GROUP IB

Криминалистический подход к выявлению угроз в инфраструктурах на основе ОС WINDOWS

WHOAMI

Олег Скулкин

Ведущий специалист по компьютерной криминалистике
skulkin@group-ib.com | @oskulkin

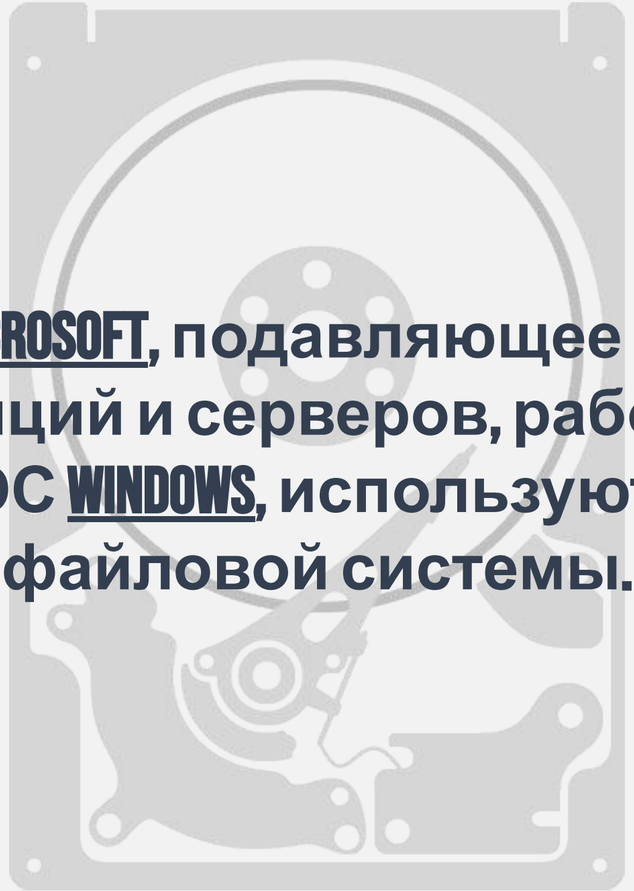
8 лет работы в области DFIR; соавтор «Windows Forensics Cookbook», «Practical Mobile Forensics», «Learning Android Forensics»; автор 100+ статей по DFIR

Жизненный цикл

SOME THINGS SHOULD BE SIMPLE; EVEN AN END HAS A START*

*Editors

Файловая система



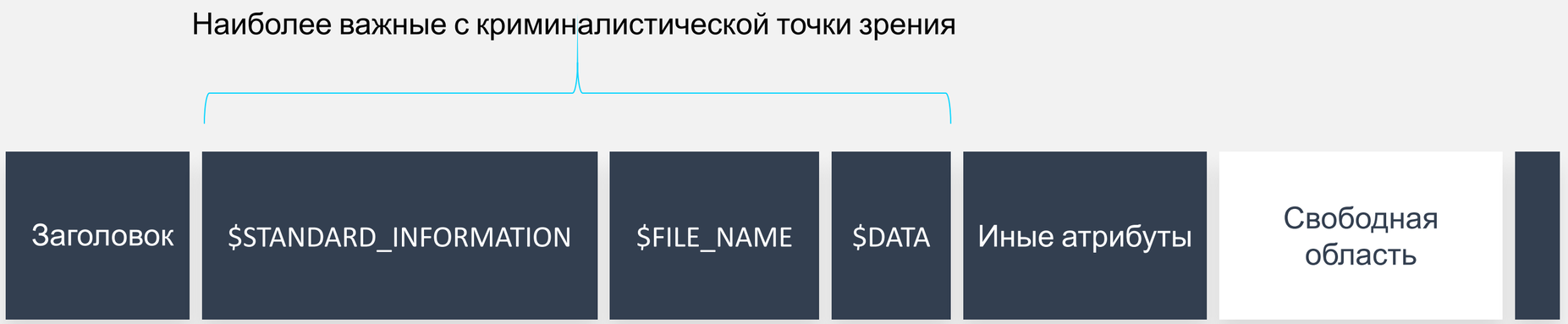
По данным MICROSOFT, подавляющее большинство рабочих станций и серверов, работающих под управлением ОС WINDOWS, используют NTFS в качестве файловой системы.

Структура NTFS

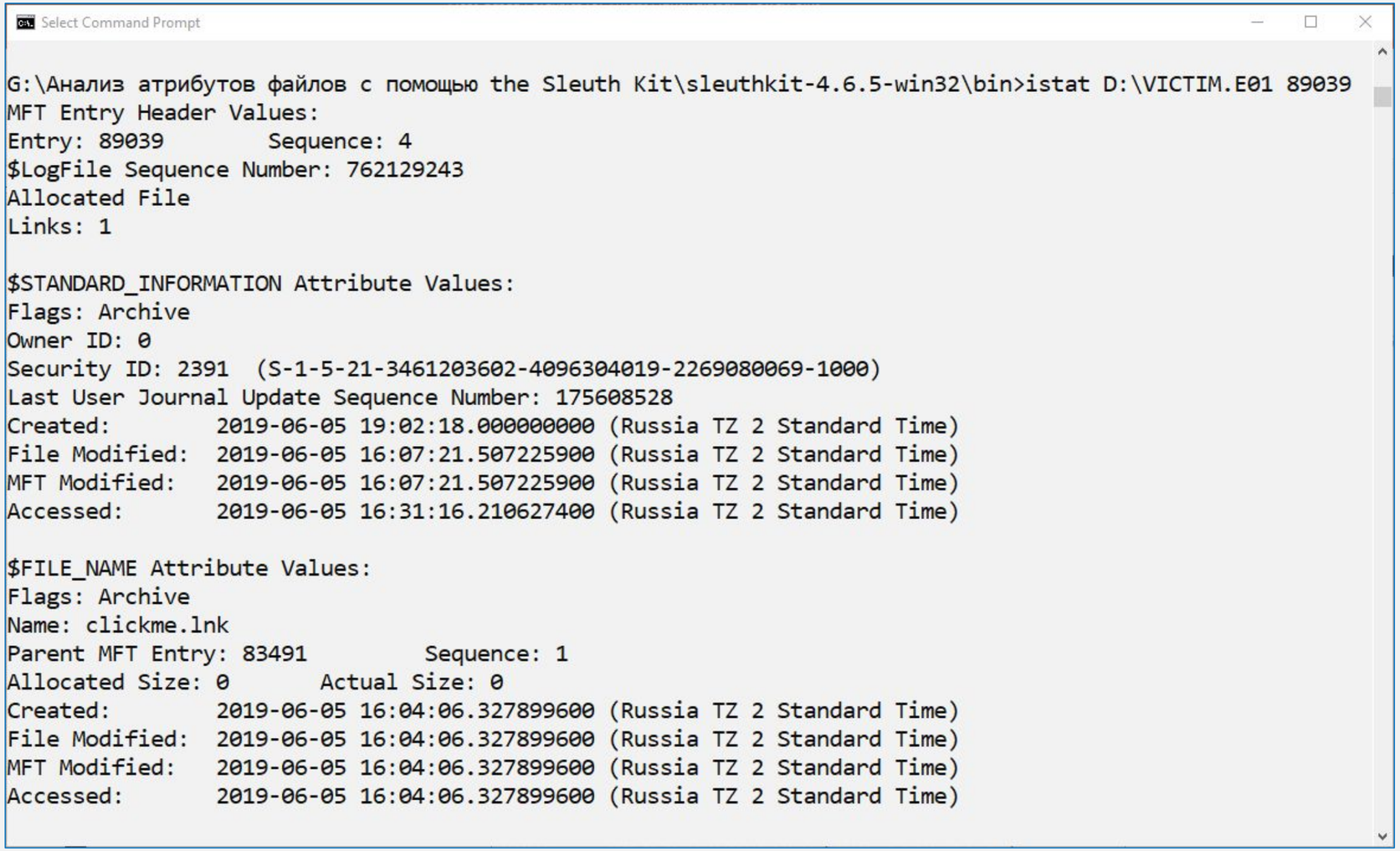
Практика: Удален != Утерян

Name	Size	Type	Date Modified
System Volume Information	1	Directory	6/26/2019 1:13:17 PM
$AttrDef	3	Regular File	6/26/2019 1:13:15 PM
$BadClus	0	Regular File	6/26/2019 1:13:15 PM
$Bitmap	32	Regular File	6/26/2019 1:13:15 PM
$Boot	8	Regular File	6/26/2019 1:13:15 PM
$I30	4	NTFS Index All...	6/26/2019 1:17:14 PM
$LogFile	4,896	Regular File	6/26/2019 1:13:15 PM
$MFT	256	Regular File	6/26/2019 1:13:15 PM
$MFTMirr	4	Regular File	6/26/2019 1:13:15 PM
$Secure	1	Regular File	6/26/2019 1:13:15 PM
$TXF_DATA	1	NTFS Logged ...	6/26/2019 1:17:14 PM
$UpCase	128	Regular File	6/26/2019 1:13:15 PM
$Volume	0	Regular File	6/26/2019 1:13:15 PM
Hi_Im_A_Deleted_Picture.jpg	319	Regular File	6/26/2019 1:16:19 PM

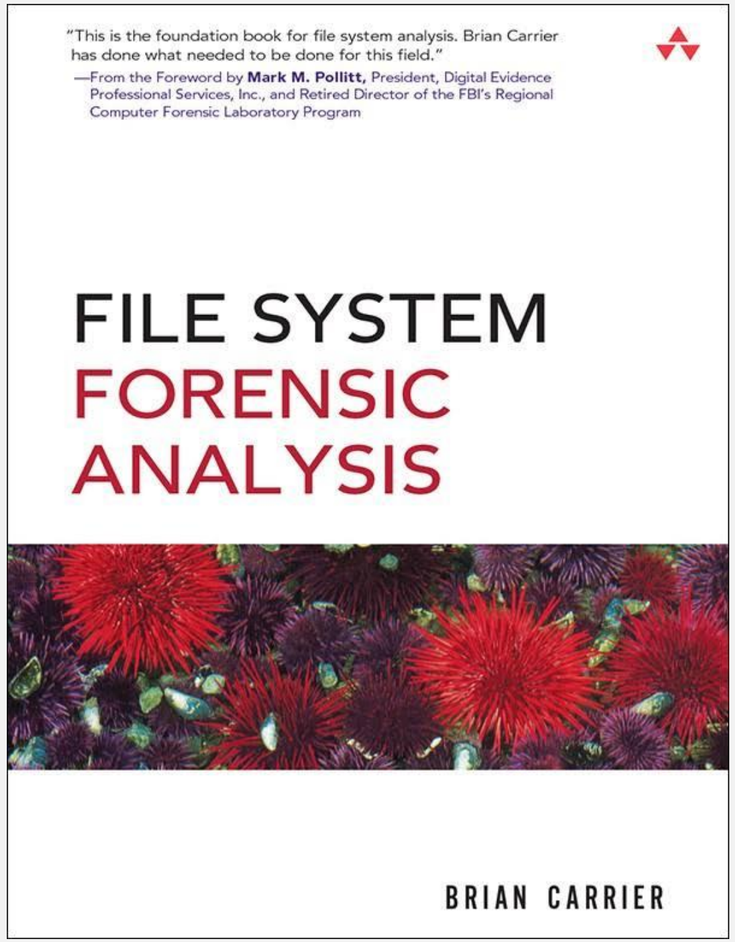
Запись в главной файловой таблице



Практика: анализ атрибутов файлов



Больше информации об NTFS



Brian Carrier, File System Forensic Analysis:

https://www.amazon.com/System-Forensic-Analysis-Brian-Carrier/dp/0321268172/

ФАЙЛЫ Реестра WINDOWS

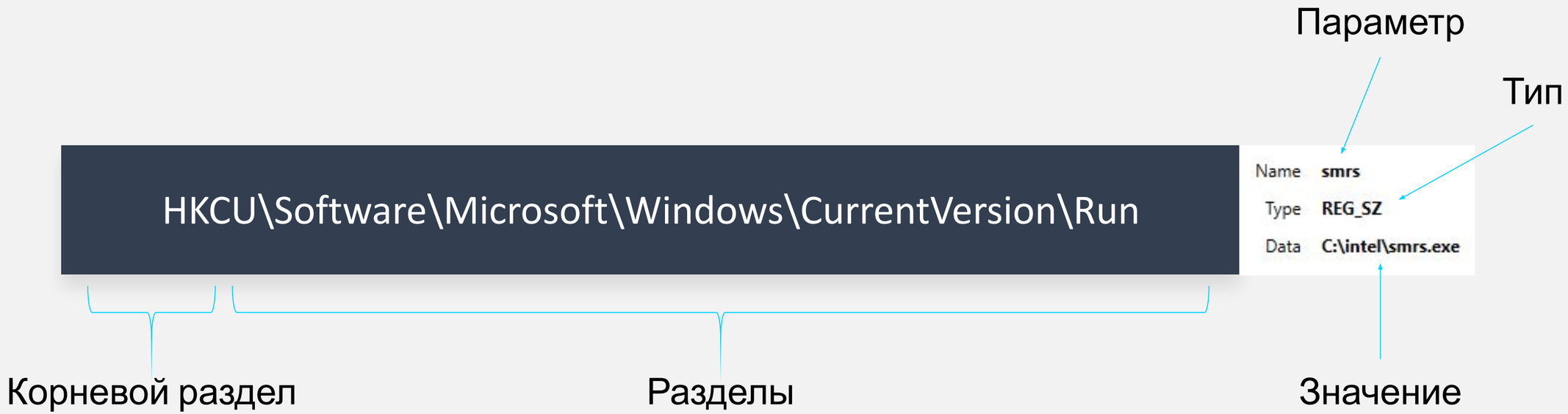
C:\Windows\System32\config

- SAM
- SECURITY
- SYSTEM
- SOFTWARE
- DEFAULT

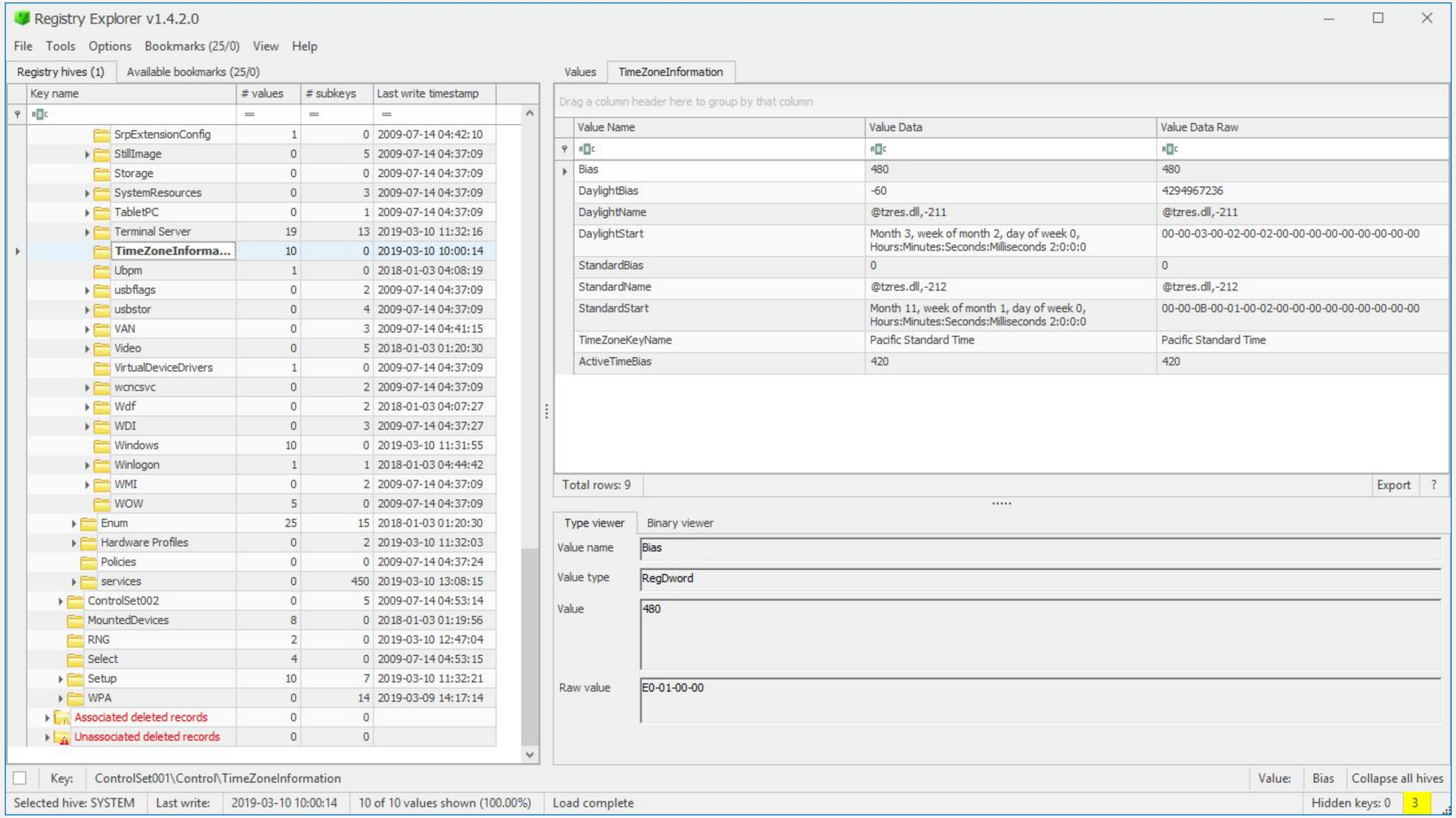
C:\Users\%username%

- NTUSER.DAT
- \AppData\Local\Microsoft\Windows\USRCLASS.DAT

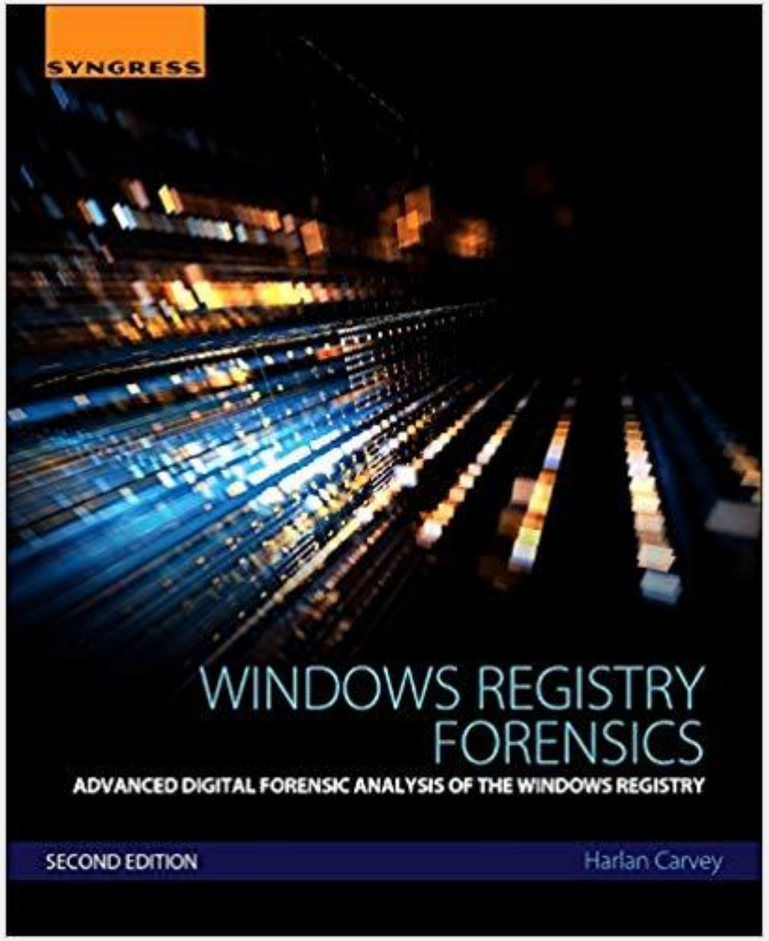
Разделы, параметры и значения



Практика: Просмотр файлов реестра



Больше информации о Реестре

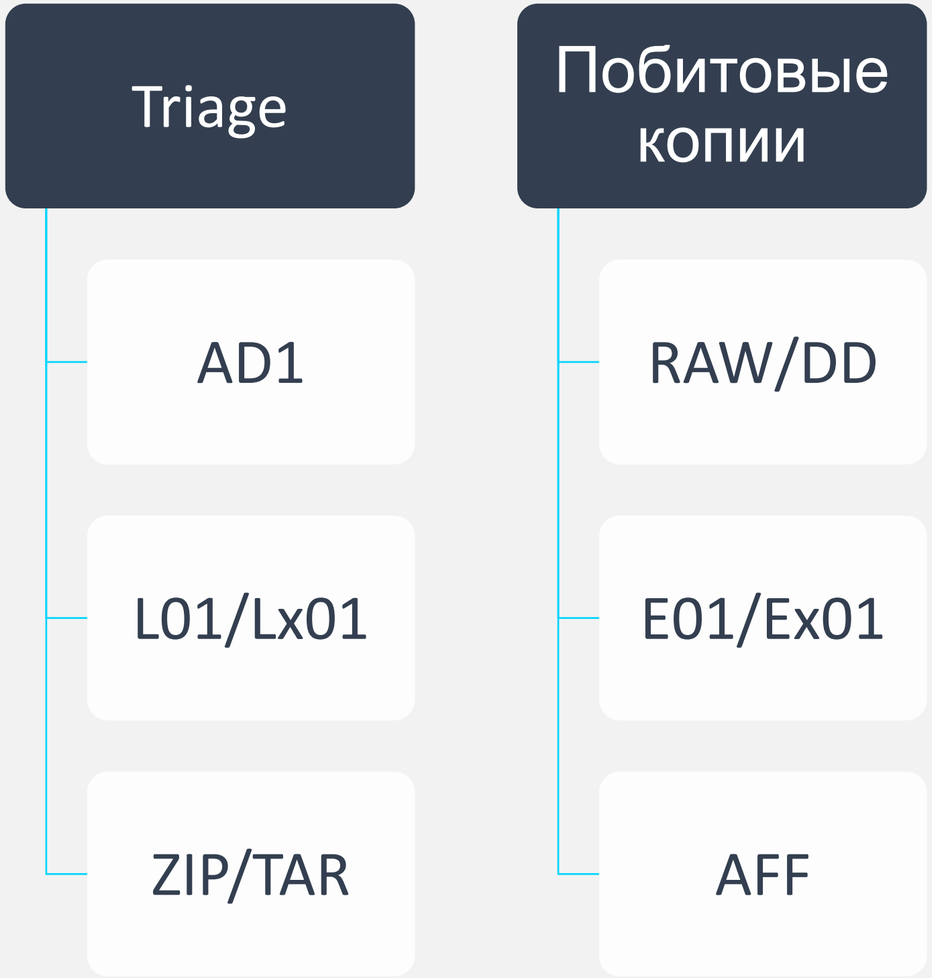


Harlan Carvey, Windows Registry Forensics:

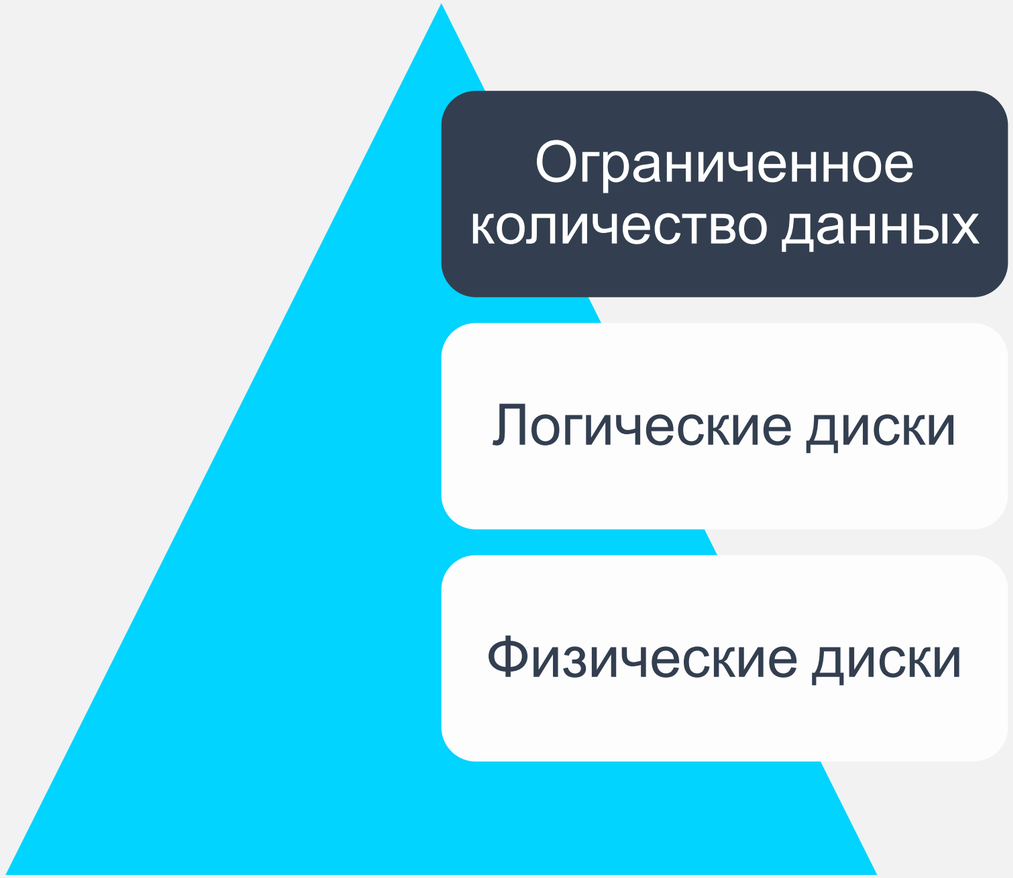
https://www.amazon.com/Windows-Registry-Forensics-Advanced-Forensic/dp/012803291X/

