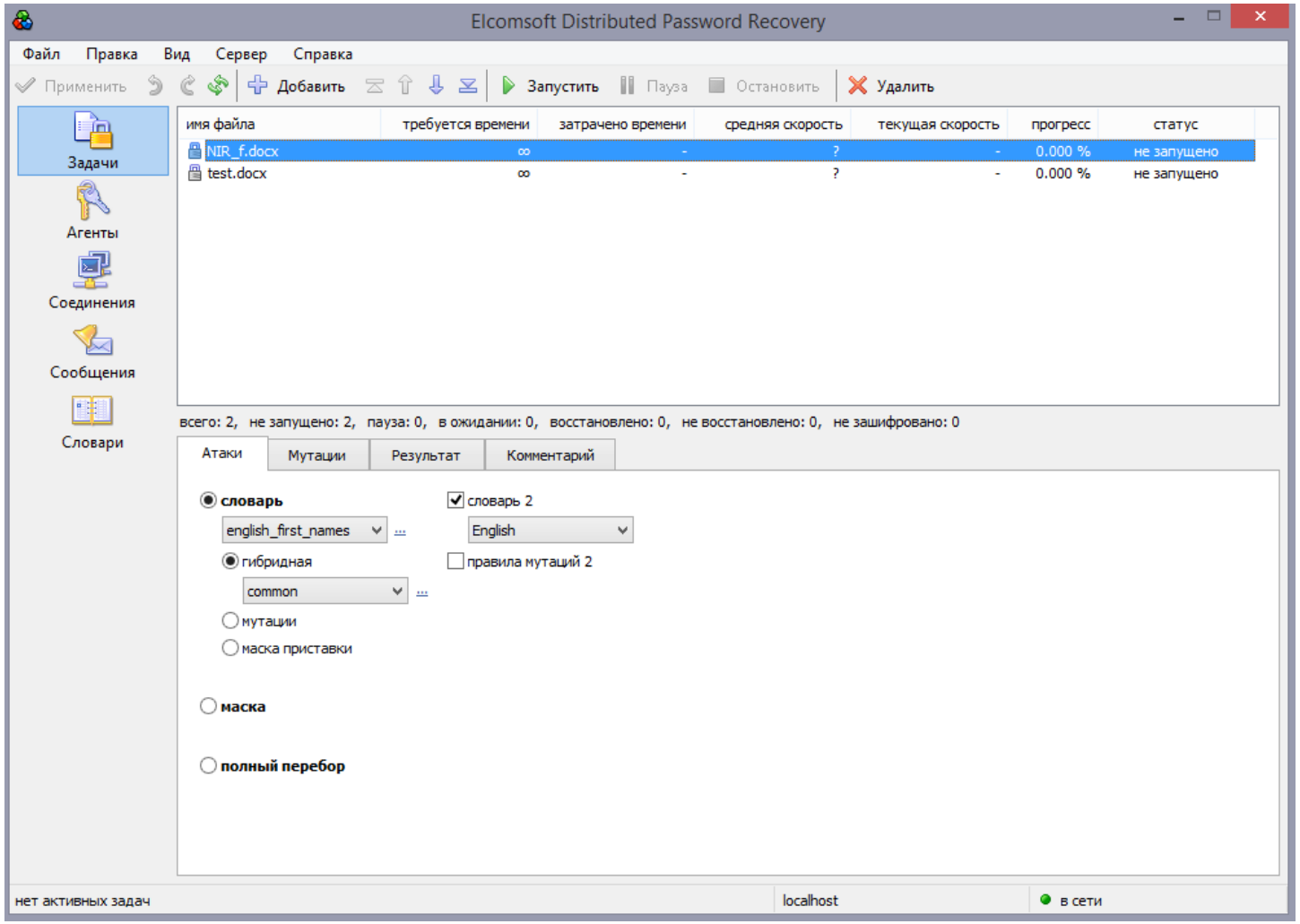
Задачи
Отображение очереди файлов для расшифровки, настройка атак и мутаций, отображение результата.

Агенты
Список доступных Агентов, их рабочие часы, вычислительные мощности и результаты работы в реальном времени.

Соединения
Настройки Сервера для соединения с Консолью и Агентами.

Сообщения
Возможность отправки сообщений о результатах работы программы по электронной почте.

