ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

Динамический анализ кода

Распаковка, procmon, fiddler/wireshark,api monitor

Пакулов Артур

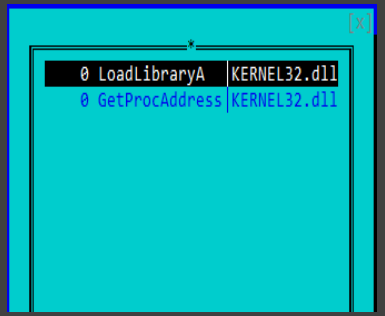
1

Распаковка

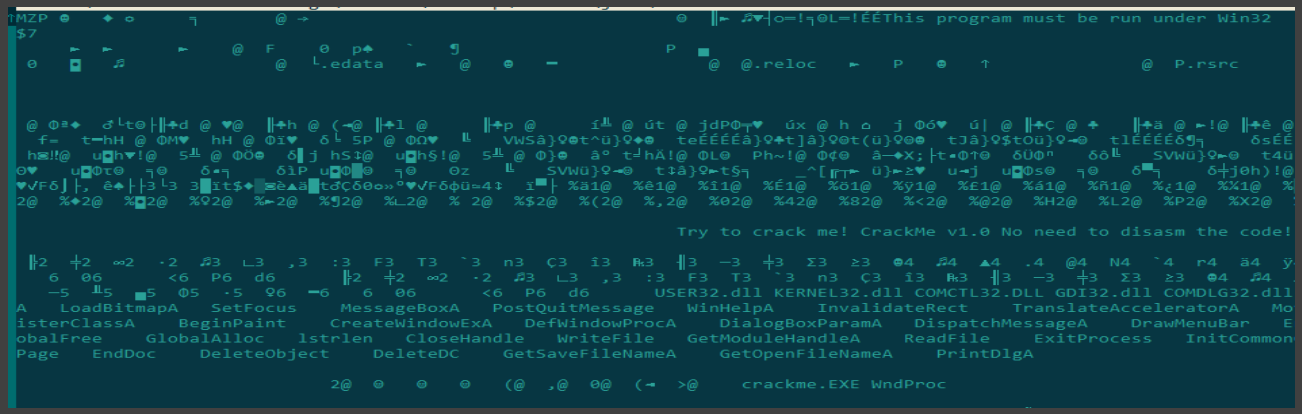
Признаки упакованного PE файла

- ✓ Очень мало строк
- ✓ Очень мало функций в таблице импорта (*)
- ✓ Высокая энтропия (> 6) ➔ мало «пустых» мест в файле

```
KERNEL32.dll▪
DLG_ABOUT
DLG_REGIS▪
3333330▪
WndProc▪
crackme.EXE▪
v18.03N4n
"Gisa&m
@ wSrk{H
pP!llhu
USER32.dql
WindowR
BitvmPp
y0[O'l?
E"%xft!
4gMpApbpoTu6
@K@u@A@
LoadLibraryA▪
GetProcAddress▪
```

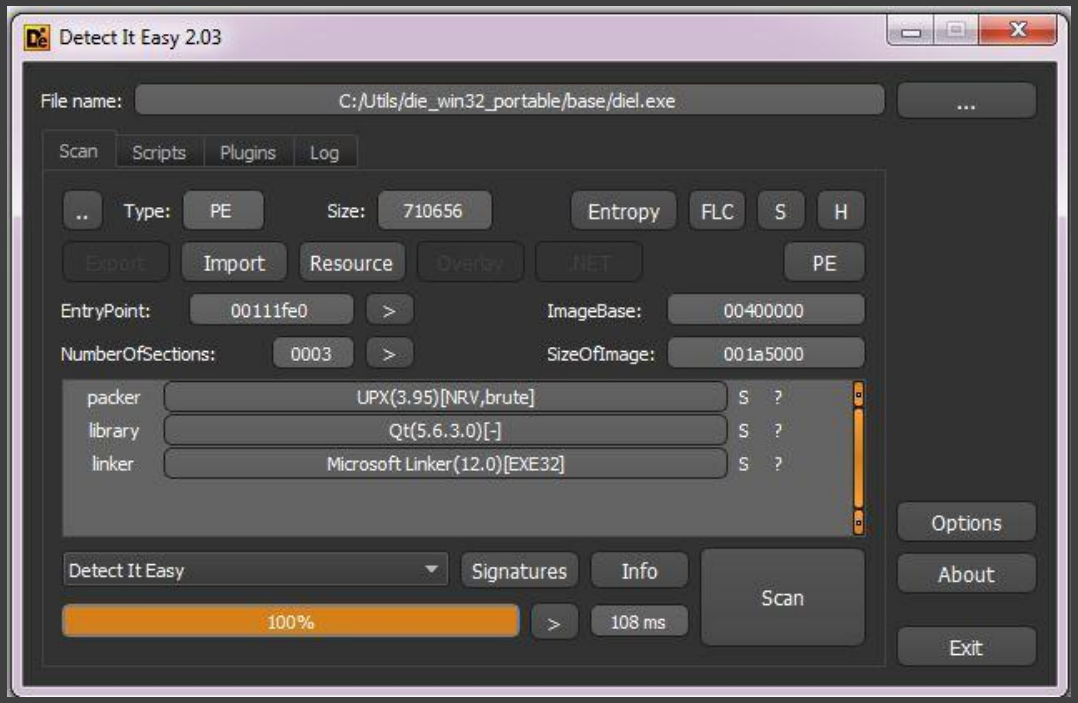


Обычный и упакованный PE файлы



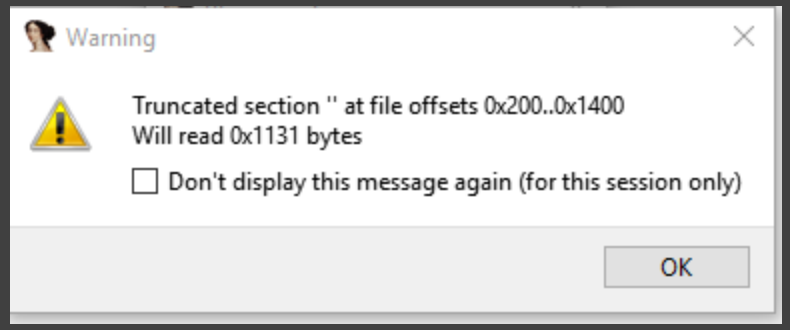
Detect it Easy (DIE)