Подготовка источников информации

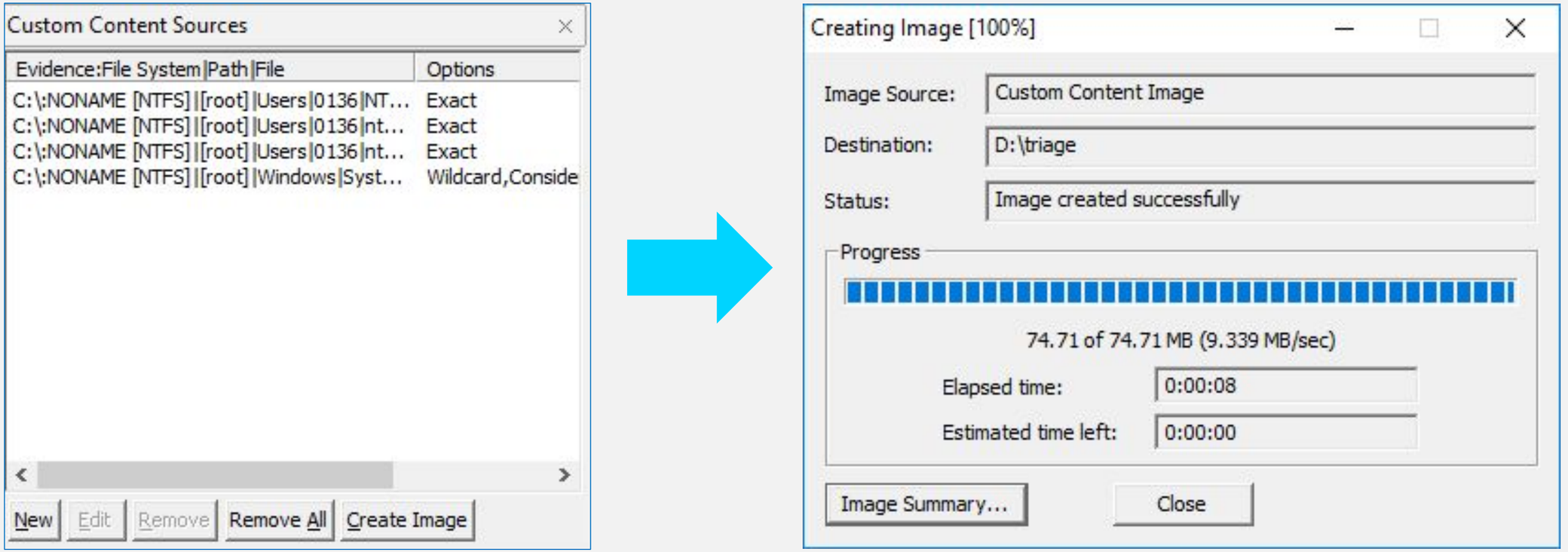
Создание криминалистических копий



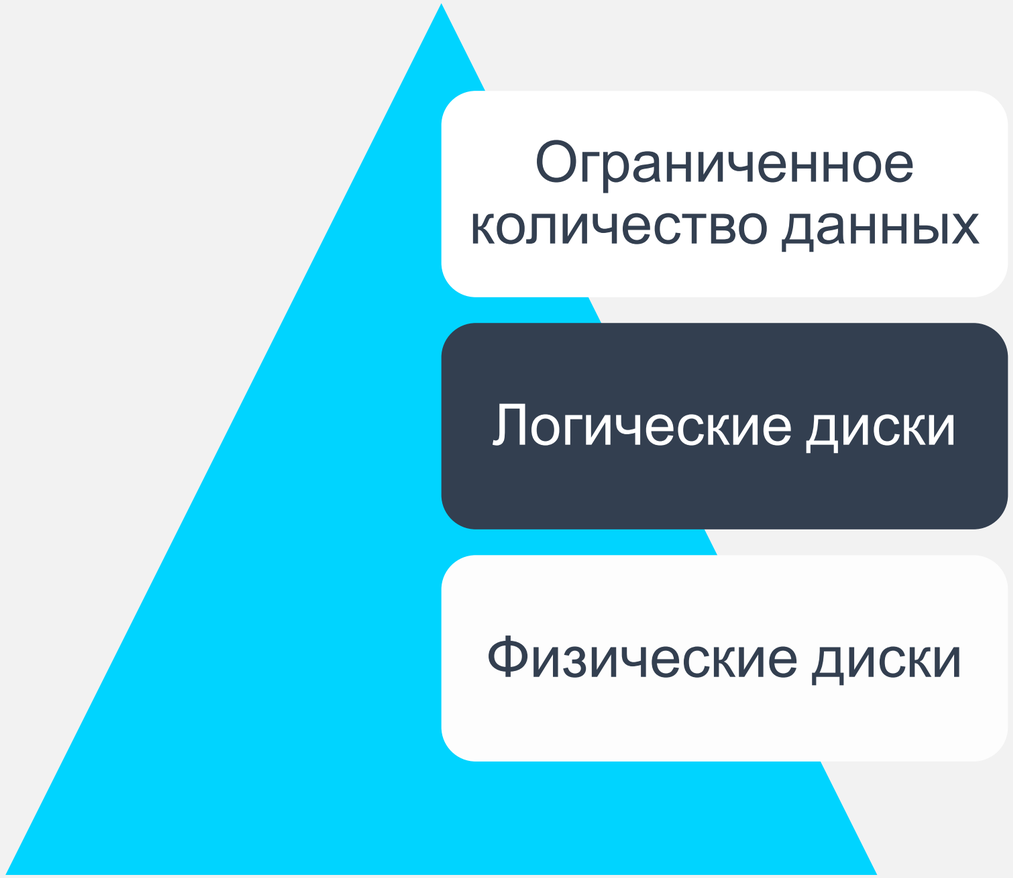
TRIAGE-копии



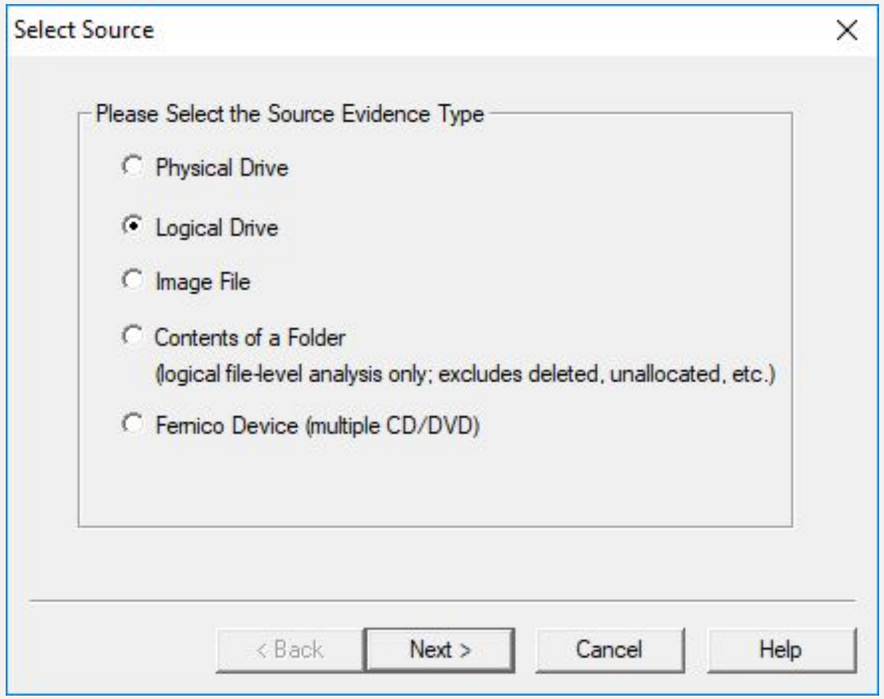
Практика: Создание TRIAGE-копии

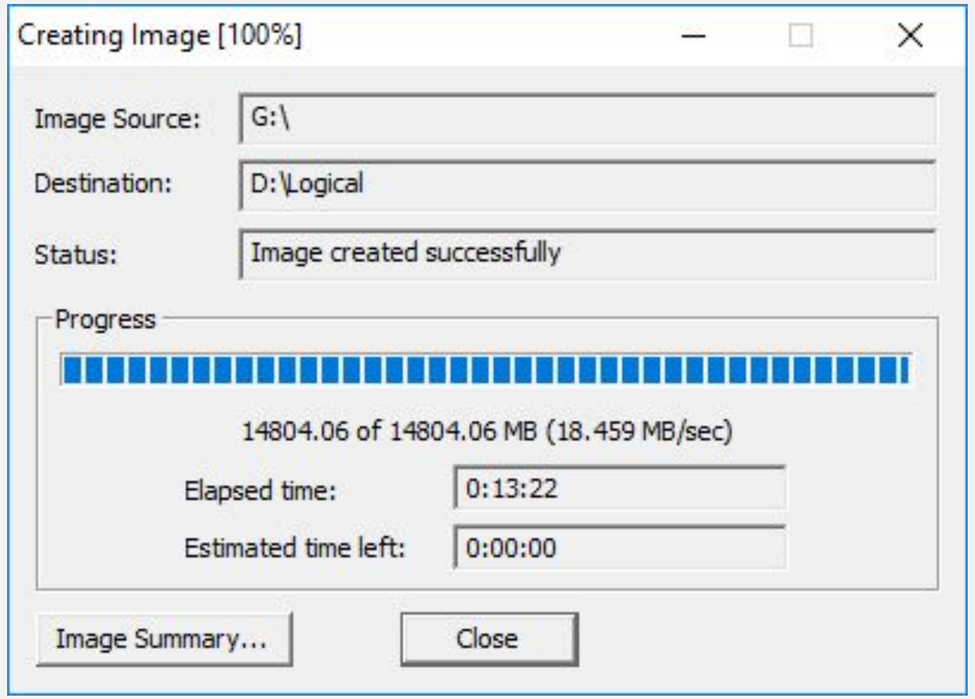


Логические диски

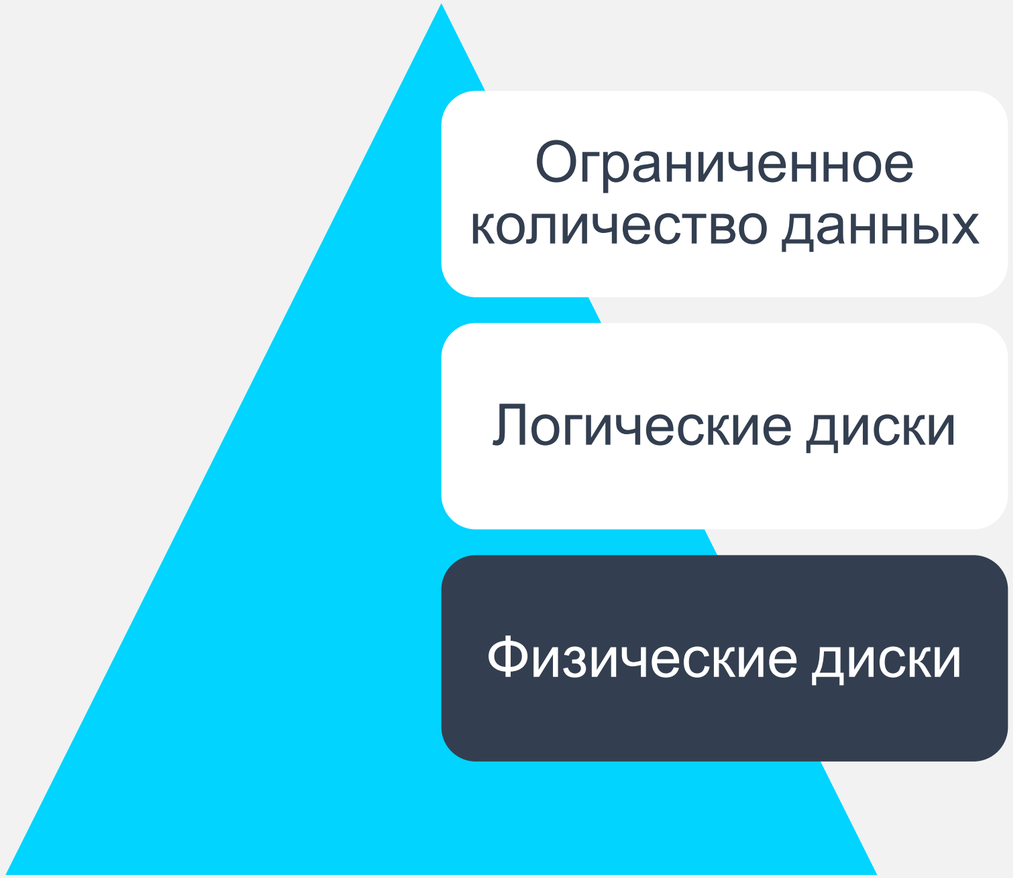


Практика: Создание Копии логического диска

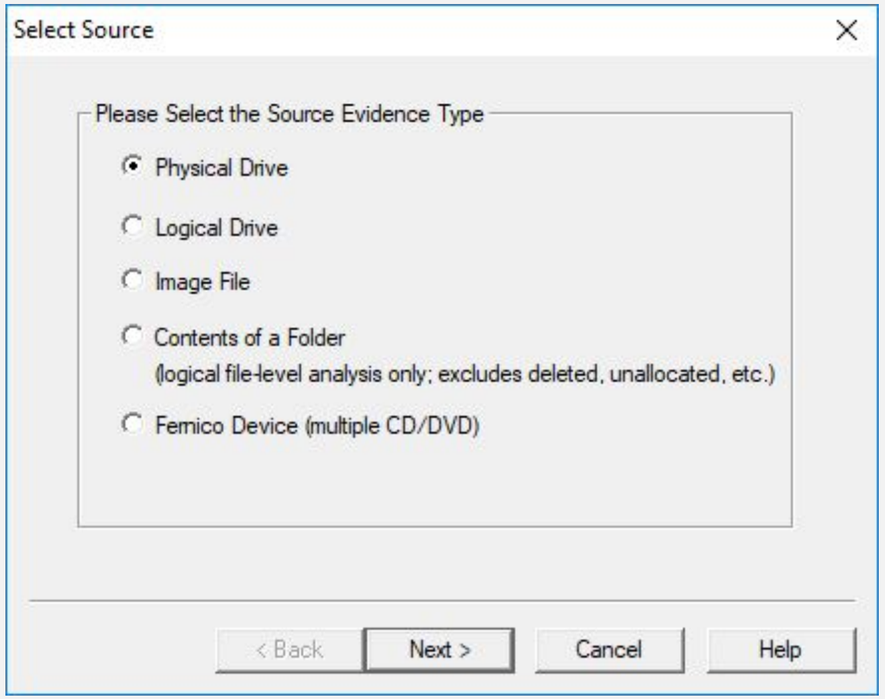


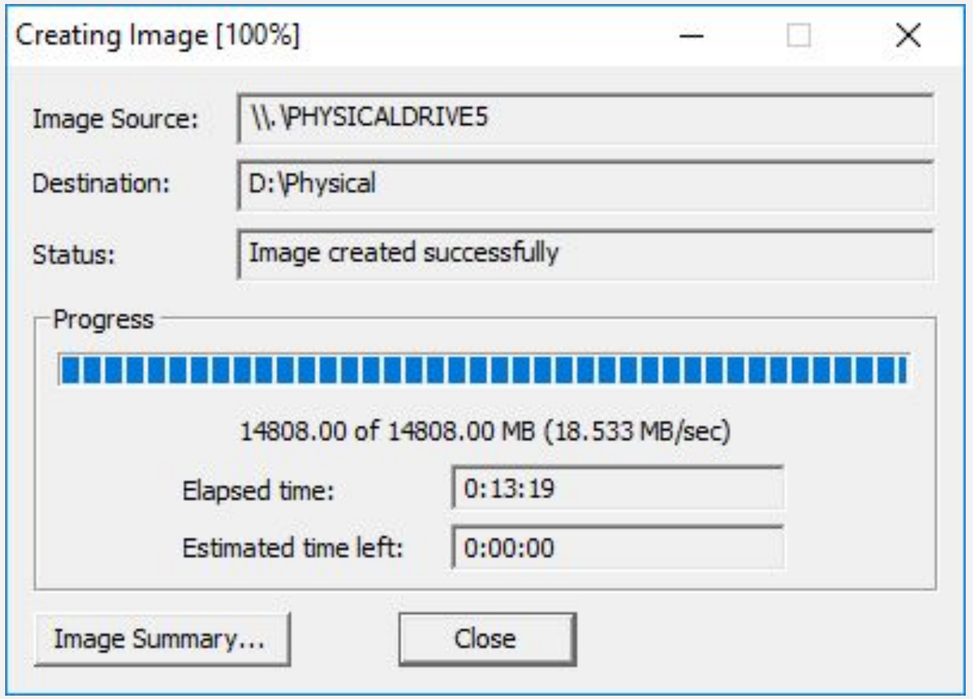


Физические диски

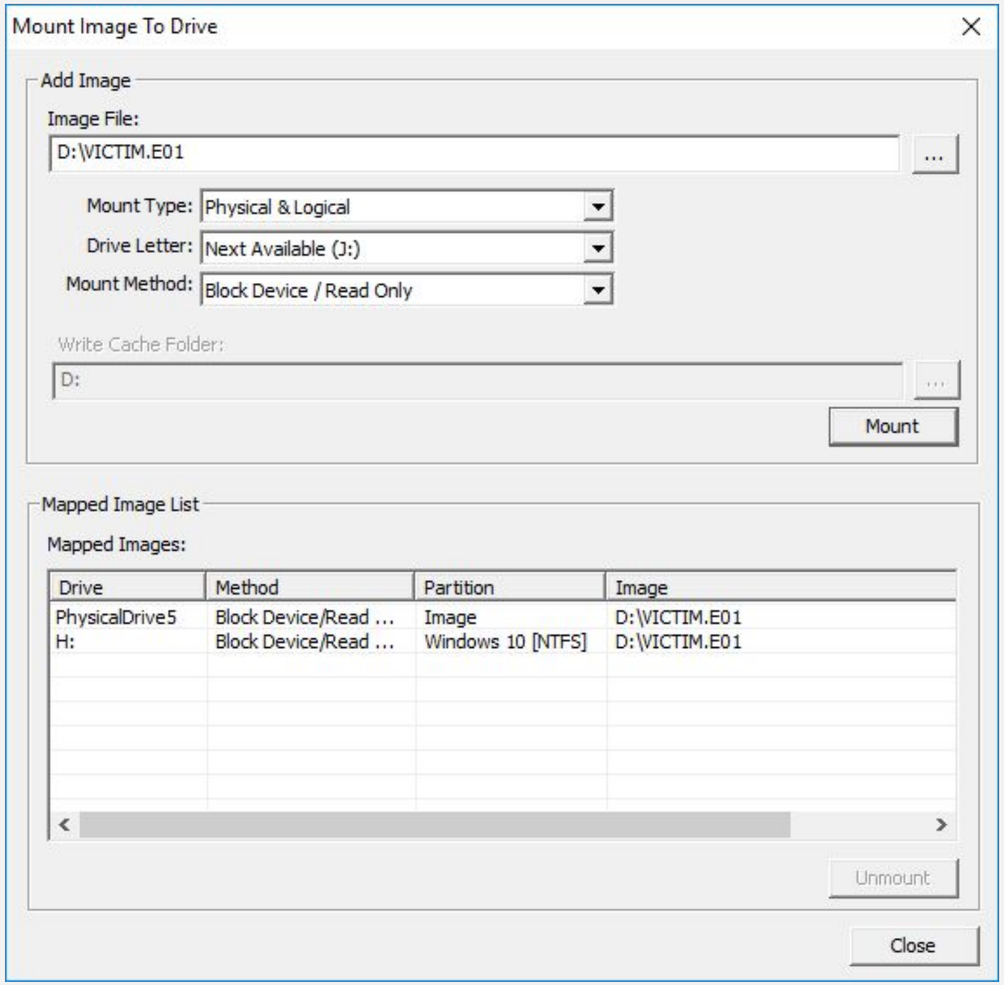


Практика: Создание Копии физического диска





Практика: Монтирование копий дисков



Контрольные суммы

MD5

- 27304b246c7d5b4e149124d5f93c5b01

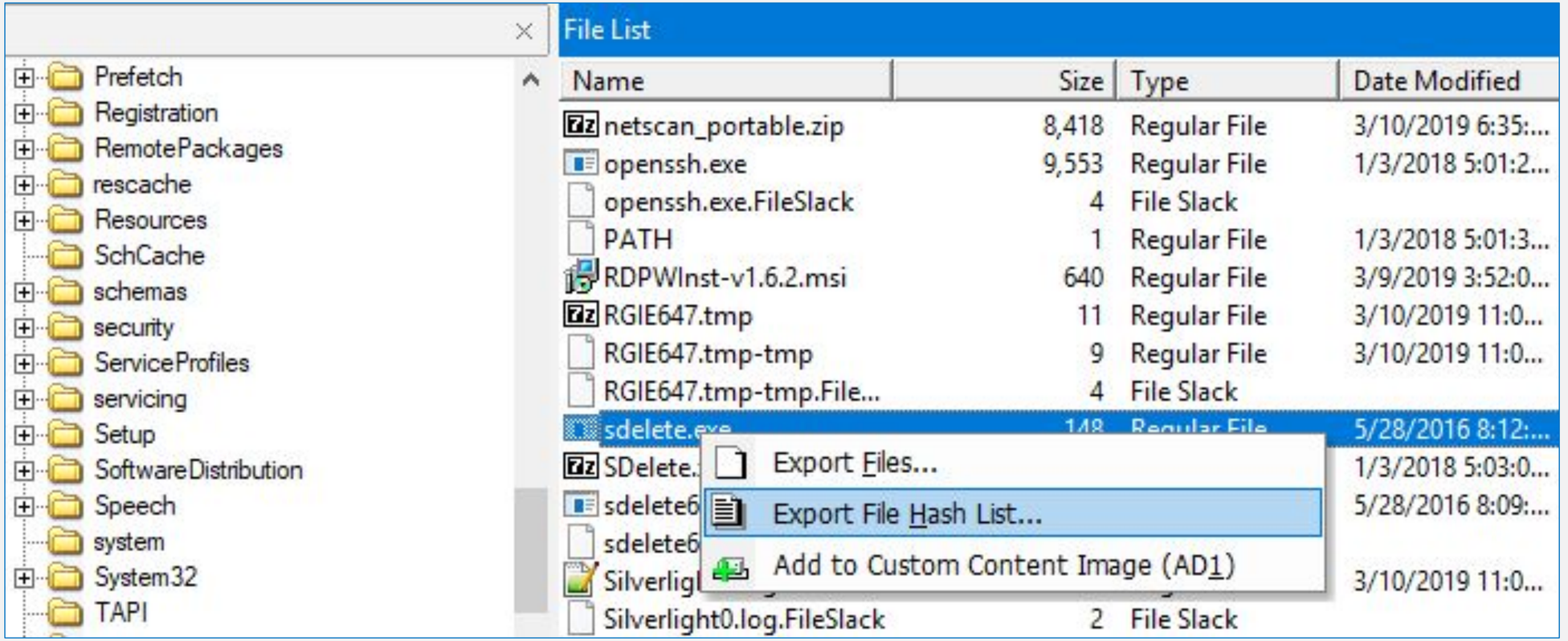
SHA1

- e50d9e3bd91908e13a26b3e23edeaf577fb3a095

SHA256

- 3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

Практика: подсчет контрольной суммы файла



YARA-ПРАВИЛА

```
rule ИмяПравила
{
    meta:
        description = “краткое описание правила”
    strings:
        $a = “уникальная строка”
        $b = “еще одна уникальная строка”
    condition:
        $a or $b
}
```

Управляющие последовательности

\”	двойные кавычки
\\	обратная косая черта
\t	горизонтальная табуляция
\n	новая строка
\xdd	любой байт в шестнадцатеричном представлении

Модификаторы

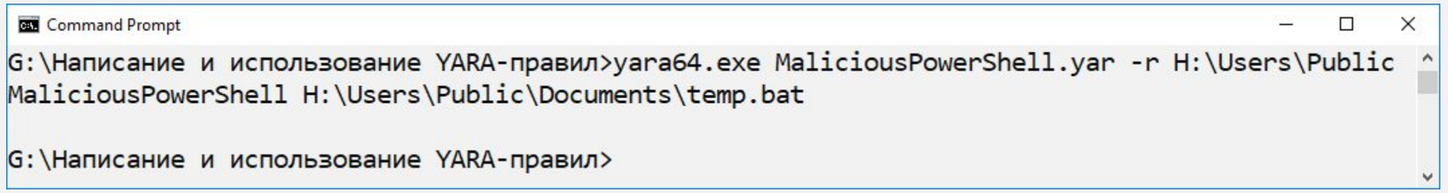
nocase	искать строку вне зависимости от регистра
wide	искать строку, закодированную широкими символами
fullword	Обнаруживать строку, только если она не окружена буквенно-цифровыми символами

Операторы

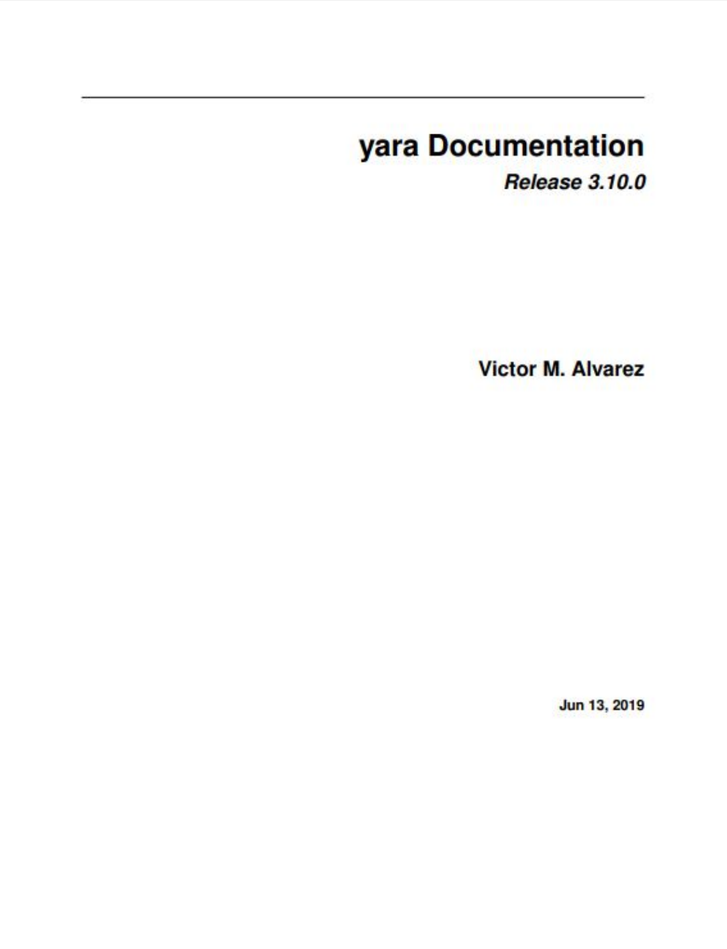
Логические	AND, OR, NOT
Сравнения	>=, <=, <, >, ==, !=
Арифметические	+, -, *, \, %
Битовые	&, |, <<, >>, ~, ^

Практика: Написание и использование YARA-правил

```
rule MaliciousPowerShell {
    meta:
        description = "Detects malicious PowerShell"
    strings:
        $p = "powershell" nocase
        $1 = "-nop" nocase
        $2 = "-w hidden" nocase
    condition:
        $p and ($1 or $2)
}
```



