Практические вопросы и виды цифровых доказательств, собираемых в процессе расследования компьютерных преступлений

Комоцкий Е.И.

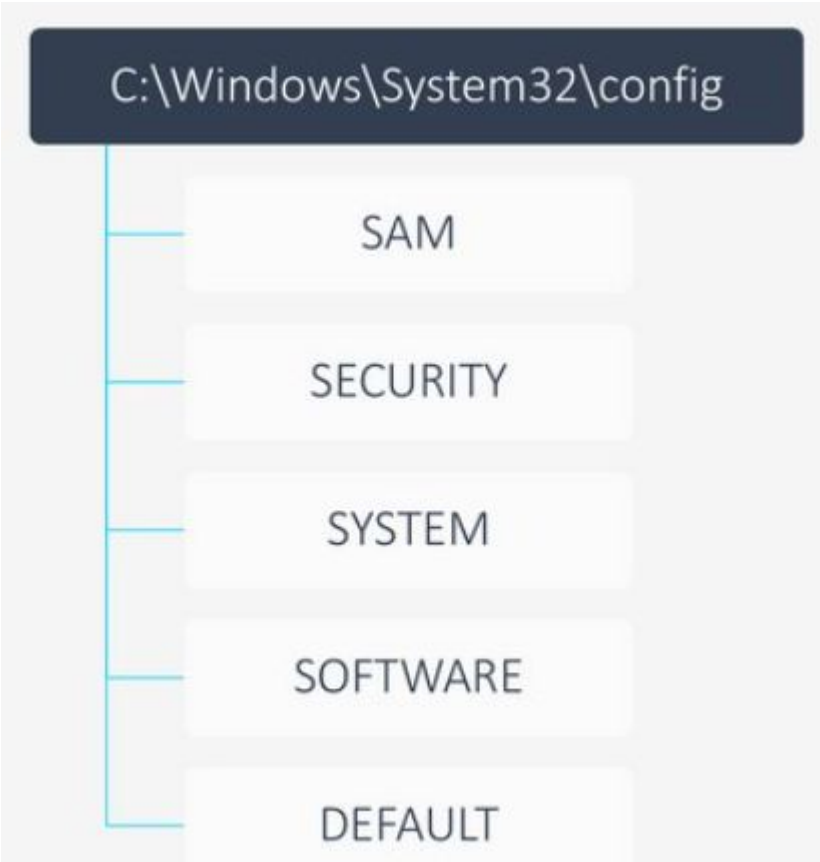
Фадичев Б.А.

УрФУ - Институт радиоэлектроники и информационных технологий - РТФ

Шаги исследования цифровых следов

- Подготовки источников данных
- Поиск следов компрометации
- Следы запуска программного обеспечения
- Поиск следов закрепления доступа
- Поиск следов горизонтального продвижения
- Поиск следов доступа к информации

Файлы реестра Windows



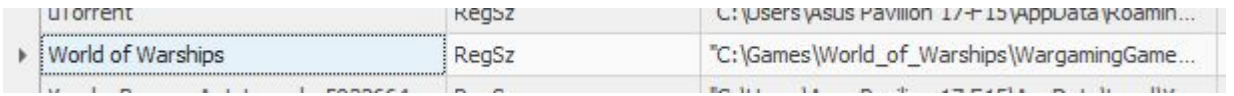
Структура реестра

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Корневой раздел

Вложенные разделы

Запись реестра



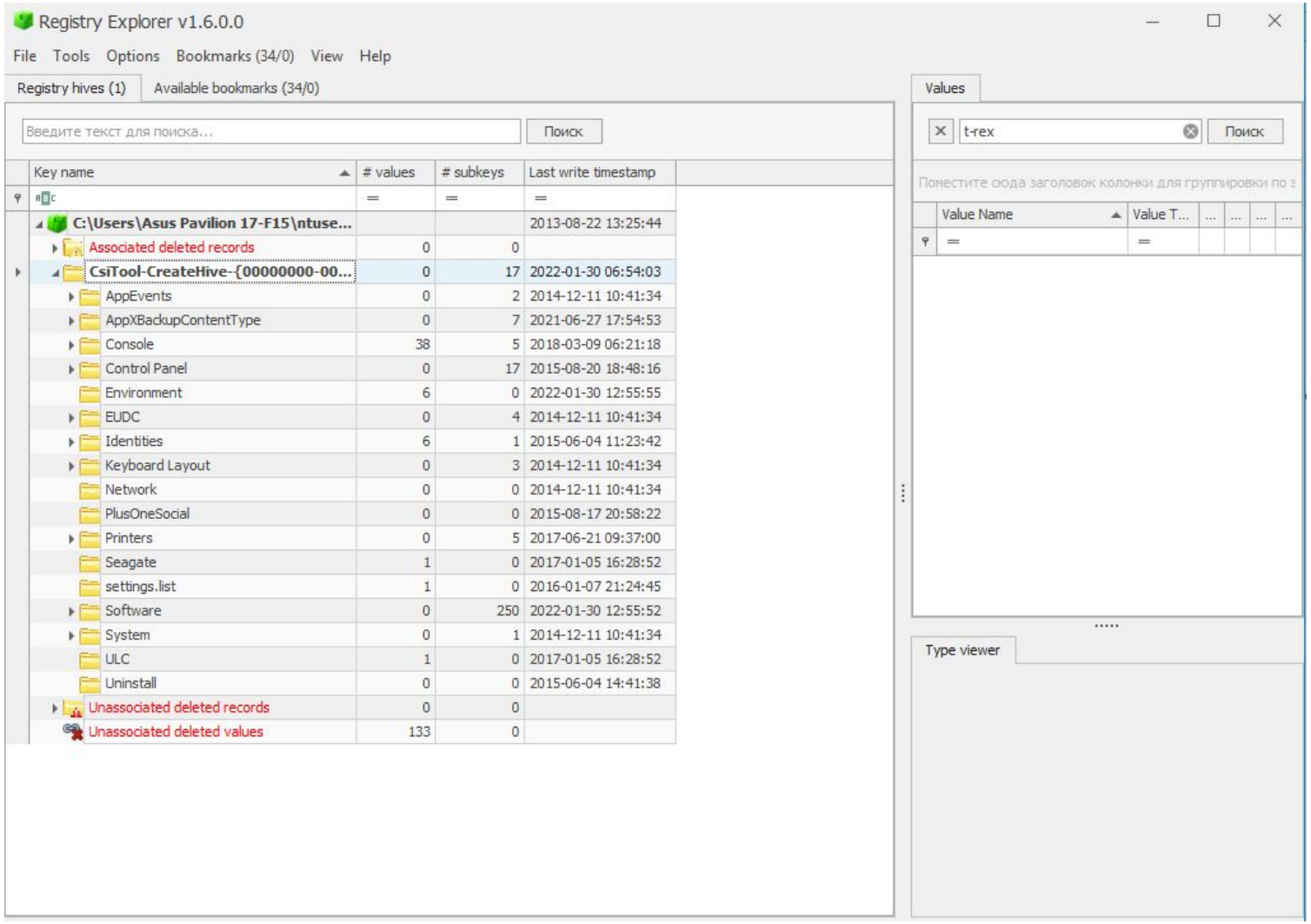
Параметр

Тип

Значение

Поиск следов компрометации

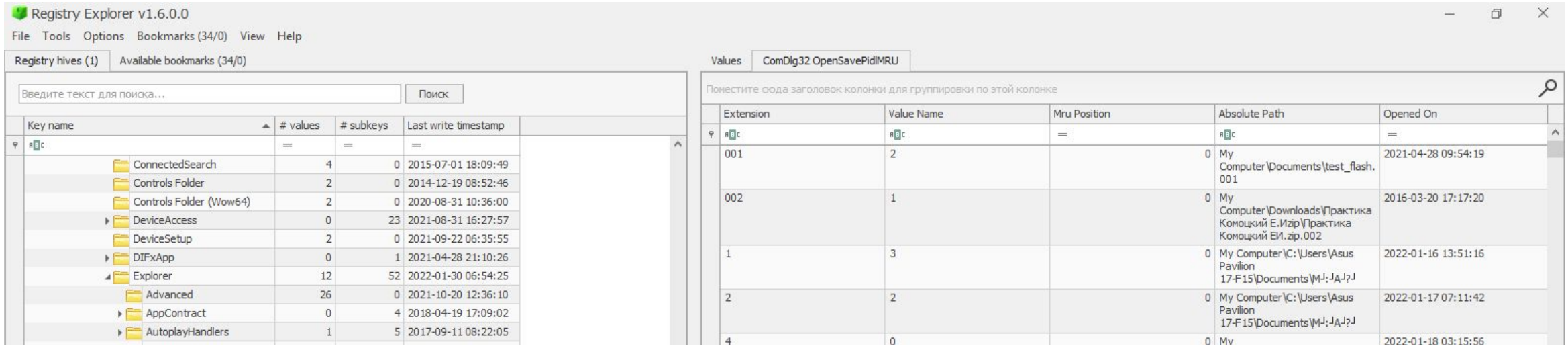
Инструмент работы с реестром Registry Explorer