Словари
Создание собственных словарей из найденных паролей и ключей.



Атаки

password
benjamin

Атака по словарю
Используется подобранный словарь (по языку и\или тематике), из которого поочередно берутся слова и подставляются в качестве вероятного пароля.

JohnAbrams
JanePassword123

Гибридная атака
Возможность задействовать несколько словарей с применением к ним мутаций, по желанию.

ih8u123
pA$$w0rd
Anna1983

Атака с мутациями
При использовании словарной атаки применяет к ней гибко задаваемые мутации – т.е. изменение слова посредством добавления различных символов, цифр, букв в начало и\или конец слова, изменение регистра, замена частей корня другими символами и т.д.

robert????
?1(3-4)?0?1(1-2)?2

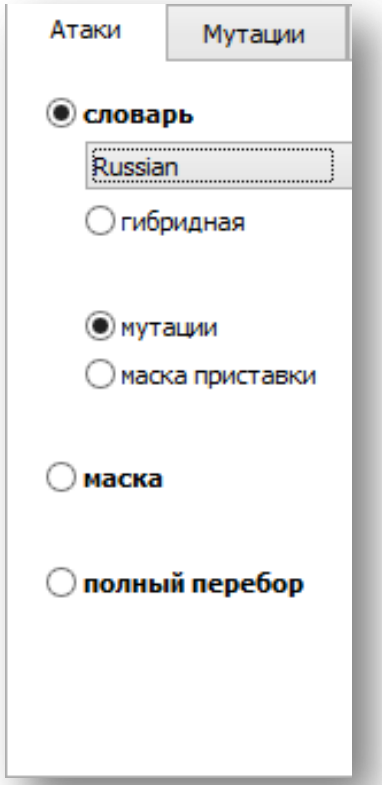
Атака по маске
Когда известна часть пароля или его шаблон, можно задать неизвестный остаток в виде маски из вероятных символов, букв и цифр.