Больше информации о YARA-Правилах



yara Documentation

Release 3.10.0

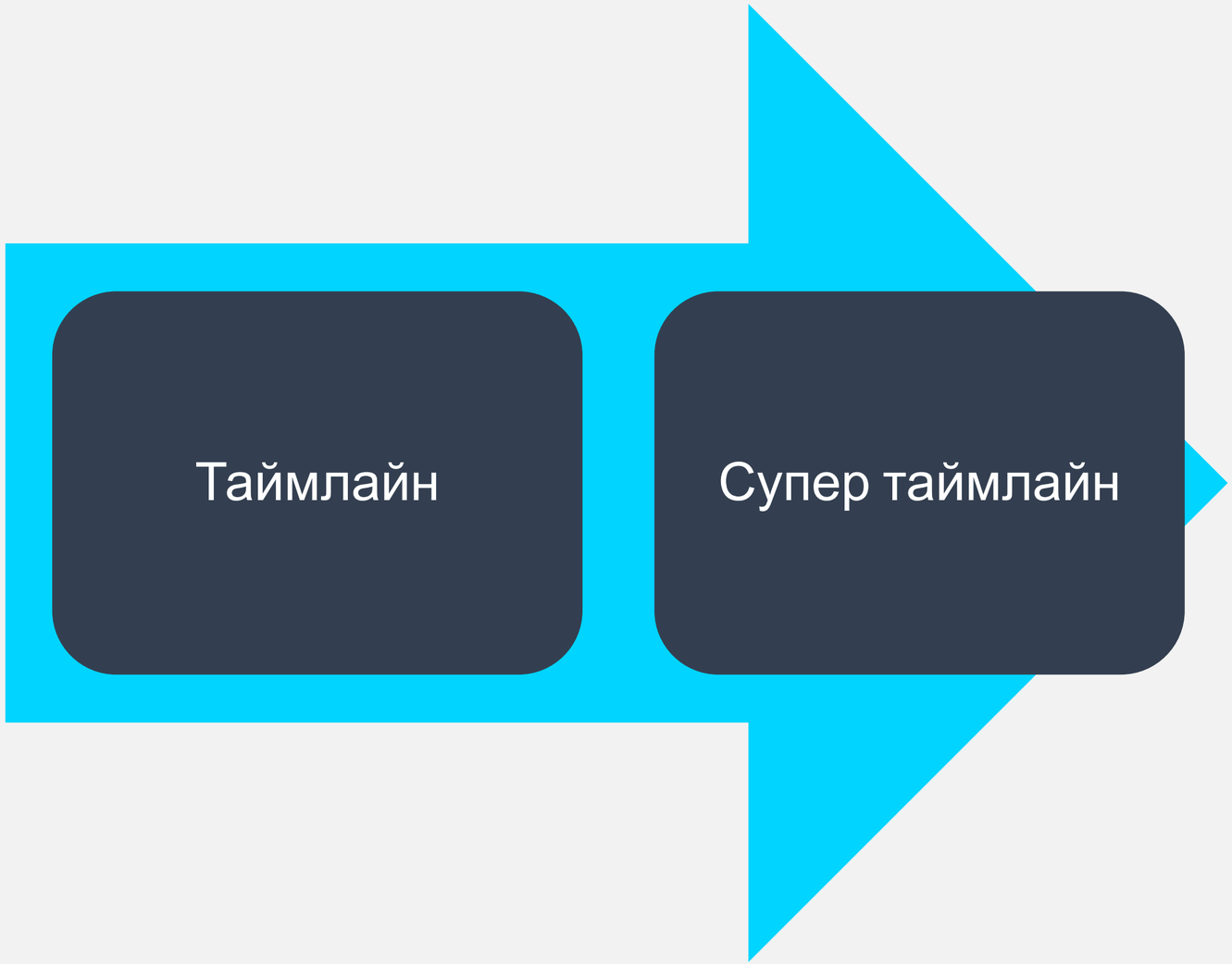
Victor M. Alvarez

Jun 13, 2019

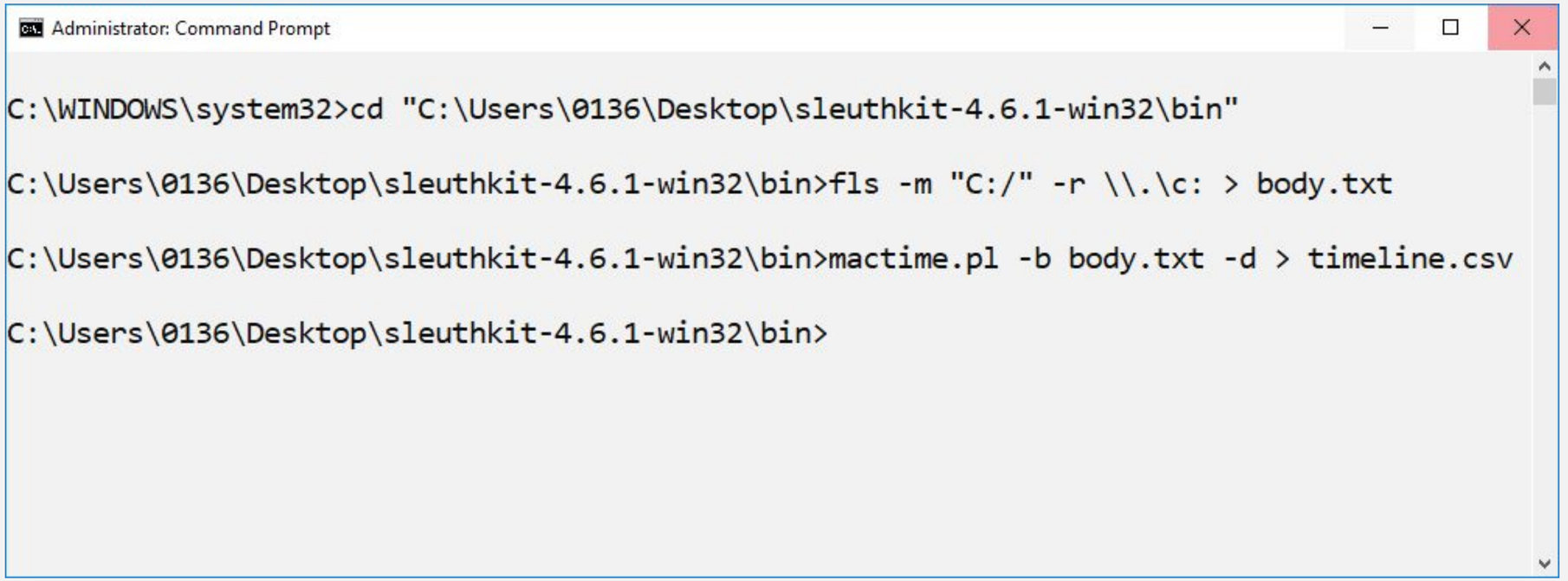
Официальная документация YARA:

https://buildmedia.readthedocs.org/media/pdf/yara/latest/yara.pdf

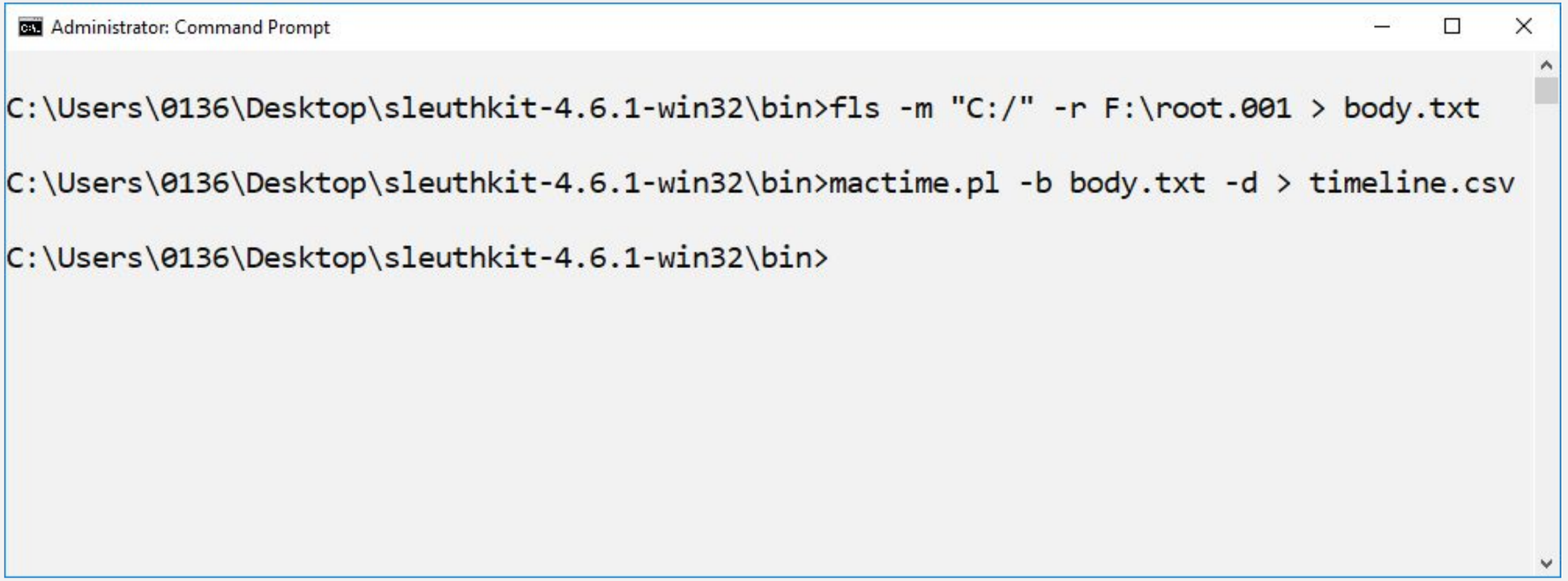
Таймлайны



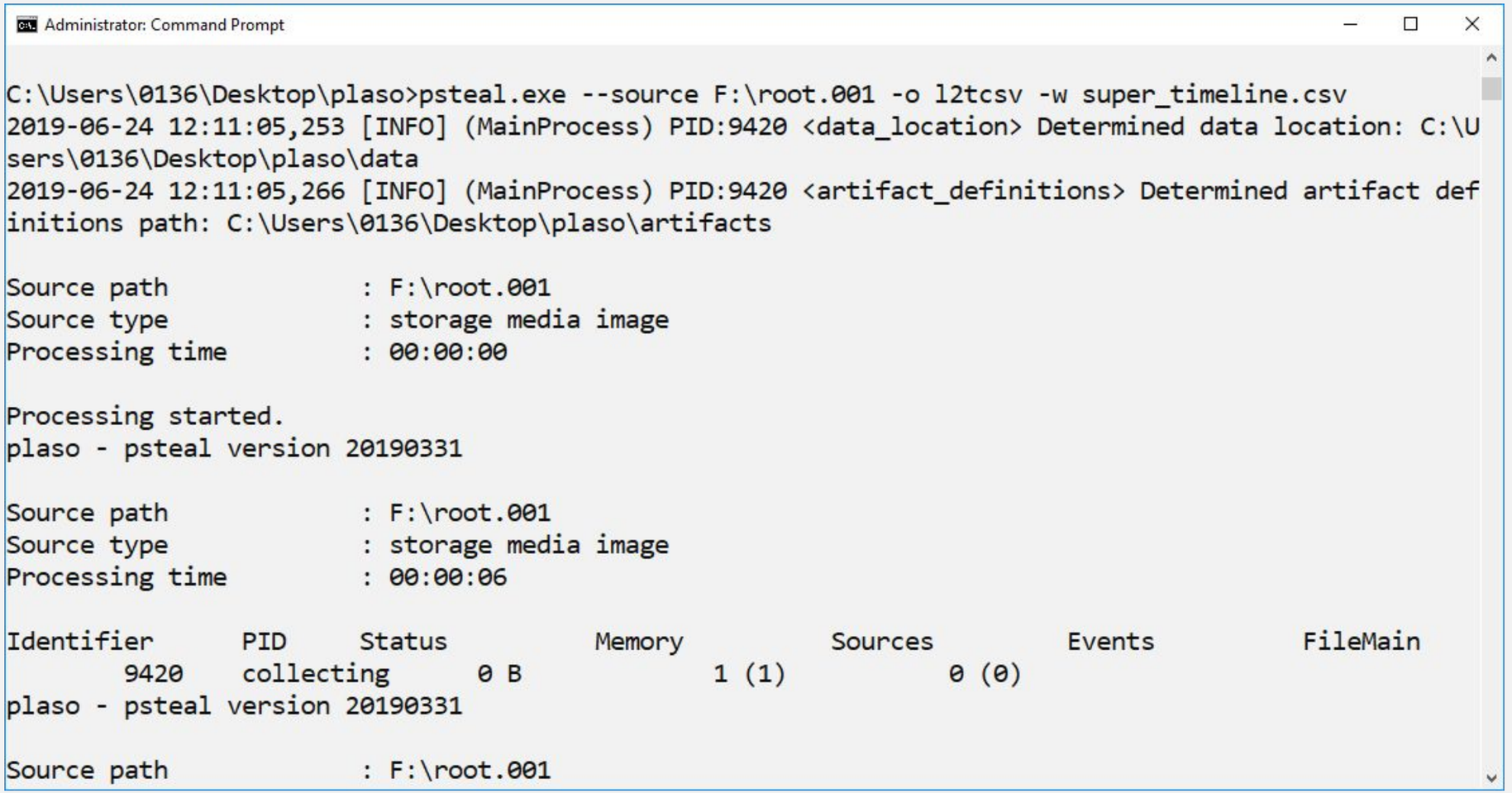
Практика: создание таймлайна на «живой» системе



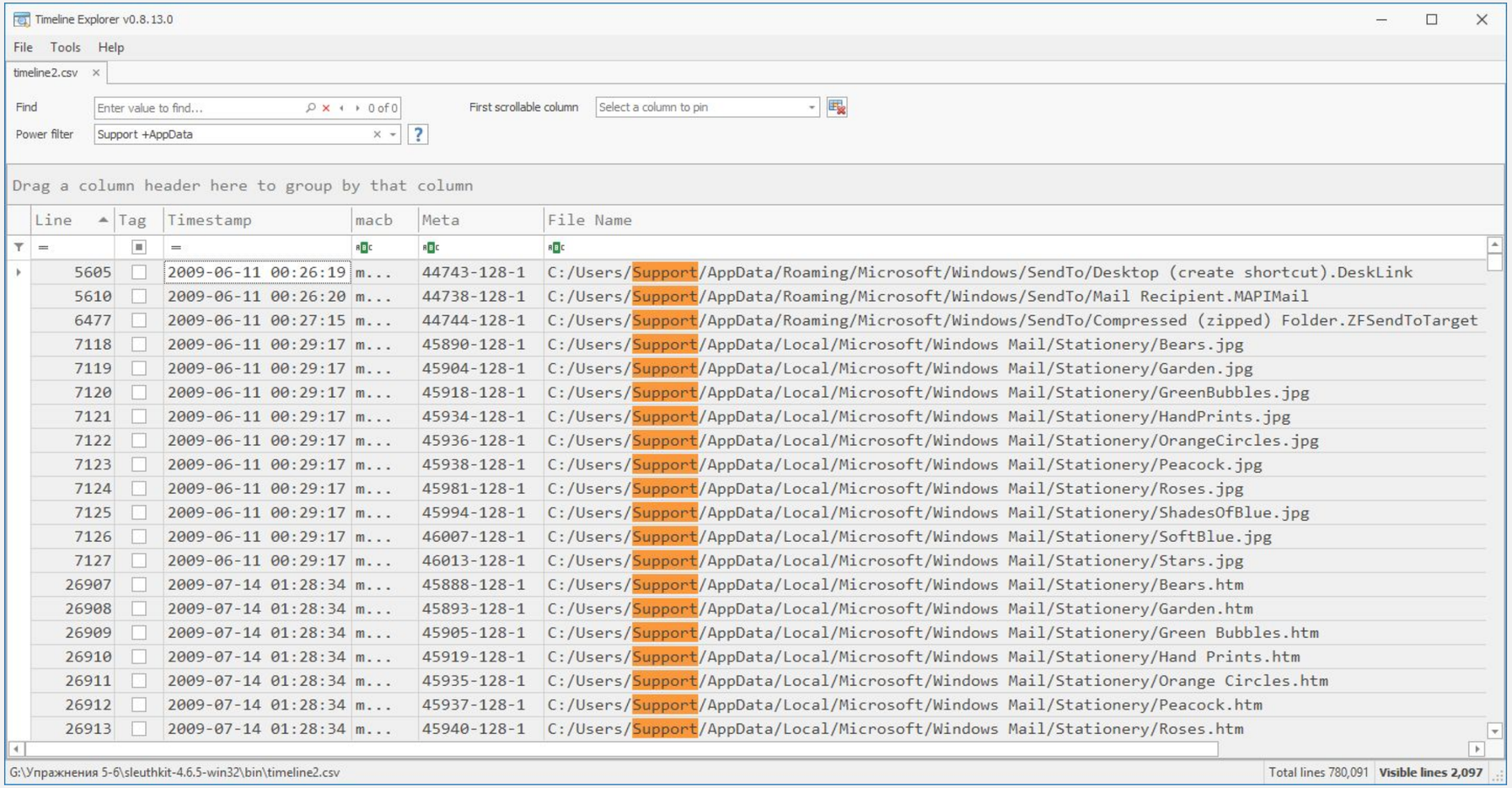
Практика: создание таймлайна с использованием копии диска



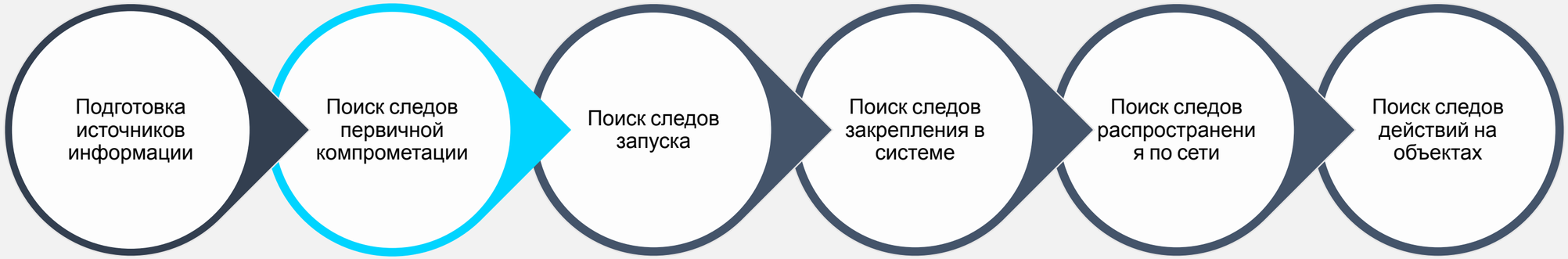
Практика: создание супер таймлайна



Практика: Просмотр таймлайнов



Поиск Следов первичной компрометации



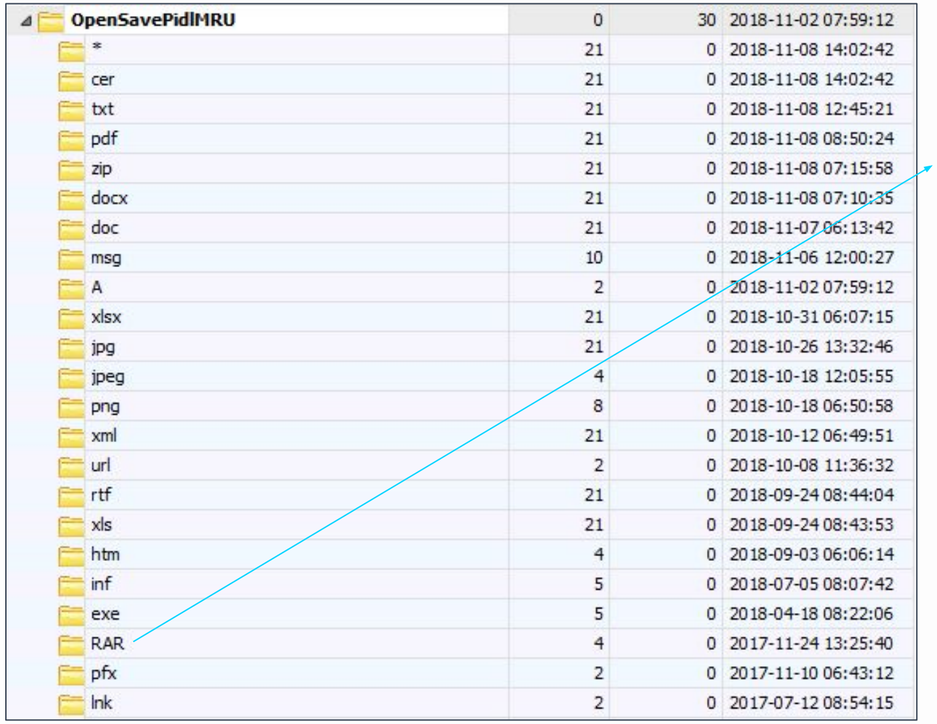
Электронная почта

вредоносных
программ
Распространяются
средствами
Электронной почты *

*Verizon Data Breach Investigations Report 2019

Следы открытия файлов: OPEN/SAVE MRU

NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU



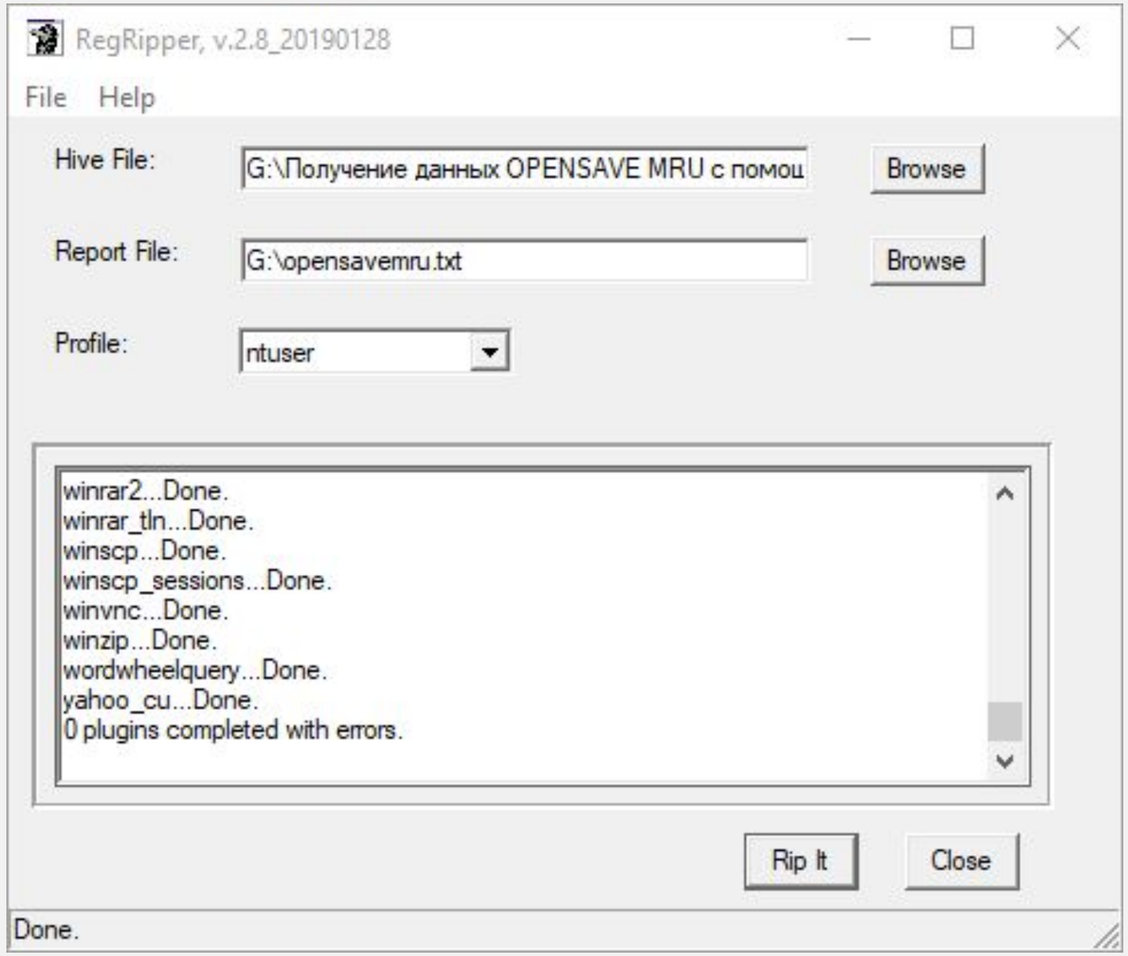
OpenSavePidlMRU	0	30	2018-11-02 07:59:12
*	21	0	2018-11-08 14:02:42
cer	21	0	2018-11-08 14:02:42
txt	21	0	2018-11-08 12:45:21
pdf	21	0	2018-11-08 08:50:24
zip	21	0	2018-11-08 07:15:58
docx	21	0	2018-11-08 07:10:35
doc	21	0	2018-11-07 06:13:42
msg	10	0	2018-11-06 12:00:27
A	2	0	2018-11-02 07:59:12
xlsx	21	0	2018-10-31 06:07:15
jpg	21	0	2018-10-26 13:32:46
jpeg	4	0	2018-10-18 12:05:55
png	8	0	2018-10-18 06:50:58
xml	21	0	2018-10-12 06:49:51
url	2	0	2018-10-08 11:36:32
rtf	21	0	2018-09-24 08:44:04
xls	21	0	2018-09-24 08:43:53
htm	4	0	2018-09-03 06:06:14
inf	5	0	2018-07-05 08:07:42
exe	5	0	2018-04-18 08:22:06
RAR	4	0	2017-11-24 13:25:40
pfx	2	0	2017-11-10 06:43:12
lnk	2	0	2017-07-12 08:54:15

Value Name	Value Type	Data	Value Slack
0	RegBinary	14-00-1F-50-E0-4F-D0-20-EA-3A-69-10-A2-D8-08-00-2B-30-...	00-6A-00
MRUListEx	RegBinary	02-00-00-00-01-00-00-00-00-00-00-00-FF-FF-FF-FF	37-43-34-38
1	RegBinary	14-00-1F-50-E0-4F-D0-20-EA-3A-69-10-A2-D8-08-00-2B-30-...	00-00-00
2	RegBinary	14-00-1F-50-E0-4F-D0-20-EA-3A-69-10-A2-D8-08-00-2B-30-...	00

OpenSavePidlMRU\RAR
LastWrite Time: Fri Feb 15 13:25:40 2019
Note: All value names are listed in MRUListEx order.

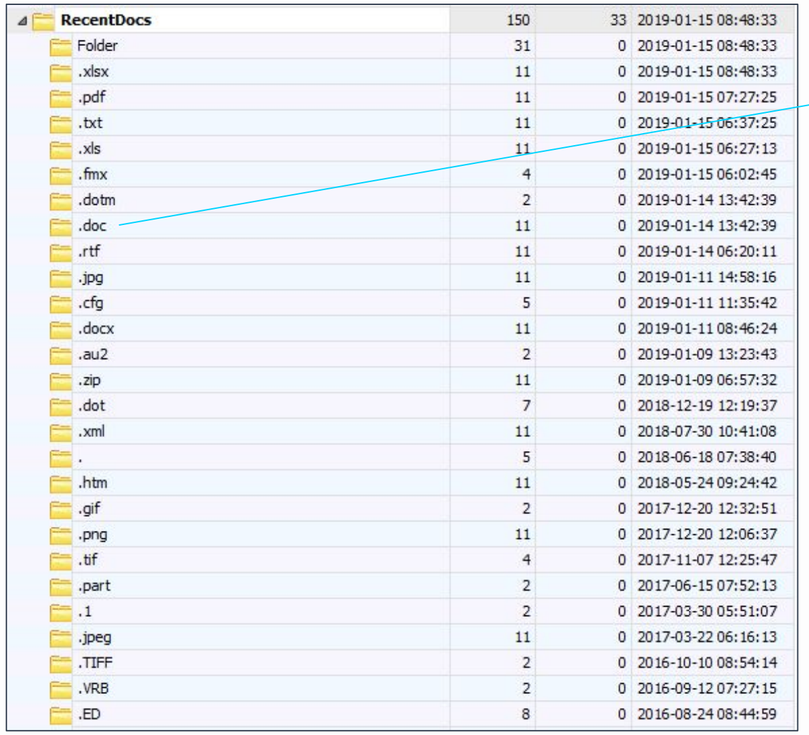
My Computer\D:\Downloads\malware.rar
My Computer\D:\Downloads\secrets.rar
My Computer\D:\Downloads\not_a_malware.rar

Практика: Получение данных OPEN/SAVE MRU



Следы открытия файлов: RECENTDOCS

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



RecentDocs	150	33	2019-01-15 08:48:33
Folder	31	0	2019-01-15 08:48:33
.xlsx	11	0	2019-01-15 08:48:33
.pdf	11	0	2019-01-15 07:27:25
.txt	11	0	2019-01-15 06:37:25
.xls	11	0	2019-01-15 06:27:13
.fmx	4	0	2019-01-15 06:02:45
.dotm	2	0	2019-01-14 13:42:39
.doc	11	0	2019-01-14 13:42:39
.rtf	11	0	2019-01-14 06:20:11
.jpg	11	0	2019-01-11 14:58:16
.cfg	5	0	2019-01-11 11:35:42
.docx	11	0	2019-01-11 08:46:24
.au2	2	0	2019-01-09 13:23:43
.zip	11	0	2019-01-09 06:57:32
.dot	7	0	2018-12-19 12:19:37
.xml	11	0	2018-07-30 10:41:08
.	5	0	2018-06-18 07:38:40
.htm	11	0	2018-05-24 09:24:42
.gif	2	0	2017-12-20 12:32:51
.png	11	0	2017-12-20 12:06:37
.tif	4	0	2017-11-07 12:25:47
.part	2	0	2017-06-15 07:52:13
.1	2	0	2017-03-30 05:51:07
.jpeg	11	0	2017-03-22 06:16:13
.TIFF	2	0	2016-10-10 08:54:14
.VRB	2	0	2016-09-12 07:27:15
.ED	8	0	2016-08-24 08:44:59

LastWrite Time Mon Jan 14 13:42:39 2018 (UTC)