- https://ericzimmerman.github.io/#!index.md -> Registry Explorer

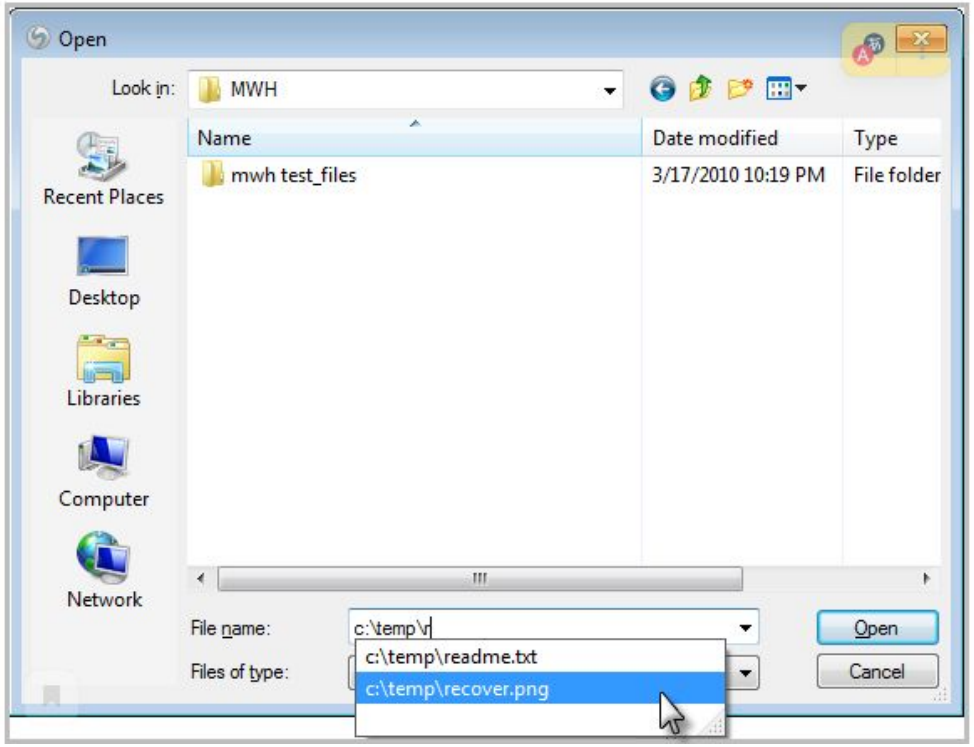
Следы сохранения и открытия файлов: MRU

Путь: NTUSER.DAT |



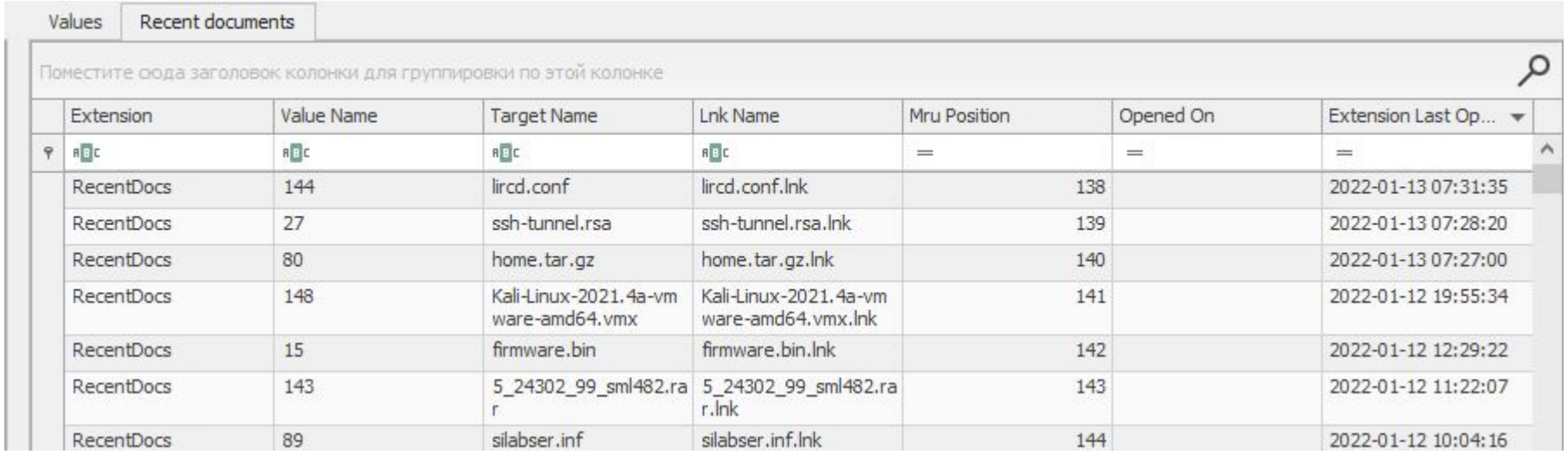
Следы открытия файлов: MRU

- В этом разделе представлена информация о файлах, которые были открыты **или сохранены (в том числе из браузера)** в диалоговом окне оболочки Windows.



Следы открытия файлов: Recent Docs

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



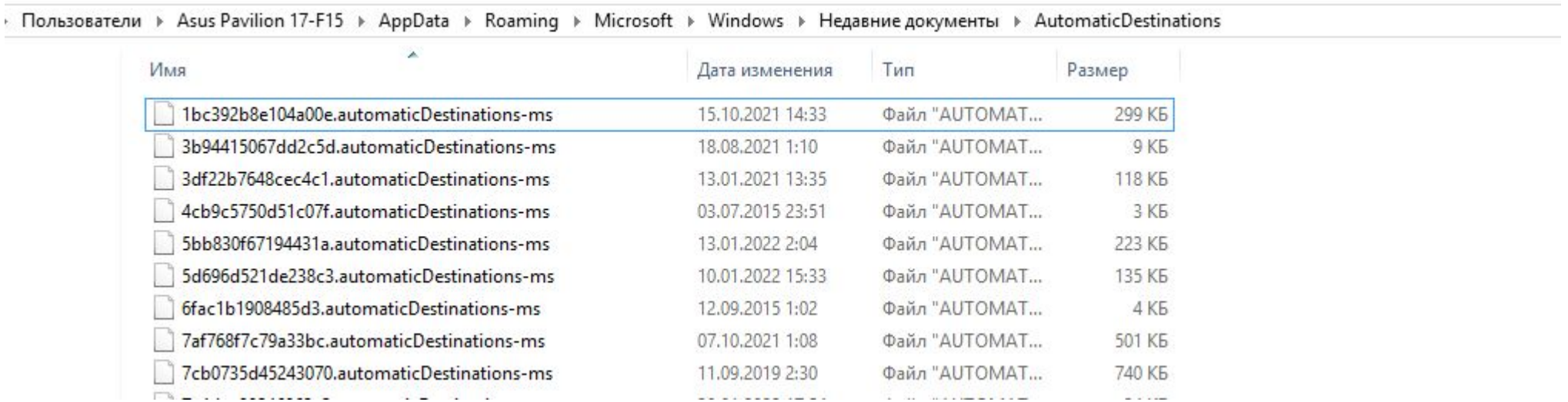
Values | Recent documents

Поместите сюда заголовок колонки для группировки по этой колонке

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Op...
RecentDocs	144	lircd.conf	lircd.conf.lnk	138		2022-01-13 07:31:35
RecentDocs	27	ssh-tunnel.rsa	ssh-tunnel.rsa.lnk	139		2022-01-13 07:28:20
RecentDocs	80	home.tar.gz	home.tar.gz.lnk	140		2022-01-13 07:27:00
RecentDocs	148	Kali-Linux-2021.4a-vmware-amd64.vmx	Kali-Linux-2021.4a-vmware-amd64.vmx.lnk	141		2022-01-12 19:55:34
RecentDocs	15	firmware.bin	firmware.bin.lnk	142		2022-01-12 12:29:22
RecentDocs	143	5_24302_99_sml482.rar	5_24302_99_sml482.rar.lnk	143		2022-01-12 11:22:07
RecentDocs	89	silabser.inf	silabser.inf.lnk	144		2022-01-12 10:04:16