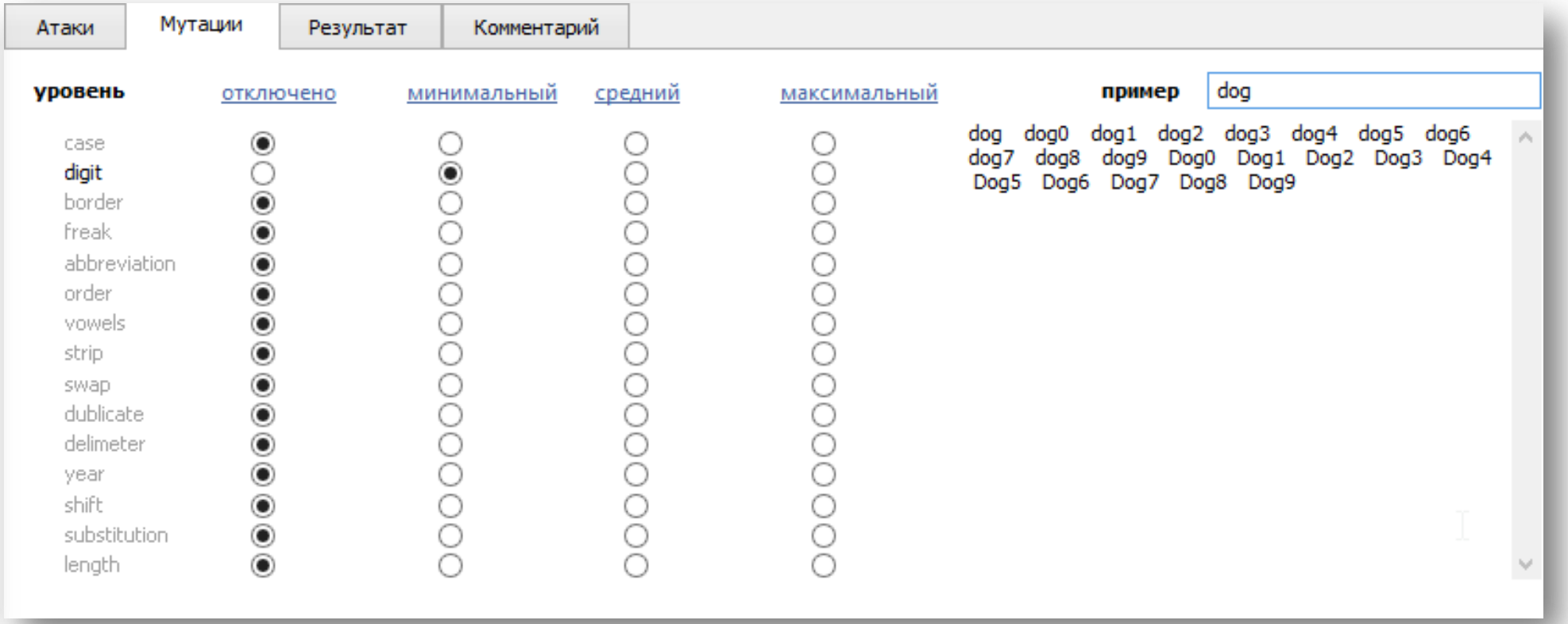
aaadcz
abczq98azx

Полный перебор (брутфорс)
Последовательный перебор всех возможных комбинаций в пределах выбранной длины и используемых символов.

Мутации

Для настройки мутаций в программе предусмотрен удобный механизм, позволяющий настраивать тип и глубину мутации.
Просмотреть результат мутации и разобраться с ее типом и степенью глубины можно, введя любое тестовое слово и посмотрев, какие варианты для его изменения видит программа с текущими настройками. Количество типов и глубина мутации прямо влияют на скорость подбора пароля.





Гибридная атака

Основное предназначение гибридной атаки – более гибкий, но более сложный способ задачи мутаций.
Помимо этого есть возможность использовать сразу два словаря для составных паролей.
Правила подробно описаны в прилагающемся текстовом документе.

common.rul — Блокнот

Файл Правка Формат Вид Справка

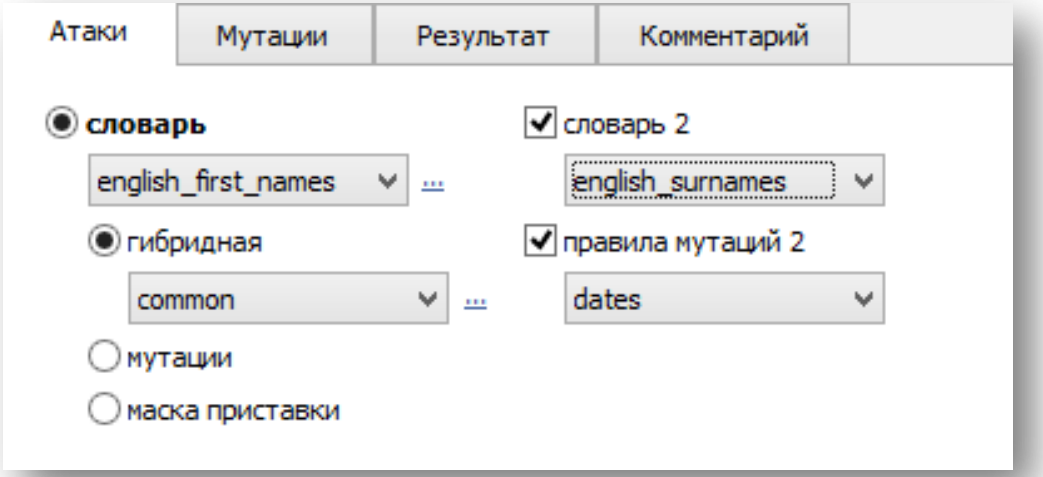
```
Hybrid attack rules:

:       Do nothing, use the original input word
{       Rotate left: password -> asswordp
}       Rotate right: password -> dpasswor
[       Delete the first character: password -> assword
]       Delete the last character: password -> passwor
c       Capitalize: password -> Password
C       Lowercase the first character, uppercase the rest: password -> pASSWORD
d       Duplicate: password -> passwordpassword
f       Reflect: password -> passworddrowssap
l       Convert to lowercase
q       Duplicate all symbols: password -> ppaasssswwoorrdd
```

Их можно задать вручную или использовать подготовленные нами правила:
common – основные мутации;
dates – мутации с датами;
numbers – мутации с цифрами.