MRUListEx = 7,0,5,6,8,4,3,2,9,1

7 = Downloader.doc

0 = Документ Microsoft Word (2).doc

5 = Документ Microsoft Word (3).doc

6 = Invoice.doc

8 = Предложение.doc

4 = CVE-2018-0802.doc

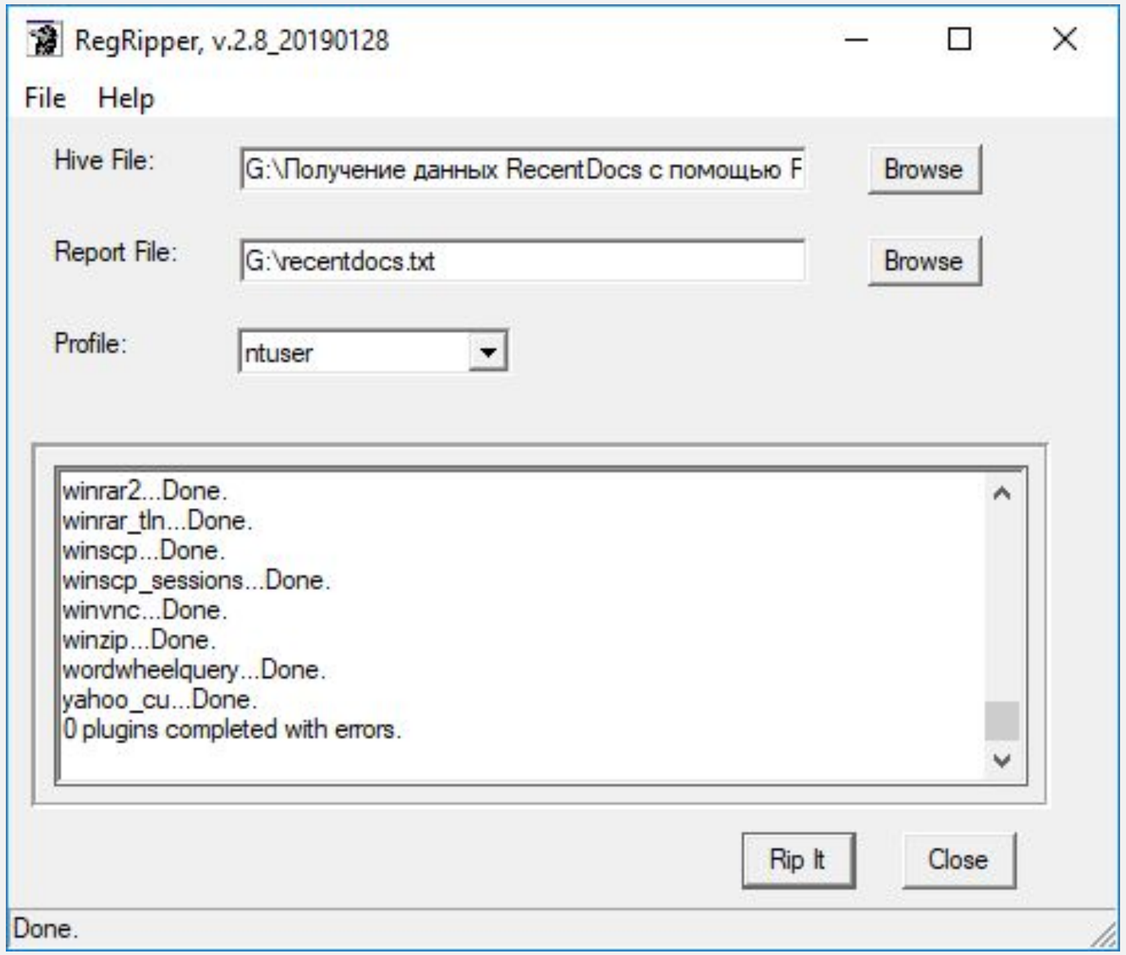
3 = VBA.doc

2 = Im_Your_Weapon.doc

9 = Not_so_safe.doc

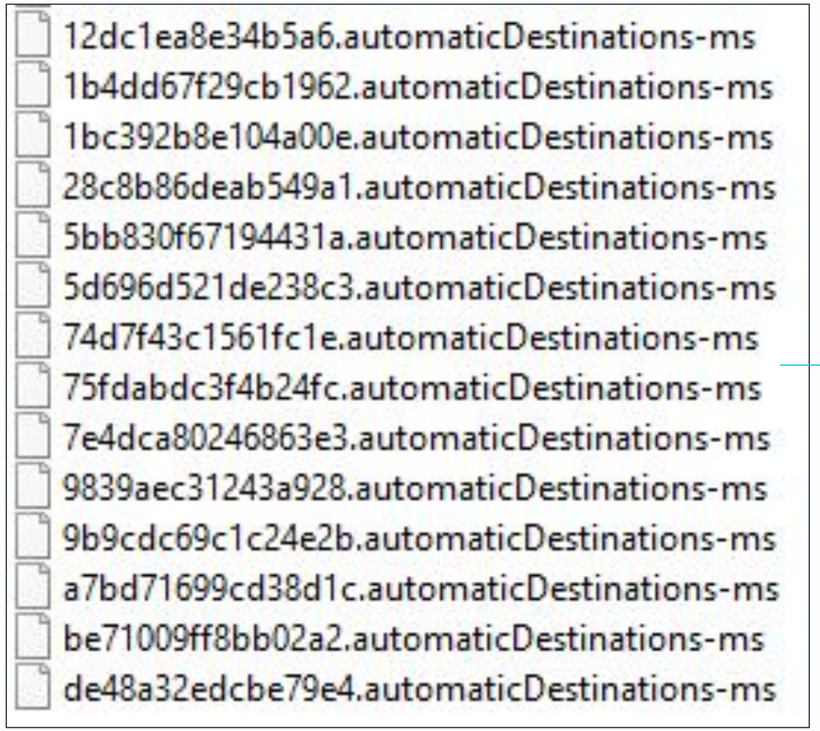
1 = Malicious.doc

Практика: Получение данных RECENTDOCS



Следы открытия файлов: JUMP LISTS

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

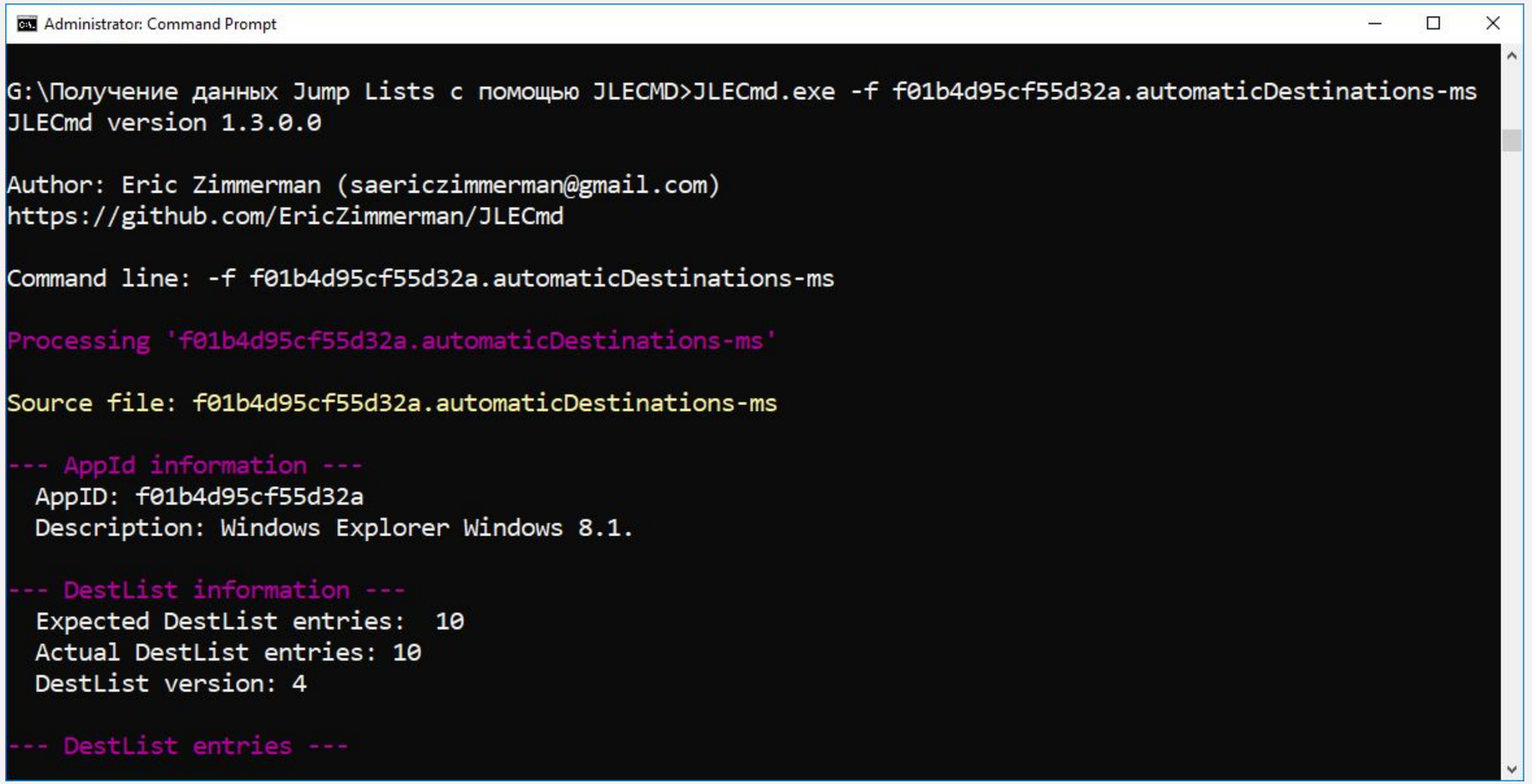


Entry #: 417
MRU: 0
Path: C:\Users\User\Downloads\not_malicious.pdf
Pinned: False
Created on: 2019-02-07 02:24:02
Last modified: 2019-02-06 15:27:03
Hostname: I_AM_PROTECTED
Mac Address: 08:00:27:08:72:ce

--- Lnk information ---

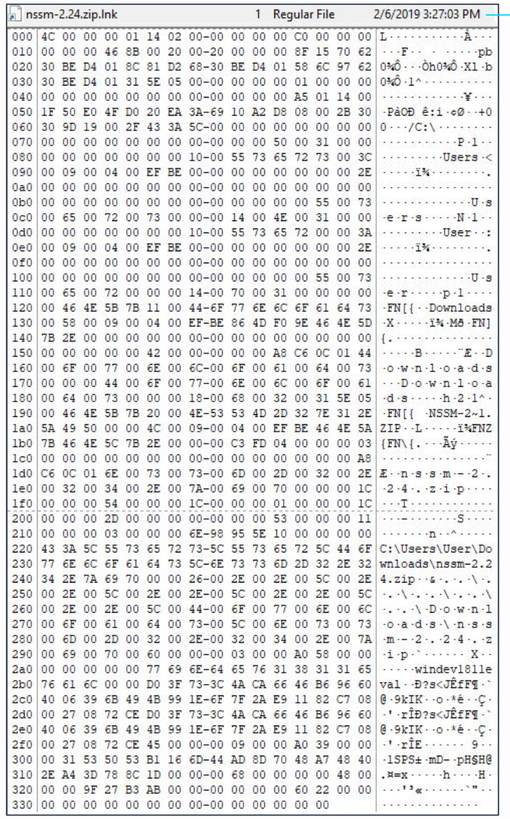
Absolute path: My Computer\C:\Users\User\Downloads\not_malicious.pdf

Практика: Получение данных JUMP LISTS



Следы открытия файлов: SHORTCUTS (LNK)

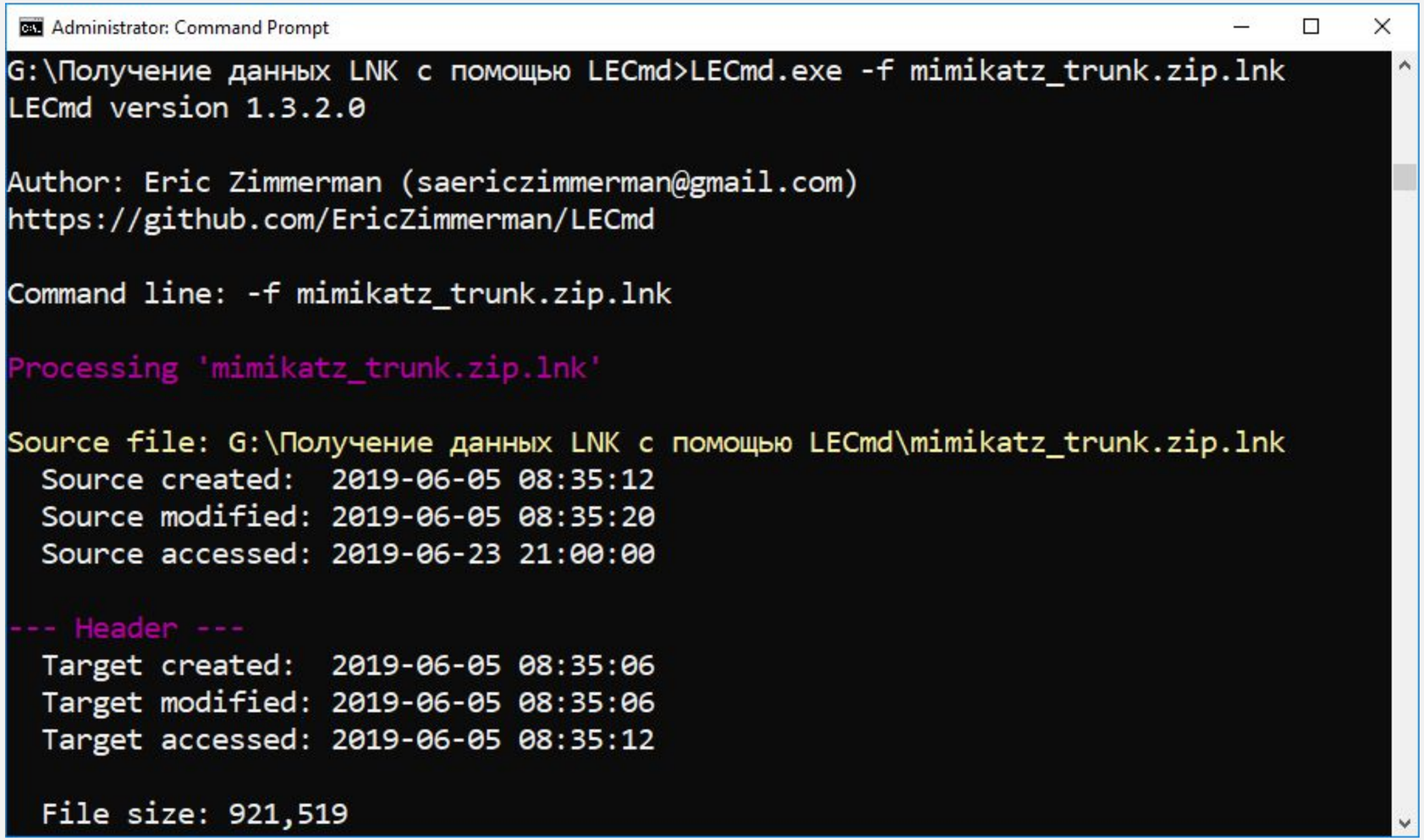
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\



…
Source file: D:\Temp\nssm-2.24.zip.lnk
  Source created: 2019-02-06 15:27:03
  Source modified: 2019-02-06 15:27:03
  Source accessed: 2019-02-06 15:27:03

--- Header ---
  Target created: 2019-02-06 15:26:51
  Target modified: 2019-02-06 15:26:52
  Target accessed: 2019-02-06 15:27:02
…
>>Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 5E95986E
  Label: (No label)
  Local path: C:\Users\User\Downloads\nssm-2.24.zip
…

Практика: Получение данных LNK



ВЕБ-ресурсы

вредоносных
[redacted]ограмм
Распространяются
средствами [redacted]*
Интернет-пространства

*Verizon Data Breach Investigations Report 2019

Следы использования веб-браузеров: EDGE/IE

C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

WebCacheV01.dat 47,104 Regular File

0000000	88	1D	D9	8C	EF	CD	AB	89-20
0000010	B2	B4	00	00	00	00	00	00-E6
0000020	0C	76	9F	04	00	00	00	00-00
0000030	00	00	00	00	03	00	00	00-B6
0000040	28	02	0E	0D	02	77	39	0E-01
0000050	68	02	40	00	25	00	00	00-28
0000060	B6	02	1B	00	26	00	00	00-01
0000070	1C	38	13	06	0C	76	0F	00-00
0000080	00	00	00	00	00	00	00	00-00
0000090	00	00	00	00	00	00	00	00-00
00000a0	00	00	00	00	00	00	00	00-00
00000b0	00	00	00	00	00	00	00	00-00
00000c0	00	00	00	00	00	00	00	00-00
00000d0	00	00	00	00	CF	00	00	00-0A
00000e0	63	45	00	00	00	00	00	00-14
00000f0	00	00	00	00	00	00	00	00-00
0000100	00	00	00	00	00	00	00	00-00
0000110	00	00	00	00	00	00	00	00-00

Url

Visited: User@about:blank
Visited: User@https://www.bing.com/search?q=netscan&form=EDGEAR&qs=PF
Visited: User@https://www.bing.com/search?q=netscan&form=EDGEAR&qs=PF
Visited: User@https://www.softperfect.com/download/
Visited: User@https://www.softperfect.com/download/files/netscan_portable.zip
Visited: User@http://nssm.cc/
Visited: User@http://nssm.cc/description
Visited: User@http://nssm.cc/download
Visited: User@http://nssm.cc/release/nssm-2.24.zip

Практика: Анализ данных веб-браузеров EDGE и IE

Containers [Table ID = 12, 14 Columns]

ContainerId	SetId	Flags	Size	Limit	LastScavengeTime	EntryMaxAge	LastAccessTime	Name	PartitionId
1	0	68	0	1024	0	0	132041938405063950	History	M
2	0	79	687422	346030080	0	0	132041938387842229	Content	M
3	1	15	0	52428800	0	0	132041940829214498	Content	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723
4	1	15	445731	52428800	0	0	132041938186128237	Content	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
5	1	1	13	1024000	0	0	132041938188620676	DOMStore	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
6	0	68	0	1024	0	0	132041945344830648	History	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194
7	0	113	0	1024	0	0	132041938196757981	MicrosoftEdge_DNTException	M
8	1	0	0	1024	0	0	132041942147789353	BackgroundTransferApi	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
9	1	0	0	1024	0	0	132041942161862250	BackgroundTransferApiGroup	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
11	1	0	0	1024	0	0	132041940842493188	BackgroundTransferApi	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723
12	1	15	0	52428800	0	0	132041940116243763	Content	S-1-15-2-1609473798-1231923017-684268153-4268514328-882773646-2760585773-1760938157
13	0	64	0	1024	0	0	132041938405811706	MSHist012019060520190606	M
14	0	79	0	346030080	0	0	132041945175615719	Content	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194
15	0	80	0	1024	0	0	132041945175767257	MicrosoftEdge_iecompat	M
16	0	80	0	1024	0	0	132041945175928384	MicrosoftEdge_iecompatua	M
17	0	81	0	1024	0	0	132041945176552500	MicrosoftEdge_EmieSiteList	M
18	0	81	0	1024	0	0	132041945176865404	MicrosoftEdge_EmieUserList	M
19	0	79	32270227	346030080	0	0	132041945253111624	Content	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-4256926629-1688279915-2739229046-3928706915
20	0	79	4192159	346030080	0	0	132041945262799428	Content	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-3513710562-3729412521-1863153555-1462103995
21	0	65	26	1024000	0	0	132041945341077475	DOMStore	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-3513710562-3729412521-1863153555-1462103995
22	0	65	260	1024000	0	0	132041945355764710	DOMStore	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-4256926629-1688279915-2739229046-3928706915
23	0	68	0	1024	0	0	132041945359988052	History	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-3513710562-3729412521-1863153555-1462103995
24	0	68	0	1024	0	0	132041945361234154	History	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-4256926629-1688279915-2739229046-3928706915
25	0	64	0	1024	0	0	132041945616410141	iedownload	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194
26	0	68	0	1024	0	0	132041945754394979	History	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-2385269614-3243675-834220592-3047885450
27	0	113	0	1024	0	0	132041945866269425	MicrosoftEdge_ieflipahead	M
28	1	79	0	346030080	0	0	132041950228689219	Content	S-1-15-2-930279079-3258969966-1203931420-3379063298-1496040207-3203565093-3038441310
29	1	1	13	1024000	0	0	132041950232733017	DOMStore	S-1-15-2-930279079-3258969966-1203931420-3379063298-1496040207-3203565093-3038441310
30	1	15	0	52428800	0	0	132041950903834535	Content	S-1-15-2-1726375552-1729233799-74693324-3851689839-2151781990-3623637752-3611872497
31	1	15	0	52428800	0	0	132041963504265335	Content	S-1-15-2-2246530975-808720366-1776470054-230329187-4153223113-3550430174-4193313734
32	0	192	0	1024	0	0	132041978055863606	Cookies	M
33	1	15	0	52428800	0	0	132042087840957580	Content	S-1-15-2-2226957697-3030467180-2301525-4248967783-2024719031-2325529081-2915787518

Следы использования веб-браузеров: FIREFOX

C:\%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles*.default\

places.sqlite 5,120 Regular File

000000	53	51	4C	69	74	65	20	66-6F	72	6D	61	74	20	33	00
000010	80	00	02	02	00	40	20	20-00	00	00	03	00	00	00	25
000020	00	00	00	00	00	00	00	00-00	00	00	1F	00	00	00	04
000030	00	00	00	00	00	00	00	00-00	00	00	01	00	00	00	34
000040	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
000050	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	03
000060	00	2E	09	28	0D	7F	F8	00-24	6A	C8	00	7F	0C	7F	C1
000070	7D	24	7C	5A	7B	60	7C	19-79	F6	79	0D	79	AB	78	33
000080	78	D4	77	E1	77	07	77	9A-75	DD	74	A2	74	38	73	EB
000090	73	7C	73	15	72	A9	72	3A-71	BA	71	42	70	D2	70	38
0000a0	6F	B2	6F	2C	6E	B9	6E	3A-6D	A6	6D	28	6C	A3	6C	01
0000b0	6B	6F	6A	C8	00	00	00	00-00	00	00	00	00	00	00	00
0000c0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
0000d0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
0000e0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
0000f0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00

url

Filter

https://support.mozilla.org/ru/products/firefox
https://support.mozilla.org/ru/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=f...
https://www.mozilla.org/ru/contribute/
https://www.mozilla.org/ru/about/
https://www.mozilla.org/ru/firefox/central/
https://yandex.ru/search?clid=2186621&text=network+scanner
https://yandex.ru/search/?clid=2186621&text=network+scanner&lr=213&redircnt=1553082105.1
https://yandex.ru/search/?clid=2186621&text=network%20scanner&lr=213&redircnt=15530821...
https://www.10-strike.ru/network-scanner/
https://www.10-strike.ru/network-scanner/download.shtml
https://www.10-strike.ru/network-scanner/network-scanner.exe

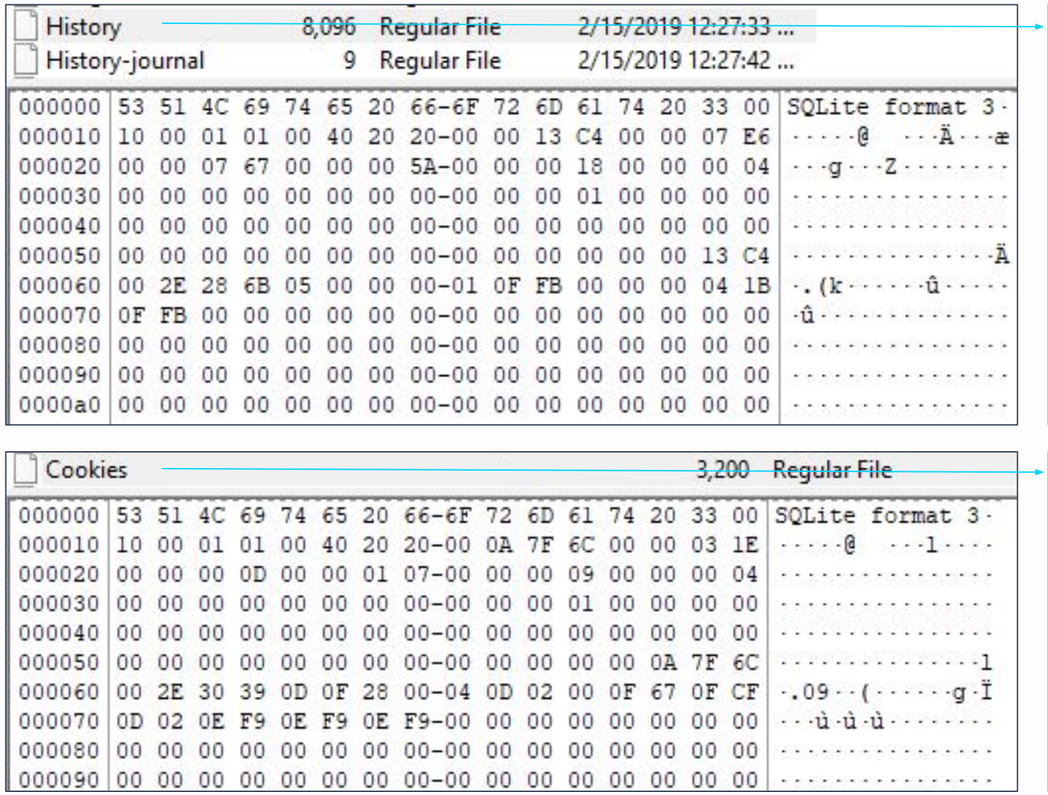
cookies.sqlite 512 Regular File

00000	53	51	4C	69	74	65	20	66-6F	72	6D	61	74	20	33	00
00010	80	00	02	02	00	40	20	20-00	00	00	05	00	00	00	04
00020	00	00	00	00	00	00	00	00-00	00	00	03	00	00	00	04
00030	00	00	00	00	00	00	00	00-00	00	00	01	00	00	00	09
00040	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
00050	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	05
00060	00	2E	09	28	0D	7F	F8	00-03	7D	A9	00	7E	1A	7F	C1

34	admetrica.ru		sync_cookie_ok	synced	.mc.admetric...
35	yandex.ru		yp	1555674107.s...	.yandex.ru
36	yandex.ru		sc_15530821...	network%20s...	.yandex.ru
37	10-strike.ru		_ym_uid	15530821146...	.10-strike.ru
38	10-strike.ru		_ym_d	1553082114	.10-strike.ru
39	10-strike.ru		_ym_isad	2	.10-strike.ru
42	10-strike.ru		_gat_gtag_UA...	1	.10-strike.ru

Следы использования веб-браузеров: CHROME

C:\%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\



History 8,096 Regular File 2/15/2019 12:27:33 ...
History-journal 9 Regular File 2/15/2019 12:27:42 ...