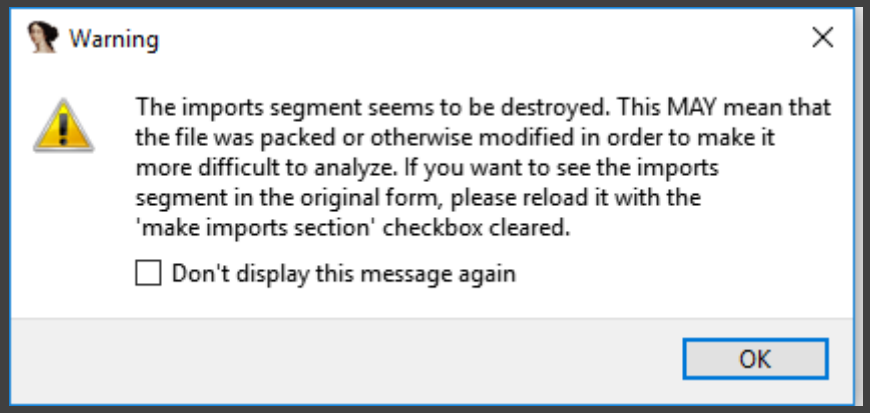
Анализатор упаковщиков



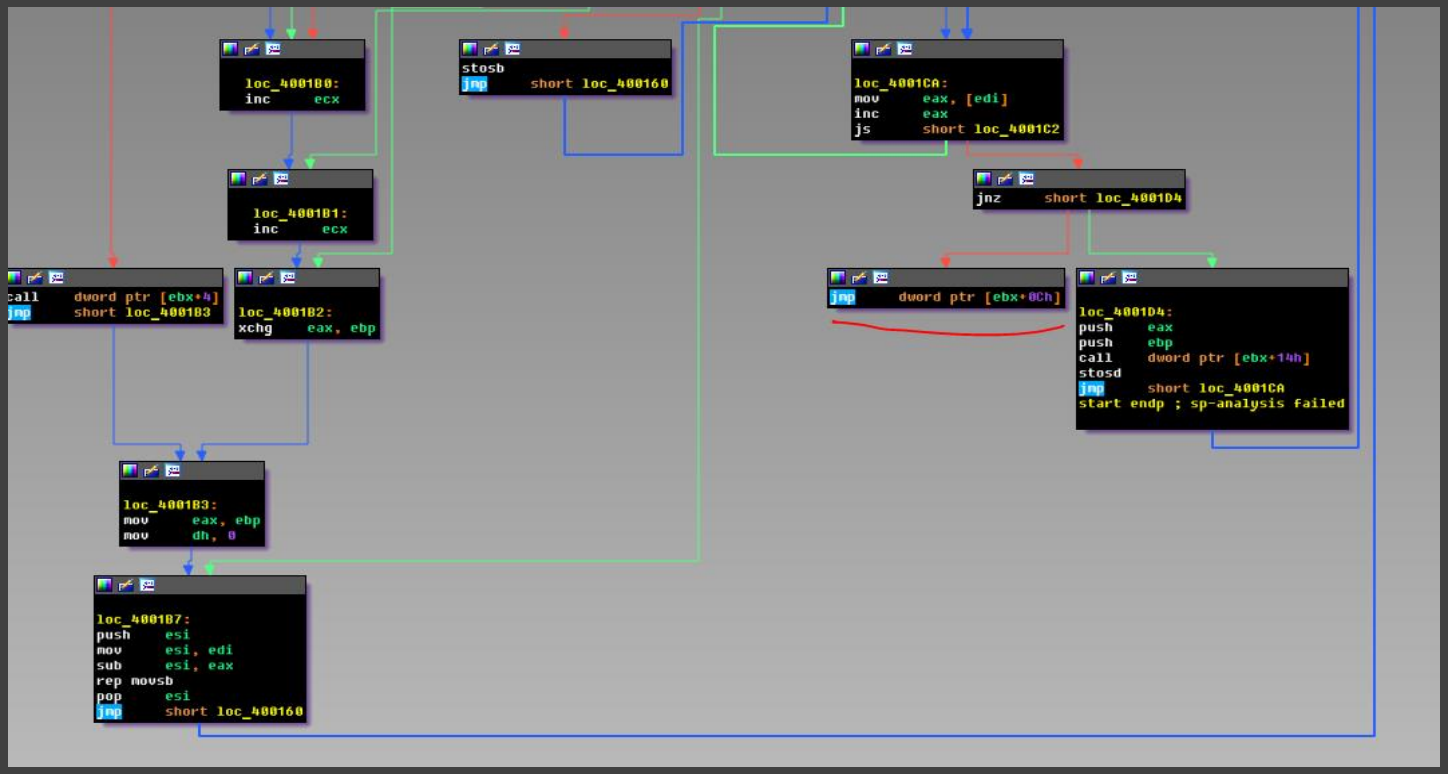
http://ntinfo.biz/index.html

Отладка запакованного PE файла

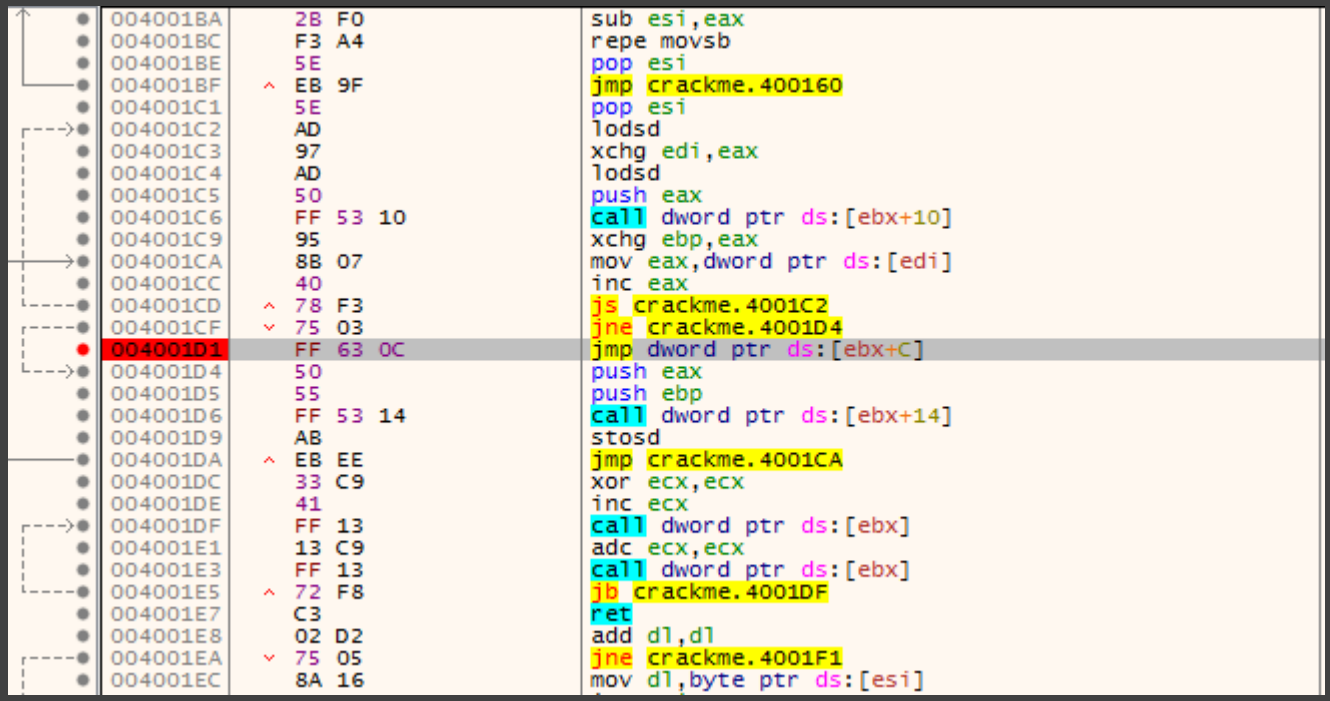




Устанавливаем breakpoint в «конец»



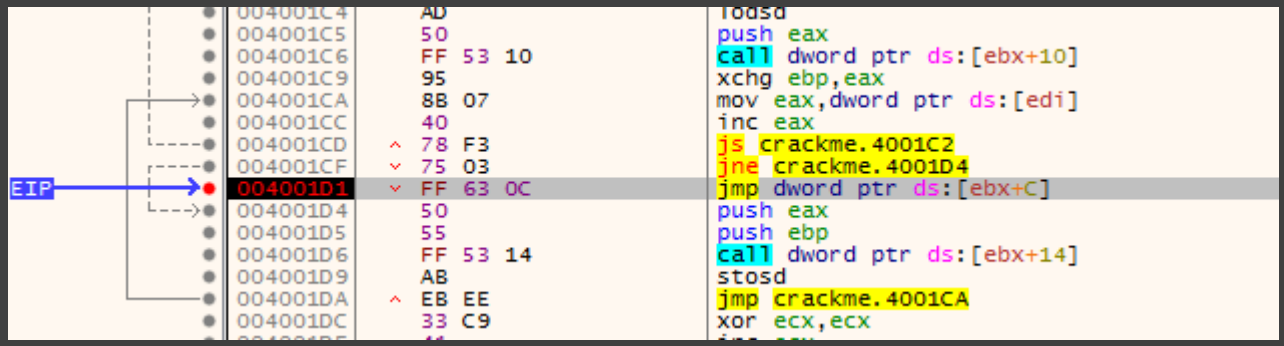
Устанавливаем breakpoint в «конец»

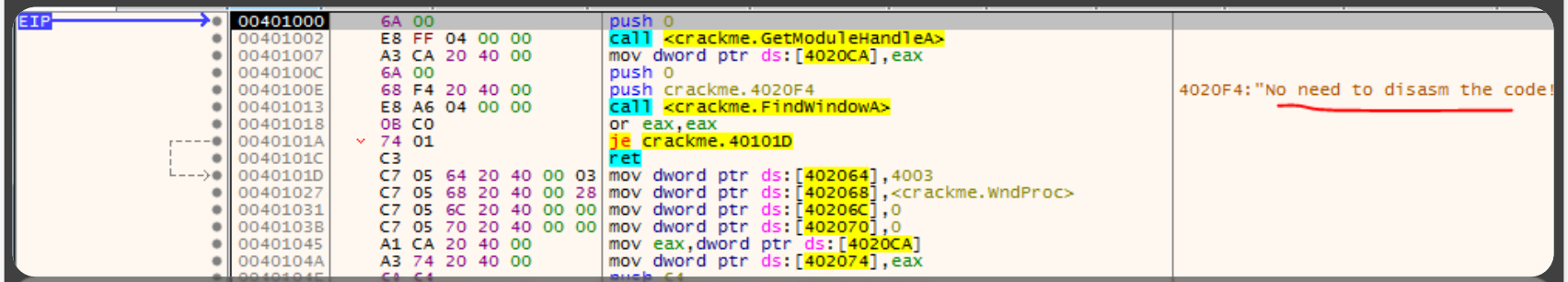


```
004001BA   2B F0          sub esi,eax
004001BC   F3 A4          repe movsb
004001BE   5E             pop esi
004001BF   EB 9F          jmp crackme.400160
004001C1   5E             pop esi
004001C2   AD             lodsd
004001C3   97             xchg edi,eax
004001C4   AD             lodsd
004001C5   50             push eax
004001C6   FF 53 10       call dword ptr ds:[ebx+10]
004001C9   95             xchg ebp,eax
004001CA   8B 07          mov eax,dword ptr ds:[edi]
004001CC   40             inc eax
004001CD   78 F3          js crackme.4001C2
004001CF   75 03          jne crackme.4001D4
004001D1   FF 63 0C       jmp dword ptr ds:[ebx+C]
004001D4   50             push eax
004001D5   55             push ebp
004001D6   FF 53 14       call dword ptr ds:[ebx+14]
004001D9   AB             stosd
004001DA   EB EE          jmp crackme.4001CA
004001DC   33 C9          xor ecx,ecx
004001DE   41             inc ecx
004001DF   FF 13          call dword ptr ds:[ebx]
004001E1   13 C9          adc ecx,ecx
004001E3   FF 13          call dword ptr ds:[ebx]
004001E5   72 F8          jb crackme.4001DF
004001E7   C3             ret
004001E8   02 D2          add dl,dl
004001EA   75 05          jne crackme.4001F1
004001EC   8A 16          mov dl,byte ptr ds:[esi]
```

Находим original entry point (OEP)

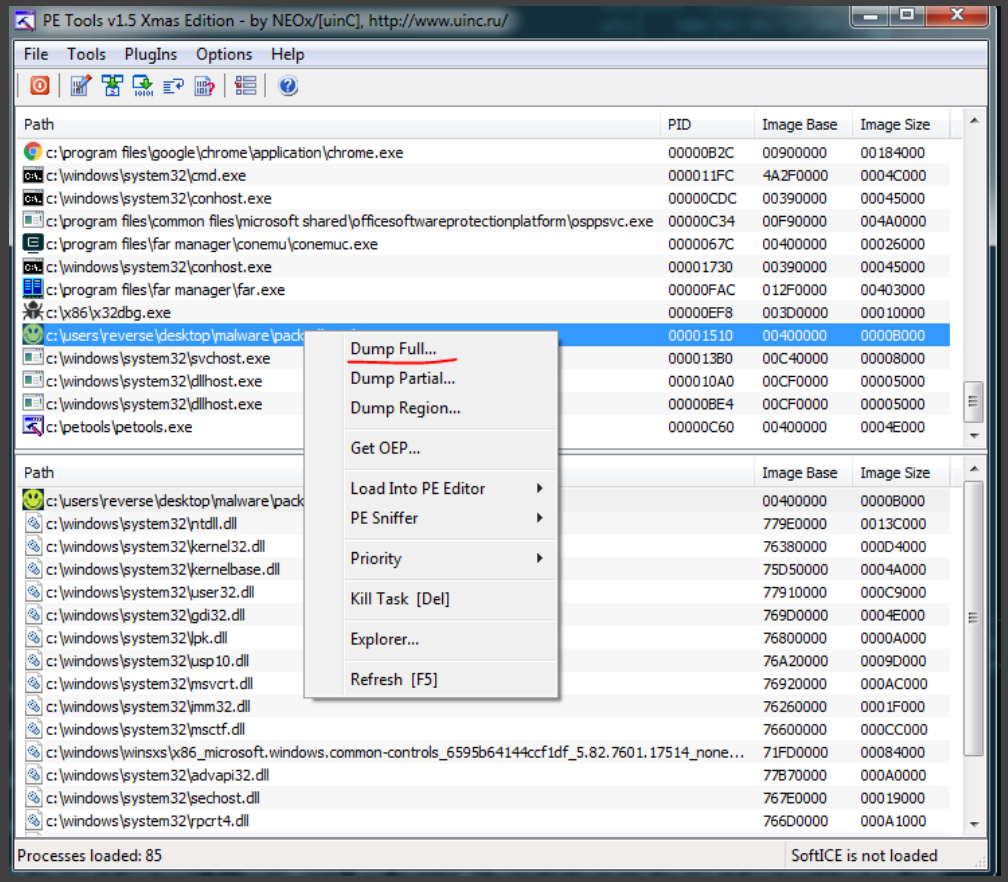
Замечаем вызовы API функций, строки...





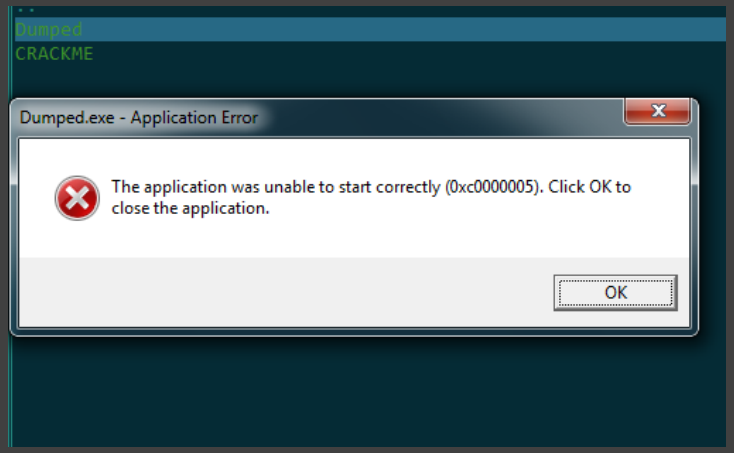
Дампим файл [PE Tools]

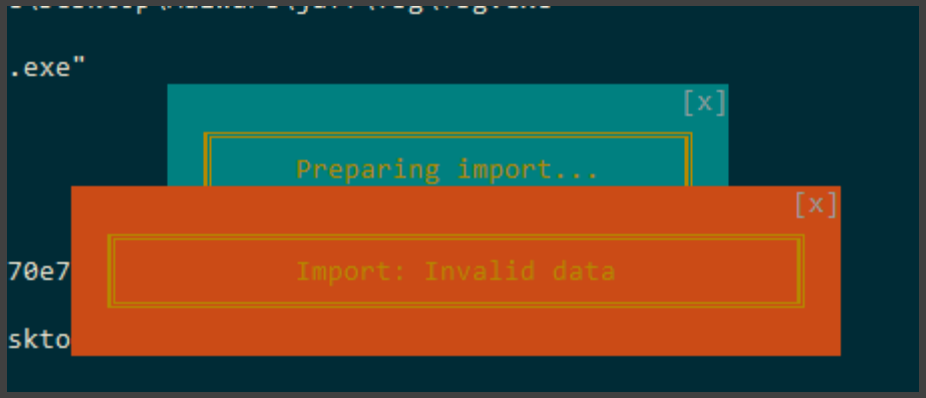
1. Находим наш процесс в списке
2. ПКМ ➔ Dump Fill…