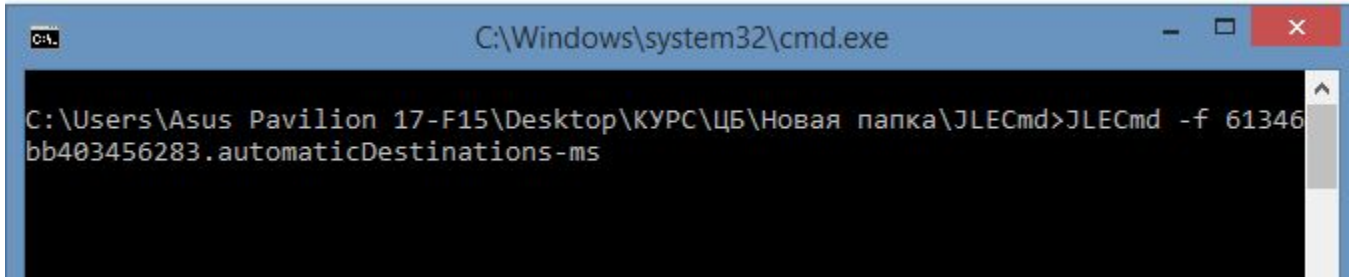
Следы открытия файлов: JumpLists

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

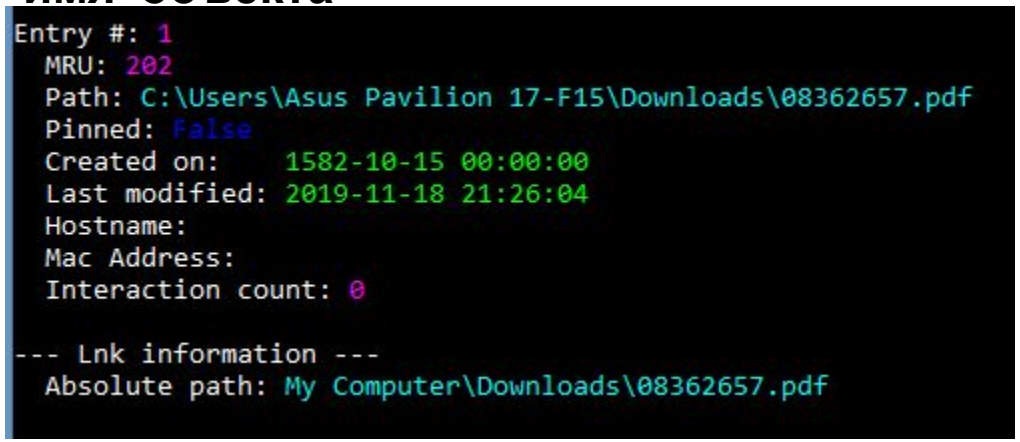


https://ericzimmerman.github.io/#!index.md -> JLEcmd

Следы открытия файлов: JumpLists

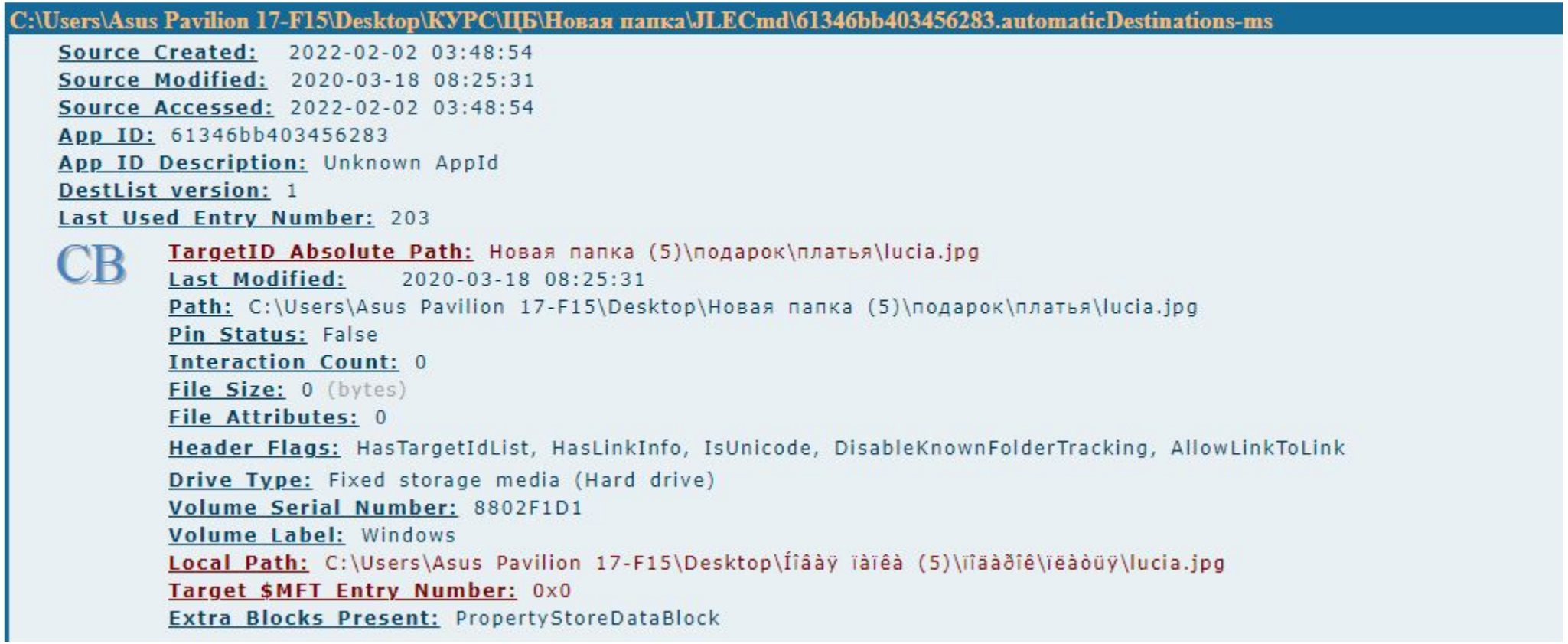


Команда – JLECmd.exe –f
имя_объекта



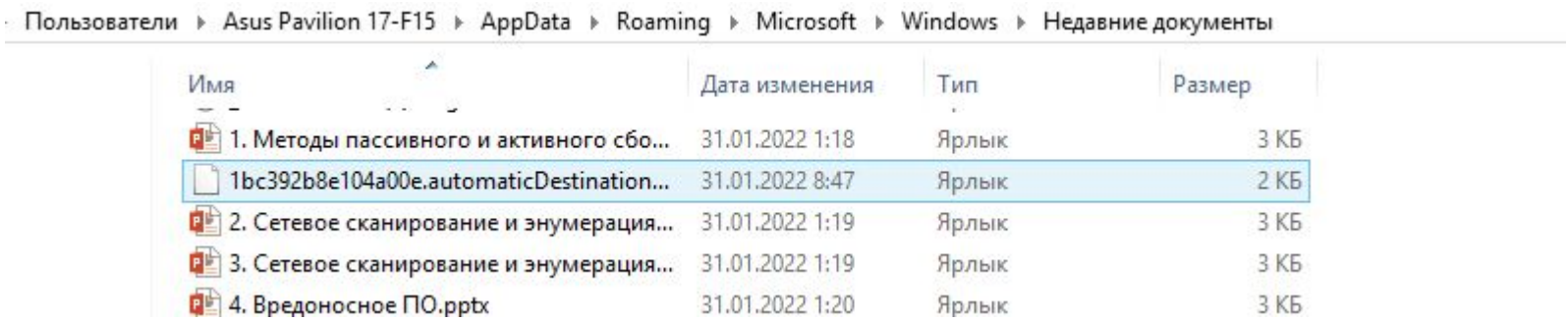
Следы открытия файлов: JumpLists

Команда – JLECmd.exe –f **имя_объекта --html путь_сохранения**
(прим. - ./ в пути сохранения сохранит в тот же каталог где находится