000000	53	51	4C	69	74	65	20	66-6F	72	6D	61	74	20	33	00
000010	10	00	01	01	00	40	20	20-00	00	13	C4	00	00	07	E6
000020	00	00	07	67	00	00	00	5A-00	00	00	18	00	00	00	04
000030	00	00	00	00	00	00	00	00-00	00	00	01	00	00	00	00
000040	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
000050	00	00	00	00	00	00	00	00-00	00	00	00	00	00	13	C4
000060	00	2E	28	6B	05	00	00	00-01	0F	FB	00	00	00	04	1B
000070	0F	FB	00	00	00	00	00	00-00	00	00	00	00	00	00	00
000080	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
000090	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
0000a0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00

22090	https://attack.mitre.org/techniques/enterprise/
22134	https://attack.mitre.org/groups/G0080/
22136	https://attack.mitre.org/techniques/T1076
22137	http://attack.mitre.org/techniques/T1076/
22138	https://attack.mitre.org/techniques/T1076/
22154	https://attack.mitre.org/techniques/T1072
22155	http://attack.mitre.org/techniques/T1072/
22156	https://attack.mitre.org/techniques/T1072/

Cookies 3,200 Regular File

000000	53	51	4C	69	74	65	20	66-6F	72	6D	61	74	20	33	00
000010	10	00	01	01	00	40	20	20-00	0A	7F	6C	00	00	03	1E
000020	00	00	00	0D	00	00	01	07-00	00	00	09	00	00	00	04
000030	00	00	00	00	00	00	00	00-00	00	00	01	00	00	00	00
000040	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
000050	00	00	00	00	00	00	00	00-00	00	00	00	00	0A	7F	6C
000060	00	2E	30	39	0D	0F	28	00-04	0D	02	00	0F	67	0F	CF
000070	0D	02	0E	F9	0E	F9	0E	F9-00	00	00	00	00	00	00	00
000080	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
000090	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00

13197541838068164	.live.com	logonLatency
13197369115538017	.live.com	wla42
13197541849088088	.live.com	xidseq
13197541907967016	.pippio.com	pxrc
13194456087418321	www.exabeam.com	DFTT_END_USER_PREV...
13197542825086313	www.gartner.com	TS01543fe9
13197542825086339	.gartner.com	TS016d2780

Практика: Анализ данных веб-браузеров FIREFOX и CHROME

GROUP-IB

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: moz_places

New Record | Delete Record

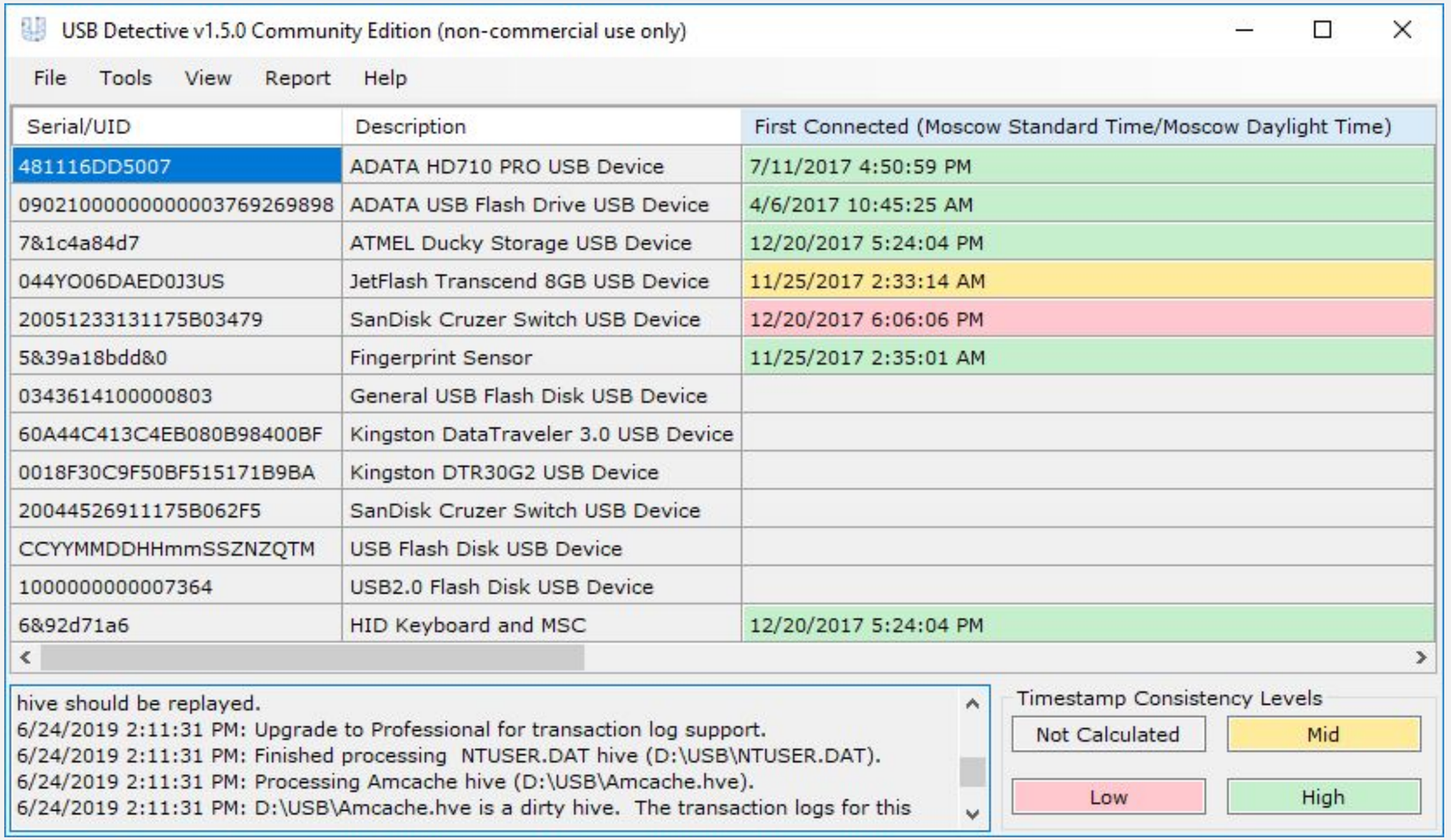
	id	url	title
	Filter	Filter	Filter
1	1	https://support.mozilla.org/en-US/products/firefox	NULL
2	2	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-browser&utm_medium=default-bookmarks&utm_campaign=customize	NULL
3	3	https://www.mozilla.org/en-US/contribute/	NULL
4	4	https://www.mozilla.org/en-US/about/	NULL
5	5	https://www.mozilla.org/en-US/firefox/central/	NULL
6	6	https://www.mozilla.org/privacy/firefox/	NULL
7	7	https://www.mozilla.org/en-US/privacy/firefox/	Firefox Privacy Notice — Mozilla
8	8	https://www.yandex.com/search?clid=2186621&text=psexec	NULL
9	9	https://www.yandex.ru/search/?clid=2186621&text=psexec&rdrnd=513010&lr=213&redircnt=1559725539.1	psexec — Яндекс: нашлось 5 тыс. рез...
10	10	https://docs.microsoft.com/en-us/sysinternals/downloads/psexec	PsExec - Windows Sysinternals | Micro...
11	11	https://download.sysinternals.com/files/PSTools.zip	PSTools.zip
12	12	http://sendspace.com/file/4c9k16	NULL
13	13	http://www.sendspace.com/file/4c9k16	NULL
14	14	https://www.sendspace.com/file/4c9k16	Download temp.zip from Sendspace.co...
15	15	https://www.sendspace.com/defaults/sendspace-pop.html	NULL
16	16	https://engine.spotscenered.info/link.engine?z=50323&guid=33be5d3b-88b1-40f2-86a2-1fd5ad5928dd	NULL
17	17	https://engine.spotscenered.info/Redirect.eng?MediaSegmentId=54898&dcid=1_ctx_27bb9e2d-4cef-4591-9eb3-db454dfeeb0c&vmId=00000000-0000-0000-0000-000000000000...	NULL
18	18	https://c2.olecktd.com/t/clk?id=AQrlVFV6J7U325ki0E0w3ik&s1=4060122d-4eee-4d76-85ce-68f1af896469&s2=12038	NULL
19	19	https://cl.untildogtop.com/t/clk?id=4k23BI60ALh7jZxHMkMgksg&s1=4060122d-4eee-4d76-85ce-68f1af896469&s2=12038&redirect-from=AQrlVFV6J7U325ki0E0w3ik&rcode=R02...	NULL
20	20	https://validationpro1.info/push_me_v8?test=30d6f864-90f8-4a97-8e31-29198537d72d&s2=12038	NULL
21	21	http://validationpro1.info/push_me_v8/?test=30d6f864-90f8-4a97-8e31-29198537d72d&s2=12038	NULL
22	22	https://validationpro1.info/push_me_v8/?test=30d6f864-90f8-4a97-8e31-29198537d72d&s2=12038	Push Me
23	23	https://fs12n4.sendspace.com/dl/5d1565ff9c8cf621b09bd47547717895/5cf78716382f75d7/4c9k16/temp.zip	temp.zip

USB-устройства

СЛЕДЫ Подключения USB-устройств

Реестр	Журналы
• SYSTEM • SOFTWARE • NTUSER.DAT • Amcache.hve	• Журналы событий (C:\Windows\System32\winevt\Logs) • Журналы Setup API (C:\Windows\INF)

Практика: Сбор информации о подключенных USB устройствах

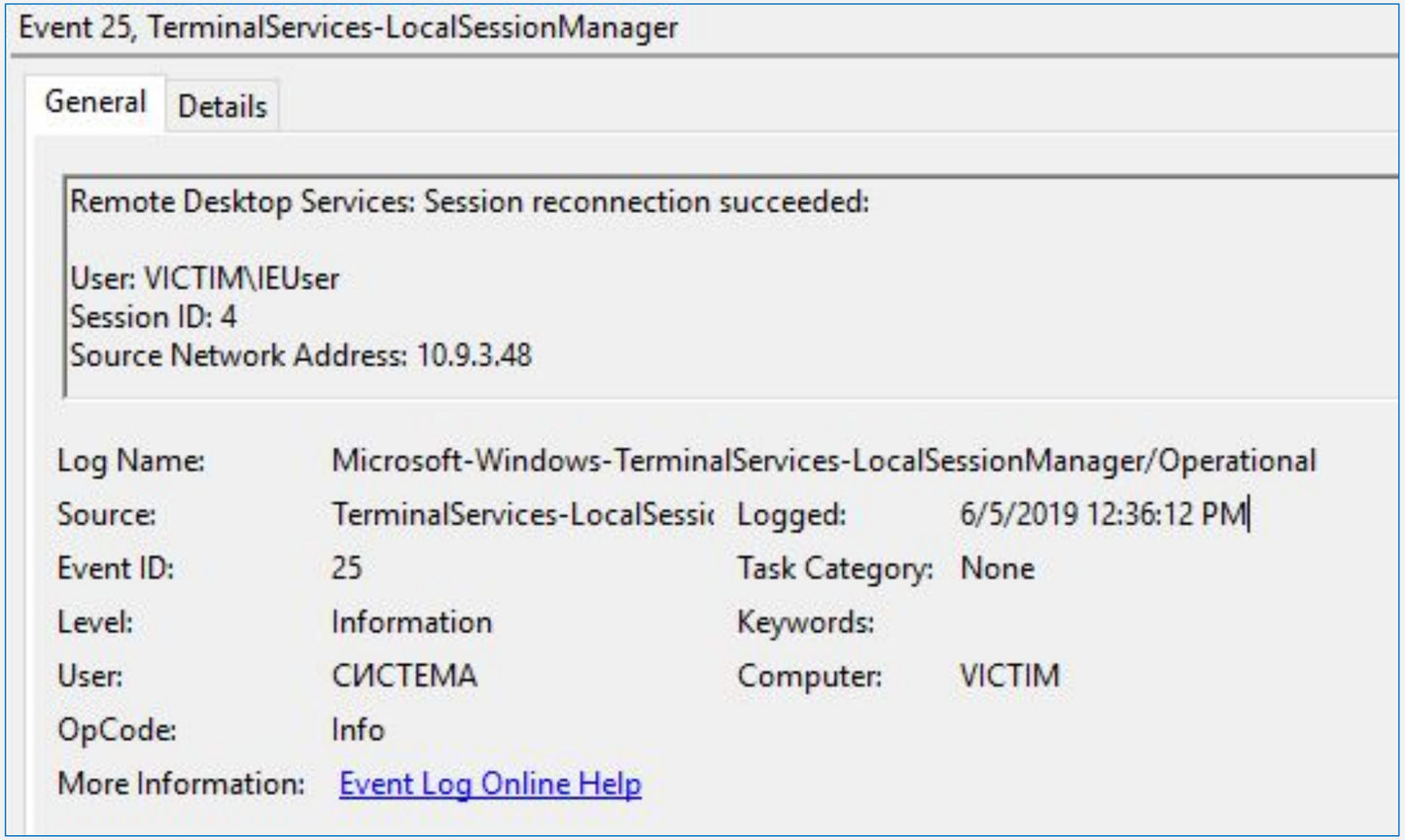


RDP BRUTE FORCE

Следы подключений по RDP: журналы событий

Event ID	Журнал	
Журналы событий	Security.evtx	ID 4624 ID 4625
	Microsoft-WindowsRemoteDesktopServicesRdpCoreTS%4Operational.evtx	ID 131 ID 98
	Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx	ID 1149
	Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	ID 21 ID 22 ID 25

Практика: Поиск информации об RDP-подключениях

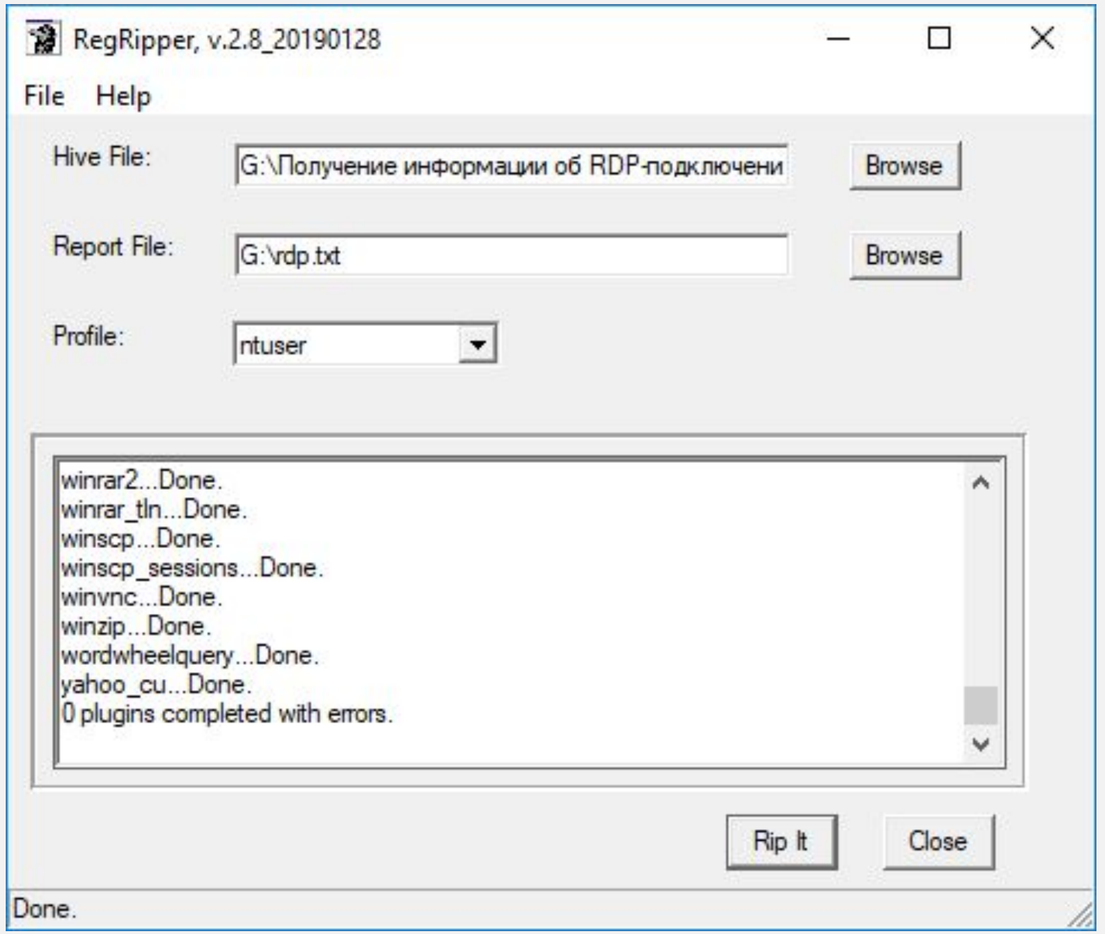


Следы подключений по RDP: Реестр

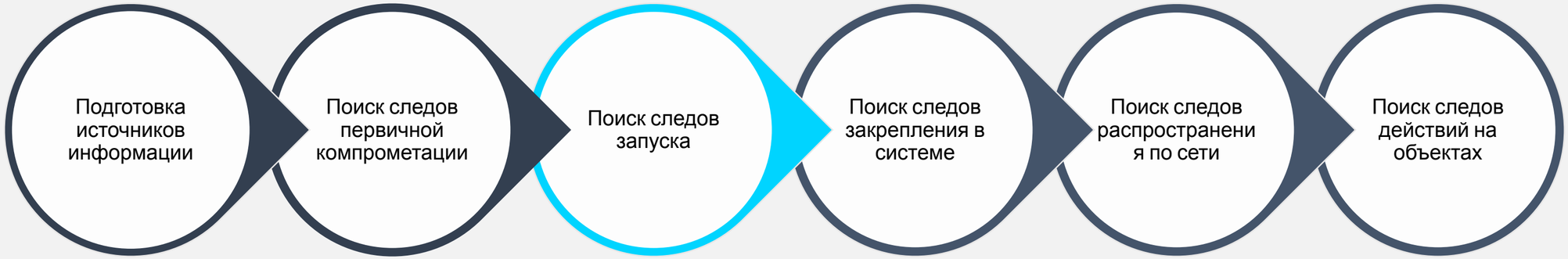
NTUSER.DAT	Software\Microsoft\Terminal Server Client\Servers

```
(NTUSER.DAT) Gets hosts logged onto via RDP and the Domain\Username

Terminal Server Client\Servers
Software\Microsoft\Terminal Server Client\Servers
LastWrite Time Wed Oct 25 12:27:27 2017 (UTC)


Hostname: 10.77.211.42
Domain/Username: nationalbank\pc13
LastWrite: Sat Sep 29 05:18:03 2018 (UTC)
```

Практика: Поиск информации об RDP-подключениях

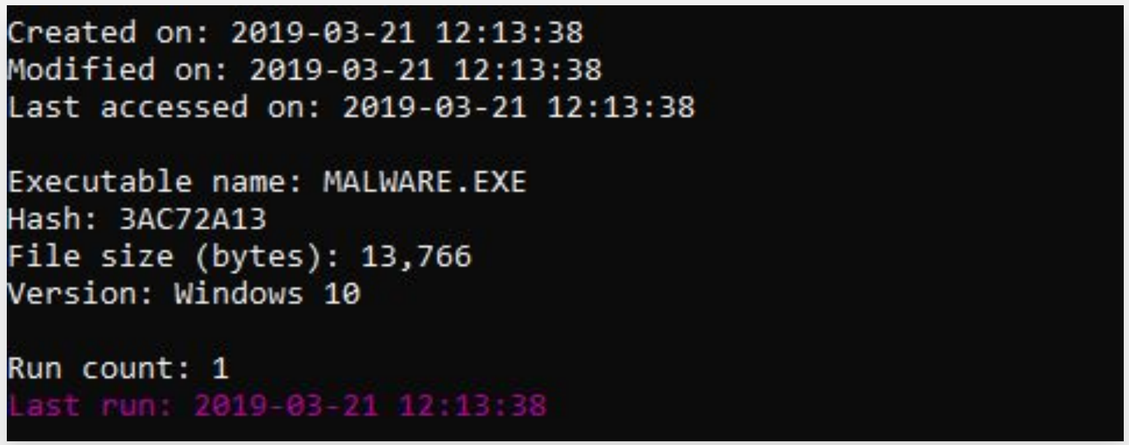


Следы запуска

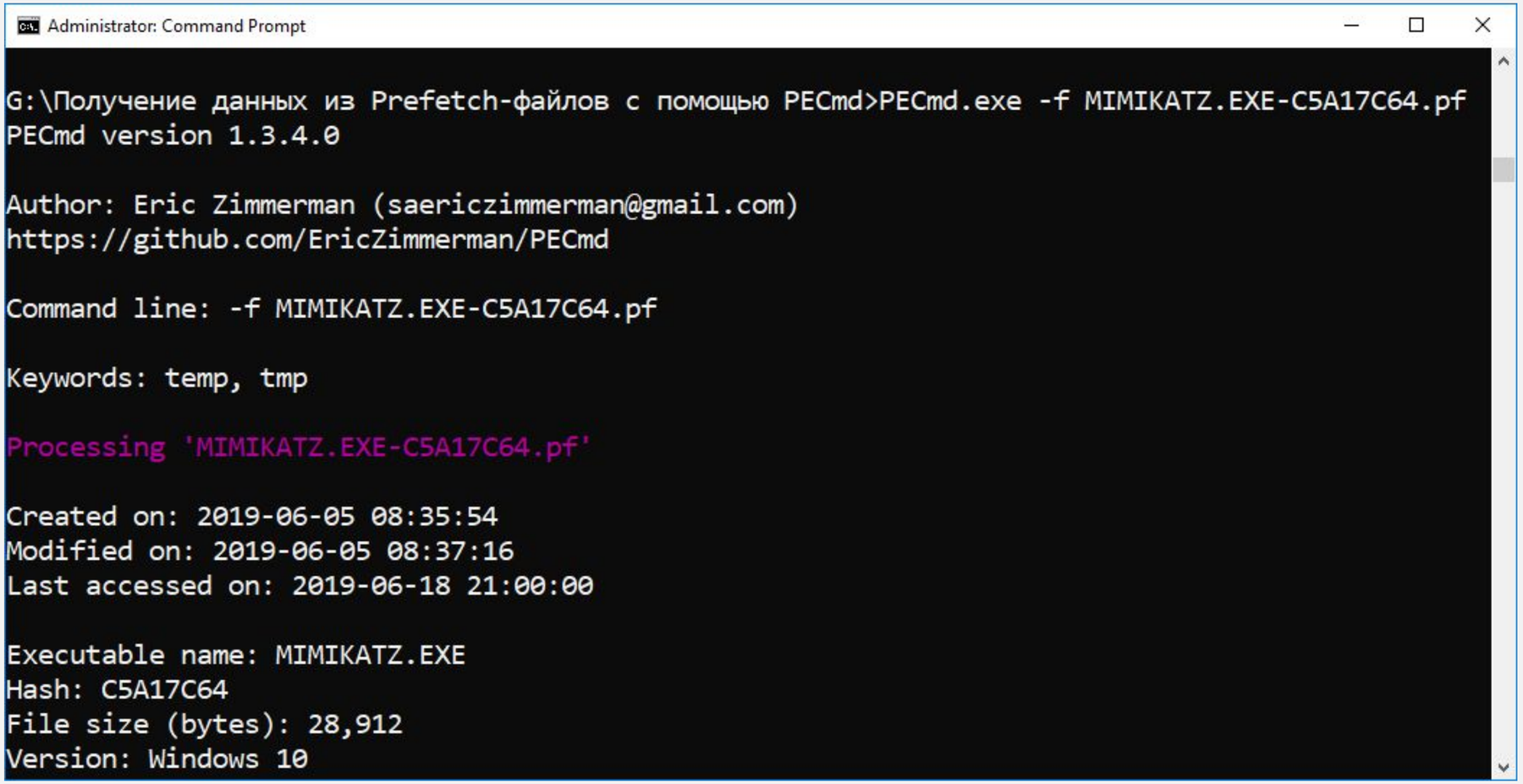


Следы запуска: PREFETCH

*.pf	C:\Windows\Prefetch

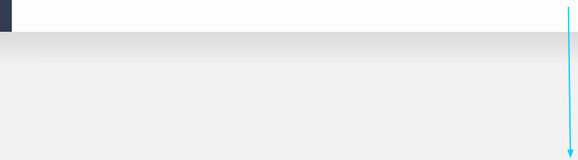


Практика: Получение информации из PREFETCH-файлов



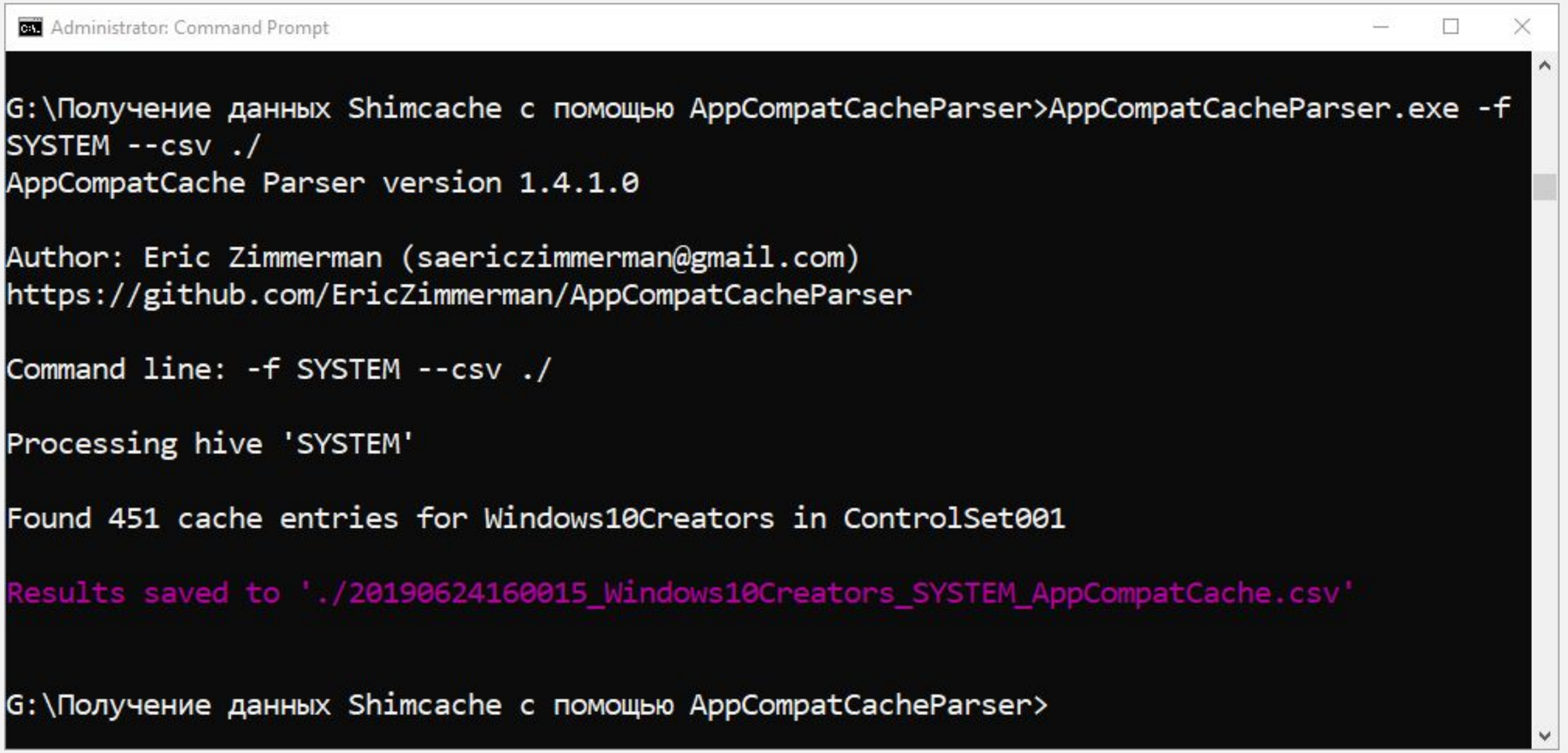
Следы запуска: SHIMCACHE

SYSTEM	ControlSet001\Control\Session Manager\AppCompatCache



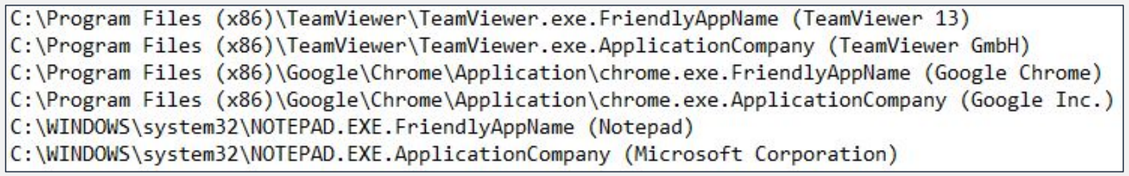
C:\Program Files (x86)\TeamViewer\tv_w32.exe	9/10/2018 13:56
C:\Program Files (x86)\TeamViewer\tv_x64.exe	9/10/2018 13:56
C:\Program Files (x86)\TeamViewer\TeamViewer_Note.exe	9/10/2018 13:56
C:\Program Files (x86)\TeamViewer\TeamViewer_Desktop.exe	9/10/2018 15:53
C:\Program Files (x86)\TeamViewer\TeamViewer.exe	9/10/2018 15:53
C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe	9/10/2018 15:53