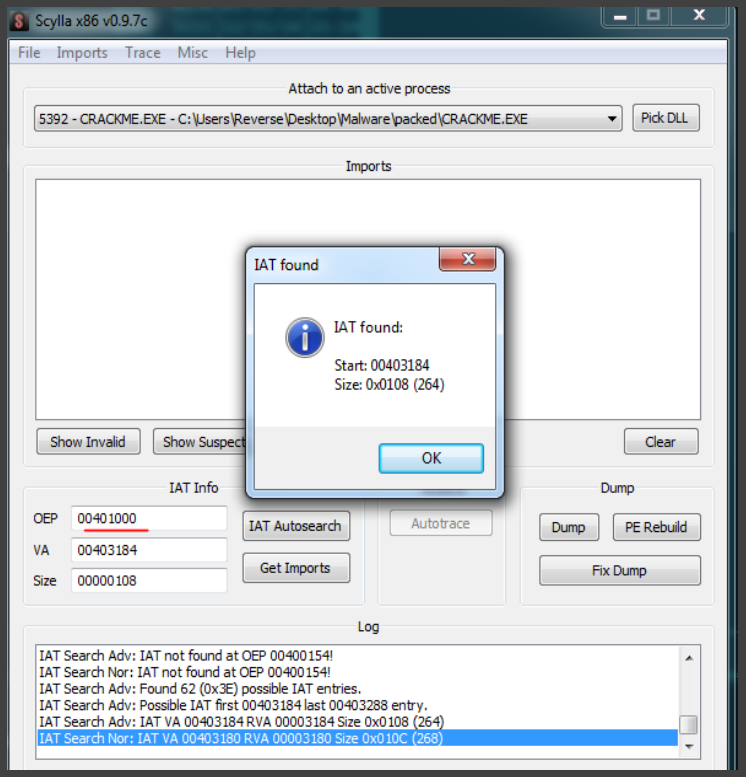
Восстановление таблицы импорта

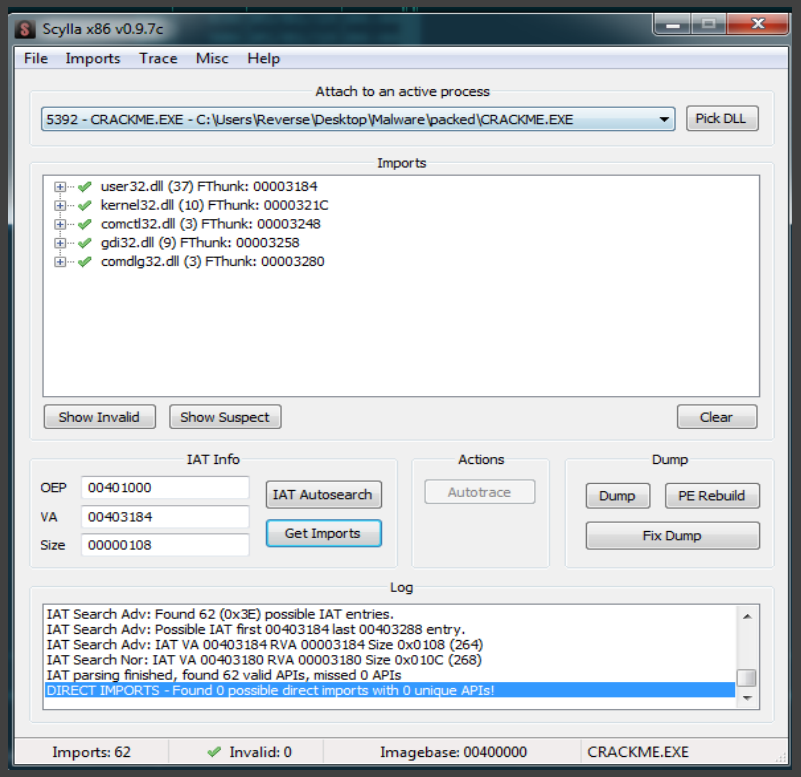
Сдампленный PE файл не отработает





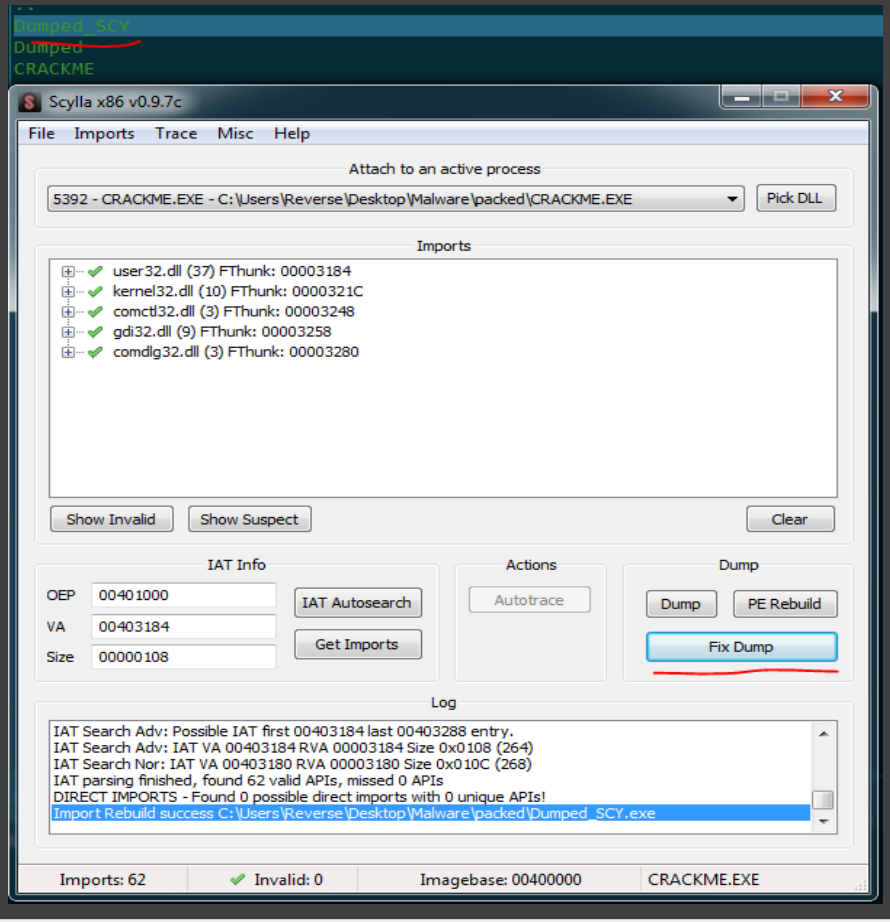
1. Выбираем наш процесс (он всё ещё под отладкой)
2. В OEP выставляем наш адрес (0x401000)
3. Жмём IAT AutoSearch
4. Жмём Get Imports





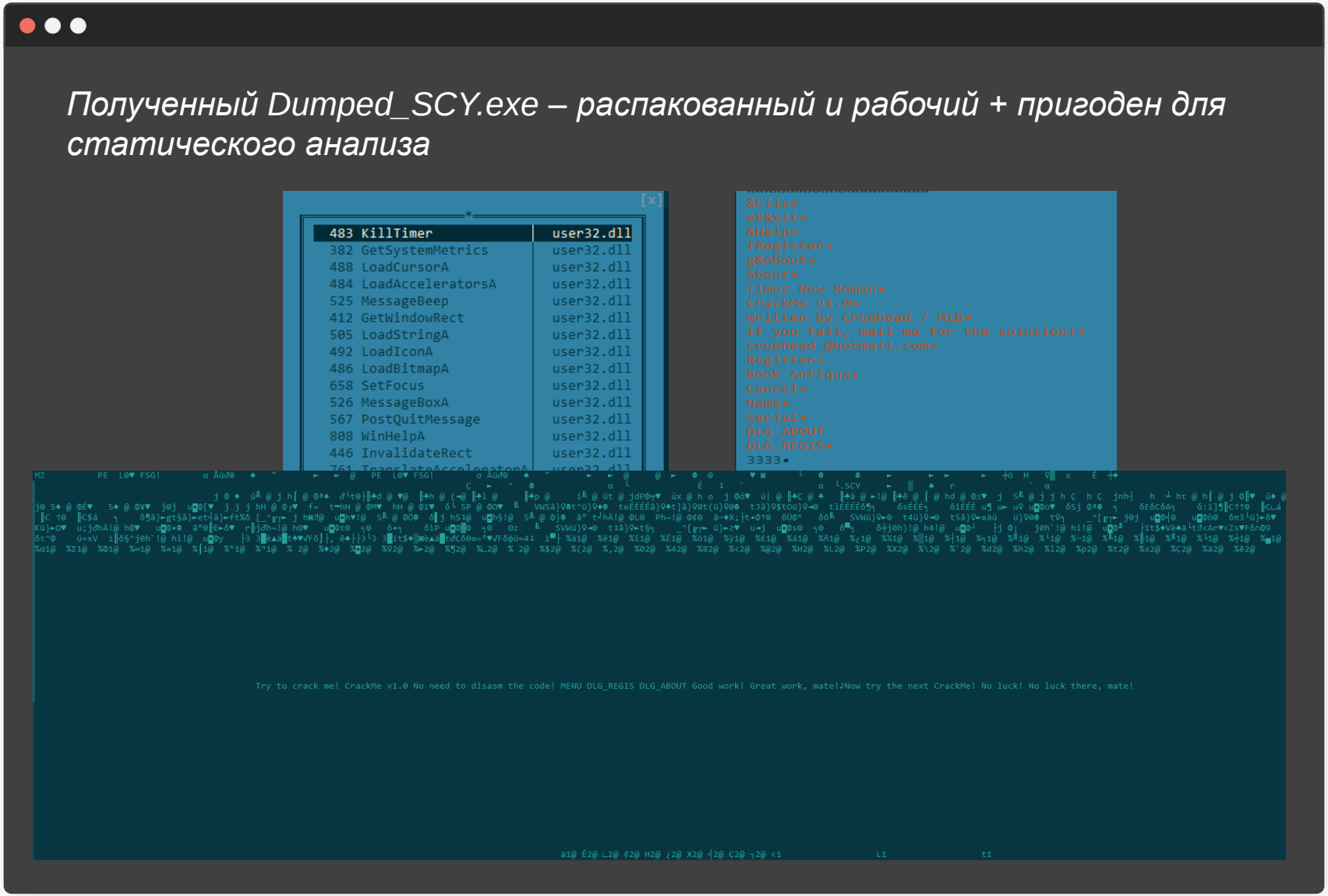
Записываем таблицу импорта в дамп

1. Жмём Fix Dump
2. Выбираем наш дамп



Результат

Полученный Dumped_SCY.exe – распакованный и рабочий + пригоден для статического анализа