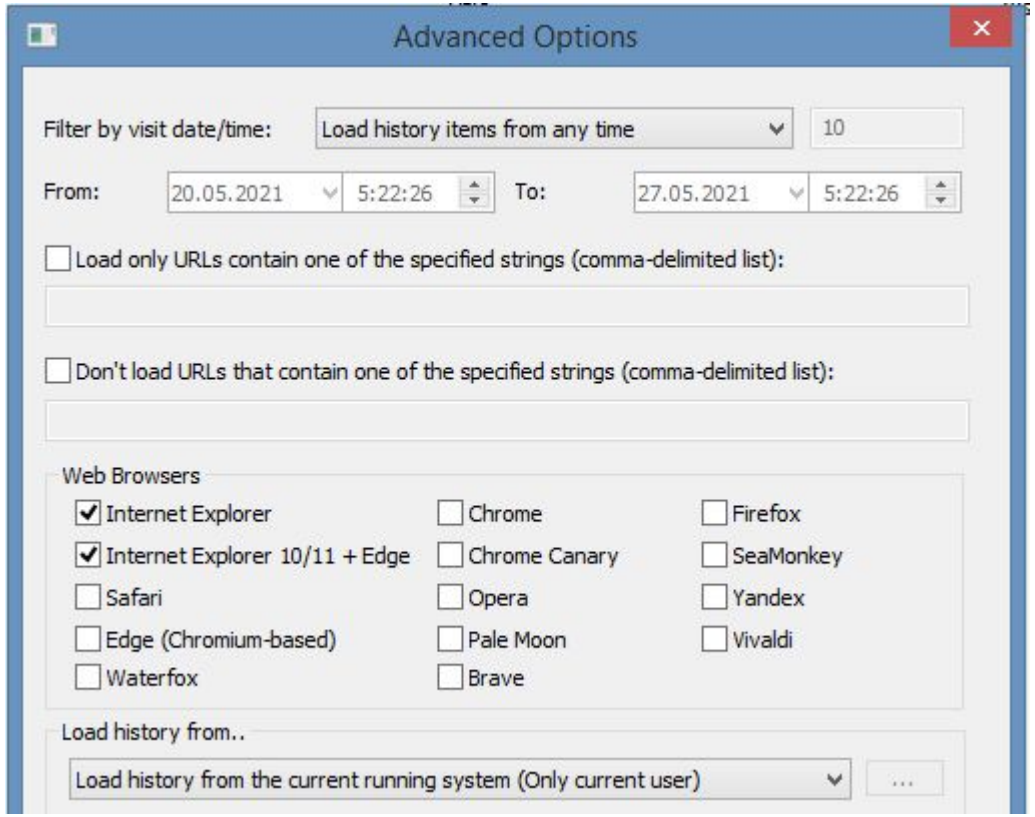
Следы открытия файлов: Recent

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



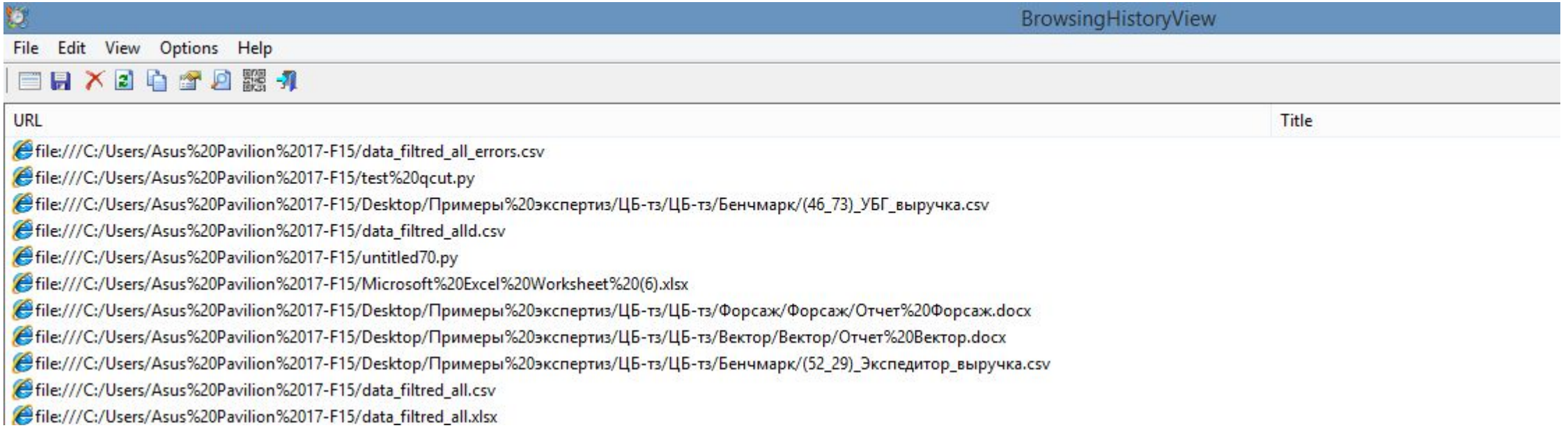
Веб-браузеры

- Основной инструмент - https://www.nirsoft.net/utils/browsing_history_view.html



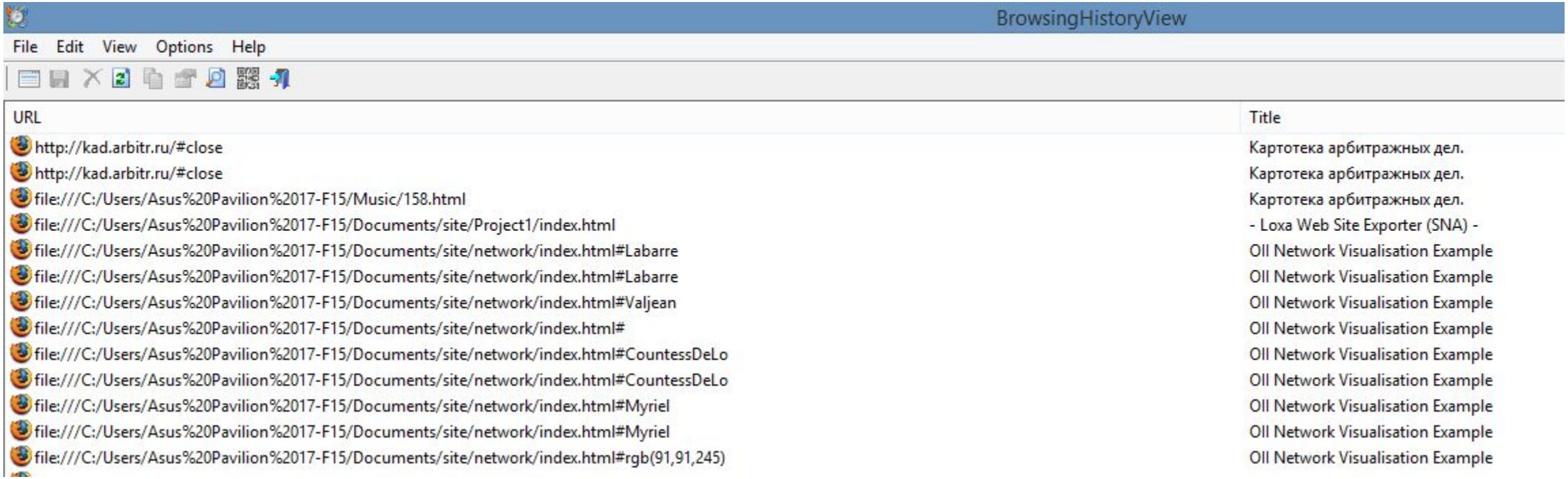
Веб-браузеры: IE/Edge

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



Веб-браузеры: Firefox

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



Веб-браузеры: Chrome

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

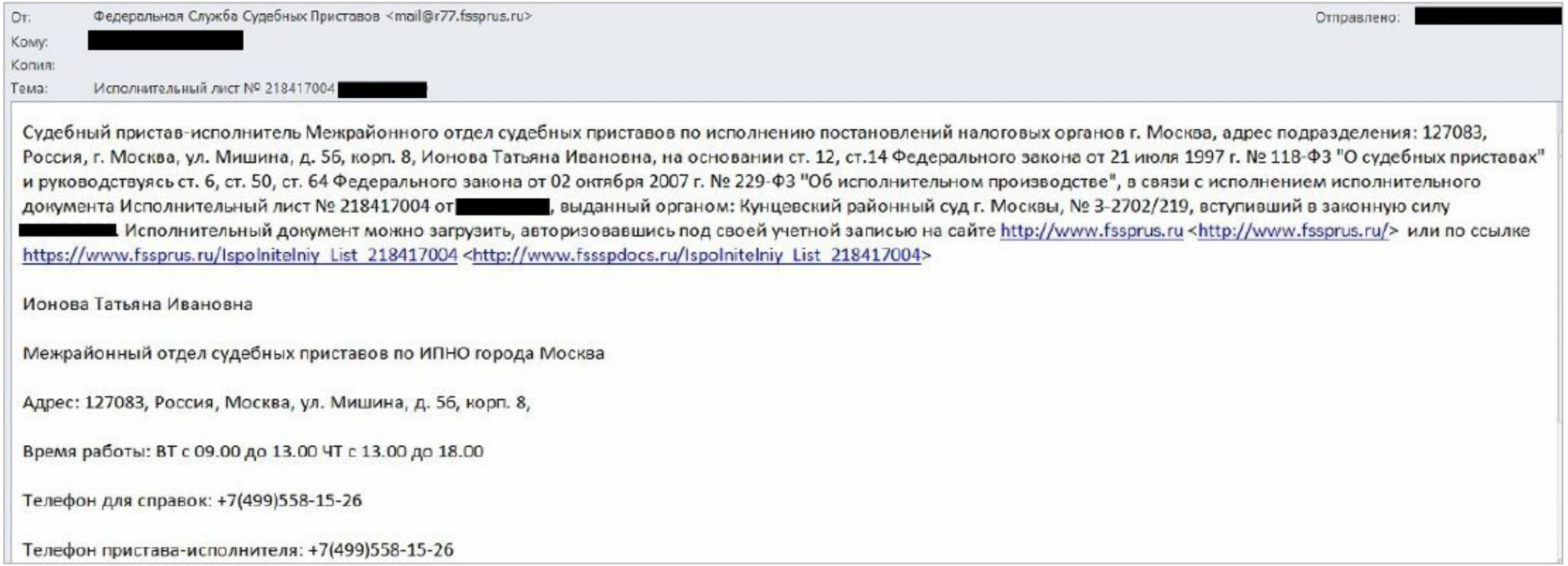
Методы доставки вредоносного ПО

- Одним из основных векторов доставки вредоносного программного обеспечения является социальная инженерия, а если говорить более конкретно – канал электронной почты.

- Поэтому, критически важным при аудите является понимание того, насколько организация устойчива к подобного рода атакам.

- Рассмотрим основные тактики применяемые злоумышленниками при использовании данного канала при доставке вредоносного ПО

Встройка URL в текст



От: Федеральная Служба Судебных Приставов <mail@r77.fssprus.ru> Отправлено: [redacted]
Кому: [redacted]
Копия:
Тема: Исполнительный лист № 218417004 [redacted]

Судебный пристав-исполнитель Межрайонного отдел судебных приставов по исполнению постановлений налоговых органов г. Москва, адрес подразделения: 127083, Россия, г. Москва, ул. Мишина, д. 56, корп. 8, Ионова Татьяна Ивановна, на основании ст. 12, ст.14 Федерального закона от 21 июля 1997 г. № 118-ФЗ "О судебных приставах" и руководствуясь ст. 6, ст. 50, ст. 64 Федерального закона от 02 октября 2007 г. № 229-ФЗ "Об исполнительном производстве", в связи с исполнением исполнительного документа Исполнительный лист № 218417004 от [redacted], выданный органом: Кунцевский районный суд г. Москвы, № 3-2702/219, вступивший в законную силу [redacted]. Исполнительный документ можно загрузить, авторизовавшись под своей учетной записью на сайте http://www.fssprus.ru <http://www.fssprus.ru/> или по ссылке https://www.fssprus.ru/Ispolnitelniy_List_218417004 <http://www.fssspdocs.ru/Ispolnitelniy_List_218417004>

Ионова Татьяна Ивановна

Межрайонный отдел судебных приставов по ИПНО города Москва

Адрес: 127083, Россия, Москва, ул. Мишина, д. 56, корп. 8,

Время работы: ВТ с 09.00 до 13.00 ЧТ с 13.00 до 18.00

Телефон для справок: +7(499)558-15-26

Телефон пристава-исполнителя: +7(499)558-15-26

Источник: Банк России: Основные типы компьютерных атак в кредитно-финансовой сфере в 2019-2020 г.

Техники обфускации URL

- Пример такого рода ссылок:

- http://youla.ru-yekaterinburg-samokaty-i-giroskutery-id@520966948

Техники обфускации URL

- Техника 1 – HTTP-аутентификация

- http://vk.com@cbr.ru

- Символ at (@) в URL исторически используется для передачи параметров аутентификации в URL-ссылке. Однако, если передавать с его помощью имя домена, то вы перенаправите жертву на домен после символа @, игнорируя часть ссылки перед ним (если не используются символы / и ?). Символ “-” является допустимым так как конкатенирует строки

Техники обфускации URL

- Техника 2 – IP-обфускация

- IP-адрес может быть представлен не только в виде канонической формы с точками (напр. http://31.13.83.36 – для Facebook) но и в других форматах:
- http://520966948 - Decimal 32 bits (напр. для cbr.ru – 3115503623)
- http://03703251444 - Octal 32 bits
- http://0x1f0d5324 - Hexadecimal 32 bits

- Техники 1 и 2 в ряде случаев можно успешно совмещать (см. пример выше)

Гомоглифические домены

- Гомоглифические домены – одна из наиболее интересных разновидностей атак с целью фишинга или доставки вредоносного ПО. Данная техника заключается в том, что для ряда доменных зон – мы можем использовать символы одного алфавита вместо символов другого (при том символы выглядят максимально правдоподобно).

- Например – apple.com и apple.com выглядят одинаково, но во втором случае – символ “a” – это русская “а” не латинская “a”

- Пример генерации - https://www.irongeek.com/homoglyph-attack-generator.php
- Домен – yoola.com

USB-устройства

- SYSTEM\CurrentControlSet\Enum\USBSTOR
- SYSTEM\CurrentControlSet\Enum\USB

1) Определяет поставщика, модель и версию USB-устройства, подключенного к машине.