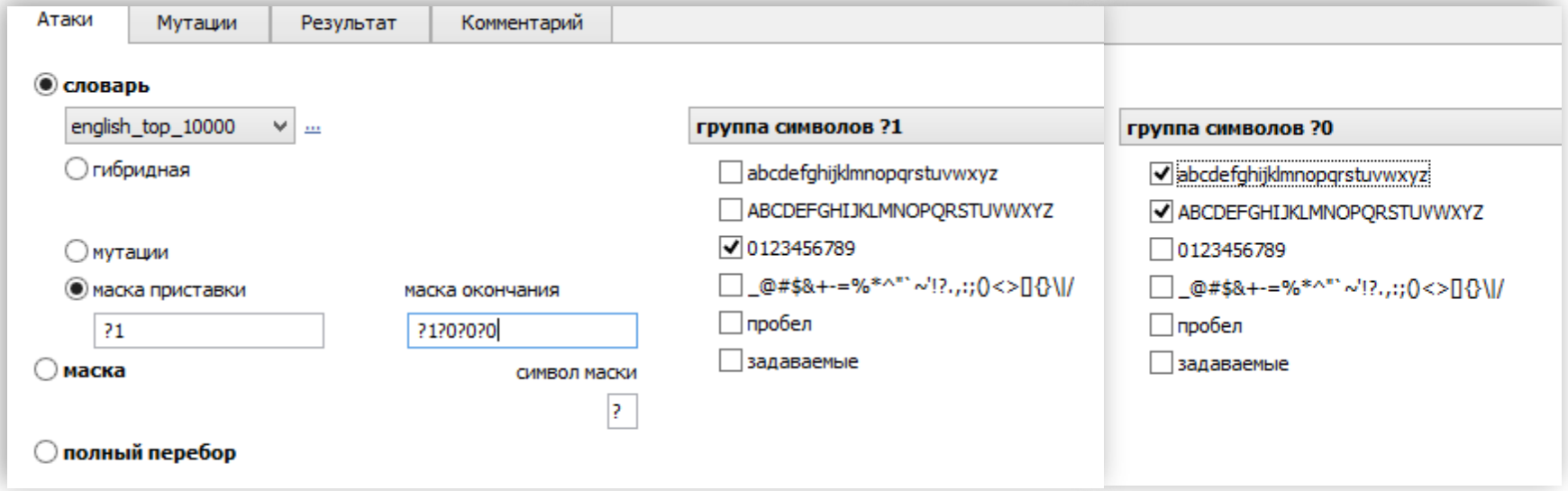
Ко второму словарю возможно применение других мутаций.

jAnEevans1986
j0hnabrams2017



Маска приставки

Подставляет маску приставки и\или окончания для слов из словаря.
Символ маски «?», после которого идет группа выбранных символов.