Практика: Получение данных SHIMCACHE

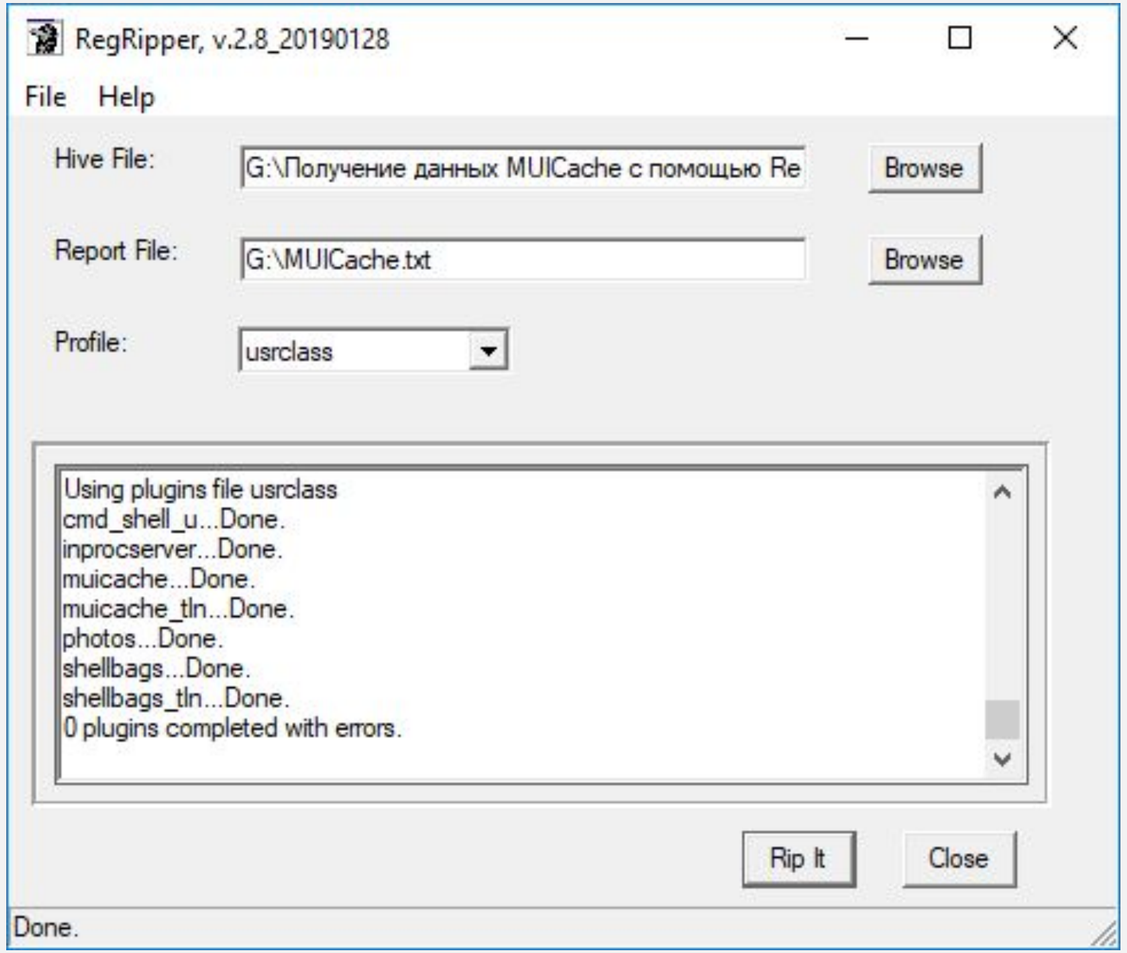


Следы запуска: MUICACHE

USRCLASS.DAT	Local Settings\Software\Microsoft\Windows\Shell\MUICache



Практика: Получение данных MUICACHE

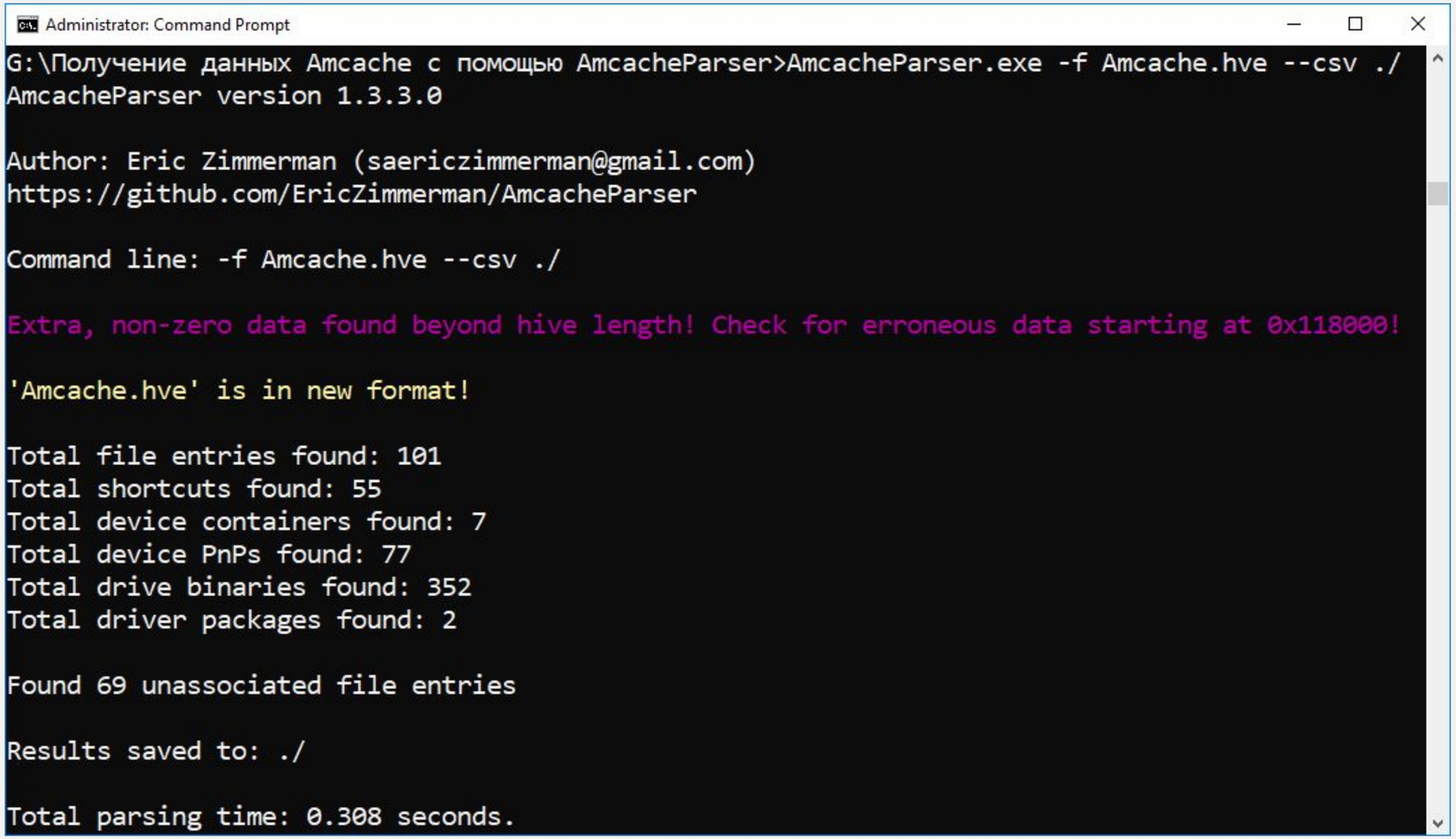


Следы запуска: AMCACHE

Amcache.hve	C:\Windows\appcompat\Programs
RecentFileCache.bcf	C:\Windows\appcompat\Programs

459ecf0b491eab12e8751f4b01631a65701ef0a5	FALSE	c:\windows\temp\malware.exe

Практика: Получение данных AMCACHE

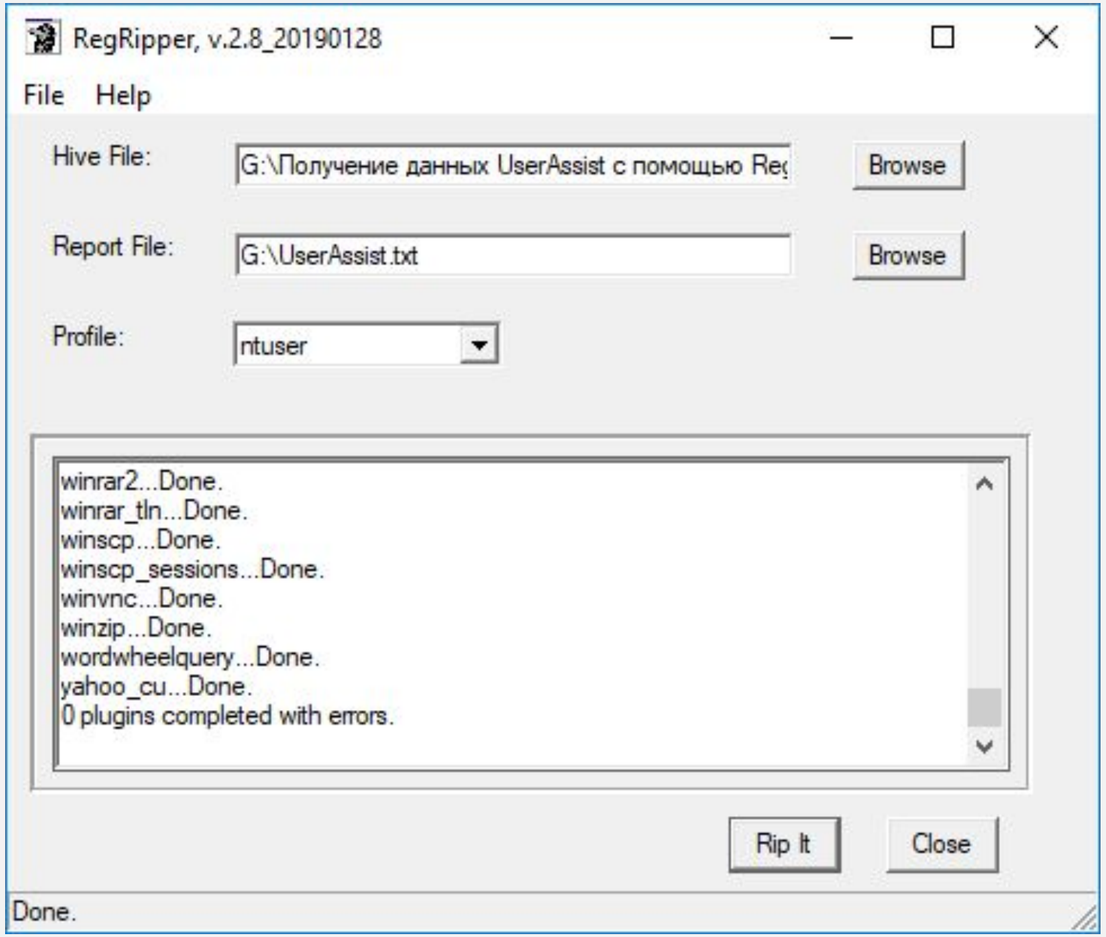


Следы запуска: UserAssist

NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

```
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Thu Mar 21 12:15:42 2019 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\7-Zip\7zFM.exe (5)
Thu Mar 21 12:13:38 2019 Z
  {F38BF404-1D43-42F2-9305-67DE0B28FC23}\Temp\malware.exe (1)
```

Практика: Получение данных USERASSIST

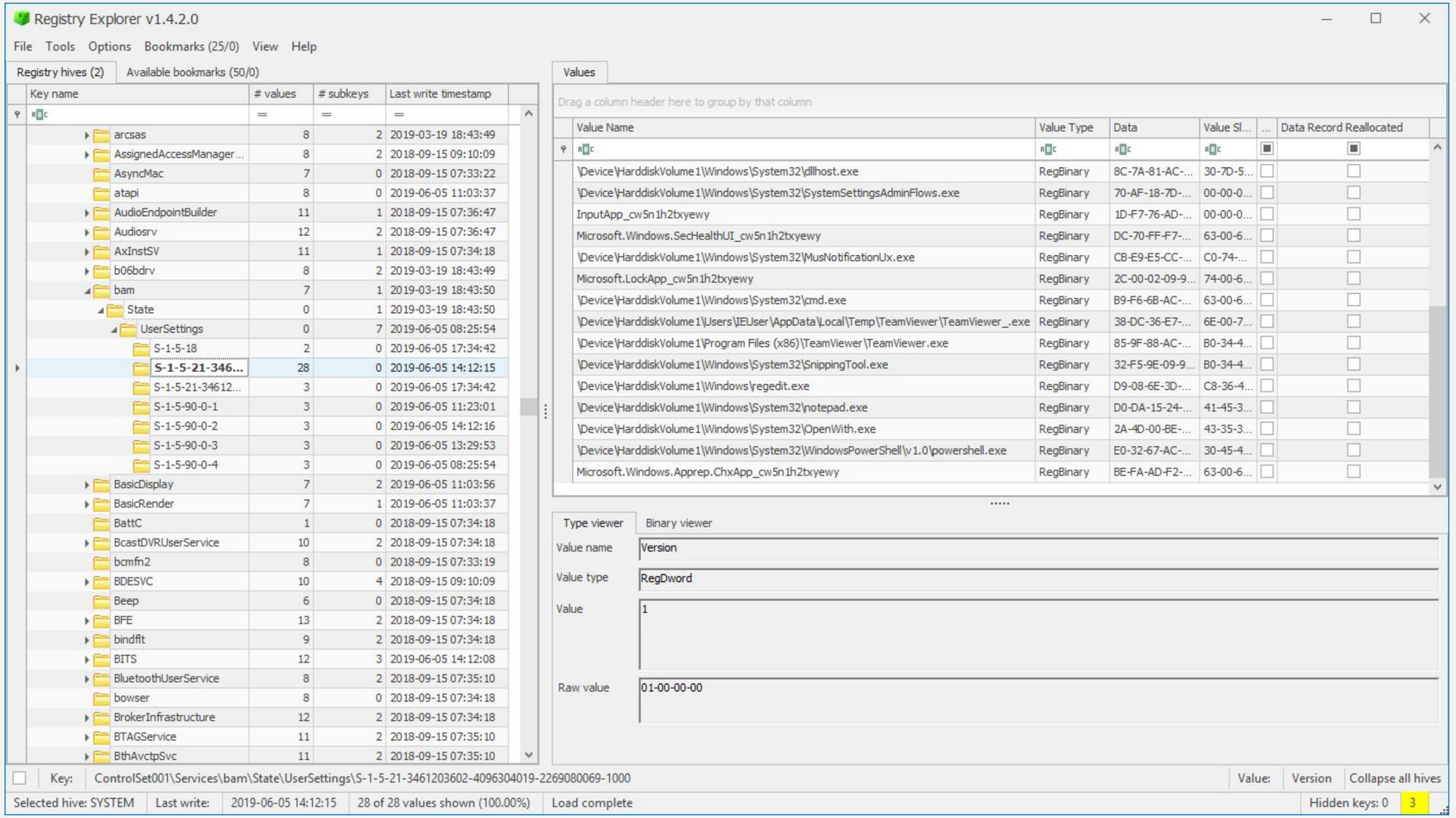


Следы запуска: BACKGROUND ACTIVITY MONITOR

SYSTEM	HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}

\Device\HarddiskVolume4\Program Files\Mozilla Firefox\firefox.exe	2019-03-20 11:42:14
\Device\HarddiskVolume4\Program Files\DB Browser for SQLite\DB Browser for SQLite.exe	2019-03-20 11:49:05
\Device\HarddiskVolume4\Users\0136\Desktop\USB Detective.exe	2019-03-21 13:00:41
\Device\HarddiskVolume4\Users\0136\Desktop\RegRipper2.8-master\rr.exe	2019-03-20 14:08:56
\Device\HarddiskVolume5\Downloads\becu.cm.all.x64.exe	2019-03-21 08:16:40

Практика: Получение данных BACKGROUND ACTIVITY MONITOR

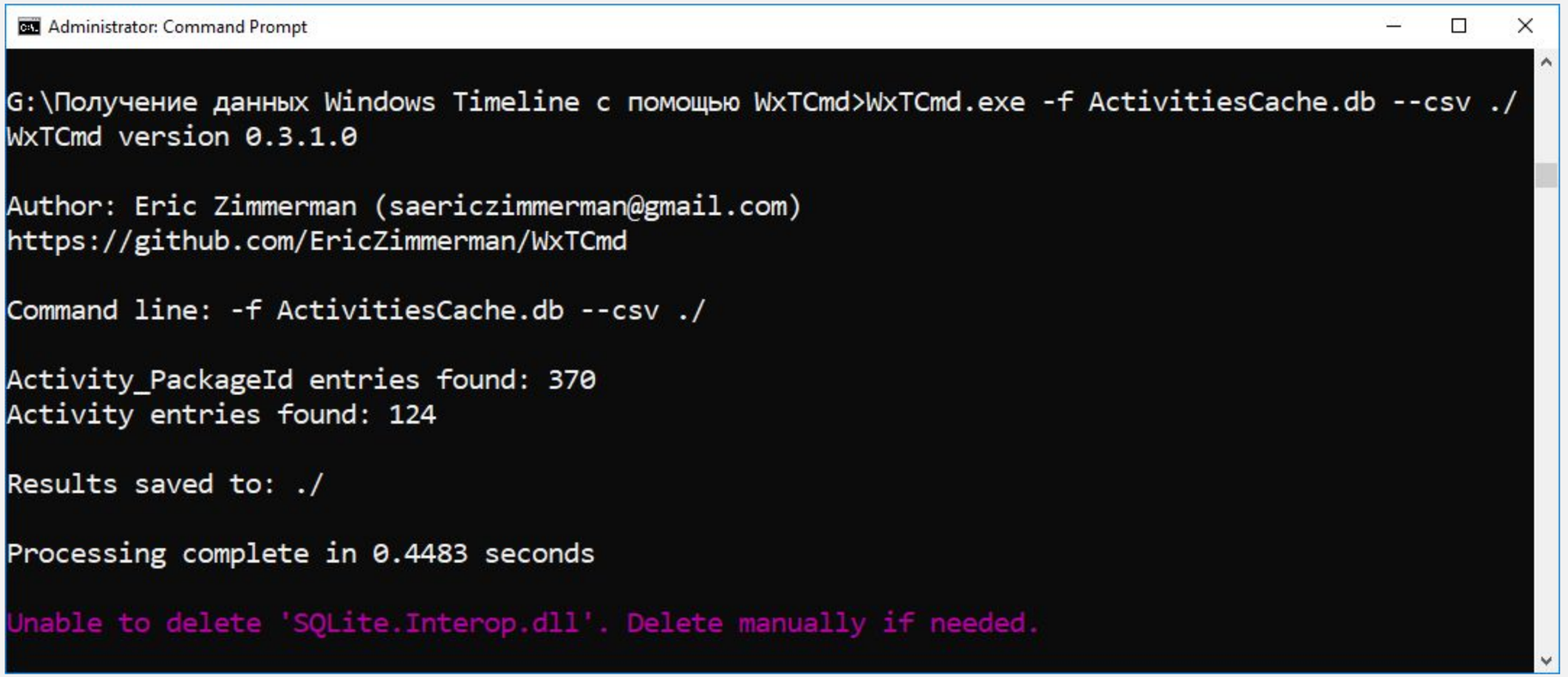


Следы запуска: WINDOWS TIMELINE

ActivitiesCache.db	C:\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\L.<profile>\

Executable	Start Time	End Time
ABC	=	=
Microsoft.Windows.Explorer	2019-03-21 12:12:13	2019-03-21 12:14:30
Windows\Temp\malware.exe	2019-03-21 12:13:38	
System32\cmd.exe	2019-03-21 12:14:30	2019-03-21 12:17:19
Microsoft.Windows.Explorer	2019-03-21 12:14:57	2019-03-21 12:18:00
Program Files X64\7-Zip\7zFM.exe	2019-03-21 12:15:05	2019-03-21 12:15:11
Program Files X64\7-Zip\7zFM.exe	2019-03-21 12:15:38	2019-03-21 12:15:40
Program Files X64\7-Zip\7zFM.exe	2019-03-21 12:15:42	2019-03-21 12:15:47

Практика: Получение данных BACKGROUND ACTIVITY MONITOR

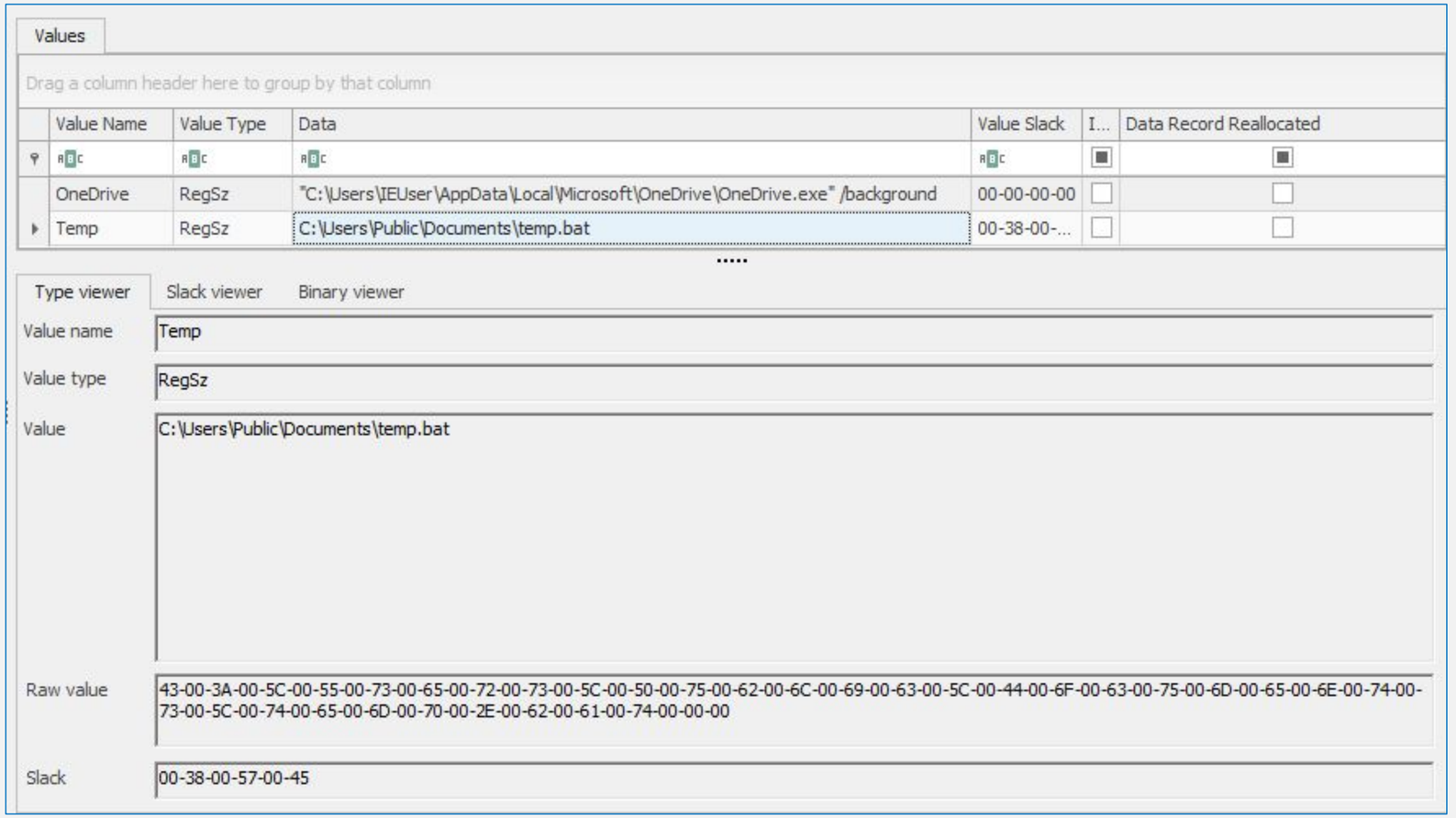


Следы закрепления в системе

Следы закрепления в системе: RUN KEYS

Файл	Раздел
NTUSER.DAT	Microsoft\Windows\CurrentVersion\Run
NTUSER.DAT	Microsoft\Windows\CurrentVersion\RunOnce
SOFTWARE	Microsoft\Windows\CurrentVersion\Run
SOFTWARE	Microsoft\Windows\CurrentVersion\RunOnce

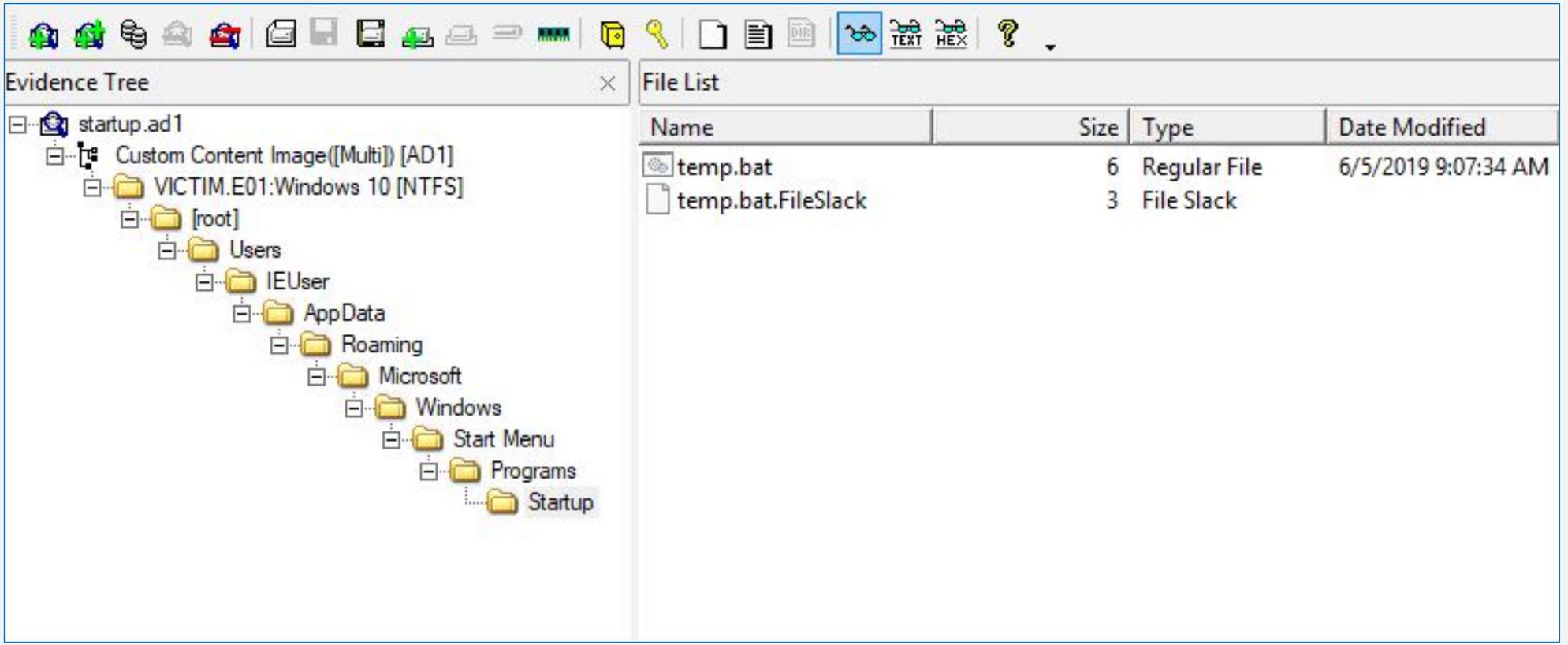
Практика: Анализ значений параметров RUN



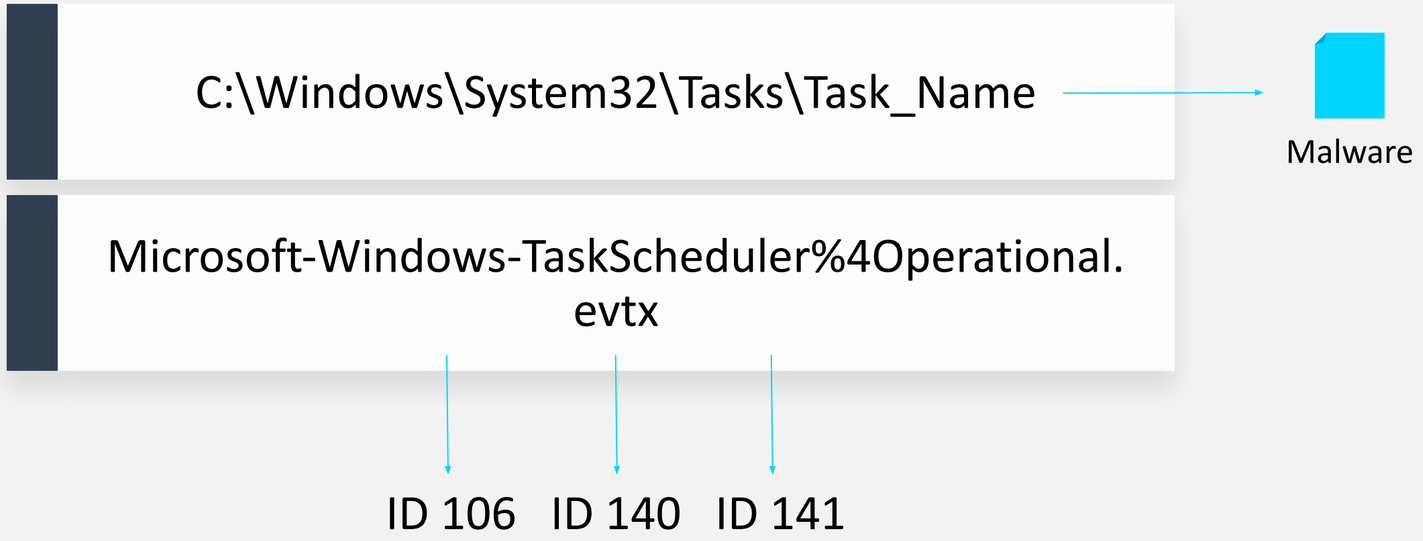
Следы закрепления в системе: STARTUP FOLDERS

