Задача: Сделать на основе RSA систему поддержки выборов тайным голосованием

Протокол тайного голосования «Все против одного»

Участники голосования

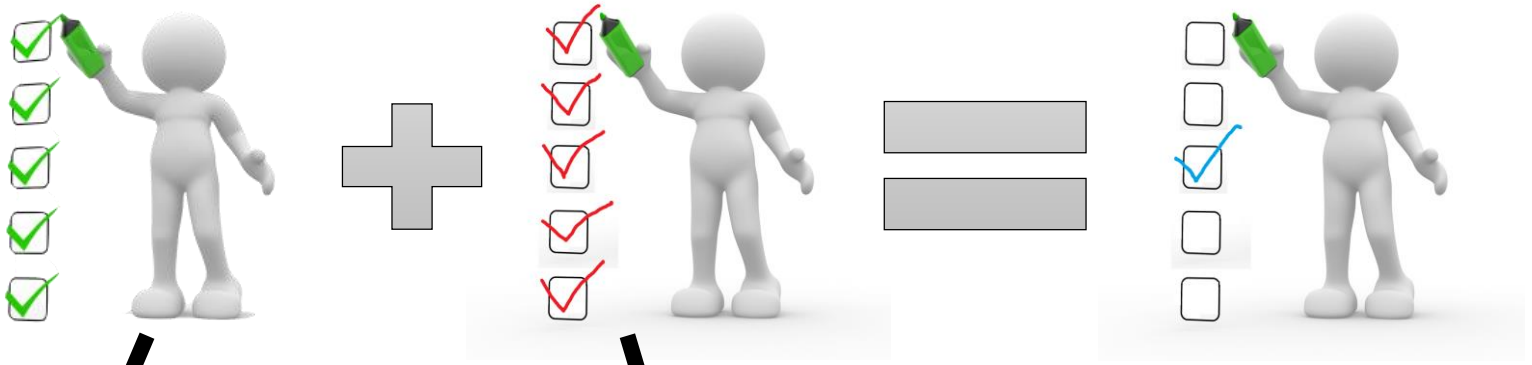
Регистратор

Избиратель

Счетчик

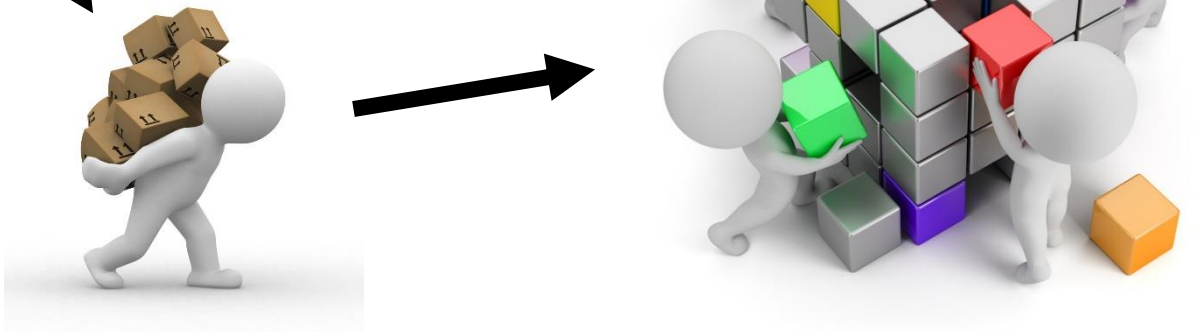
Основная идея

Этап 1:



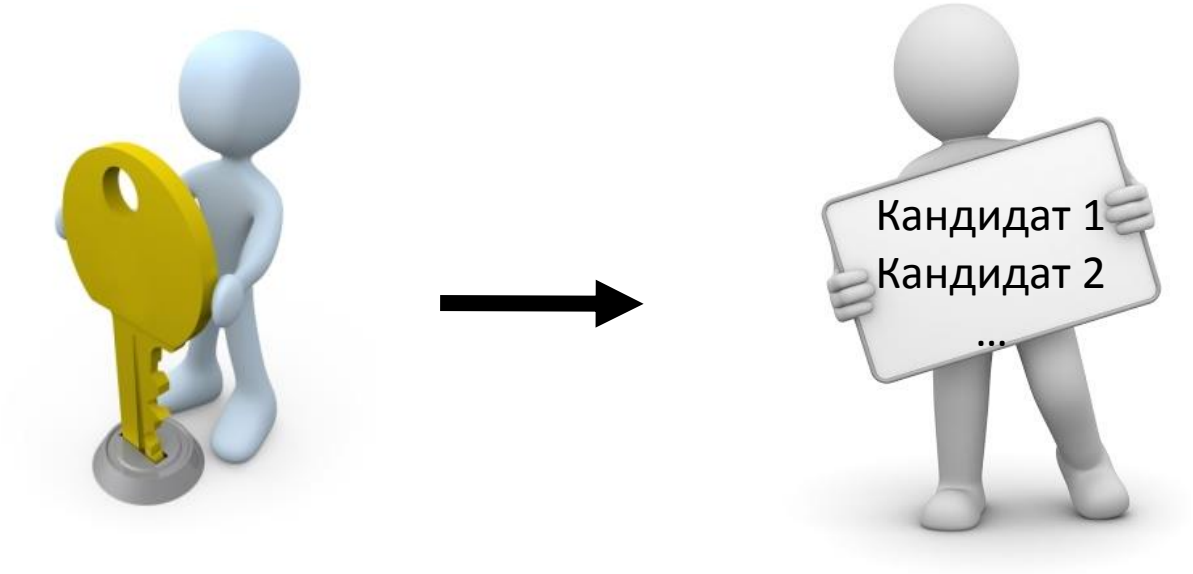
Этап 2:

Этап 3:



Алгоритм
Этап 1

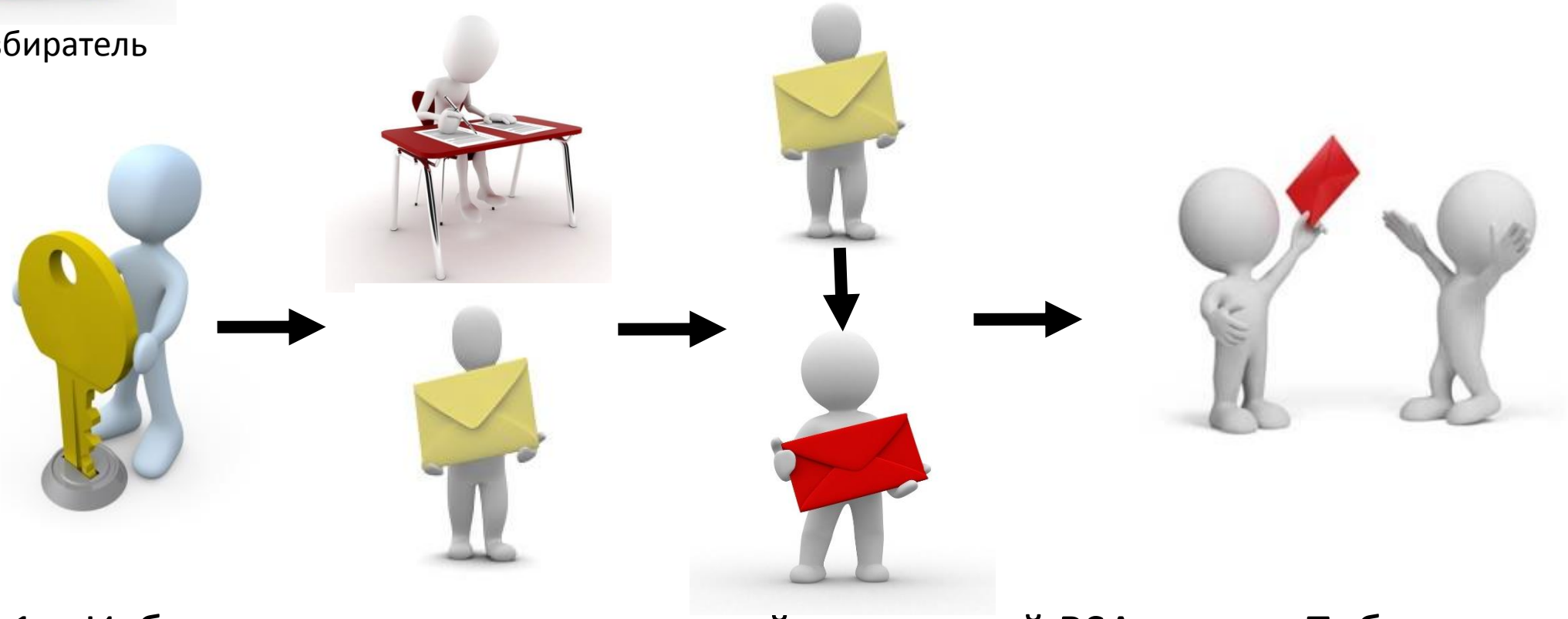
Регистратор



1. Регистратор генерирует открытый и закрытый RSA ключи
2. Составляет список избирателей
3. Регистратор публикует список кандидатов и открытый ключ

Алгоритм
Этап 2

Избиратель



1. Избиратель генерирует открытый и закрытый RSA ключи. Публикует открытый ключ
2. Шифрует свои личные данные открытым ключом регистратора и отправляет ему

