

Фидбек по таскам олимпиады 2011

Подготовил Евелев Ю.Е.

evelev@hacker.ru

[Vk.com/yuevelev](https://vk.com/yuevelev)

Задание «Шифр»

В школе по пятницам на двух последних уроках химии мы любили бездельничать, потому что уже устали за неделю, хотели отдохнуть. И чтобы не скучать, мы придумывали различные шифры. Вот один из них. Используя этот шифр, можно было быстро составить и расшифровать сообщение

Что здесь зашифровано?

=====

207^2 14^2 40^3 10^2 95^1 72^5 126^1

112^4 186^2 65^3 74^5

262^4 132^2 55^1 44^4 1^2

цифры со знаком ^ записываются как степень

=====

Формат ответа:

Задание Face

Вчера на нашем объекте было предотвращено вторжение. Грабителей поймать не удалось, но один из них был похож на очень известного парня, кстати вот его фото :

Кто бы мог подумать что такой знаменитый человек может опуститься до воровства? или это был очень похожий на него человек?

Выясните, пожалуйста, имя и фамилию этого человека.



Задание СПАМ

Такое странное спам-сообщение пришло по нашему секретному каналу связи:

Dear E-Commerce professional ; This letter was specially selected to be sent to you . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 1916 , Title 2 ; Section 302 . This is not multi-level marketing ! Why work for somebody else when you can become rich in 76 months . Have you ever noticed nearly every commercial on television has a .com on in it plus nearly every commercial on television has a .com on in it ! Well, now is your chance to capitalize on this . WE will help YOU deliver goods right to the customer's doorstep and decrease perceived waiting time by 200% . You can begin at absolutely no cost to you ! But don't believe us ! Prof Ames of Florida tried us and says "Now I'm rich many more things are possible" ! This offer is 100% legal ! We BESEECH you - act now ! Sign up a friend and you'll get a discount of 50% . Thanks .

Задание Apple

Наш респондент Александр Мясников прислал нам вот этот файл:

<http://cs-new.engesc.ru/apple.bmp>

Пожалуйста, поразбирайтесь в нем. Возможно, там есть некий скрытый смысл.

От него же пришла еще одна короткая заметка, смысл который нам пока не до конца ясен: "пароль-год создания apple II".

Нам не понятно, что за пароль и куда его вводить.

Надеюсь, вы разберетесь. Успехов!