Пользователь	Путь
Current user	C:\Users\<profile>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
All users	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

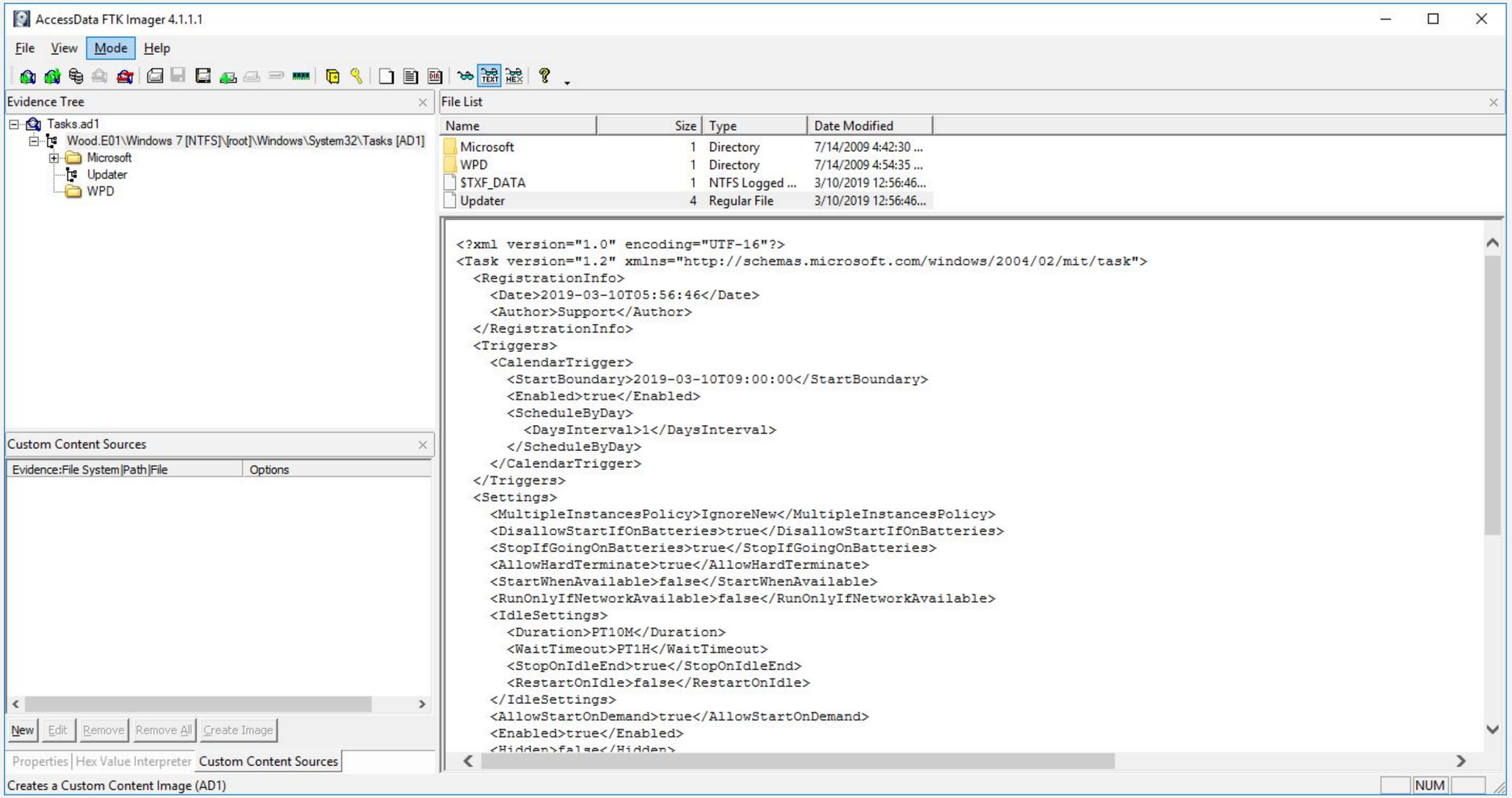
Практика: Анализ содержимого STARTUP FOLDERS



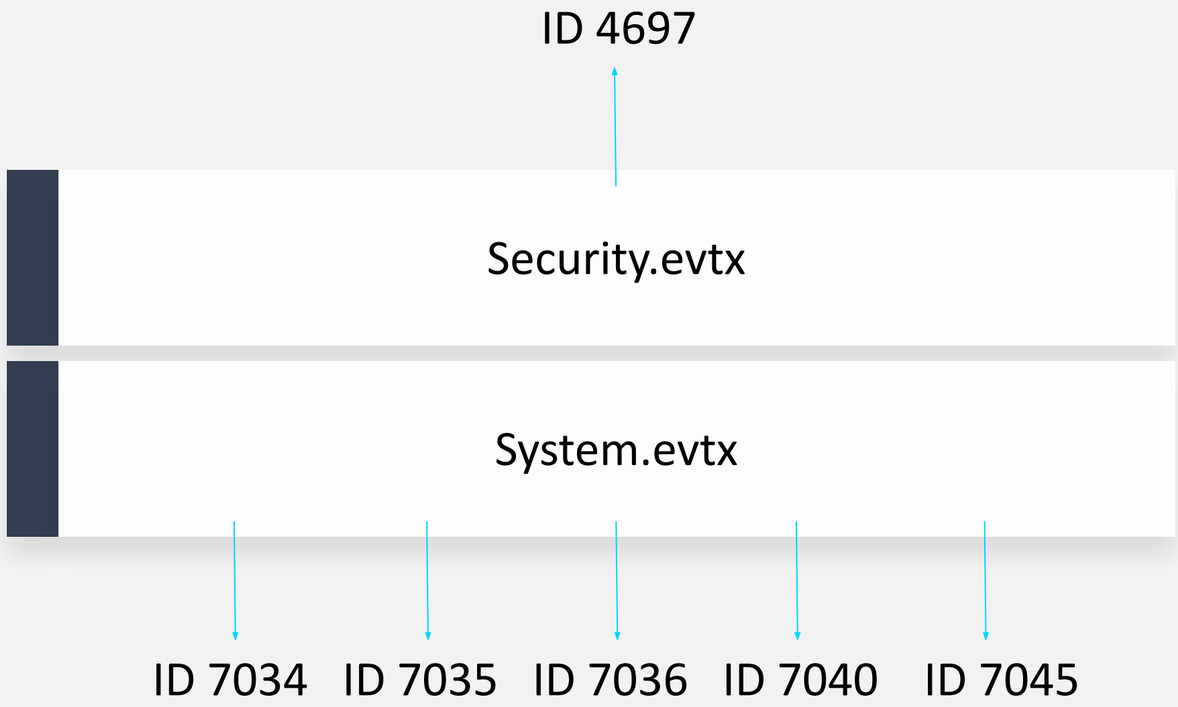
Следы закрепления в системе: TASKS



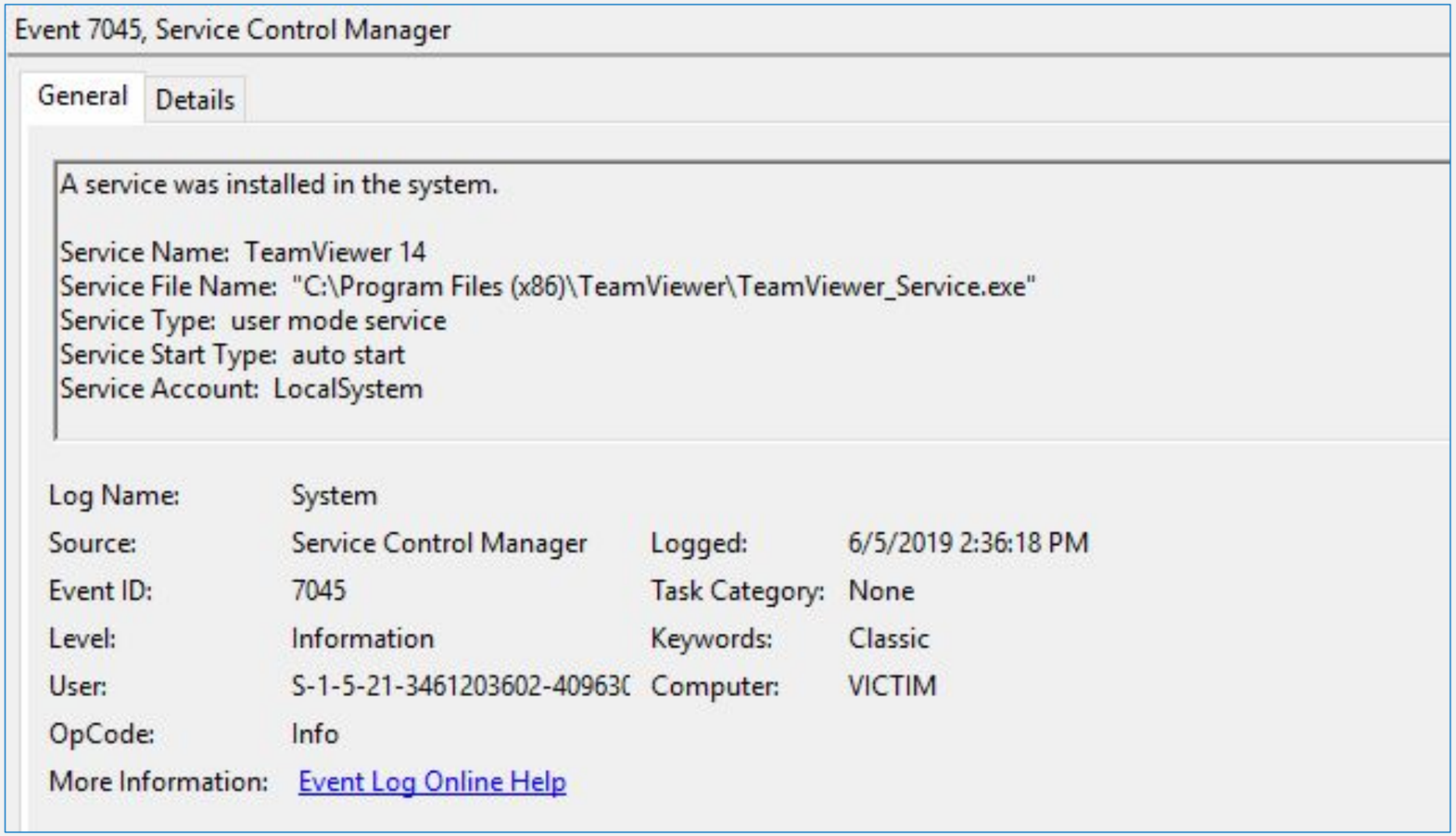
Практика: Анализ запланированных заданий



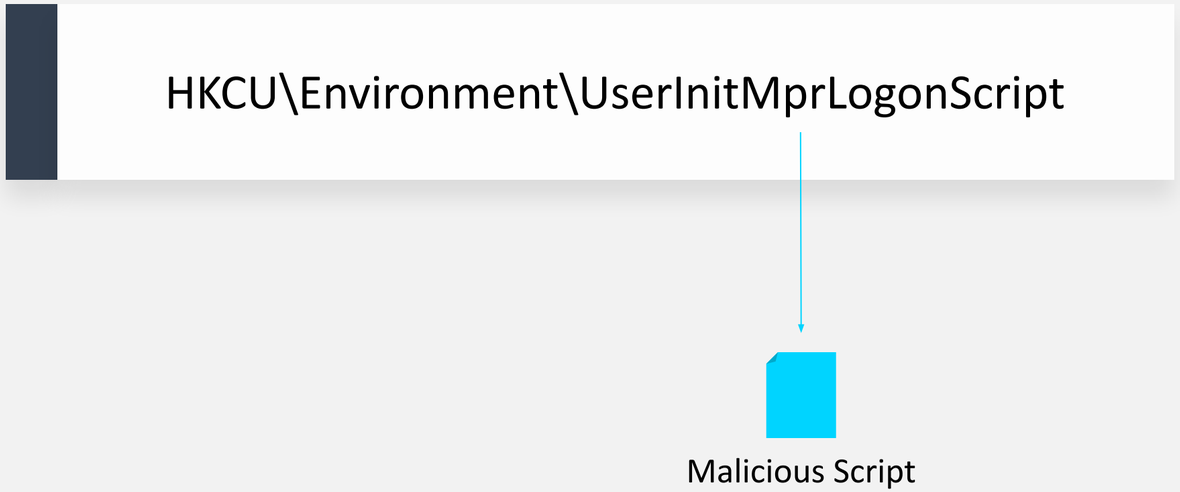
Следы закрепления в системе: SERVICES



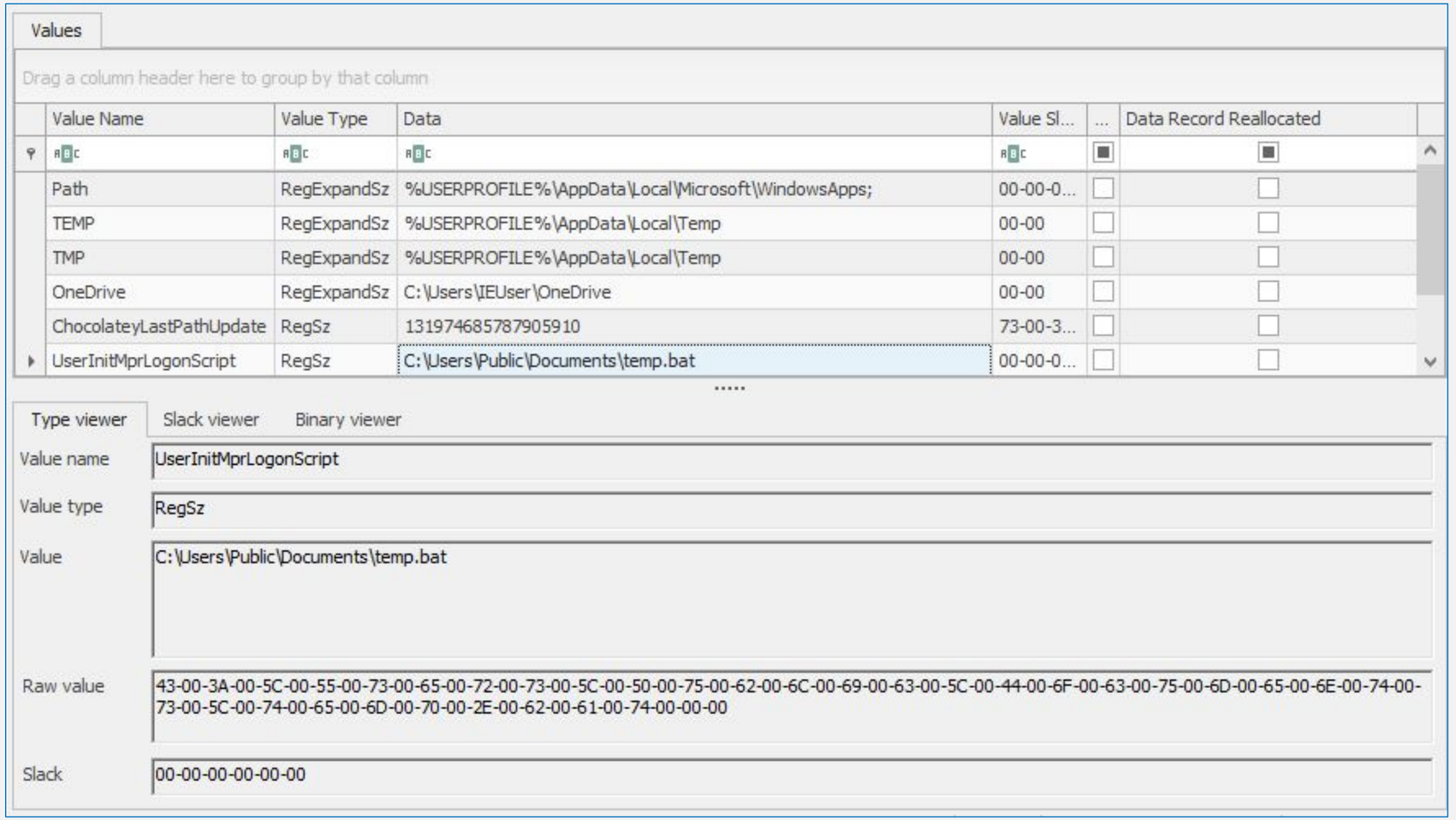
Практика: Поиск информации о создании служб



Следы закрепления в системе: LOGON SCRIPTS

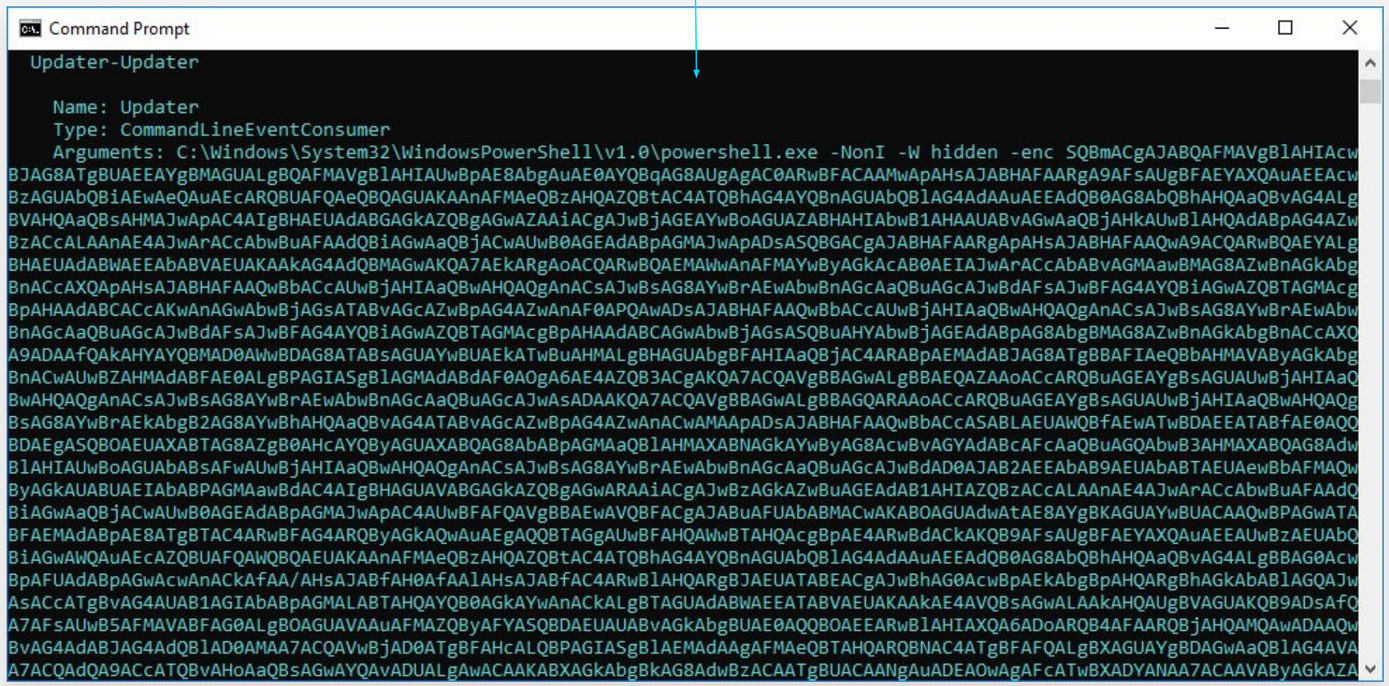


Практика: Анализ значений параметра UserInitMprLogonScript

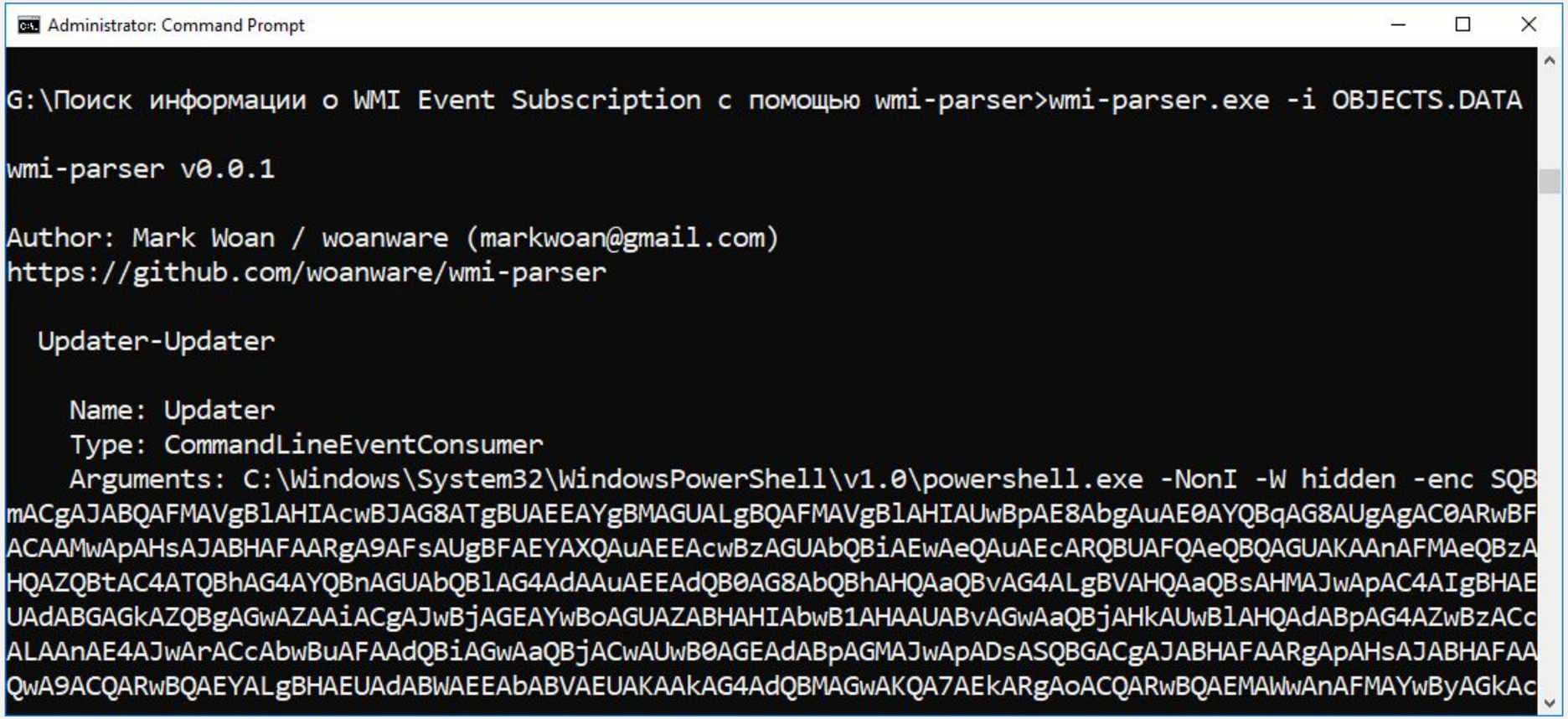


Следы закрепления в системе: WMI EVENT SUBSCRIPTION

C:\WINDOWS\system32\wbem\Repository\OBJECTS.DATA



Практика: Поиск информации о WMI EVENT SUBSCRIPTION

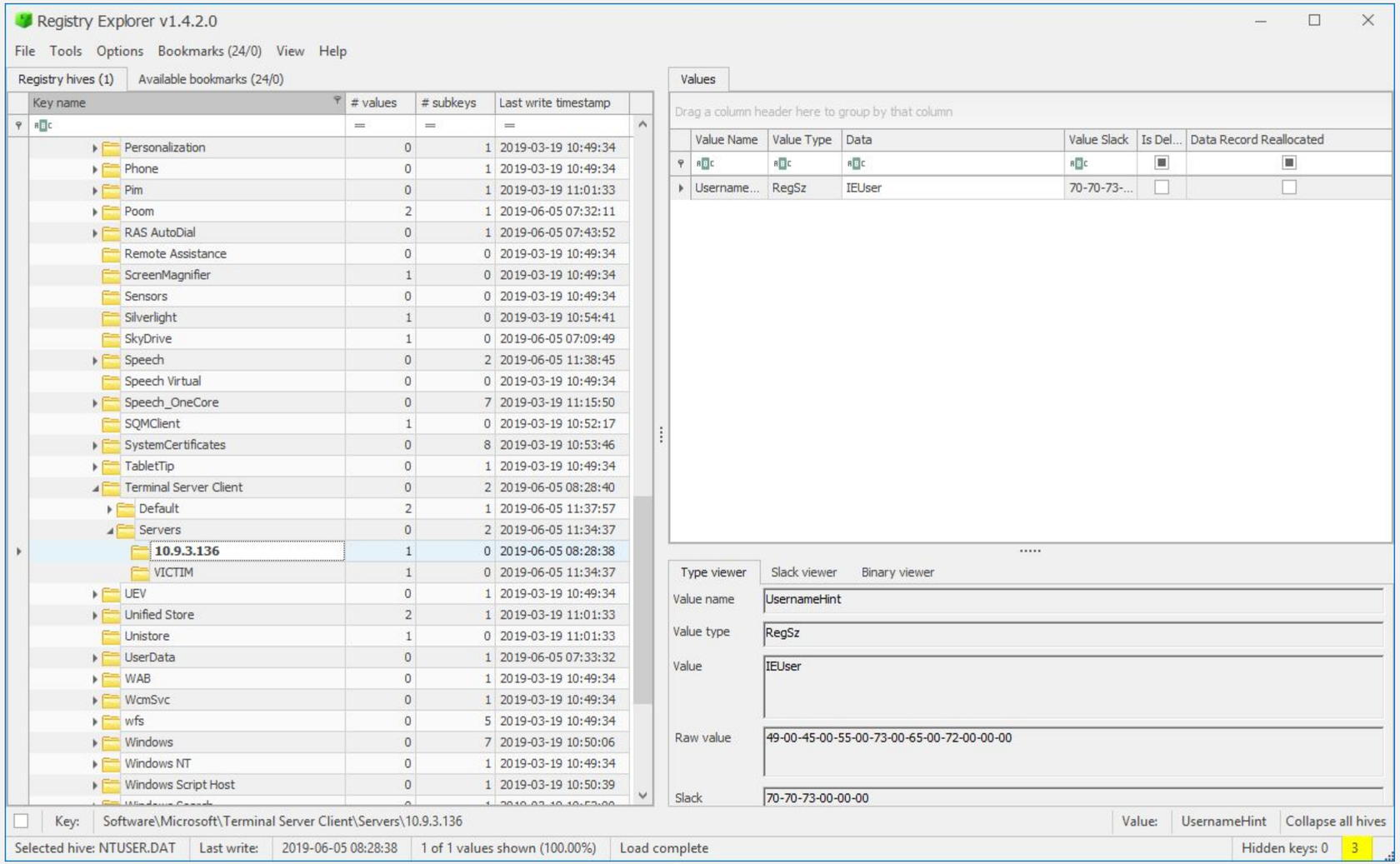


Следы распространения по сети

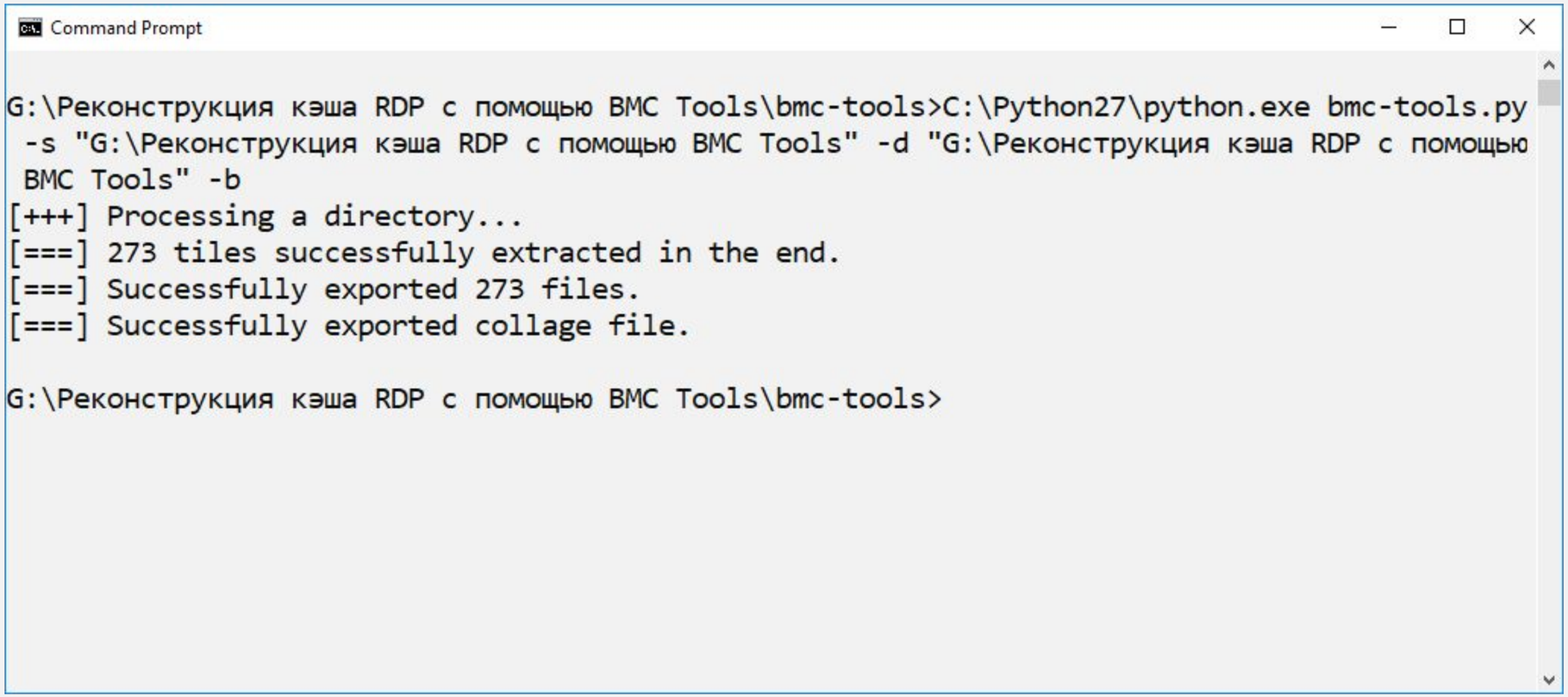
Следы Распространения по сети: RDP

Источник		
Журналы событий	Security.evtx	ID 4648
	Microsoft-WindowsTerminalServicesRDPClient%4Operational.evtx	ID 1024 ID 1102
Реестр	NTUSER.DAT|Software\Microsoft\Terminal Server Client\Servers	
Файловая система	C:\Users\<profile>\AppData\Local\Microsoft\Terminal Server Client\Cache	