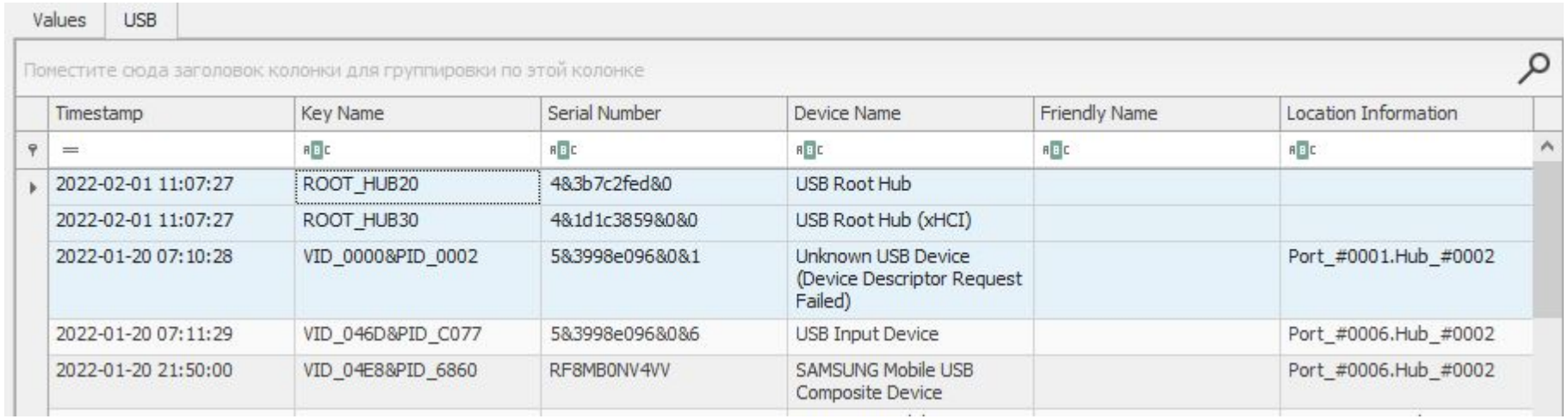
2) Определяет уникальные USB-устройства, подключенные к машине

3) Определяет время, когда устройство было подключено к машине

4) Устройства, не имеющие уникального серийного номера, будут иметь «&» во втором символе серийного номера.

USB-устройства

SYSTEM\CurrentControlSet\Enum\USB



Values | USB

Поместите сюда заголовок колонки для группировки по этой колонке

Timestamp	Key Name	Serial Number	Device Name	Friendly Name	Location Information
2022-02-01 11:07:27	ROOT_HUB20	4&3b7c2fed&0	USB Root Hub		
2022-02-01 11:07:27	ROOT_HUB30	4&1d1c3859&0&0	USB Root Hub (xHCI)		
2022-01-20 07:10:28	VID_0000&PID_0002	5&3998e096&0&1	Unknown USB Device (Device Descriptor Request Failed)		Port_#0001.Hub_#0002
2022-01-20 07:11:29	VID_046D&PID_C077	5&3998e096&0&6	USB Input Device		Port_#0006.Hub_#0002
2022-01-20 21:50:00	VID_04E8&PID_6860	RF8MB0NV4VV	SAMSUNG Mobile USB Composite Device		Port_#0006.Hub_#0002

USB-устройства

SYSTEM\CurrentControlSet\Enum\USBSTOR

	Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
▶	2022-01-29 0...	Ven_Generic	Prod_Flash_Disk	Rev_8.07	E8770C39&0	Generic Flash Disk USB Device	2021-10-01 0...	2021-10-01 0...	2022-03-29 1...	2022-03-29 1...
	2022-03-25 0...	Ven_Wilk	Prod_USB_DISK_2.0	Rev_PMAP	07011AB0DC207705&0	Wilk USB DISK 2.0 USB Device	2022-03-25 0...	2022-03-25 0...	2022-03-29 1...	2022-03-29 1...

USB-устройства – взаимодействие с пользователем

- Шаг 1 – Смотрим GUID устройства в SYSTEM\MountedDevices
- Шаг 2 – Смотрим кто его установил NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer \MountPoints2

- Этот GUID будет использоваться для идентификации пользователя, подключившего устройство. Время последней записи этого ключа также соответствует времени последнего подключения устройства к машине этим пользователем.

USB-устройства – взаимодействие с пользователем

\??\Volume{a6c6c501-8121-11e4-825e-b01041eabcbc}	_??_USBSTOR#Disk&Ven_QUMO&Prod_QUMO&Rev_1100#03357140300009 82&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
\??\Volume{7b2dafdb-87df-11e4-825f-b01041eabcbc}	_??_USBSTOR#Disk&Ven_UFD_2.0&Prod_Silicon-Power4G&Rev_1100#1401549901900167&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
\??\Volume{44cbddc9-8a67-11e4-8262-8cdcd47b0aa0}	_??_USBSTOR#Disk&Ven_UFD_2.0&Prod_Silicon-Power4G&Rev_1100#1401549901500160&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
\??\Volume{1bc5e8cb-d4e3-11e4-82db-8cdcd47b0aa0}	_??_USBSTOR#Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07#DD7C0BA9&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

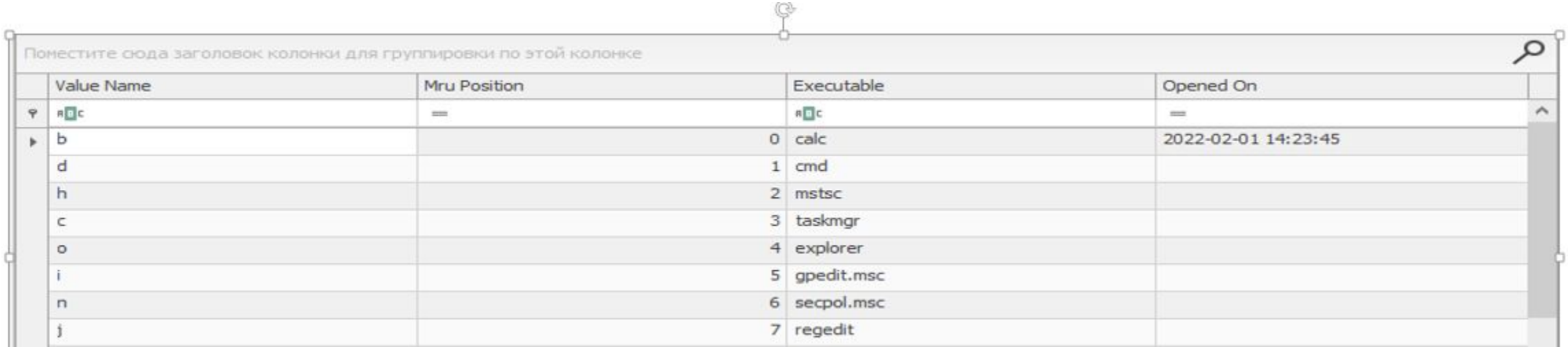
SYSTEM\MountedDevices

{05934580-b29d-11eb-872a-8cdcd47b0aa0}	0	1	2021-09-15 04:33:11
{06b04209-99bf-11e6-8429-8cdcd47b0aa0}	0	0	2017-01-24 10:03:56
{06b0420b-99bf-11e6-8429-8cdcd47b0aa0}	0	1	2017-01-24 10:01:05
{0743cb0e-d9bf-11e7-853d-8cdcd47b0aa0}	0	1	2017-12-07 10:10:35

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Запуск команд через “Выполнить”

NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

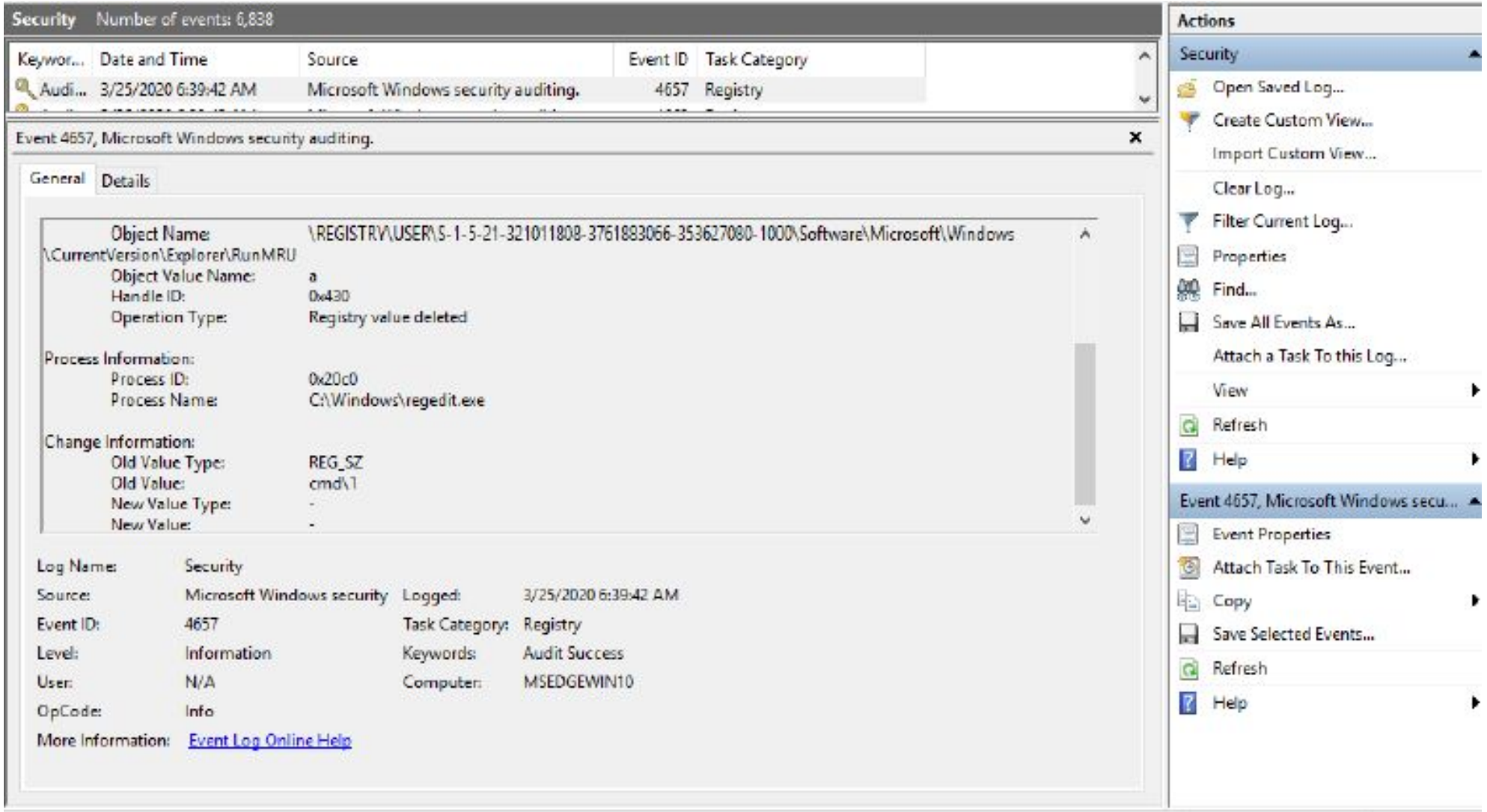


Поместите сюда заголовок колонки для группировки по этой колонке

Value Name	Mru Position	Executable	Opened On
b	0	calc	2022-02-01 14:23:45
d	1	cmd	
h	2	mstsc	
c	3	taskmgr	
o	4	explorer	
i	5	gpedit.msc	
n	6	secpol.msc	
j	7	regedit	