Результат

Полученный Dumped_SCY.exe – распакованный и рабочий + пригоден для статического анализа

```
C:\Documents and Settings\Reverse\Desktop\Malware\packed\Dumped_SCY.exe
.00401000: 6A00                    push        0
.00401002: E8FF040000              call        GetModuleHandleA --↓1
.00401007: A3CA204000              mov         [0004020CA],eax --↓2
.0040100C: 6A00                    push        0
.0040100E: 68F4204000              push        0004020F4 ;'No need to disasm the code!' --↓3
.00401013: E8A6040000              call        FindWindowA --↓4
.00401018: 0BC0                    or          eax,eax
.0040101A: 7401                    jz          .00040101D --↓5
.0040101C: C3                      retn ; -^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-
.0040101D: C7056420400003400000   5mov         d,[000402064],000004003 --↓6
.00401027: C7056820400028114000    mov         d,[000402068],000401128 --↓7 --↓8
.00401031: C7056C20400000000000    mov         d,[00040206C],0 --↓9
.0040103B: C7057020400000000000    mov         d,[000402070],0 --↓A
.00401045: A1CA204000              mov         eax,[0004020CA] --↓2
.0040104A: A374204000              mov         [000402074],eax --↓B
.0040104F: 6A64                    push        064 ;'d'
.00401051: 50                      push        eax
.00401052: E8D1030000              call        LoadIconA --↓C
.00401057: A378204000              mov         [000402078],eax --↓D
.0040105C: 68007F0000              push        000007F00 ;'  ⌂ '
.00401061: 6A00                    push        0
.00401063: E8A2030000              call        LoadCursorA --↓E
.00401068: A37C204000              mov         [00040207C],eax --↓F
.0040106D: C7058020400005000000    mov         d,[000402080],5 --↓G
.00401077: C7058420400010214000    mov         d,[000402084],000402110 --↓H ;'MENU' --↓I
.00401081: C70588204000F4204000    mov         d,[000402088],0004020F4 --↓J ;'No need to disasm the code!' --↓3
.0040108B: 6864204000              push        000402064 --↓6
.00401090: E8F3030000              call        RegisterClassA --↓K
.00401095: 6A00                    push        0
.00401097: FF35CA204000            push        d,[0004020CA] --↓2
```

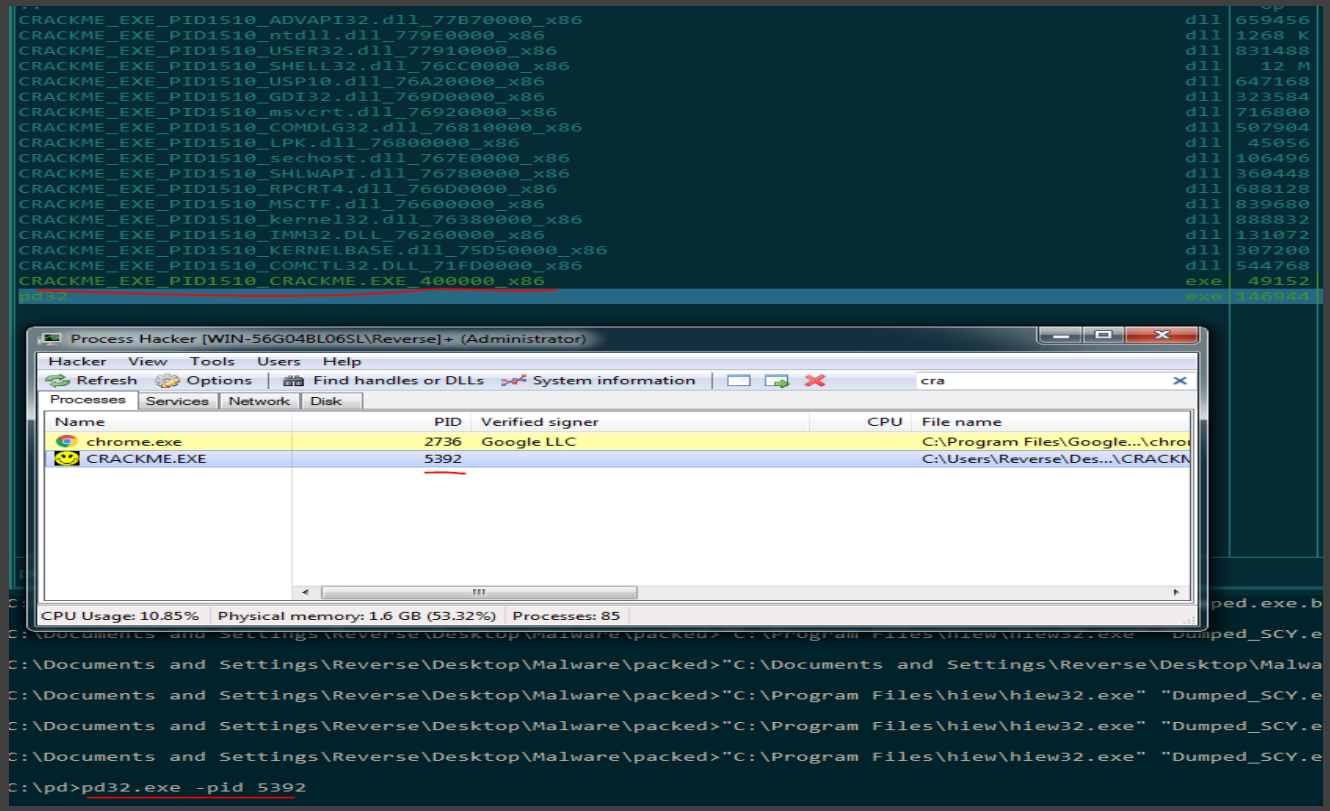
Внимание!

Не всегда возможно «оживить» дамп!

```
C:\Documents and Settings\Reverse\Desktop\Malware\packed\Dumped_SCY.exe
.00401000: 6A00                    push        0
.00401002: E8FF040000              call        GetModuleHandleA --↓1
.00401007: A3CA204000              mov         [0004020CA],eax --↓2
.0040100C: 6A00                    push        0
.0040100E: 68F4204000              push        0004020F4 ;'No need to disasm the code!' --↓3
.00401013: E8A6040000              call        FindWindowA --↓4
.00401018: 0BC0                    or          eax,eax
.0040101A: 7401                    jz          .00040101D --↓5
.0040101C: C3                      retn ; -^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-
.0040101D: C7056420400003400000   5mov         d,[000402064],000004003 --↓6
.00401027: C705682040002811400 0   mov         d,[000402068],000401128 --↓7 --↓8
.00401031: C7056C20400000000000    mov         d,[00040206C],0 --↓9
.0040103B: C705702040000000000 0   mov         d,[000402070],0 --↓A
.00401045: A1CA204000              mov         eax,[0004020CA] --↓2
.0040104A: A374204000              mov         [000402074],eax --↓B
.0040104F: 6A64                    push        064 ;'d'
.00401051: 50                      push        eax
.00401052: E8D1030000              call        LoadIconA --↓C
.00401057: A378204000              mov         [000402078],eax --↓D
.0040105C: 68007F0000              push        000007F00 ;'  ⌂ '
.00401061: 6A00                    push        0
.00401063: E8A2030000              call        LoadCursorA --↓E
.00401068: A37C204000              mov         [00040207C],eax --↓F
.0040106D: C705802040000500000 0   mov         d,[000402080],5 --↓G
.00401077: C705842040001021400 0   mov         d,[000402084],000402110 --↓H ;'MENU' --↓I
.00401081: C70588204000F4204000    mov         d,[000402088],0004020F4 --↓J ;'No need to disasm the code!' --↓3
.0040108B: 6864204000              push        000402064 --↓6
.00401090: E8F3030000              call        RegisterClassA --↓K
.00401095: 6A00                    push        0
.00401097: FF35CA204000            push        d,[0004020CA] --↓2
```

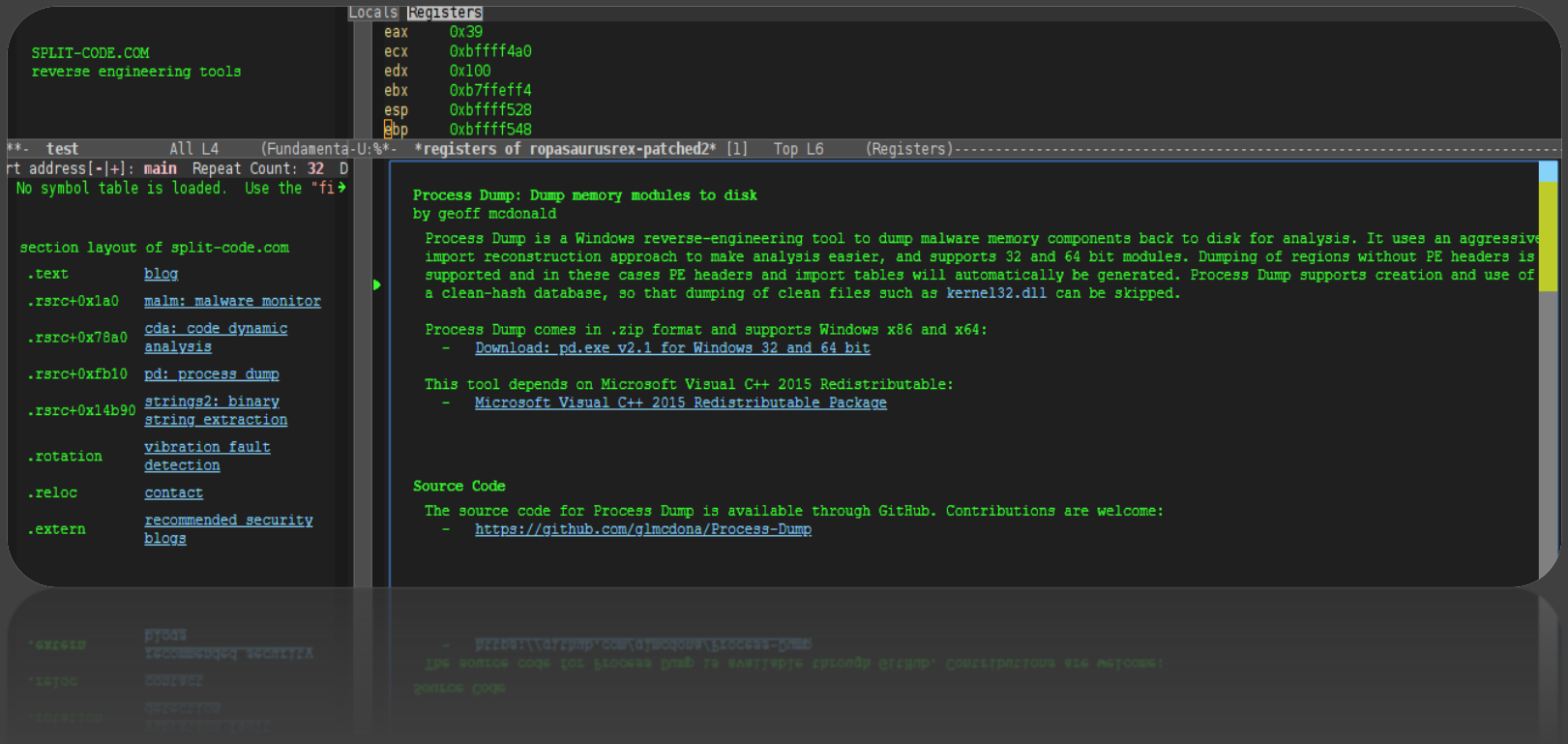
Автоматический дамп и восстановление IAT

Pd32.exe –pid xxxx



PD – лучшая в своём деле!