Олимпиада InfoSec

II

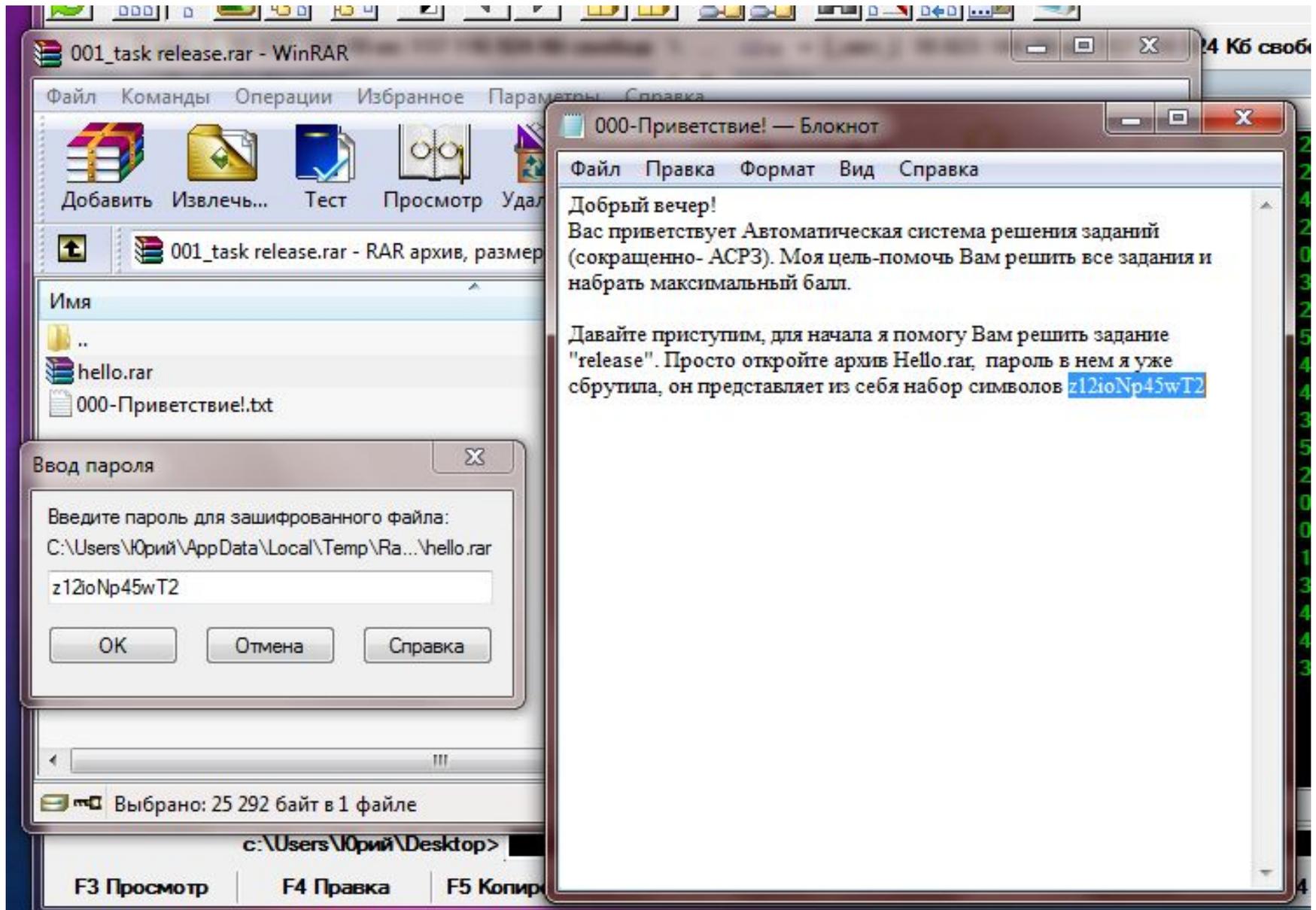
ФИДБЕК

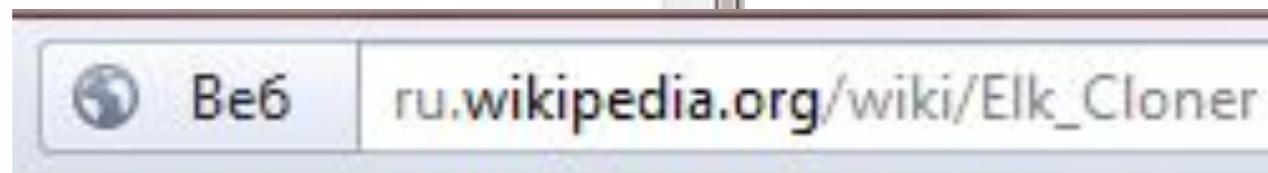
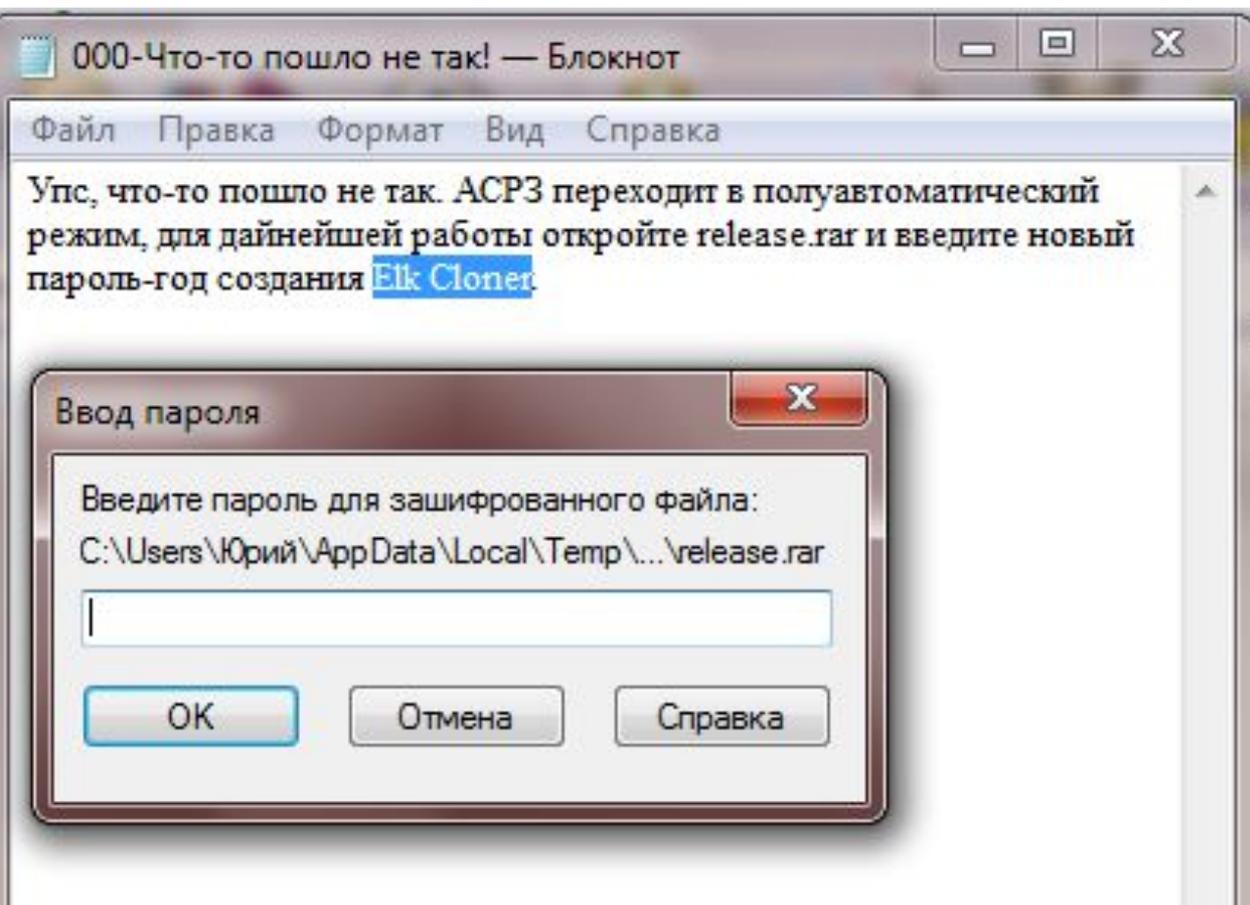
Как решать

таски.

18 ноября 2011 г. Инжэкон

001_task release





вых компьютерных вирусов, распространившийся
ил написан в 1981 году 15-летним школьником Рич

C:\Users\D36B~1\AppData\Local\Temp\Rar\$EX01.477\001.exe

Everyone knows information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Enter the number of requirement from this standard that prescribe you store cryptographic keys securely in the fewest possible locations and forms.

Payment Card Industry (PCI) Data Security Standard

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.

3.6 Fully document and implement all key-management processes and

3.
u:

3.5.2
Great! First part of key=9p07

Kakoi nomer standarta iz kompleksa Banka Rossii po IB sootvetstvet standartu 'Metodika ocenki riskov narusheniya informacionnoi bezopasnosti'? Format otveta ...

Яндекс

Нашлось
119 тыс. ответов

сто бр иббс

в найденном в Санкт-Петербурге

W [СТО БР ИББС — Википедия](#)

Стандарт Банка России по обеспечению безопасности банковской системы Российской Федерации...

[ru.wikipedia.org > wiki/СТО_БР_ИББС](http://ru.wikipedia.org/wiki/СТО_БР_ИББС)

- РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности;
- РС БР ИББС-2.3-2010. Требования по обеспечению безопасности персональных данных в...

2.2-2009

Well done! Second part of key = Iw6z

C:\Users\D36B~1\AppData\Local\Temp\Rar\$EX53.103\003.exe

What is better known name for DoDD 5200.28-STD? Format otveta *****_**** .
orange_book
it was rather difficult, but you did it! Third part of key is Ym3u
-

C:\Users\D36B~1\AppData\Local\Temp\Rar\$EX61.791\004.exe

What's number of ISO/IEC standart, called 'Information technology-Security techniques-Code of practice for information security management'?