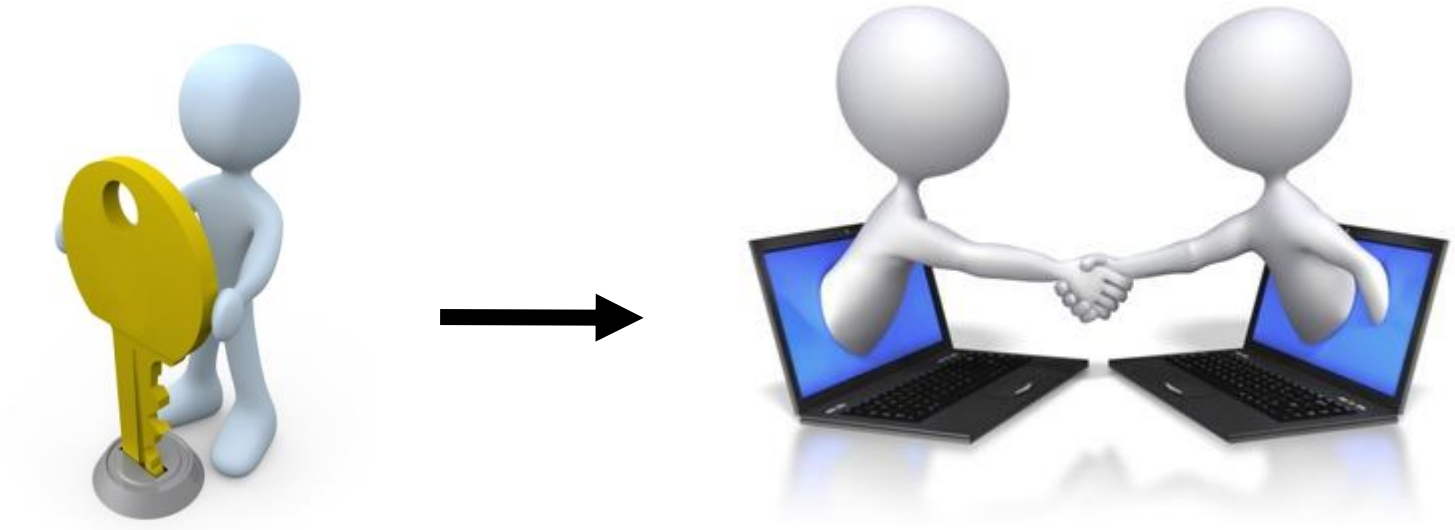
Алгоритм
Этап 3

Регистратор

1. Регистратор расшифровывает личные данные избирателя своим закрытым ключом
2. Если имя пользователя было в списке избирателей, сохраняет IP пользователя и дает разрешение на голосование

Алгоритм
Этап 4

Счетчик



1. Счетчик генерирует открытый и закрытый RSA ключи. Публикует открытый ключ
2. Подключается к регистратору