Если включен аудит реестра - https://4sysops.com/archives/audit-changes-in-the-windows-registry/ то в журнале Security с кодом события 4657 можно обнаружить следы удаления значений

Запуск команд через “Выполнить”



Документы открываемые в MS Office

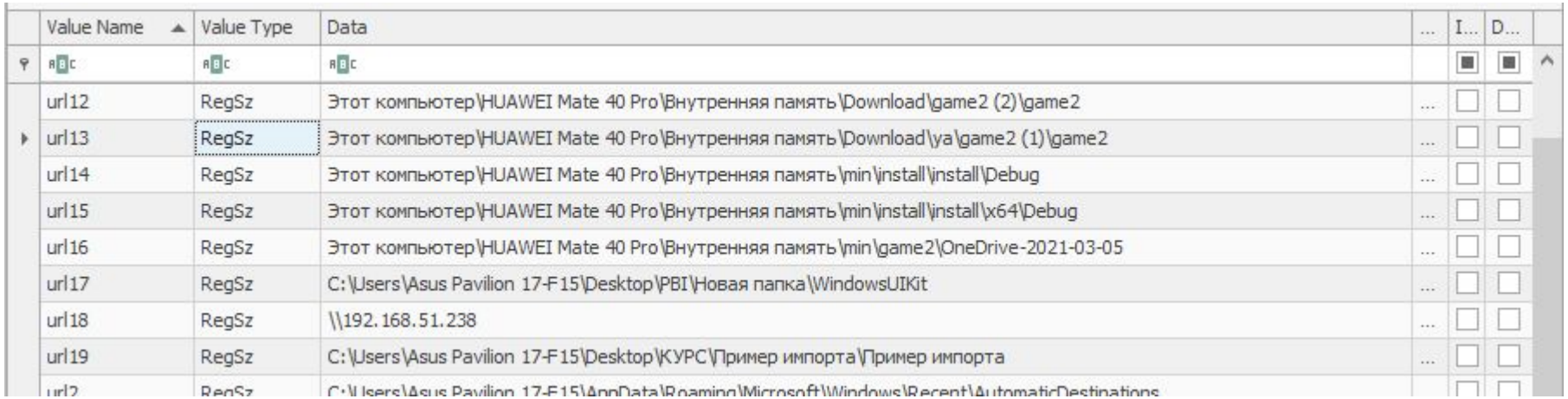
NTUSER.DAT| Software\Microsoft\Office\версия\Word, Excel и т. п.\FileMRU и PlaceMRU

Value Name	Value Type	Data	...	...	Data R...
Item 1	RegSz	[F00000000][T01D81779D47A0DC0][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\Примеры экспертиз\ЦБ-тз\Ц...	...	☐	☐
Item 10	RegSz	[F00000000][T01D81771E5C18D40][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\Примеры экспертиз\ЦБ-тз\ЦБ...	...	☐	☐
Item 11	RegSz	[F00000000][T01D816A06810CEA0][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\Примеры экспертиз\Эксперти...	...	☐	☐
Item 12	RegSz	[F00000000][T01D8168833EB94B0][O00000000]*C:\Users\Asus Pavilion 17-F15\Downloads\Список ПО Тема 1.docx	...	☐	☐
Item 13	RegSz	[F00000000][T01D81682500C69E0][O00000000]*C:\Users\Asus Pavilion 17-F15\Downloads\Мануал по деанонимизации...	...	☐	☐
Item 14	RegSz	[F00000000][T01D8167376002240][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\КУРС\ЦБ\Дополнительные ма...	...	☐	☐

Value Name	Value Type	Data	...	...	Data R...
Item 1	RegSz	[F00000000][T01D81779D47C57B0][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\Примеры экспертиз\ЦБ-тз\ЦБ...	...	☐	☐
Item 10	RegSz	[F00000000][T01D81771E5C18D42][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\Примеры экспертиз\ЦБ-тз\ЦБ...	...	☐	☐
Item 11	RegSz	[F00000000][T01D816A068100B50][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\Примеры экспертиз\	...	☐	☐
Item 12	RegSz	[F00000000][T01D8168833EAD160][O00000000]*C:\Users\Asus Pavilion 17-F15\Downloads\	...	☐	☐
Item 13	RegSz	[F00000000][T01D8167375FE2670][O00000000]*C:\Users\Asus Pavilion 17-F15\Desktop\КУРС\ЦБ\Дополнительные ма...	...	☐	☐
Item 14	RegSz	[F00000000][T01D81656FA493590][O00000000]*C:\EVIDENCE\эксп\Цифровые следы\Документы\	...	☐	☐

Пути набранные в Проводнике

NTUSER.DAT| Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths



Value Name	Value Type	Data	...	I...	D...
url12	RegSz	Этот компьютер\HUAWEI Mate 40 Pro\Внутренняя память\Download\game2 (2)\game2	...		
url13	RegSz	Этот компьютер\HUAWEI Mate 40 Pro\Внутренняя память\Download\ya\game2 (1)\game2	...		
url14	RegSz	Этот компьютер\HUAWEI Mate 40 Pro\Внутренняя память\min\install\install\Debug	...		
url15	RegSz	Этот компьютер\HUAWEI Mate 40 Pro\Внутренняя память\min\install\install\x64\Debug	...		
url16	RegSz	Этот компьютер\HUAWEI Mate 40 Pro\Внутренняя память\min\game2\OneDrive-2021-03-05	...		
url17	RegSz	C:\Users\Asus Pavilion 17-F15\Desktop\PBI\Новая папка\WindowsUIKit	...		
url18	RegSz	\\192.168.51.238	...		
url19	RegSz	C:\Users\Asus Pavilion 17-F15\Desktop\КУРС\Пример импорта\Пример импорта	...		
url2	RegSz	C:\Users\Asus Pavilion 17-F15\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations			

Подсказки в Проводнике

NTUSER.DAT| Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Search Term	Mru Position	Key Name	Last Write Timestamp
DADATA	0	WordWheelQuery	2022-02-01 14:55:41
Anaco	0	{F9785269-044B-4CA1-8CE5-1D5D31ED6B79}	2021-04-09 04:37:10
dada	1	WordWheelQuery	
Stee	1	{F9785269-044B-4CA1-8CE5-1D5D31ED6B79}	
GSM	2	WordWheelQuery	
con	2	{F9785269-044B-4CA1-8CE5-1D5D31ED6B79}	
gsn	3	WordWheelQuery	
py	3	{F9785269-044B-4CA1-8CE5-1D5D31ED6B79}	

Логины и пароли

- Команда – lazagne.exe all > имя_файла.txt

```
[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Kalash_nick
Password: 12345678NUL
```

```
[+] Password found !!!
URL: ASUS\adm
Login: ASUS\adm
Password: 1NUL2NUL3NUL
```

```
[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Police of your heart
Password: domadoma51NUL
```

```
[-] Password not found !!!
URL: Domain:target=TERMSRV/192.168.1.72
Login: me
```

https://github.com/AlessandroZ/LaZagne/releases

Подключенные сети

Microsoft\Windows NT\CurrentVersion\NetworkList

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

Network Name	Name Type	First Connect LOCAL	Last Connected L...	Managed	DNS Suffix	Gateway Mac Add...	Profile GUID
Сеть 78	Wired	2019-07-17 23:06...	2019-07-19 11:25...	☐	<отсутствует>	4C-5E-0C-39-4B-EC	{00DA5301-A981-43AF-A0DD-826D36096F22}
Сеть 5	Wired	2016-08-12 17:27...	2020-01-03 13:52...	☐	localnet	00-0B-2B-43-3B-45	{00E5F892-AA66-4B77-A826-1687219CDF2F}
Сеть 105	Wired	2020-03-18 12:59...	2020-03-18 13:24...	☐	<отсутствует>	60-14-66-89-61-47	{01D93DE7-A687-477B-9BED-DA78730396EB}