27002

Great! You finished! Final part of key is 90Ut

Альтернативный путь

011E10C0	> 8A10	MOV DL, BYTE PTR DS:[EAX]	
011E10C2	> 3A11	CMP DL, BYTE PTR DS:[ECX]	
011E10C4	> 75 1A	JNE SHORT 011E10E0	
011E10C6	> 94D2	TEST DL, DL	
011E10C8	> 74 12	JE SHORT 011E10DC	
011E10CA	> 8A50 01	MOV DL, BYTE PTR DS:[EAX+1]	
011E10CC	> 3A51 01	CMP DL, BYTE PTR DS:[ECX+1]	
011E10DE	> 75 0E	JNE SHORT 011E10E0	
011E10E0	> 83C0 02	ADD EAX, 2	
011E10E2	> 83C1 02	ADD ECX, 2	
011E10E4	> 84D2	TEST DL, DL	
011E10E6	> 75 E4	JNE SHORT 011E10C0	
011E10E8	> 33C0	XOR EAX, EAX	
011E10EA	> EB 05	JMP SHORT 011E10E5	
011E10EC	> 1BC8	SBB EAX, EAX	Calculates sign(EAX)
011E10EE	> 83D8 FF	SBB EAX, -1	
011E10F0	> 85C0	TEST EAX, EAX	
011E10F2	> 74 00	JE SHORT 011E10F6	
011E10F4	> A1 88301E01	MOV EAX, DWORD PTR DS:[<&MSUCP100.?count	
011E10F6	> 68 84321E01	PUSH OFFSET 011E32B4	ASCII "you failed. Try again"
011E10F8	> 50	PUSH EAX	
011E10FA	> EB 0C	JMP SHORT 011E1102	
011E10FC	> 68 88301E01	MOV ECX, DWORD PTR DS:[<&MSUCP100.?count	ASCII "Great! First part of key=9p07"
011E10FE	> 68 CC321E01	PUSH OFFSET 011E32CC	
011E1100	> 51	PUSH ECX	
011E1102	> E8 99010000	CALL std:operator<<<std:char_traits<<std:operator<<<std:char_traits<char>>>_Dstr	
011E1104	> 50	PUSH EAX	
011E1106	> E8 E3030000	CALL std:operator<<<std:char_traits<<std:operator<<<std:char_traits<char>>>	
011E1108	> 83C4 0C	ADD ESP, 0C	
011E110A	> 4E	DEC ESI	
011E110C	> 75 8D	JNE SHORT 011E10A0	
011E110E	> 8B8C24 AC00	MOV ECX, DWORD PTR SS:[LOCAL.1]	
011E1110	> 5E	POP ESI	
011E1112	> 33CC	XOR ECX, ESP	
011E1114	> 33C0	XOR EAX, EAX	
011E1116	> E8 10080000	CALL security_check_cookie	c_security_check_cookie
011E1118	> 8BE5	MOV ESP, EBP	
011E111A	> 5D	POP EBP	
011E111C	> C3	RETN	

Registers (FPU)

EAX	7697E05A	kernel32.BaseThreadInitThunk
ECX	00000000	
EDX	011E1C30	001.<ModuleEntryPoint>
EBX	7FFD6000	
ESP	0016F970	
EBP	0016F978	
ESI	00000000	
EDI	00000000	
EIP	011E1C30	001.<ModuleEntryPoint>
C 0	ES 0023 32bit	0(FFFFFFFF)
P 1	CS 001B 32bit	0(FFFFFFFF)
A 0	SS 0023 32bit	0(FFFFFFFF)
Z 1	DS 0023 32bit	0(FFFFFFFF)
S 0	FS 003B 32bit	7FFD000(4000)
T 0	GS 0000	NULL
D 0		
O 0	LastErr	00000000 ERROR_SUCCESS
EFL	00000246	(NO, NB, E, BE, NS, PE, GE, LE)
ST0	empty	0.0
ST1	empty	0.0
ST2	empty	0.0
ST3	empty	0.0
ST4	empty	0.0
ST5	empty	0.0
ST6	empty	0.0
ST7	empty	0.0
FST	0000	Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FSM	002E	Err NERR_F3

ASCII "you failed. Try again"