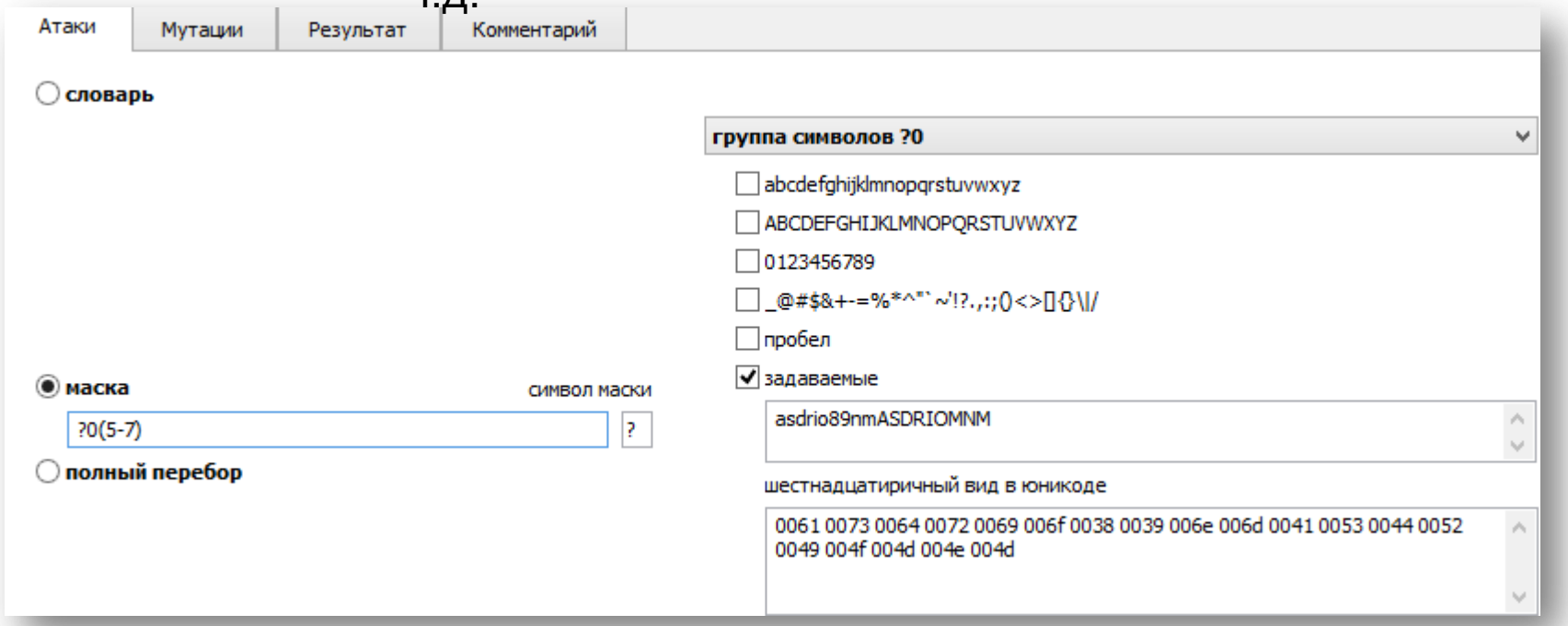


8password8AbC
6starwars9war

Маска

Маска используется, когда вы знаете шаблон пароля или его часть.
Символ маски «?», после которого идет группа выбранных символов.
Можно использовать до 10 групп, в том числе задаваемые. Они используются, когда:

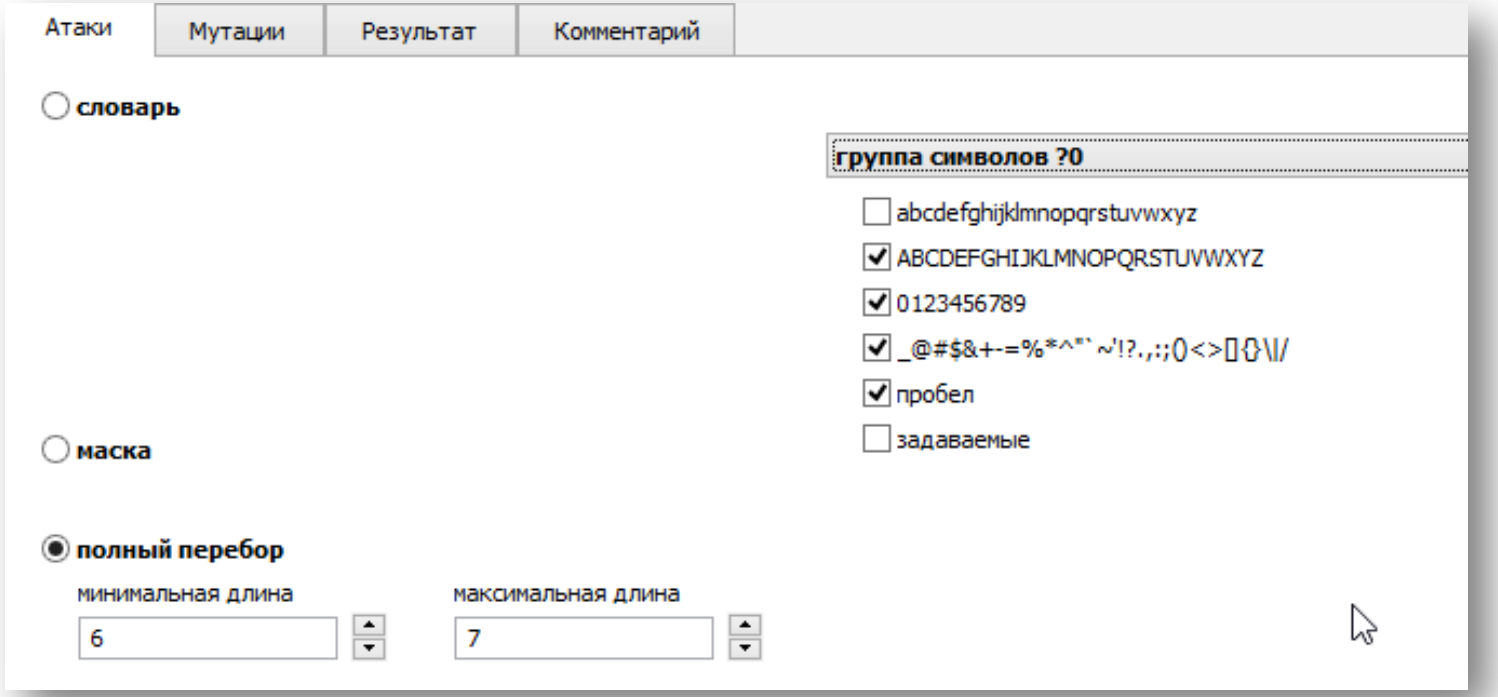
- Вы примерно знаете, какие символы вводил человек
- Когда в пароле могут встречаться символы другого алфавита (русские буквы, иероглифы, спец. символы и т.д.