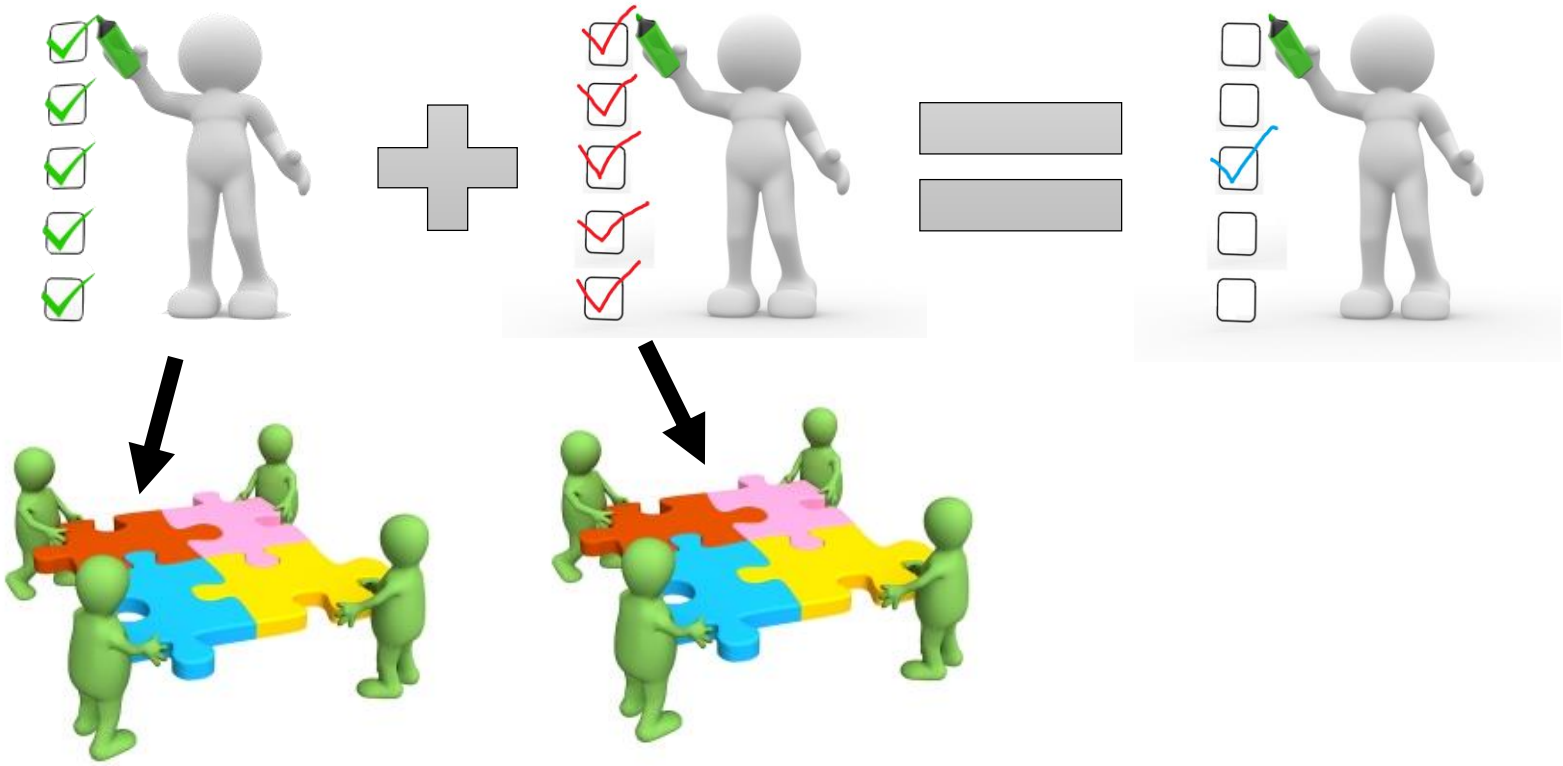
Алгоритм
Этап 5

Регистратор

1. Регистратор дожидается, пока к нему подключатся все избиратели и счетчик
2. Передает сохраненные IP адреса каждому избирателю и счетчику по защищенному каналу

Алгоритм
Этап 6

Избиратель



1. Избиратель делает свой выбор. Составляет две партии голосов, разбивая каждую на кусочки, равные количеству избирателей
2. Отправляет кусочек голоса соответствующему избирателю по защищенному каналу, предварительно подписав его уникальным кодом и зашифровав открытым ключом счетчика

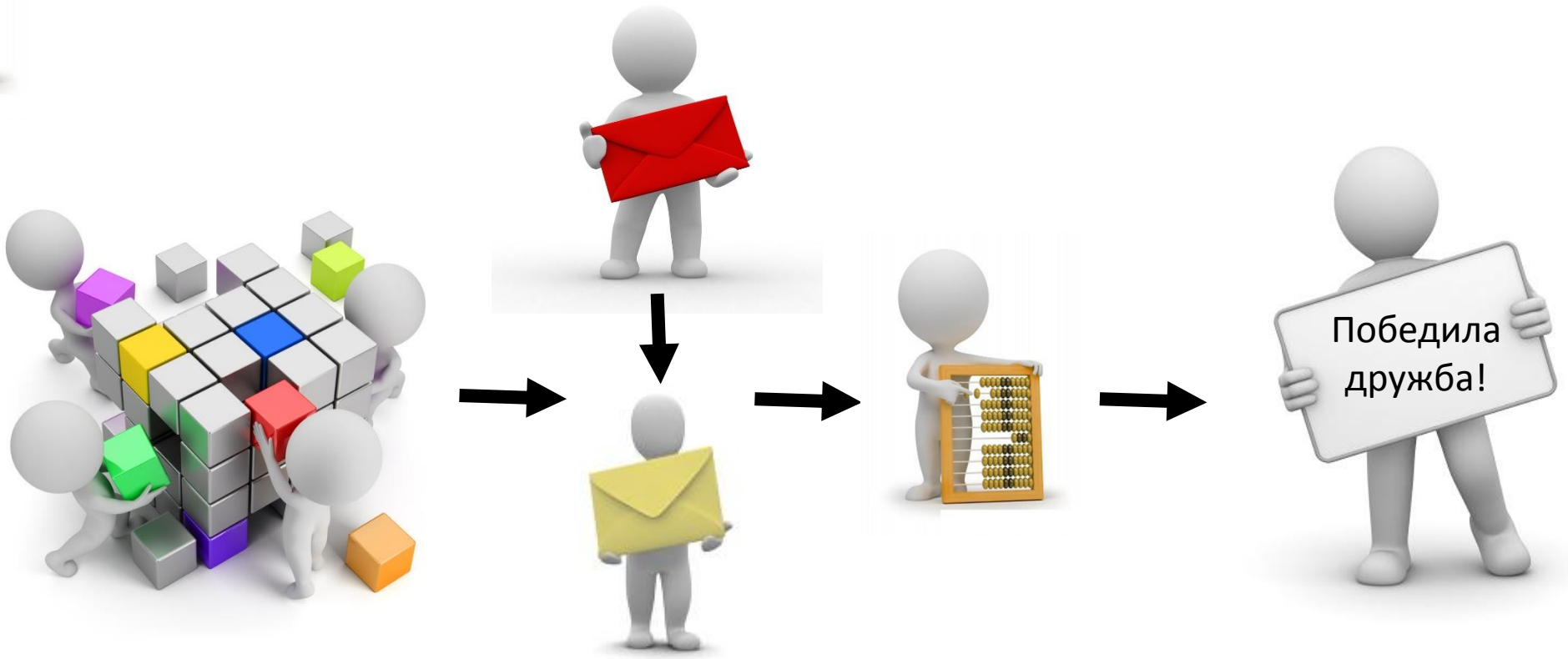
Алгоритм
Этап 7

Избиратель

1. Избиратель ждет, пока каждый участник передаст ему два кусочка своего голоса (подписанного и зашифрованного)
2. Отправляет полученные кусочки голосов счетчику