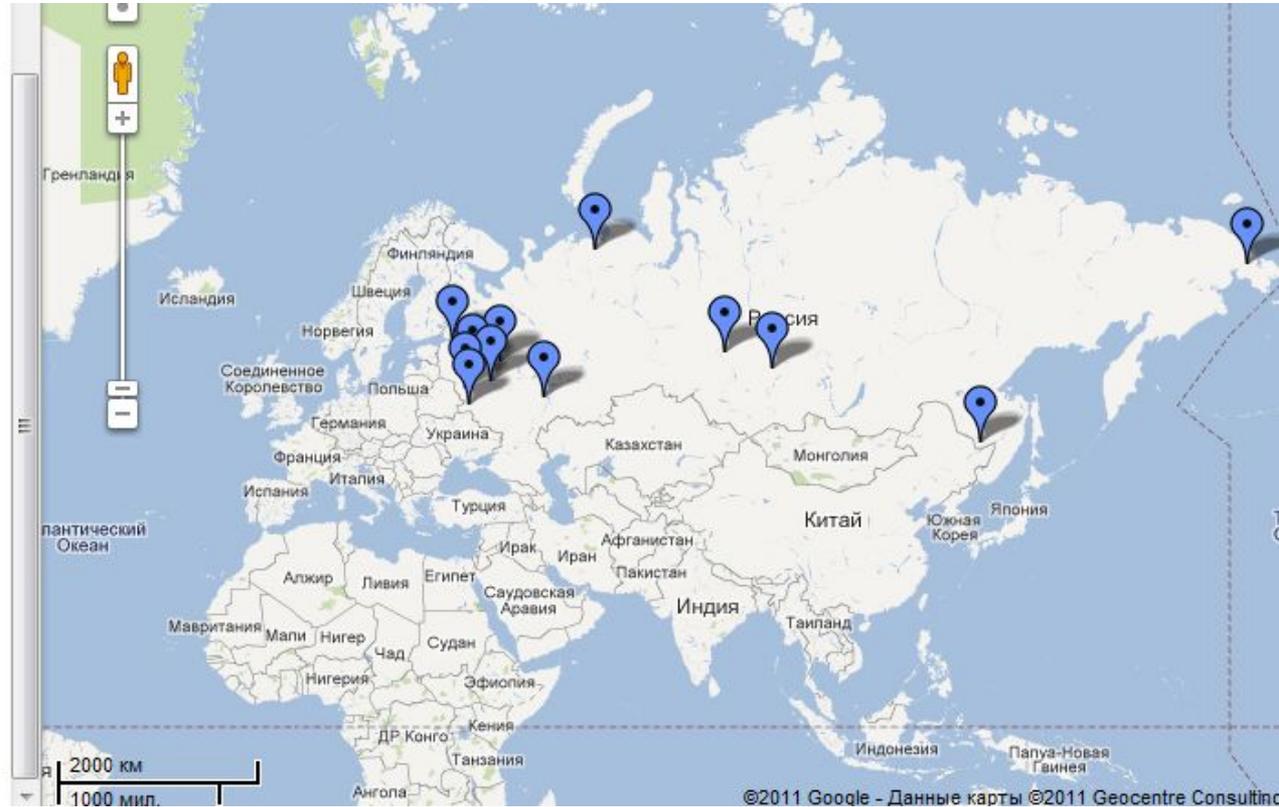
ASCII "Great! First part of key=9p07"

Address	Hex dump	ASCII
011E5000	60 31 1E 01 00 00 00 00 2E 3F 41 56 74 79 70 65	'1A0 .?AUtype
011E5010	5F 69 6E 66 6F 40 40 00 4E E6 40 8B B1 19 5F 44	_info@@ Nu的器4D
011E5020	FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00	
011E5030	FE FF FF FF 01 00 00 00 60 31 1E 01 00 00 00 00	= 0 '1A0
011E5040	2E 3F 41 56 65 70 63 65 70 74 69 6F 6E 40 73 74	.?AUexception@st
011E5050	64 40 40 00 60 31 1E 01 00 00 00 00 2E 3F 41 56	d@ '1A0 .?AU
011E5060	62 61 64 5F 63 61 73 74 40 73 74 64 40 40 00 00	bad_cast@std@
011E5070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E50A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E50B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E50C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E50D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E50E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E50F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E5190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E51A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
011E51B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