Автоматический дамп и восстановление IAT



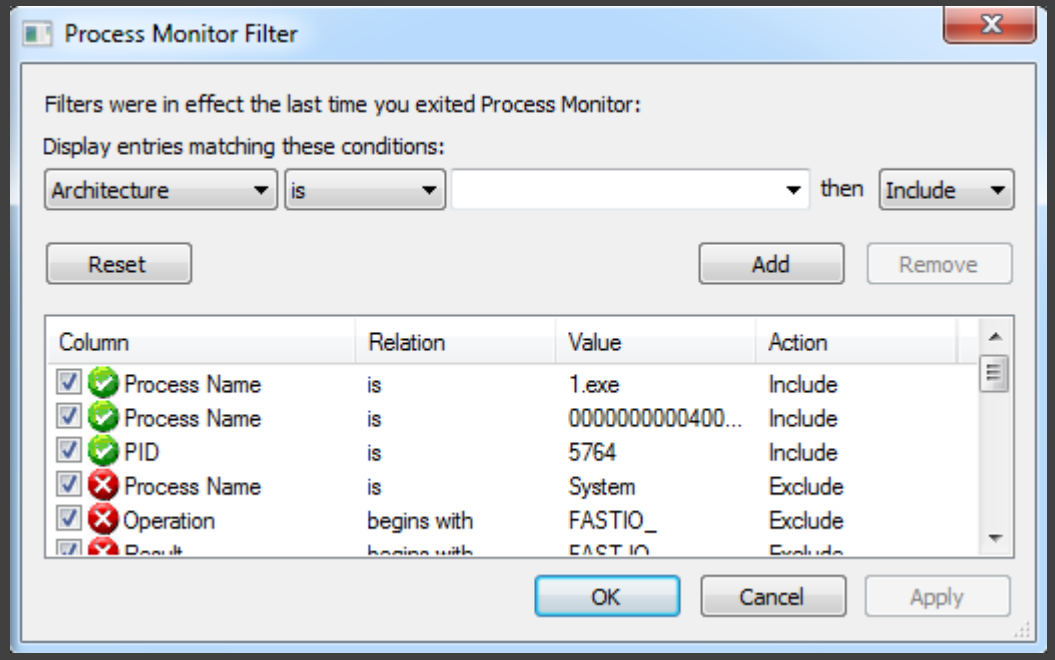
http://split-code.com/processdump.html

2

ProcMon

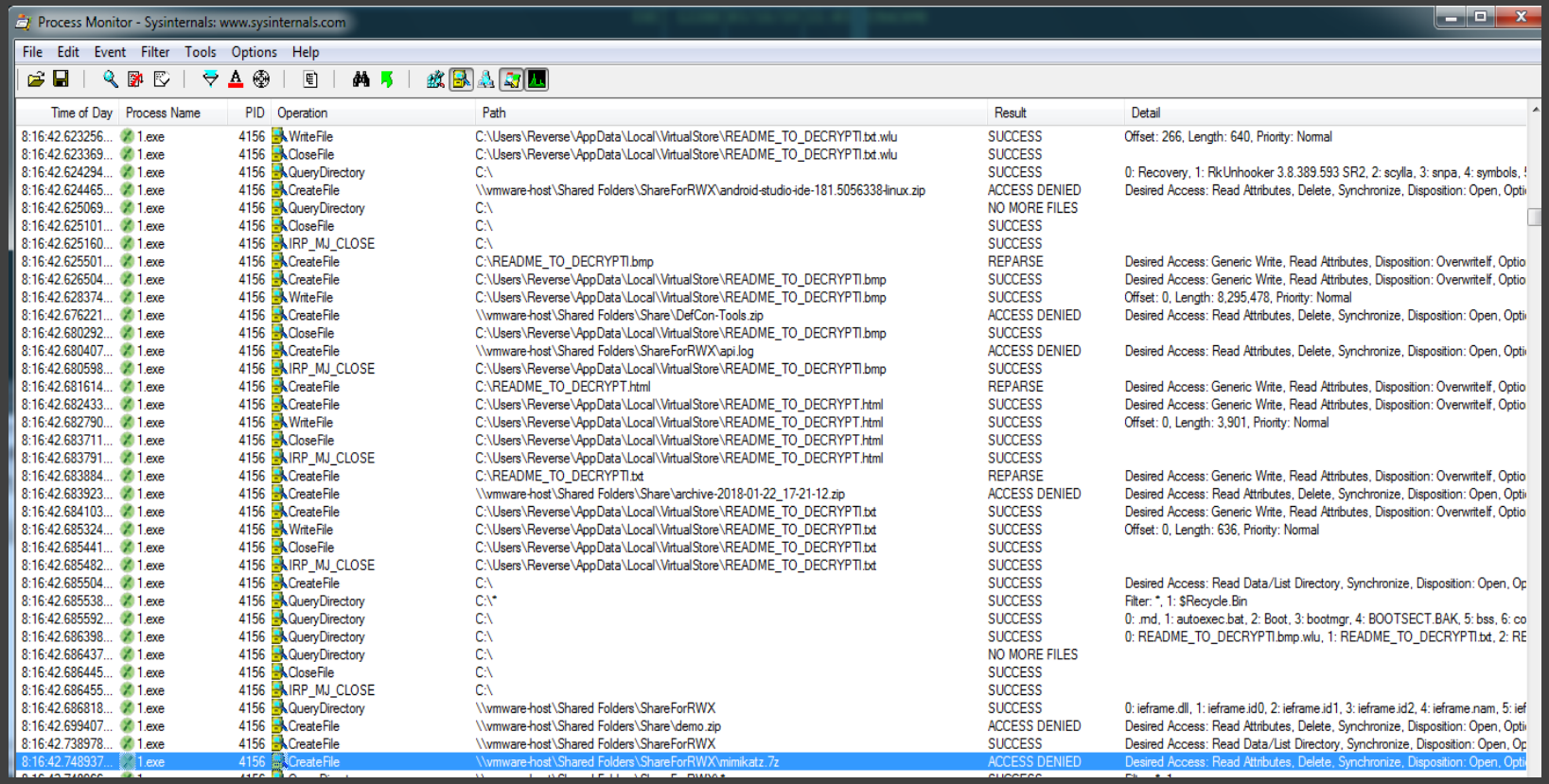
Задача – определить активность программы

1. Запускаем ProcMon
2. Выставляем нужные фильтры (Ctrl + L)



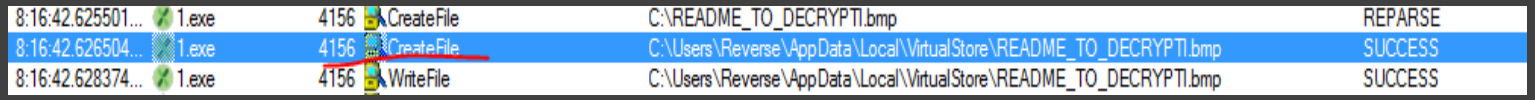
Задача – определить активность программы

Можно отфильтровать вывод по категориям событий: реестр, доступ к файлам, сетевая активность и тд



Определение места вызова функций в коде

Как найти место в PE файле, где вызваласть нужная функция, например, CreateFile?

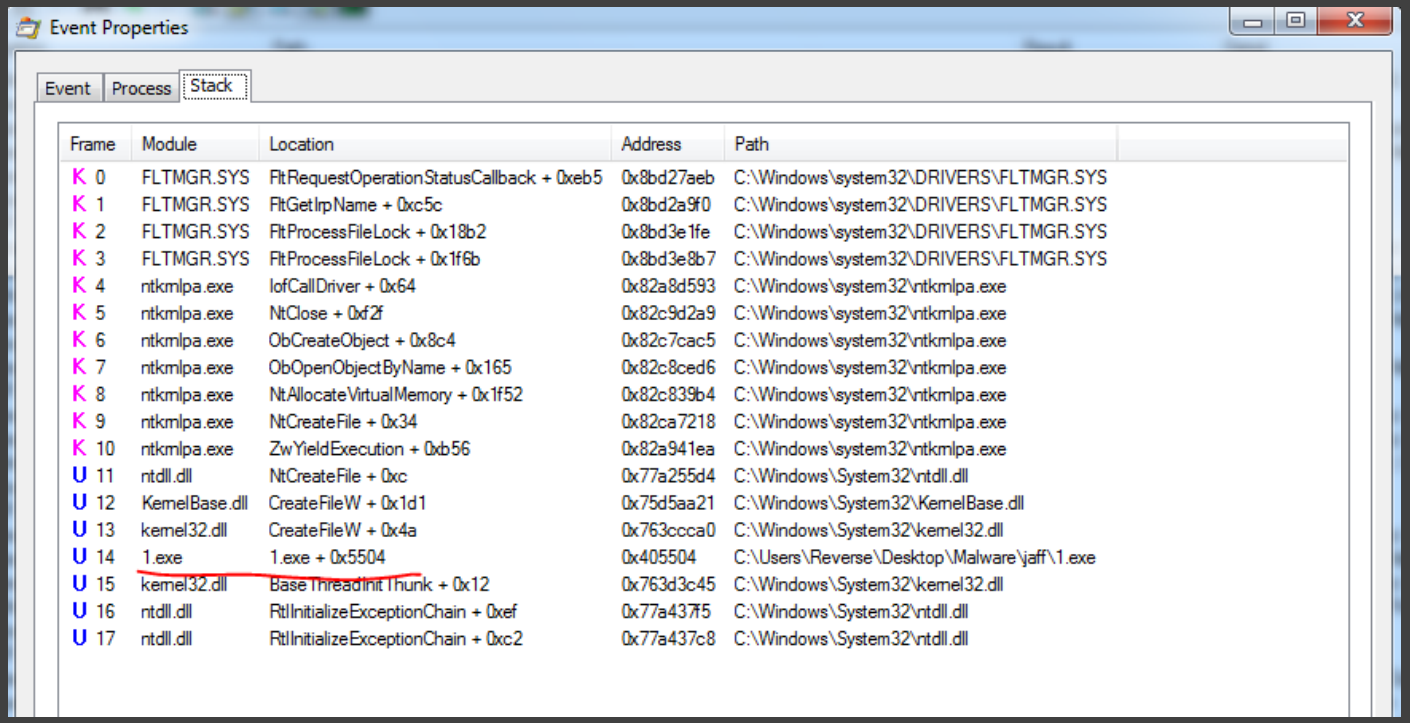


8:16:42.625501...	1.exe	4156	CreateFile	C:\README_TO_DECRYPTI.bmp	REPARSE
8:16:42.626504...	1.exe	4156	CreateFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bmp	SUCCESS
8:16:42.628374...	1.exe	4156	WriteFile	C:\Users\Reverse\AppData\Local\VirtualStore\README_TO_DECRYPTI.bmp	SUCCESS

1. Жмём Enter по интересующему событию
2. Переходим на вкладку Stack

Определение места вызова функций в коде

Как найти место в PE файле, где вызваласть нужная функция, например, CreateFile?



Определение места вызова функций в коде

Как найти место в PE файле, где вызваласть нужная функция, например, CreateFile?

U	12	KernelBase.dll	CreateFileW + 0x1d1	0x75d5aa21	C:\Windows\System32\KernelBase.dll
U	13	kernel32.dll	CreateFileW + 0x4a	0x763ccca0	C:\Windows\System32\kernel32.dll
U	14	1.exe	1.exe + 0x5504	0x405504	C:\Users\Reverse\Desktop\Malware\jaff\1.exe
U	15	kernel32.dll	BaseThreadInitThunk + 0x12	0x763d3c45	C:\Windows\System32\kernel32.dll
U	16	ntdll.dll	RtlInitializeExceptionChain + 0xef	0x77a437f5	C:\Windows\System32\ntdll.dll
U	17	ntdll.dll	RtlInitializeExceptionChain + 0xc2	0x77a437c8	C:\Windows\System32\ntdll.dll

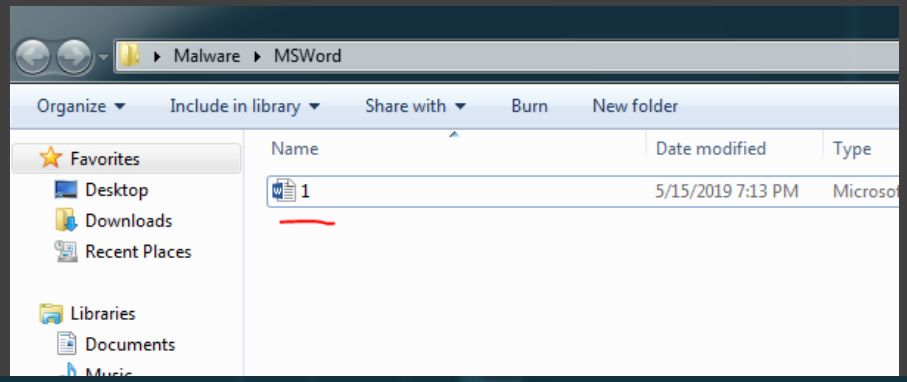
```
004054D6    8D 84 24 7C 02 00 00    lea eax,dword ptr ss:[esp+27C]
004054DD    50                      push eax
004054DE    FF 15 DC 70 40 00       call dword ptr ds:[<&lstrcatW>]
004054E4    6A 00                   push 0
004054E6    68 80 00 00 00          push 80
004054EB    6A 02                   push 2
004054ED    6A 00                   push 0
004054EF    6A 00                   push 0
004054F1    68 00 00 00 40          push 40000000
004054F6    8D 8C 24 90 02 00 00    lea ecx,dword ptr ss:[esp+290]
004054FD    51                      push ecx
004054FE    FF 15 E4 70 40 00       call dword ptr ds:[<&CreateFileW>]
00405504    8B F8                   mov edi,eax
00405506    83 FF FF                cmp edi,FFFFFFFF
00405509    74 25                   je 1.405530
0040550B    8B 46 04                mov eax,dword ptr ds:[esi+4]
```