ASDr8m

Полный перебор

Подставляет все возможные комбинации выбранных символов.
Такая атака дает гарантированный результат, но пароль может подбираться как от нескольких минут, так и до нескольких десятков лет.



2AB-C=D

Кейсы

1. Найти все зашифрованные данные на устройстве.
Если файл не зашифрован, наша программа предупредит вас об этом.

2. Определить скорости подбора пароля для каждого типа файла.
Посмотрите нашу таблицу скоростей для различных типов файлов на разных видеокартах или запустите атаку на каждом типе файла, фиксируя скорость на каждом файле после 5 минут.

3. Навести справки о человеке: какими языками владеет, какие хобби и профессия.
Это поможет выбрать правильный словарь для подбора или хотя бы отсеять лишние. Имена, года рождения и т.д. могут быть полезны при задании масок.

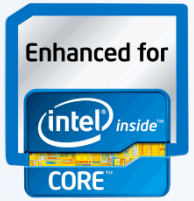
4. Взламывать тот файл, что показал наибольшую скорость. Использовать атаки по маске или конкретному словарю. Использовать мутации в зависимости от мощности оборудования.
Выбирайте количество типов и глубину мутации согласно мощностям своего железа.

5. Найденный пароль применить к остальным файлам. Если не подошел – задать маску по его шаблону или пробовать над ним разные мутации.
Чаще всего люди используют один и тот же сложный пароль везде или средней сложности с применением схожих мутаций.

6. В крайнем случае использовать брутфорс.
Стоит пробовать, если позволяет железо, а формат файла относится к быстро взламываемым.

О нас

Мы работаем с



Мы поддерживаем

Наши клиенты

ЮниКредит Банк

Транснефть

О нас

Компания «Элкомсофт» основана в 1990 году в Москве.
С 1997 года Элкомсофт специализируется на разработке решений в сфере информационной безопасности и цифровой криминалистики. Компанией созданы полные линейки продуктов для извлечения информации из мобильных устройств, восстановления паролей к широкому ряду приложений, а также для восстановления доступа к зашифрованной информации. Корпоративным пользователям предлагаются решения для доступа к учётным записям Windows, аудита паролей, используемых сотрудниками организаций, и аудита безопасности беспроводных сетей (Wi-Fi).

Мы предлагаем:

Поддержка и обучение
Возможны тренинги для специалистов с целью углубленного изучения проблем восстановления доступа к зашифрованным компьютерным, мобильным и “облачным” данным.

Индивидуальная помощь
Мы с радостью окажем профессиональную консультацию и помощь в проведении извлечения и экспертизы компьютерных, мобильных и облачных данных.

Microsoft Partner
Gold Application Development
Gold Intelligent Systems

intel Software Partner

ELCOMSOFT
PROACTIVE SOFTWARE

ELCOMSOFT

PROACTIVE SOFTWARE

www.elcomsoft.ru
www.blog.elcomsoft.com/ru/
info@elcomsoft.com
Телефон: +7 (495) 974 1162