0016F984	772A37CE	RETURN from ntdll.772A37CE to ntdll.772A37CE
0016F988	00000000	
0016F98C	00000000	
0016F990	7FFD6000	'h0
0016F994	00000000	
0016F998	00000000	
0016F99C	00000000	
0016F9A0	0016F984	D.-
0016F9A4	00000000	
0016F9A8	FFFFFFFF	
0016F9AC	7725E0ED	sdw SE handler
0016F9B0	02A041FC	NRH0
0016F9B4	00000000	
0016F9B8	0016F900	.-
0016F9BC	772A37C8	h7w
0016F9C0	011E1C30	001.<ModuleEntryPoint>
0016F9C4	7FFD6000	'h0
0016F9C8	00000000	
0016F9CC	00000000	
0016F9D0	00000000	
0016F9D4	00000000	
0016F9D8	011E1C30	001.<ModuleEntryPoint>
0016F9DC	7FFD6000	'h0
0016F9E0	00000000	
0016F9E4	00000000	

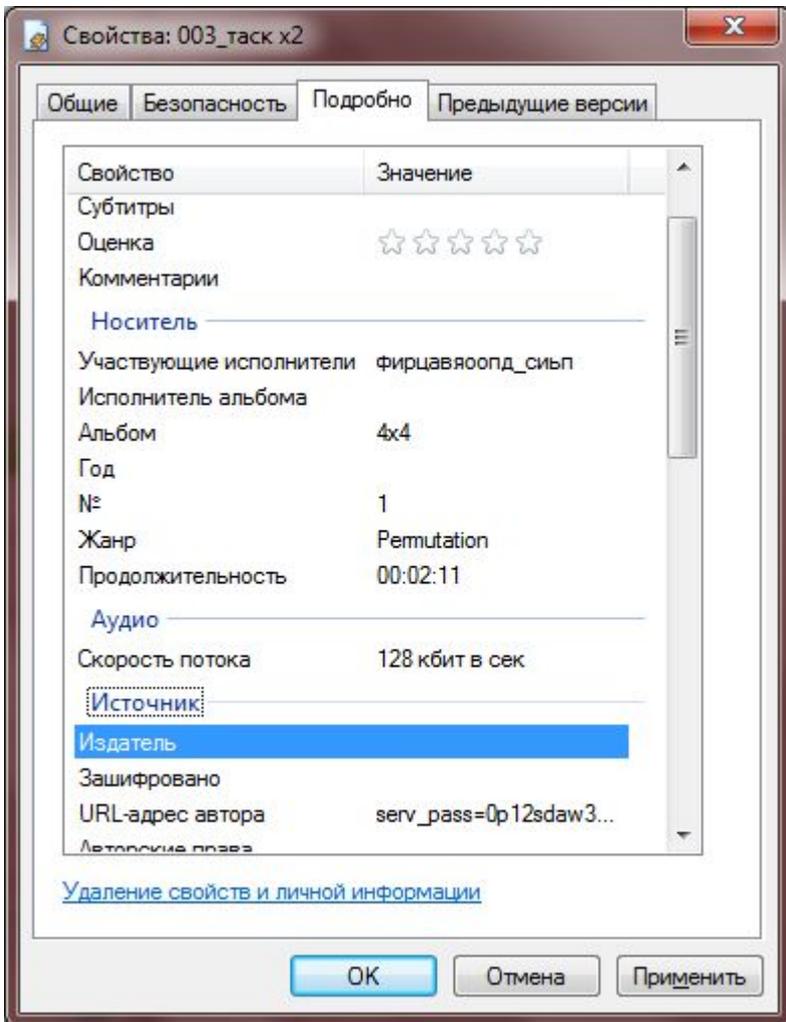
002_map

- Ярославская область
3
- Смоленская область
4, 18
- Санкт-Петербург
13
- Чукотский автономный округ
1
- Еврейская автономная область
5, 10, 15
- Брянская область
8, 11
- Ульяновская область
12
- Москва
6
- Тверская область
2, 7, 17
- Красноярский край
9
- Ненецкий автономный округ
16
- Томская область
14