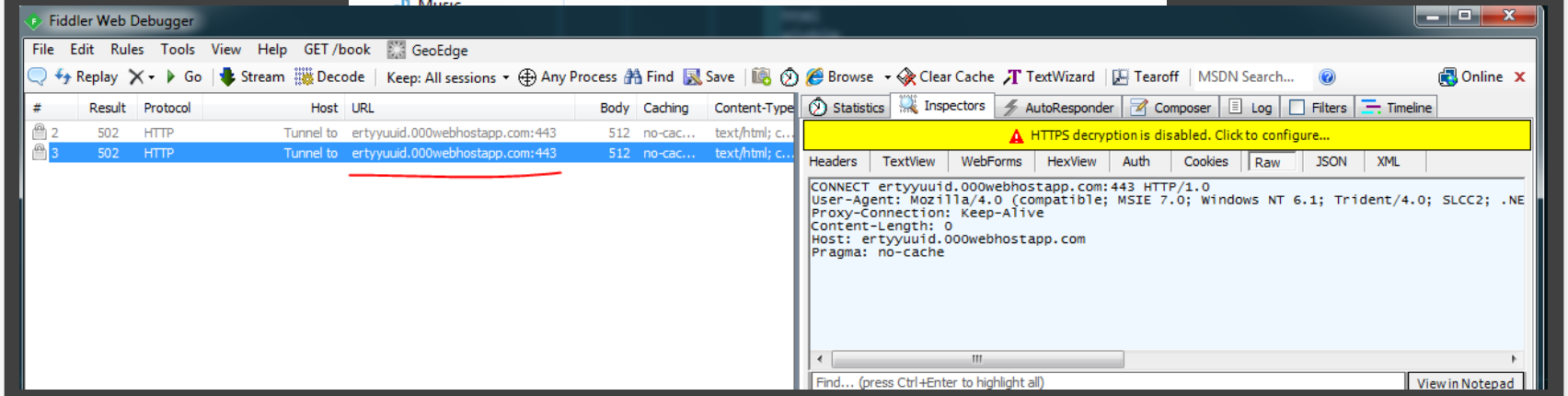
3

Fidder/WireShark

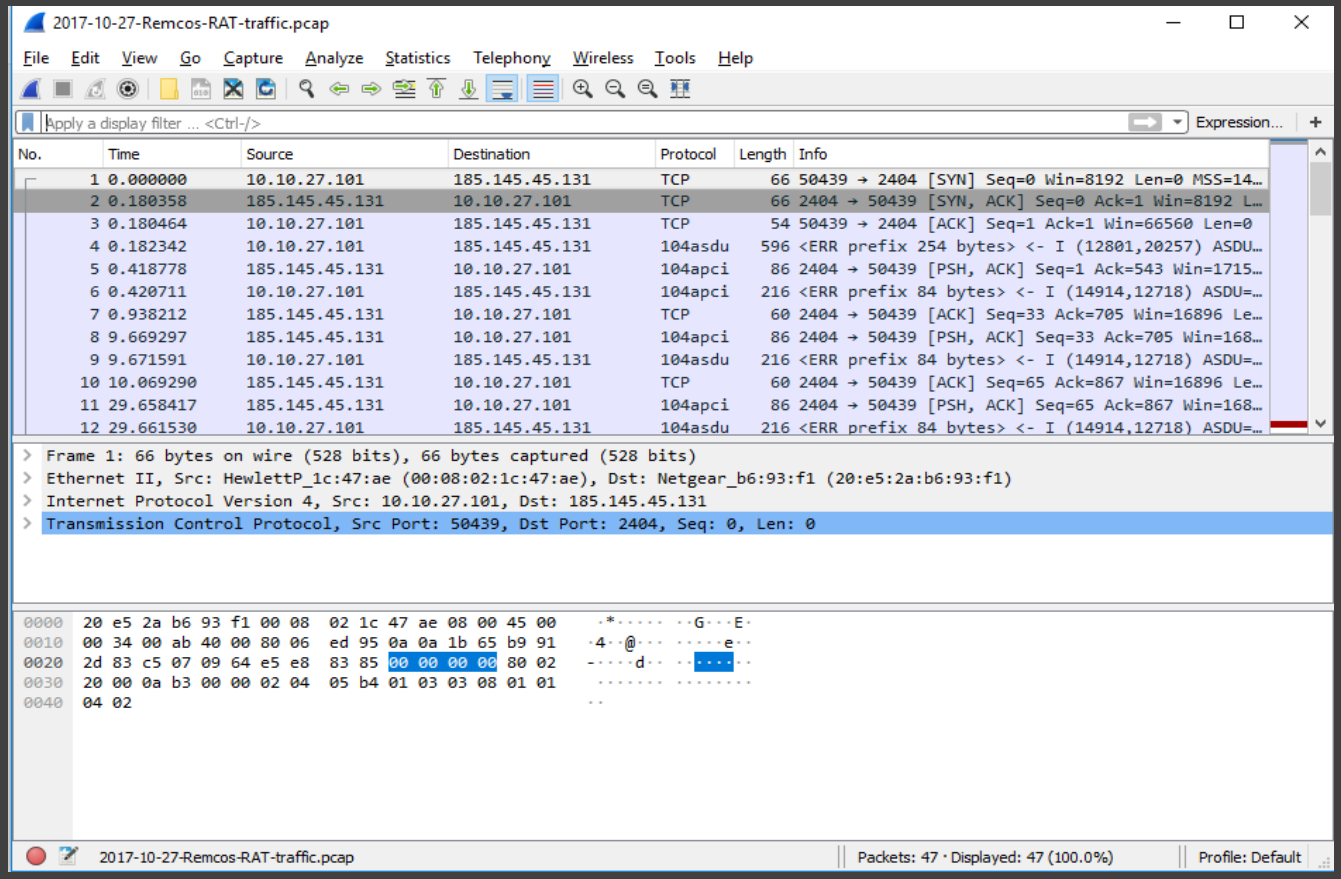
Просмотр http запросов

Запускаем вредоносный файлик

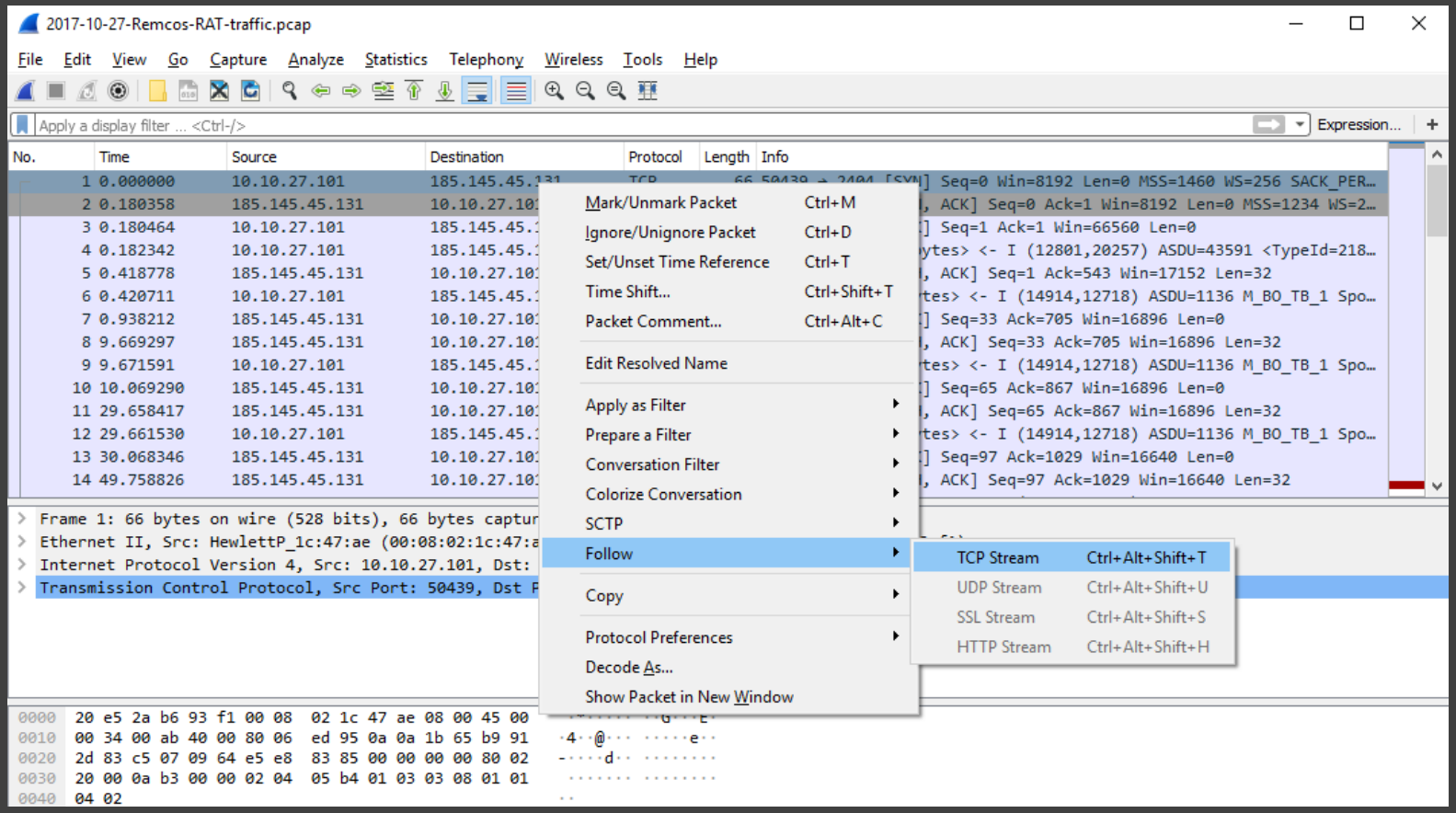




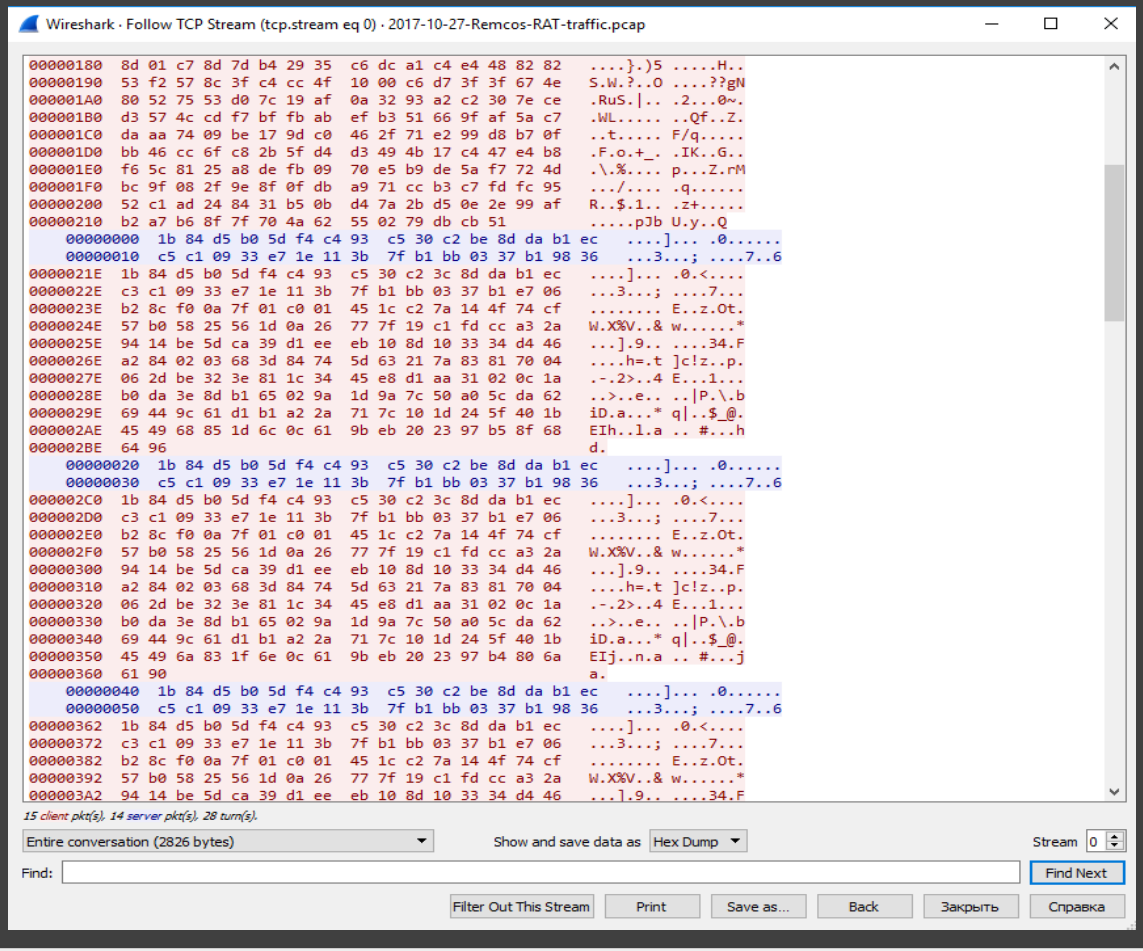
Remcos RAT traffic



Follow to TCP Stream

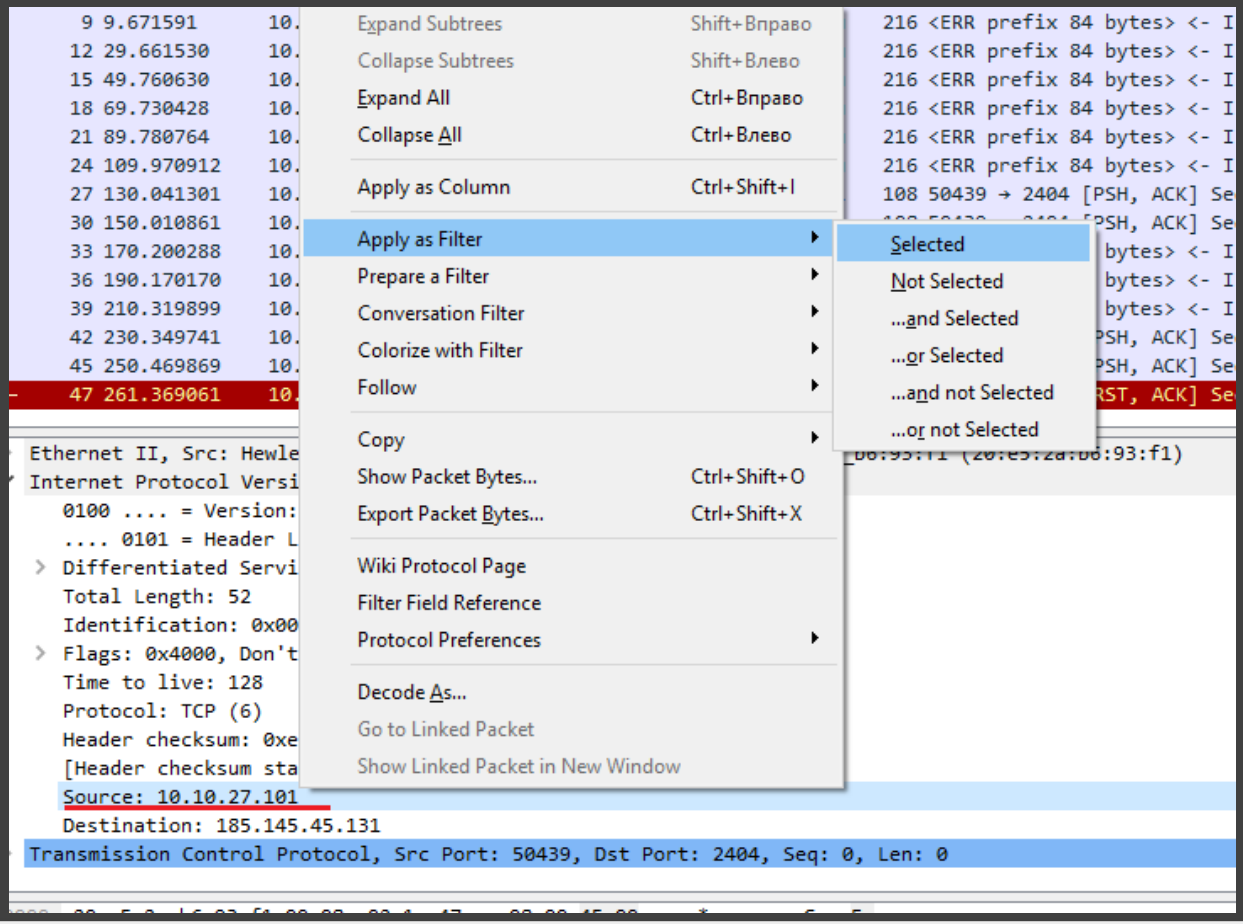


Общение с CC


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2017-10-27-Remcos-RAT-traffic.pcap
00000180 8d 01 c7 8d 7d b4 29 35 c6 dc a1 c4 e4 48 82 82 ....}.)5 .....H..
00000190 53 f2 57 8c 3f c4 cc 4f 10 00 c6 d7 3f 3f 67 4e S.W.?..O ....??gN
000001A0 80 52 75 53 d0 7c 19 af 0a 32 93 a2 c2 30 7e ce .RuS.|.. .2...0~.
000001B0 d3 57 4c cd f7 bf fb ab ef b3 51 66 9f af 5a c7 .WL..... ..Qf..Z.
000001C0 da aa 74 09 be 17 9d c0 46 2f 71 e2 99 d8 b7 0f ..t..... F/q.....
000001D0 bb 46 cc 6f c8 2b 5f d4 d3 49 4b 17 c4 47 e4 b8 .F.o.+_. .IK..G..
000001E0 f6 5c 81 25 a8 de fb 09 70 e5 b9 de 5a f7 72 4d .\.%.... p...Z.rM
000001F0 bc 9f 08 2f 9e 8f 0f db a9 71 cc b3 c7 fd fc 95 .../.... .q......
00000200 52 c1 ad 24 84 31 b5 0b d4 7a 2b d5 0e 2e 99 af R..$.1.. .z+.....
00000210 b2 a7 b6 8f 7f 70 4a 62 55 02 79 db cb 51 .....pJb U.y..Q
00000000 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 be 8d da b1 ec ....]... .0......
00000010 c5 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 98 36 ...3...; ....7..6
0000021E 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 3c 8d da b1 ec ....]... .0.<....
0000022E c3 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 e7 06 ...3...; ....7...
0000023E b2 8c f0 0a 7f 01 c0 01 45 1c c2 7a 14 4f 74 cf .... E..z.Ot.
0000024E 57 b0 58 25 56 1d 0a 26 77 7f 19 c1 fd cc a3 2a W.X%V..& w......*
0000025E 94 14 be 5d ca 39 d1 ee eb 10 8d 10 33 34 d4 46 ...].9.. ....34.F
0000026E a2 84 02 03 68 3d 84 74 5d 63 21 7a 83 81 70 04 ....h=.t]c!z..p.
0000027E 06 2d be 32 3e 81 1c 34 45 e8 d1 aa 31 02 0c 1a .-.2>..4 E...1...