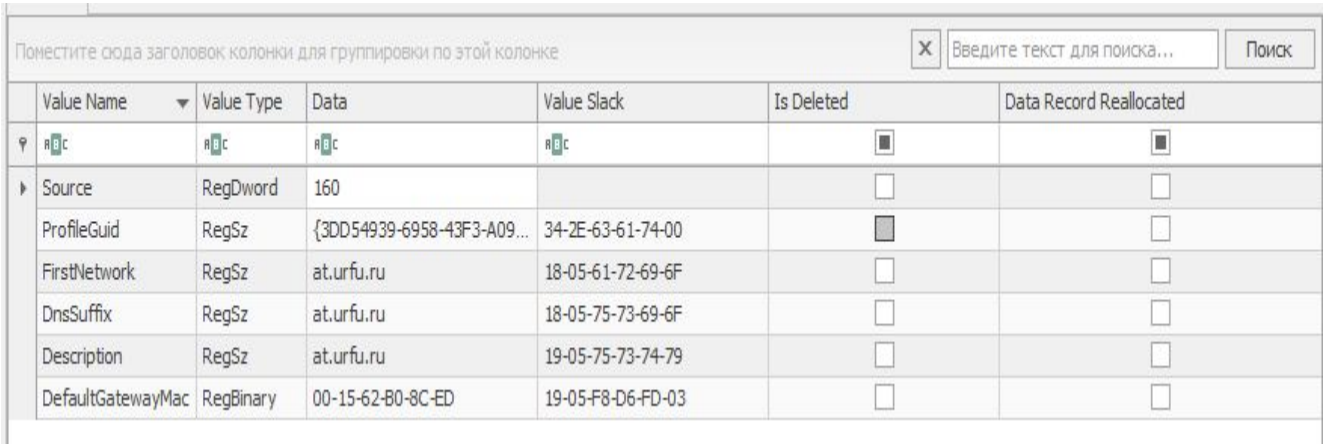
Подключенные сети

Microsoft\Windows NT\CurrentVersion\NetworkList

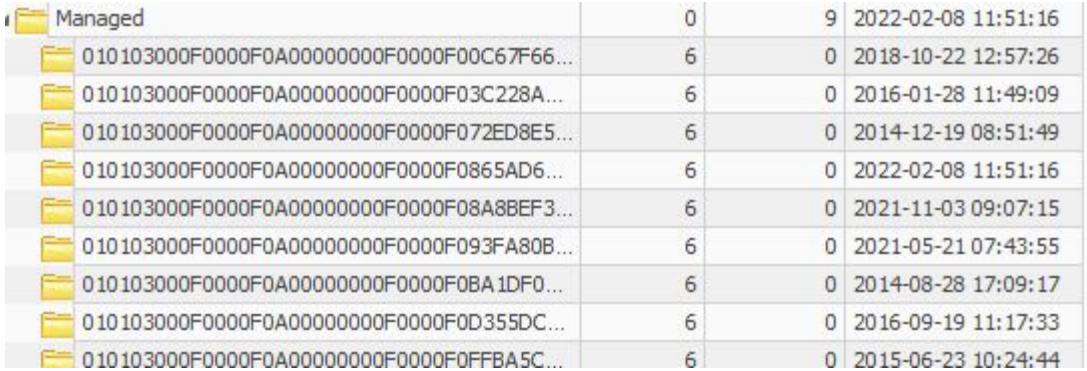
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache



Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
Source	RegDword	160		☐	☐
ProfileGuid	RegSz	{3DD54939-6958-43F3-A09...	34-2E-63-61-74-00	■	☐
FirstNetwork	RegSz	at.urfu.ru	18-05-61-72-69-6F	☐	☐
DnsSuffix	RegSz	at.urfu.ru	18-05-75-73-69-6F	☐	☐
Description	RegSz	at.urfu.ru	19-05-75-73-74-79	☐	☐
DefaultGatewayMac	RegBinary	00-15-62-B0-8C-ED	19-05-F8-D6-FD-03	☐	☐



Managed	0	9	2022-02-08 11:51:16
010103000F0000F0A00000000F0000F00C67F66...	6	0	2018-10-22 12:57:26
010103000F0000F0A00000000F0000F03C228A...	6	0	2016-01-28 11:49:09
010103000F0000F0A00000000F0000F072ED8E5...	6	0	2014-12-19 08:51:49
010103000F0000F0A00000000F0000F0865AD6...	6	0	2022-02-08 11:51:16
010103000F0000F0A00000000F0000F08A8BEF3...	6	0	2021-11-03 09:07:15
010103000F0000F0A00000000F0000F093FA80B...	6	0	2021-05-21 07:43:55
010103000F0000F0A00000000F0000F0BA1DF0...	6	0	2014-08-28 17:09:17
010103000F0000F0A00000000F0000F0D355DC...	6	0	2016-09-19 11:17:33
010103000F0000F0A00000000F0000F0FFBA5C...	6	0	2015-06-23 10:24:44

Подключенные сети

Microsoft\Windows NT\CurrentVersion\NetworkList

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

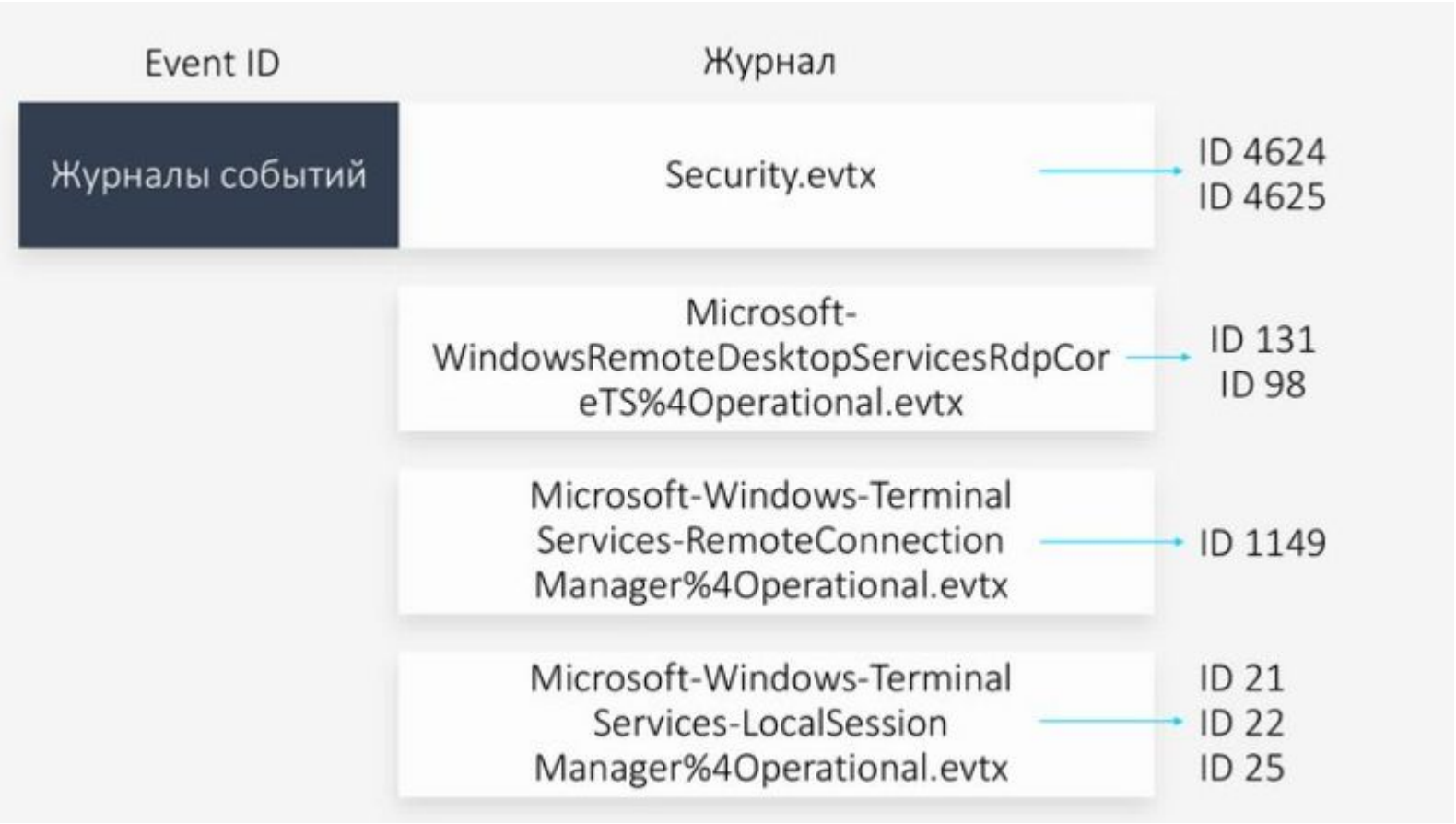
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

Value Name	Value Type	Data	Value Slack
Source	RegDword	8	
ProfileGuid	RegSz	{201305E0-74A9-4D2D-852...	74-65-67-65-72-73
FirstNetwork	RegSz	Сеть 103	
DnsSuffix	RegSz	tagil.cloud	65-73-0D-00
Description	RegSz	Сеть 103	
DefaultGatewayMac	RegBinary	02-41-94-76-98-50	D2-09-38-22-2E-06

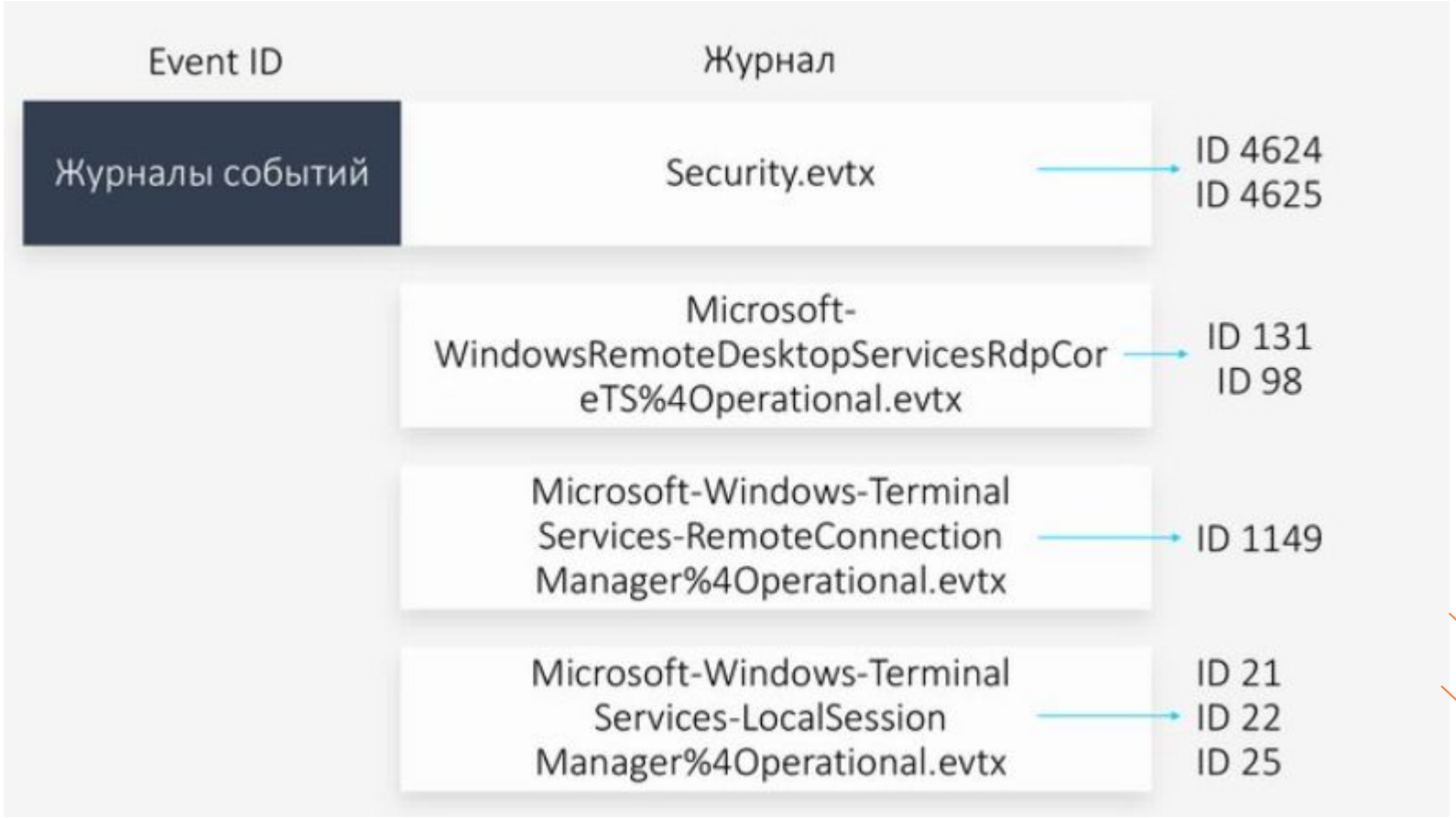
010103000F0000F0080000000F0000F01B...	6	0	2020-03-16 08:52:13
010103000F0000F0080000000F0000F01C029B1...	6	0	2015-08-07 04:38:16
010103000F0000F0080000000F0000F020E95FC...	6	0	2017-06-15 12:40:16
010103000F0000F0080000000F0000F021A38C7...	6	0	2015-06-22 07:08:58
010103000F0000F0080000000F0000F022B5464...	6	0	2021-03-02 12:58:57
010103000F0000F0080000000F0000F02364C60...	6	0	2017-06-30 12:05:21