Практика: Поиск Следов Исходящих RDP-Подключений



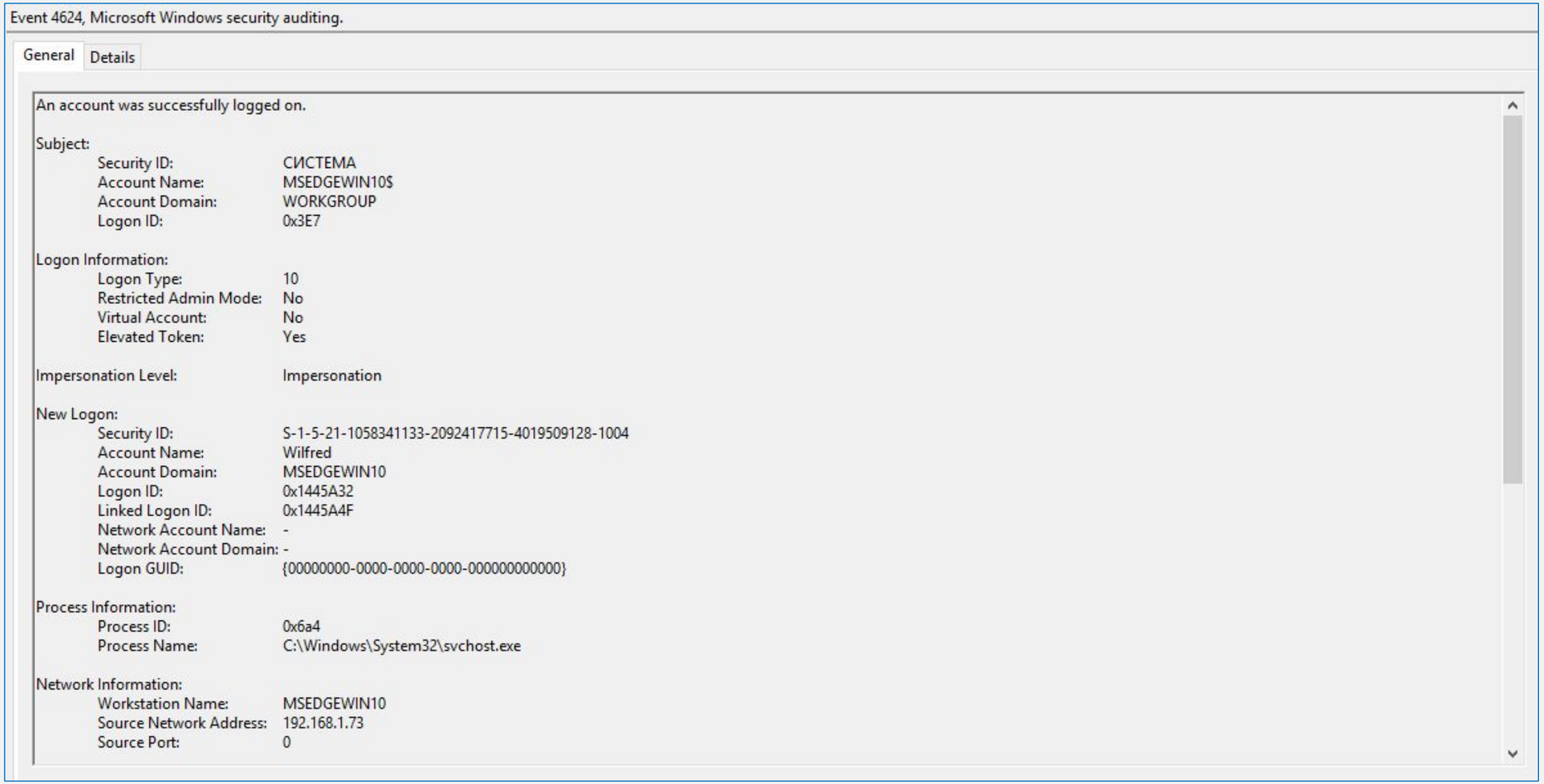
Практика: Реконструкция RDP-кэша



Следы Распространения по сети: RDP

	Назначение	
Журналы событий	Security.evtx	ID 4624 ID 4778 ID 4779
	Microsoft-WindowsRemoteDesktopServicesRdpCoreTS%4Operational.evtx	ID 131 ID 98
	Microsoft-Windows-Terminal Services-RemoteConnection Manager%4Operational.evtx	ID 1149
	Microsoft-Windows-Terminal Services-LocalSession Manager%4Operational.evtx	ID 21 ID 22 ID 25

Практика: Поиск входящих RDP-Подключений



Следы Распространения по сети: Административные общие ресурсы

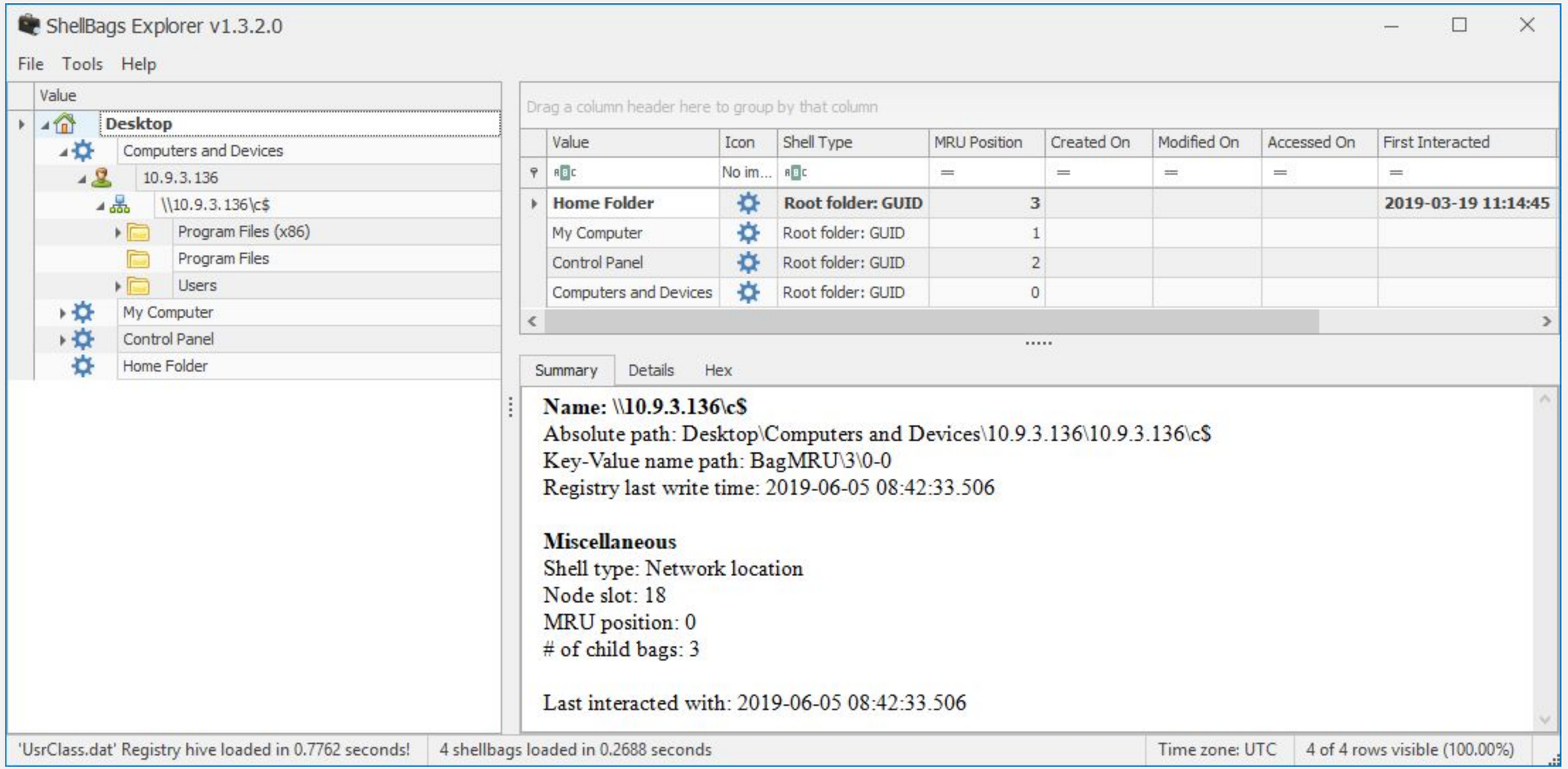
Источник

Журналы событий	Security.evtx	ID 4648
Реестр	USRCLASS.DAT|Local Settings\Software\Microsoft\Windows\Shell\Bags	
	USRCLASS.DAT|Local Settings\Software\Microsoft\Windows\Shell\BagsMRU	

Назначение

Журналы событий	Security.evtx	ID 4624

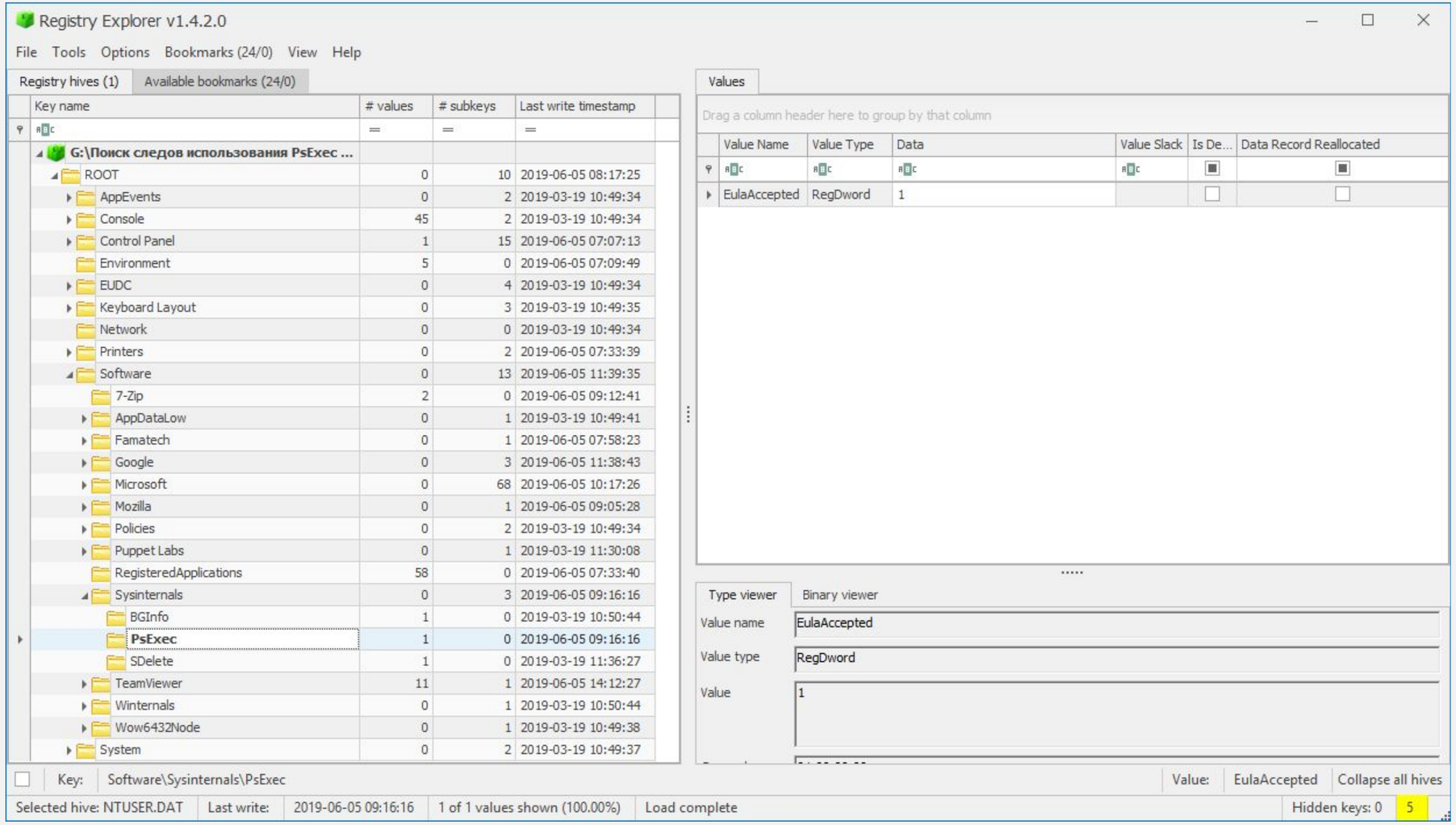
Практика: Административные общие ресурсы



Следы Распространения по сети: PSEXEC

Источник		
Журналы событий	Security.evtx	→ ID 4648
Реестр	NTUSER.DAT|Software\SysInternals\PsExec\EulaAccepted	
Файловая система	psexec.exe	+ Следы запуска

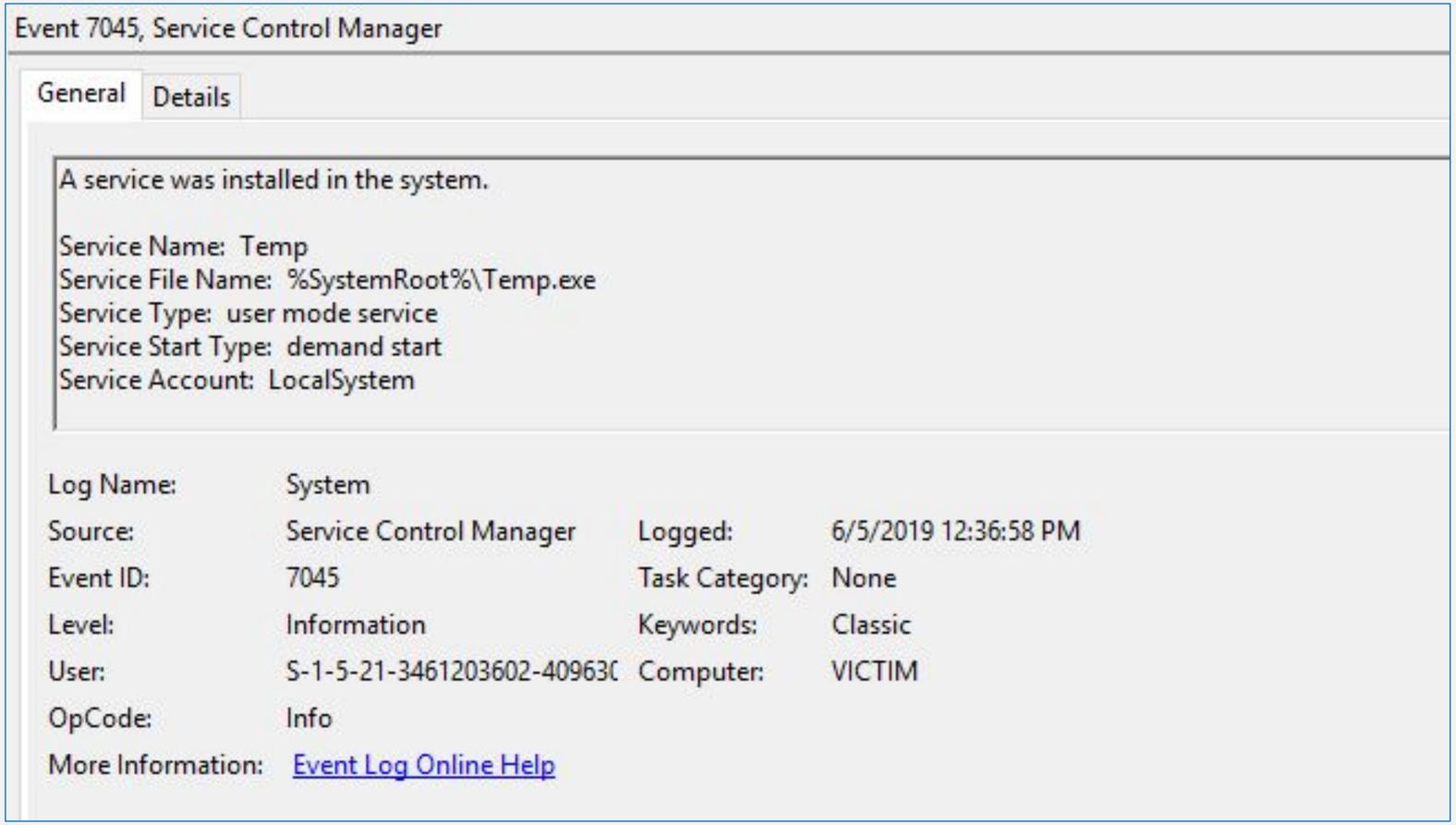
Практика: Поиск следов PSEXEC на хосте-источнике



Следы Распространения по сети: PSEXEC

Назначение		
Журналы событий	Security.evtx	ID 4624 ID 4672 ID 5140
	System.evtx	ID 7045
Реестр	SYSTEM| CurrentControlSet\ Services\PSEXESVC	
Файловая система	C:\Windows\psexecsvc.exe	

Практика: Поиск следов PSEXEC на хосте-Назначении



Следы Распространения по сети: WMI

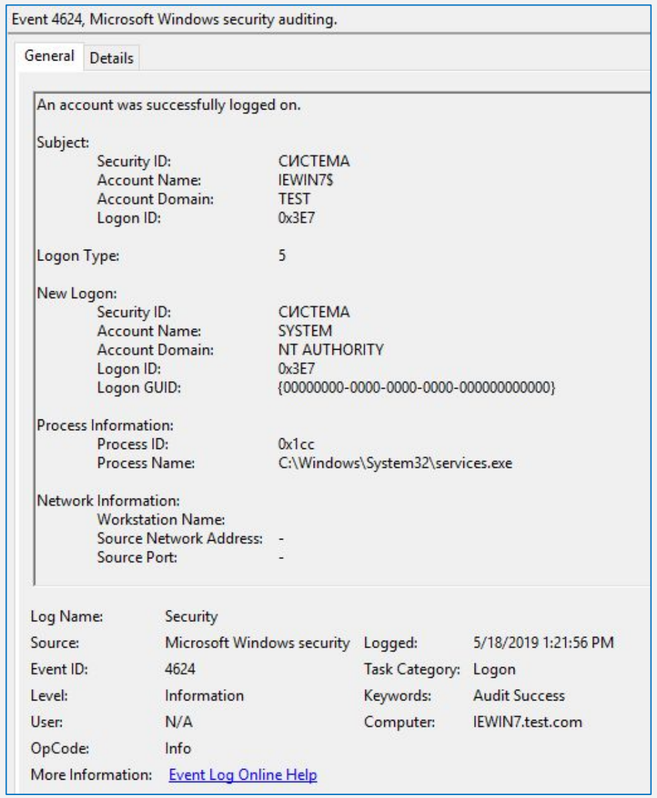
Источник

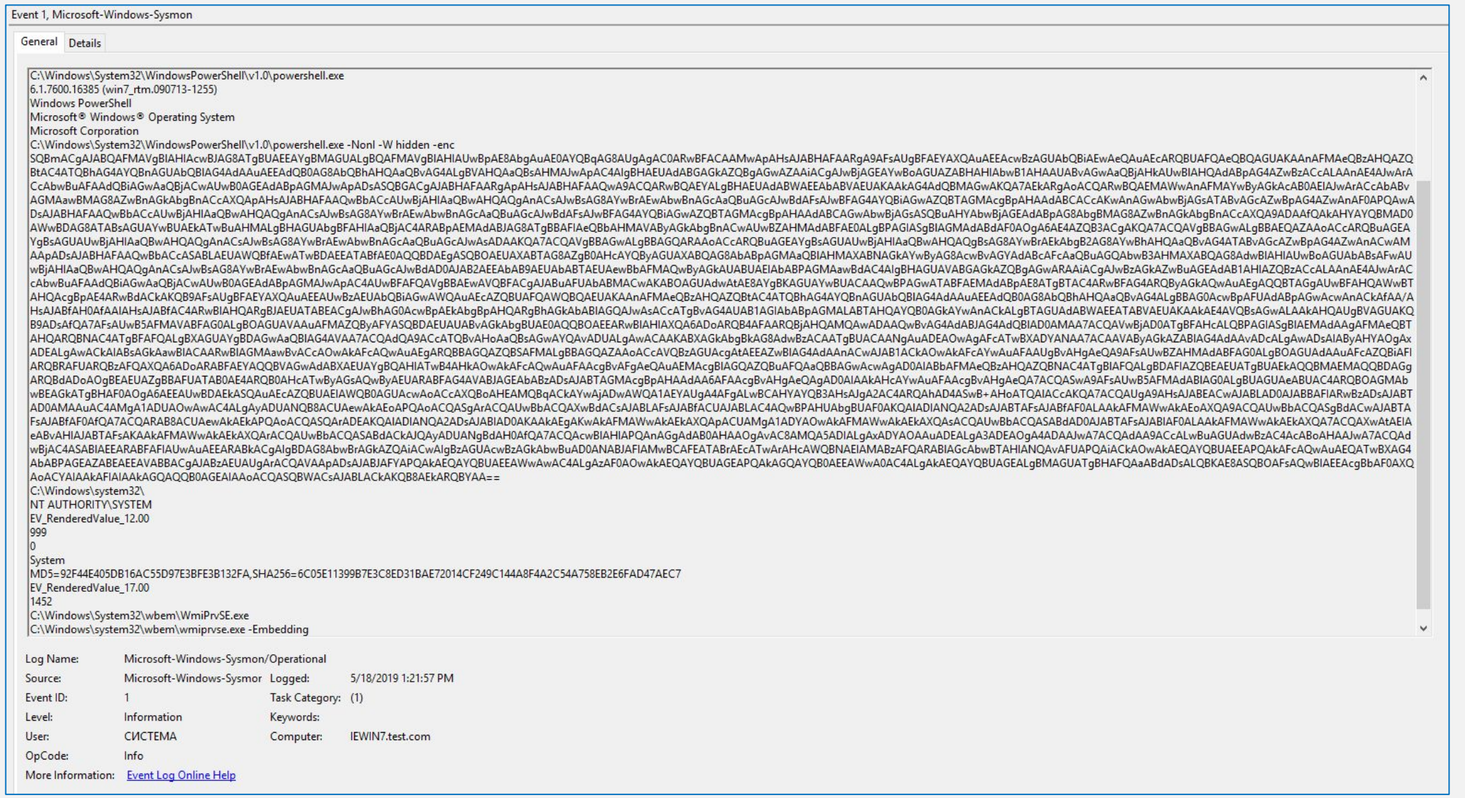
Журналы событий	Security.evtx	ID 4648

Назначение

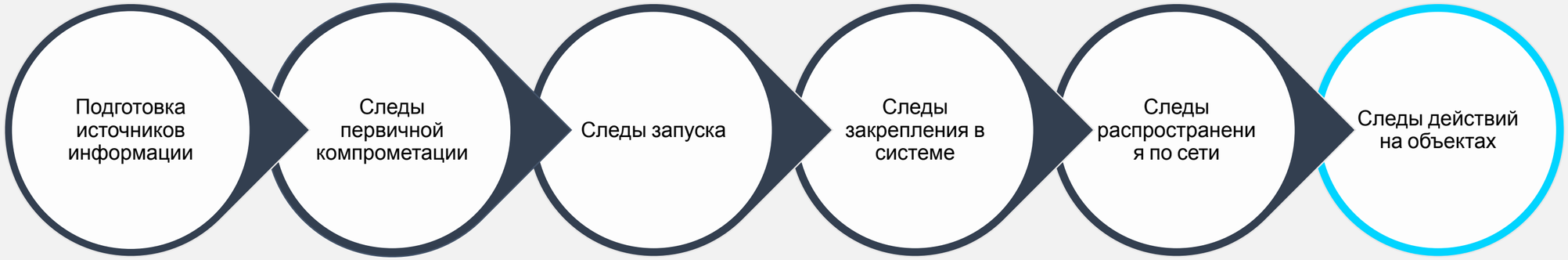
Журналы событий	Security.evtx	ID 4624 ID 4672
	Microsoft-Windows-WMIActivity%4Operational.evtx	ID 5857 ID 5860 ID 5861

Практика: Поиск следов подключений через WMI





Следы Действий на объектах



Получение аутентификационных данных

Следы исполнения программ, позволяющих получить доступ к аутентификационным данным

Следы создания файлов / доступа к файлам, содержащим аутентификационные данные

Следы исполнения программ, предназначенных для перебора паролей

Создание учетных записей

Следы создания профилей новых учетных записей

Следы аутентификации с использованием новых учетных записей

Сканирование сетевой инфраструктуры

Следы исполнения программ, позволяющих осуществлять сканирование сетевой инфраструктуры

Следы создания файлов / доступа к файлам, содержащим результаты сканирования

Инсталляция и использование Программ для удаленного управления

- Следы создания / исполнения файлов, предназначенных для инсталляции программ для удаленного управления
- Следы запуска программ для удаленного управления
- Анализ журналов программ для удаленного управления

Кража данных

Следы создания архивов с данными, имеющимися на целевой рабочей станции или сервере

Следы загрузки данных на веб-ресурсы

Следы копирования данных с помощью программ для удаленного управления

Использование имеющегося программного обеспечения

Следы запуска программного обеспечения, имеющегося на скомпрометированных серверах или рабочих станциях

Создание / модификация файлов средствами имеющегося на скомпрометированных хостах программного обеспечения

Загрузка дополнительного вредоносного / потенциально вредоносного программного обеспечения или его модулей

Следы создания / исполнения вредоносного / потенциально вредоносного программного обеспечения или его модулей

Следы загрузки вредоносного / потенциально вредоносного программного обеспечения или его модулей

Практика

Использование файлов Реестра NTUSER.DAT и USRCLASS.DAT для реконструкции Действий атакующего

Практика

Реконструкция тактик и техник Атакующих согласно матрице MITRE ATT&CK на основе Анализа криминалистических копий

О компании GROUP-IB

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий

1000+

успешных расследований по всему миру, 160 особо сложных уголовных дел

$300 млн

возвращено клиентам Group-IB благодаря нашей работе

Официальный партнёр EUROPOL и INTERPOL

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

Постоянный член Всемирного экономического форума

Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester и Gartner

Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider

Лидер российского рынка по исследованию киберугроз

О нас говорят:

theguardian Bloomberg Forbes REUTERS Esquire

ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