Алгоритм
Этап 8

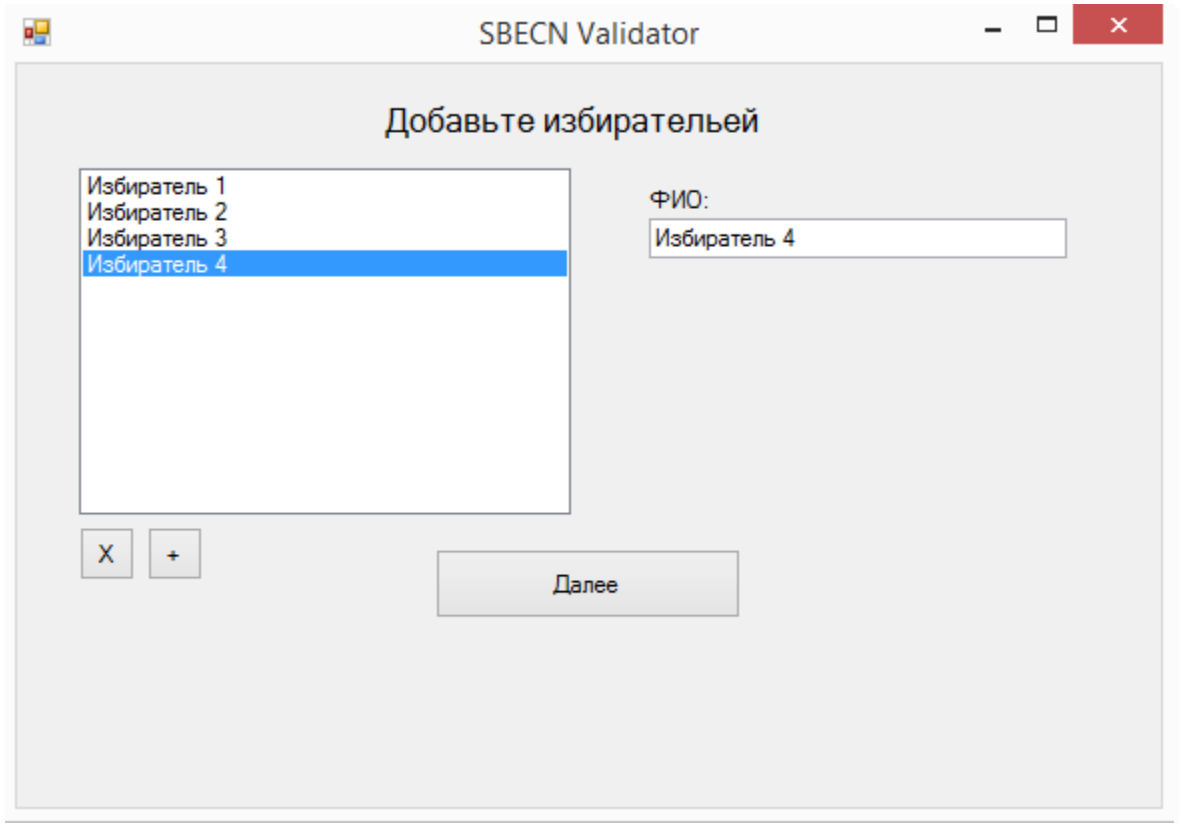
Счетчик

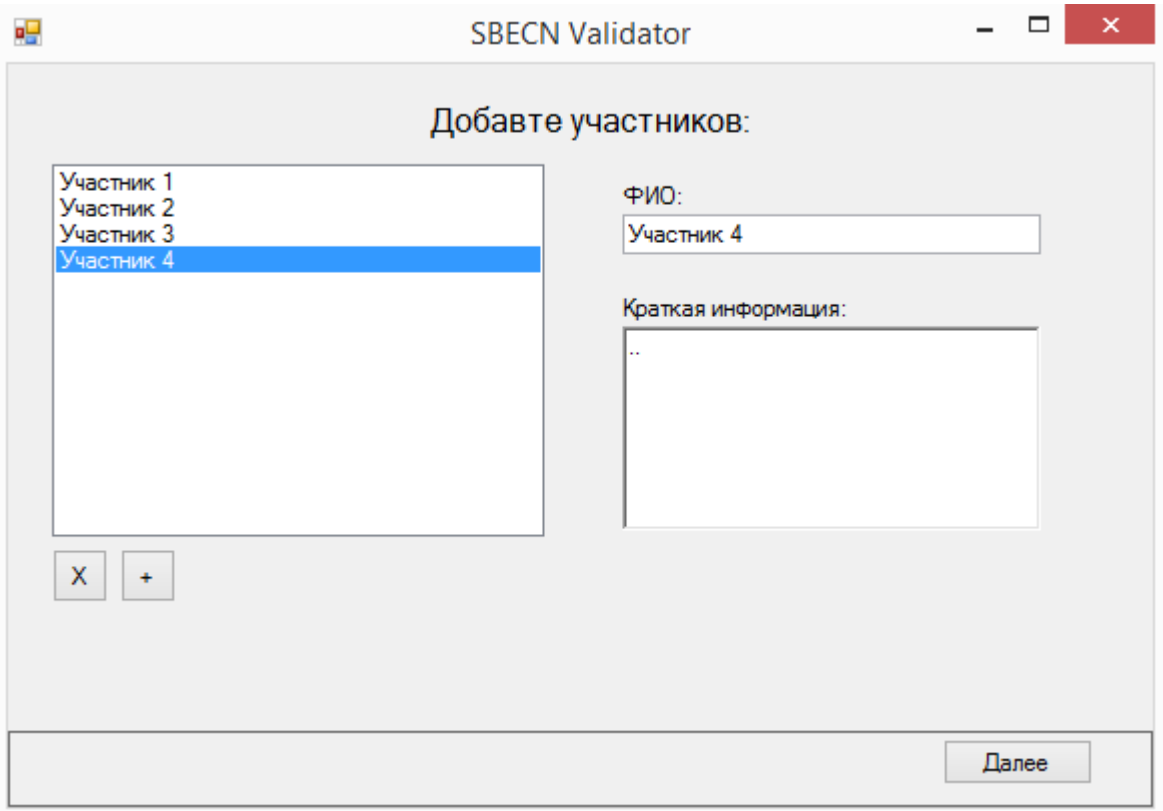


1. Счетчик получает кусочки голосов от избирателей
2. Расшифровывает каждый кусочек голоса + его подпись
3. Подсчитывает голоса (складывает все кусочки)