1	Регион	Код региона	ASCII-коды
2	Чукотский АО		87 W
3	Тверская область		69 E
4	Ярославская область		76 L
5	Смоленская область		67 C
6	Еврейский АО		79 O
7	Москва	77, 97, 99, 177, 197, 199	M
8	Тверская область		69 E
9	Брянская область		32 (пробел)
10	Краснодарский край	24, 84, 88, 124	T
11	Еврейский АО		79 O
12	Брянская область		32 (пробел)
13	Ульяновская область		73,173 I
14	Санкт-Петербург	78, 98, 178	N
15	Томская область		70 F
16	Еврейский АО		79 O
17	Ненецкий АО		83 S
18	Тверская область		69 E
19	Смоленская область		67 C

003_task x2



Участвующие исполнители фирцавяоопд_сийп
Исполнитель альбома
Альбом 4x4
Год
№ 1
Жанр Permutation
Продолжительность 00:02:11

Источник
Издатель
Зашифровано
URL-адрес автора serv_pass=0p12sdaw32vb
Авторские права

Участвующие исполнители фирцавяоопд_сийп
Исполнитель альбома
Альбом 4x4
Год
№ 1
Жанр Permutation
Продолжительность 00:02:11

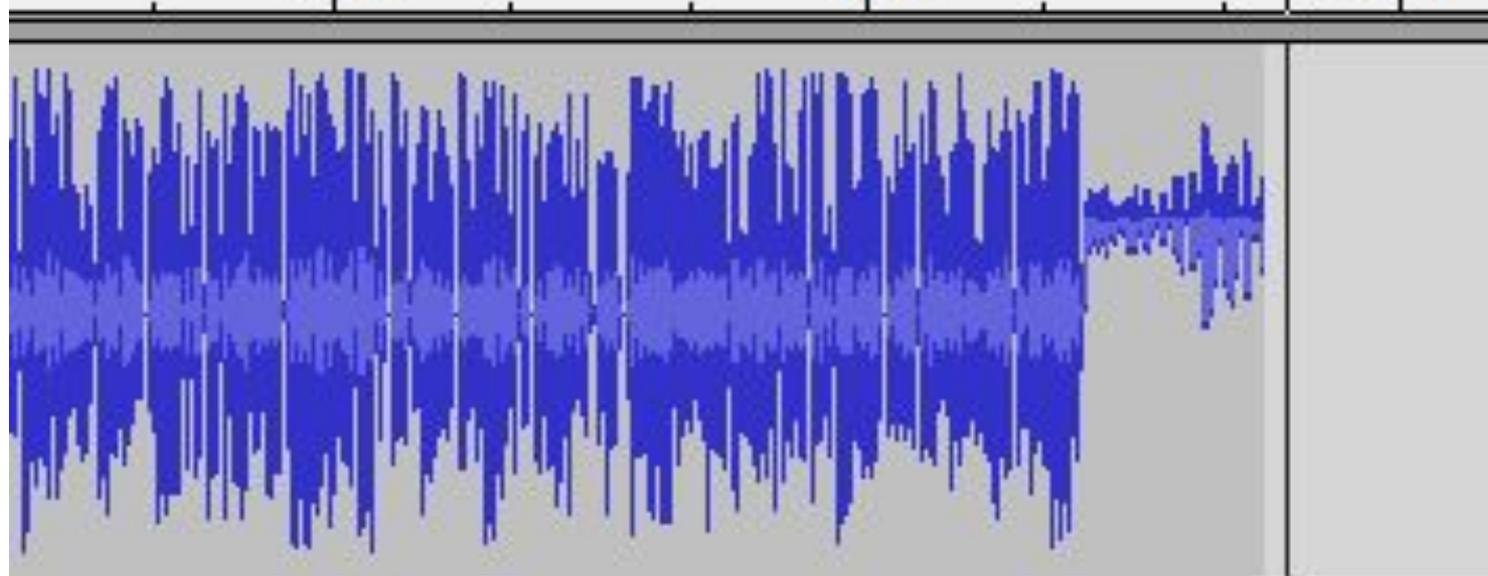
	1	2	3	4	
1	ф	и	р	ц	
2	а	в	я	о	
3	о	п	д	_	
4	с	и	ь	п	

	4	2	1	3	
1	ц	и	ф	р	
2	о	в	а	я	
3	_	п	о	д	
4	п	и	с	ь	

1:45

2:00

2:15



Доп.