0000028E b0 da 3e 8d b1 65 02 9a 1d 9a 7c 50 a0 5c da 62 ..>..e.. ..|P.\.b
0000029E 69 44 9c 61 d1 b1 a2 2a 71 7c 10 1d 24 5f 40 1b iD.a...* q|..$_@.
000002AE 45 49 68 85 1d 6c 0c 61 9b eb 20 23 97 b5 8f 68 EIh..l.a .. #...h
000002BE 64 96 d.
00000020 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 be 8d da b1 ec ....]... .0......
00000030 c5 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 98 36 ...3...; ....7..6
000002C0 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 3c 8d da b1 ec ....]... .0.<....
000002D0 c3 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 e7 06 ...3...; ....7...
000002E0 b2 8c f0 0a 7f 01 c0 01 45 1c c2 7a 14 4f 74 cf .... E..z.Ot.
000002F0 57 b0 58 25 56 1d 0a 26 77 7f 19 c1 fd cc a3 2a W.X%V..& w......*
00000300 94 14 be 5d ca 39 d1 ee eb 10 8d 10 33 34 d4 46 ...].9.. ....34.F
00000310 a2 84 02 03 68 3d 84 74 5d 63 21 7a 83 81 70 04 ....h=.t]c!z..p.
00000320 06 2d be 32 3e 81 1c 34 45 e8 d1 aa 31 02 0c 1a .-.2>..4 E...1...
00000330 b0 da 3e 8d b1 65 02 9a 1d 9a 7c 50 a0 5c da 62 ..>..e.. ..|P.\.b
00000340 69 44 9c 61 d1 b1 a2 2a 71 7c 10 1d 24 5f 40 1b iD.a...* q|..$_@.
00000350 45 49 6a 83 1f 6e 0c 61 9b eb 20 23 97 b4 80 6a EIj..n.a .. #...j
00000360 61 90 a.
00000040 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 be 8d da b1 ec ....]... .0......
00000050 c5 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 98 36 ...3...; ....7..6
00000362 1b 84 d5 b0 5d f4 c4 93 c5 30 c2 3c 8d da b1 ec ....]... .0.<....
00000372 c3 c1 09 33 e7 1e 11 3b 7f b1 bb 03 37 b1 e7 06 ...3...; ....7...
00000382 b2 8c f0 0a 7f 01 c0 01 45 1c c2 7a 14 4f 74 cf .... E..z.Ot.
00000392 57 b0 58 25 56 1d 0a 26 77 7f 19 c1 fd cc a3 2a W.X%V..& w......*
000003A2 94 14 be 5d ca 39 d1 ee eb 10 8d 10 33 34 d4 46 ...].9.. ....34.F
15 client pkt(s), 14 server pkt(s), 28 turn(s).
Entire conversation (2826 bytes)
Show and save data as
Hex Dump
Stream
0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Закрыть
Справка