4. Публикует результат голосования + подписанные кусочки голосов

Критический анализ и пример работы программы

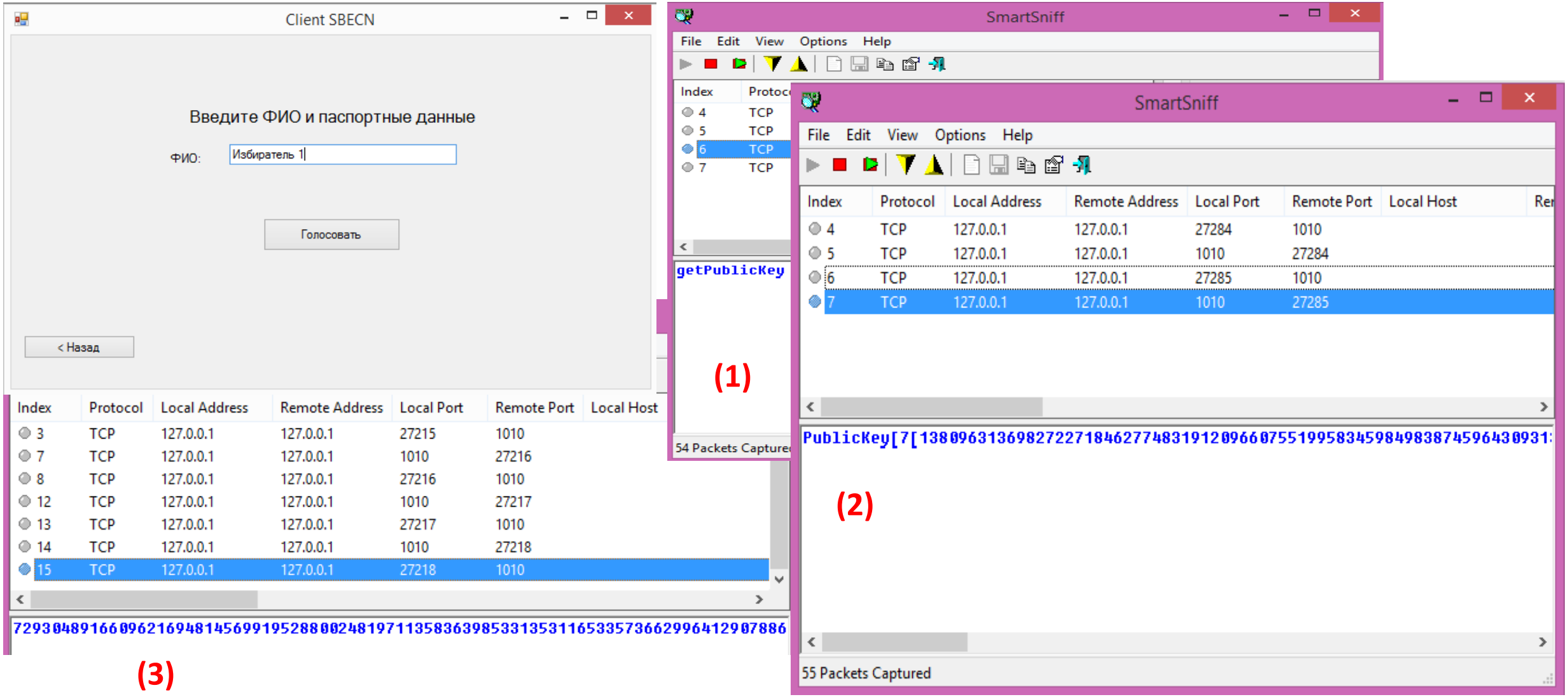
1. Настроим регистратор
2. Добавим 4 избирателя и 4 кандидата для голосования



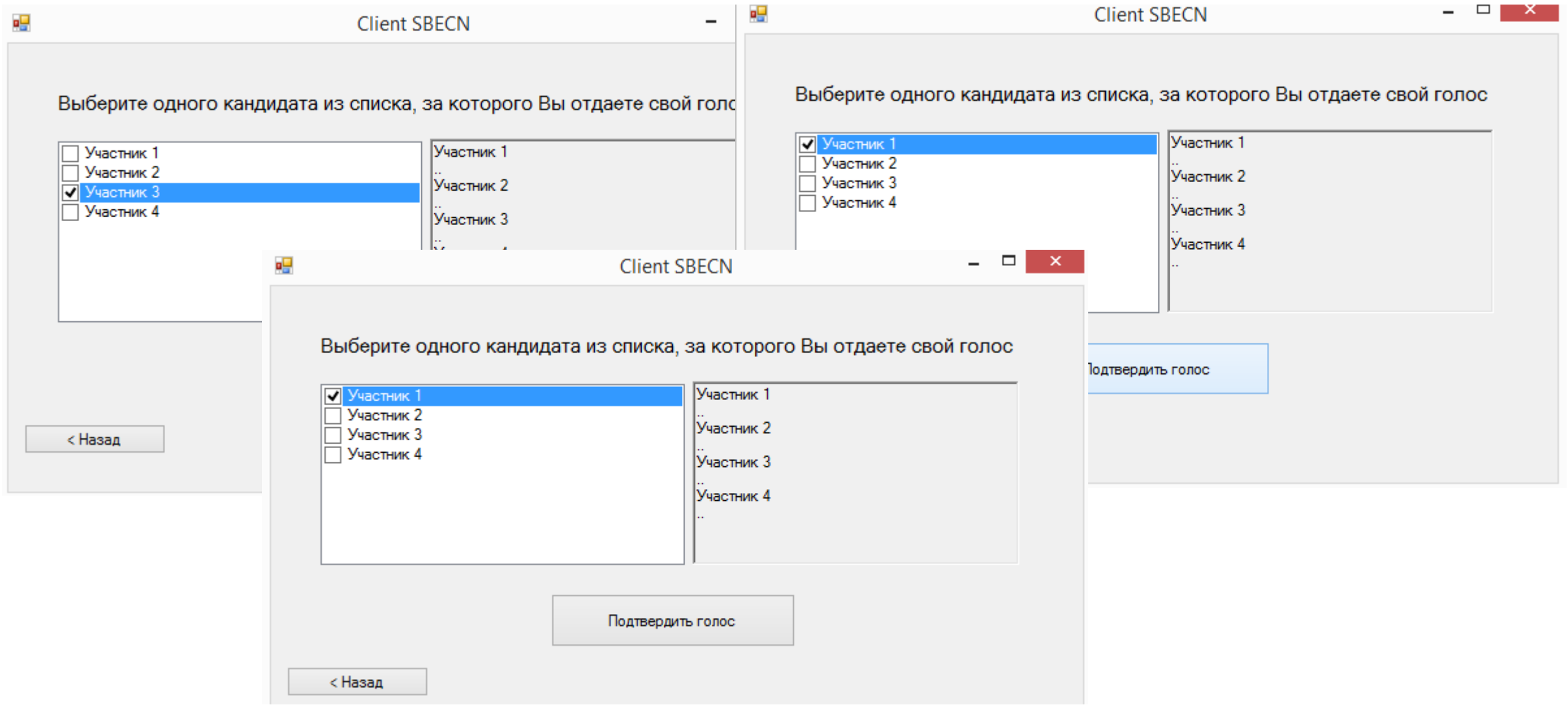


Критический анализ и пример работы программы

Подключаемся каждым клиентом к регистратору



Критический анализ и пример работы программы



Критический анализ и пример работы программы

Ваши пакеты голосов:

&6YRC6PK#%9@Z&YMDJ3W|0|-7|4|-3
&E8H6S$BUBW@C$$FG4ZM|0|3|-2|0

NOYX#E8J8$R217O7*O*9|0|0|4|-1
2$SFP1QR#XK%1024&UW7|1|1|0|2

C$V7GZINM*P%SHP4QJK4|0|0|0|-1
VB7F1@T9GX%8LRN2@19$|0|0|-1|2

CXN%L8TNHD@V&TIBIQFM|-1|0|0|0
FQH6BX1B0596QL2*4@00|0|3|-4|1

(1)

Исходящий пакет №1
192.169.1.71|192.169.1.71
1011
&6YRC6PK#%9@Z&YMDJ3W|0|-7|4|-3

Coded by Egor Antonchikov

Clie

Ваши пакеты голосов:

&3P@HU$0GV17L1SGWBF4|1|3|0|2
T&UEJ@BABXIQ42AAIX#C|0|-3|0|-2

NL&#HSNJ#HL1NT*9YNJC|0|0|-6|1
1ZR$#CC3WLR00S46EYA*|0|-1|1|0

3YDED6BN85@*AFP1357R|0|1|0|0
8@6I4ANM3IYZACPUZRH3|0|-2|4|-1

9V2#@HX@Y65MCVF90%RC|0|2|0|1
S52YFK**7%BLXDZLJ6NW|-1|0|1|0

(2)