WireShark - фильтры

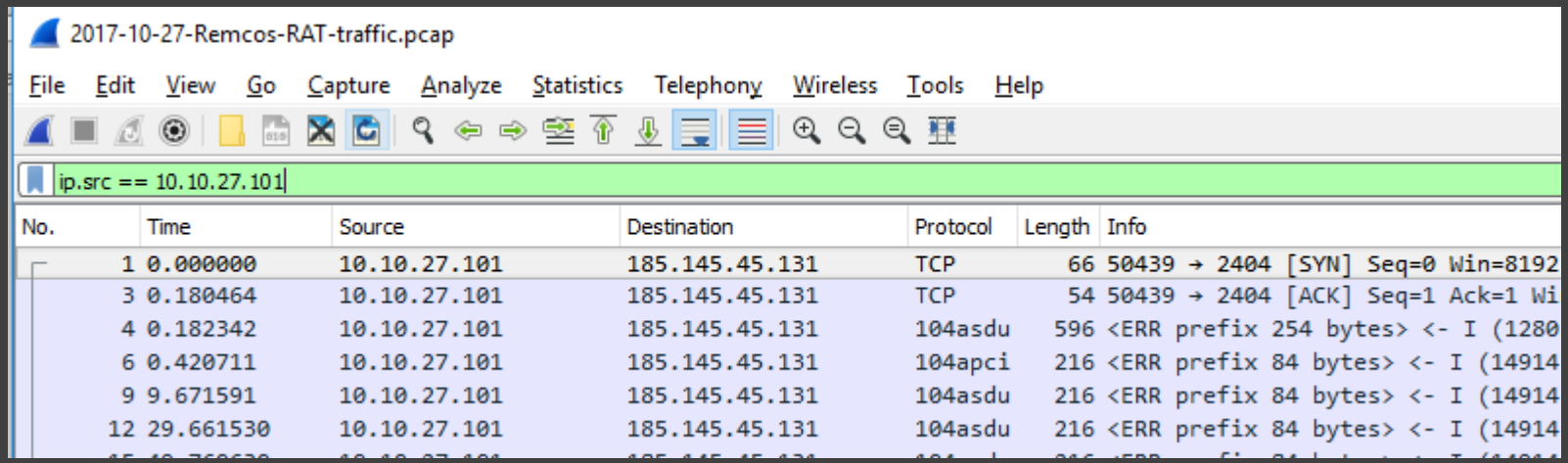
Находим интересный нам параметр → ПКМ Apply as Filter



WireShark - фильтры

OTUS

- Фильтры по протоколам
- Фильтры по портам



WireShark - фильтры

OTUS

Фильтры по протоколам

Фильтры по портам

Фильтр	Описание
ip.src	ip отправителя
ip.dst	ip получателя
ip.addr	ip отправителя или получателя
http | dns	Показать только http и dns
http contains user-agent	Поиск «user-agent»

https://www.wireshark.org/docs/man-pages/wireshark-filter.html

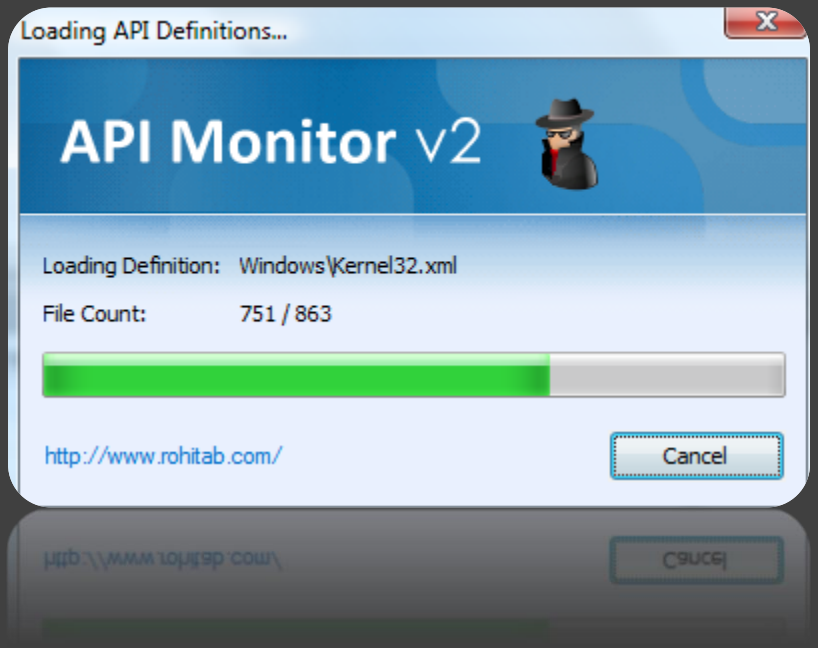
WireShark – операторы сравнения

Оператор	Описание
eq, ==	Равно
ne, !=	Не равно
gt, >	Больше, чем
lt, <	Меньше, чем
ge, >=	Больше, либо равно
le, <=	Меньше, либо равно

4

API monitor

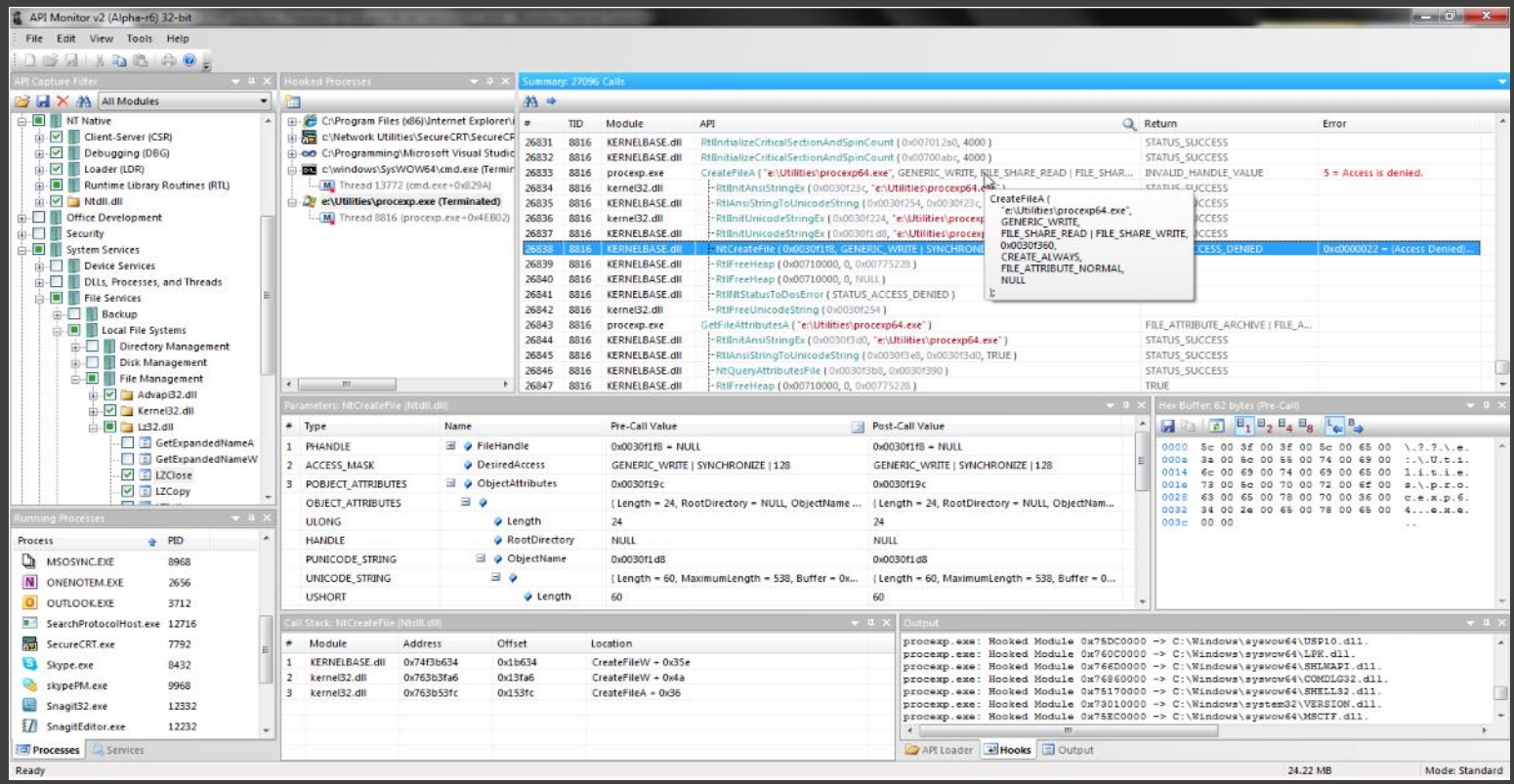
Позволяет проследить, какие функции вызываются программой с возможностью просмотра параметров



http://www.rohitab.com/apimonitor

API Monitor

Позволяет проследить, какие функции вызываются программой с возможностью просмотра параметров



Возможности инструмента

5

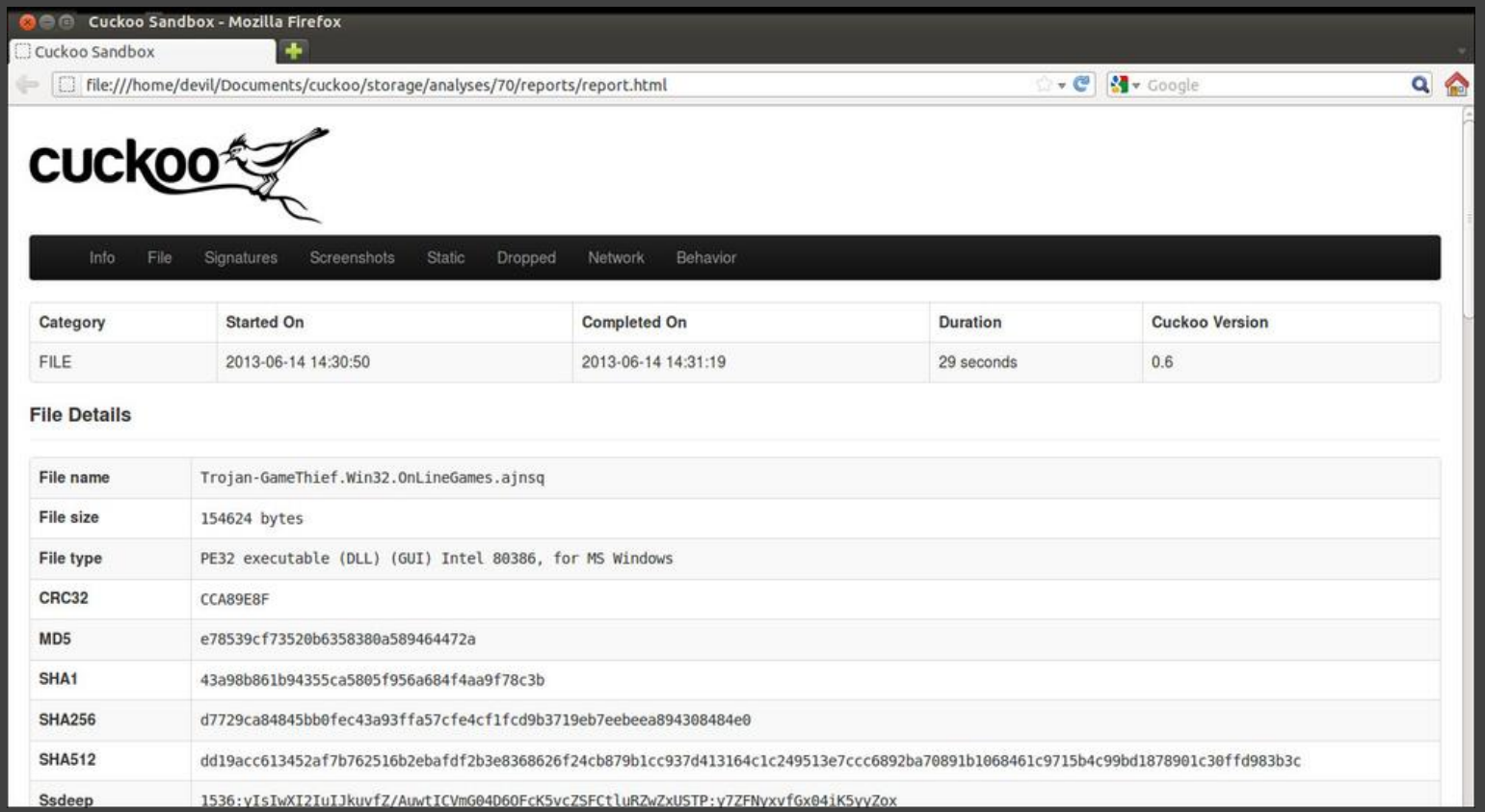
SandBox

Это система для автоматического исследования вредоносного ПО

cuckoo

https://cuckoosandbox.org/

Страница из отчёта



Online системы:

malwr.com
cuckoo.cert.ee
hybrid-analysis.com

OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!