Входящий пакет №1
233056437003604683524661454699787142653
207362970586488947839248503170694082290
317945911067565422836225673421324427047

SmartSniff

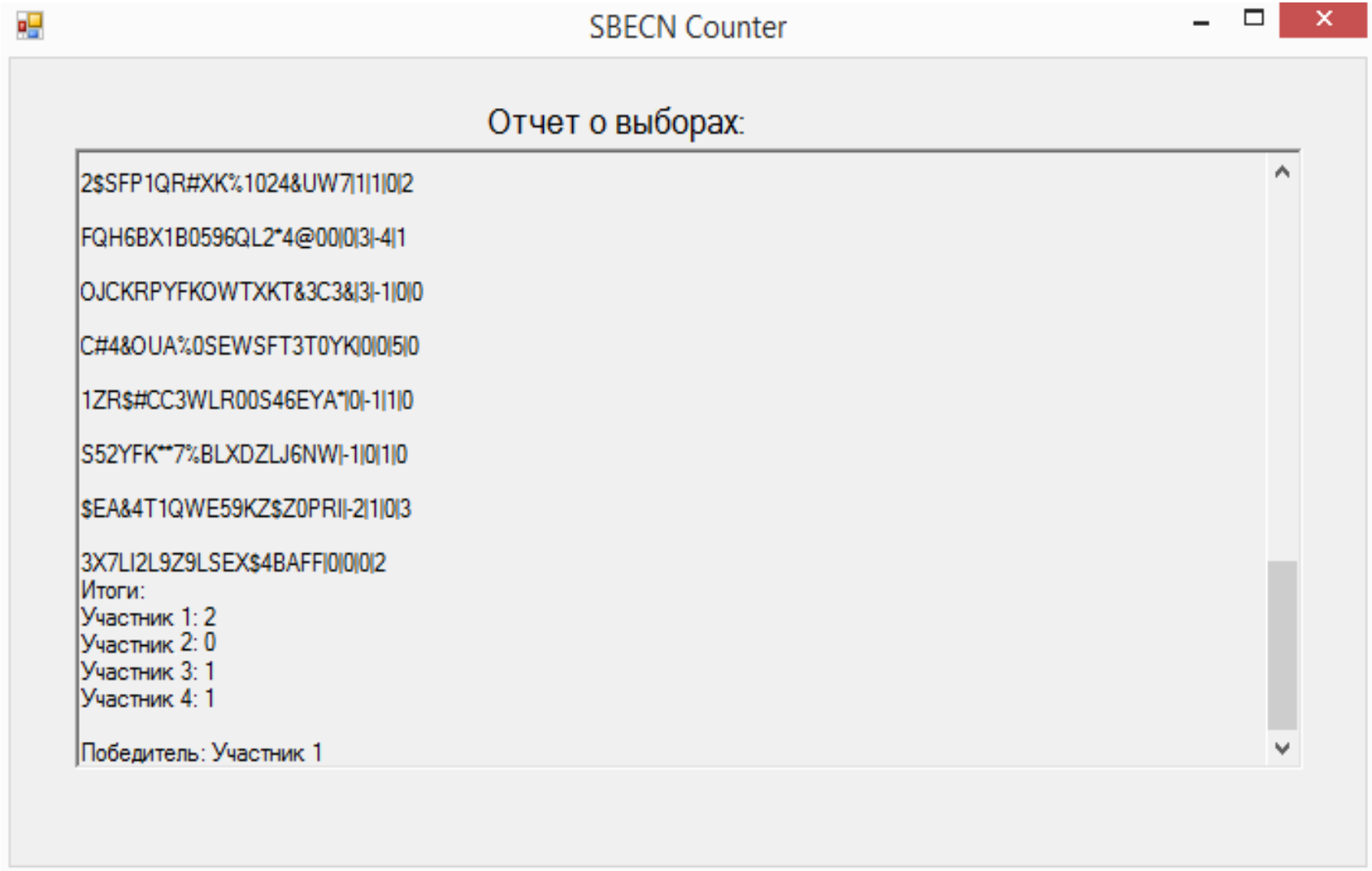
File Edit View Options Help

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host
13	TCP	192.169.1.71	192.169.1.71	28915	1011		
14	TCP	192.169.1.71	192.169.1.71	28916	1011		
15	TCP	192.169.1.71	192.169.1.71	28917	1012		
16	TCP	192.169.1.71	192.169.1.71	28918	1012		
17	TCP	192.169.1.71	192.169.1.71	28919	1011		
18	TCP	192.169.1.71	192.169.1.71	28920	1012		
19	TCP	192.169.1.71	192.169.1.71	28921	1011		
20	TCP	192.169.1.71	192.169.1.71	28922	1012		
21	TCP	192.169.1.71	192.169.1.71	28923	1011		
22	TCP	192.169.1.71	192.169.1.71	28924	1012		
23	TCP	192.169.1.71	192.169.1.71	28925	1013		

258825397395451548140210654752671708543665069749118698429113161729088931467091719662 88

24 TCP/IP conversations, 1 Selected

Критический анализ и пример работы программы



Вывод

Спасибо за внимание!

Автор:

Антончиков Егор
youtoolife@gmail.com