Подключения по RDP

- C:\Windows\System32\winevt\Logs



Подключения по RDP

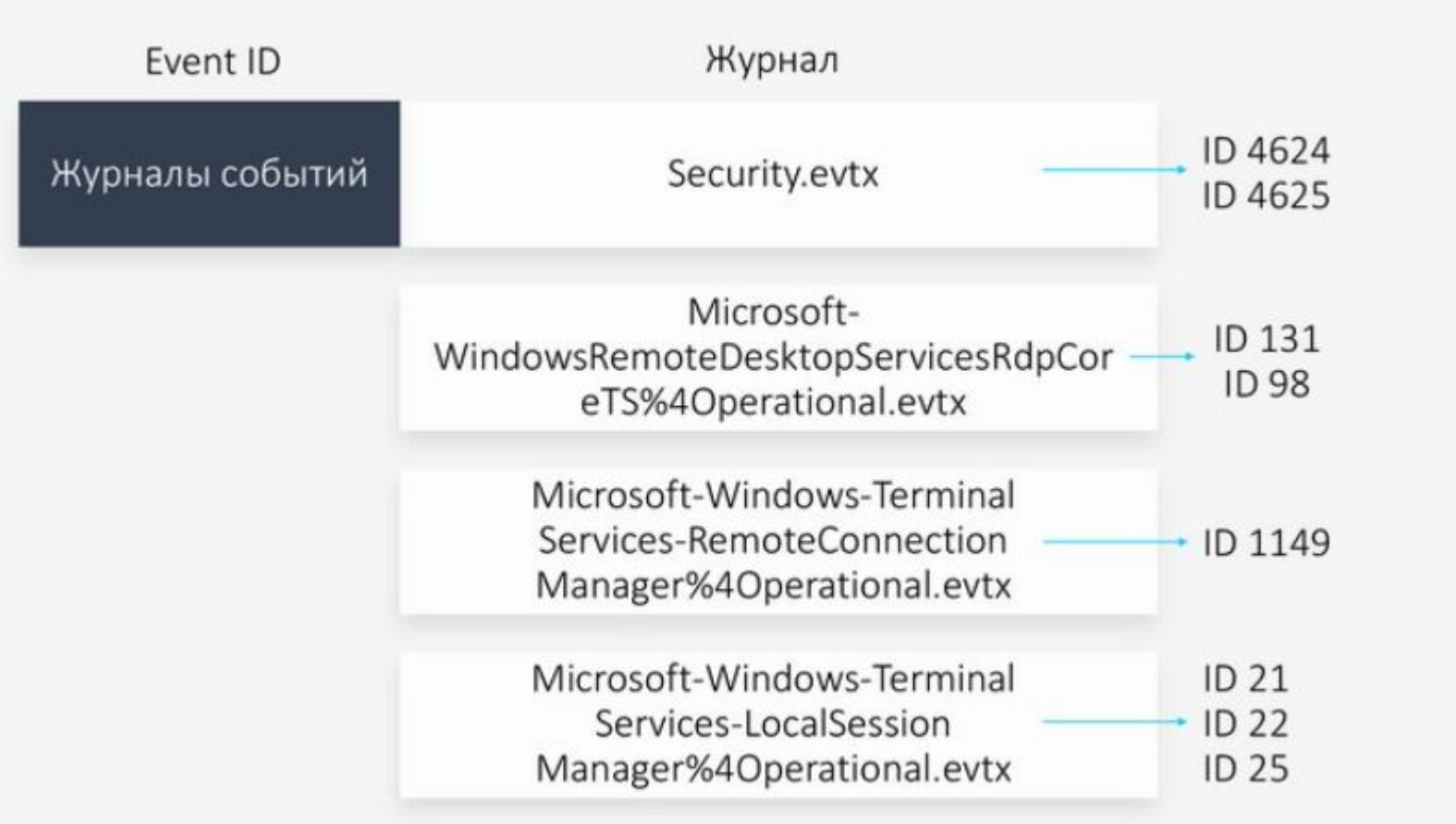


Код	Описание
4624	Успешный логин
4625	Неуспешный логин

Interpretation

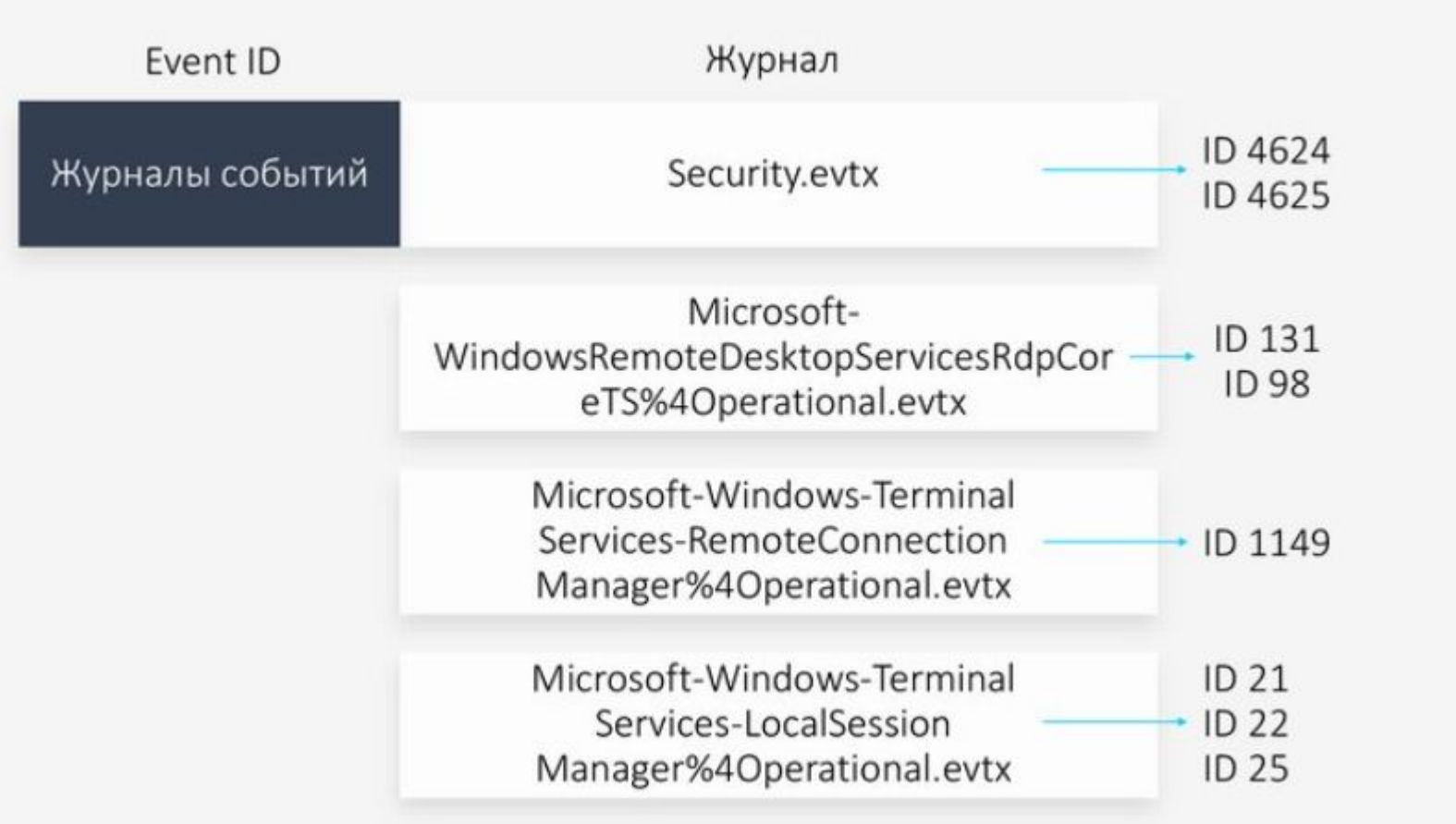
Logon Type	Explanation
2	Logon via console
3	Network Logon
4	Batch Logon
5	Windows Service Logon
7	Credentials used to unlock screen
8	Network logon sending credentials (cleartext)
9	Different credentials used than logged on user
10	Remote interactive logon (RDP)
11	Cached credentials used to logon
12	Cached remote interactive (similar to Type 10)
13	Cached unlock (similar to Type 7)

Подключения по RDP



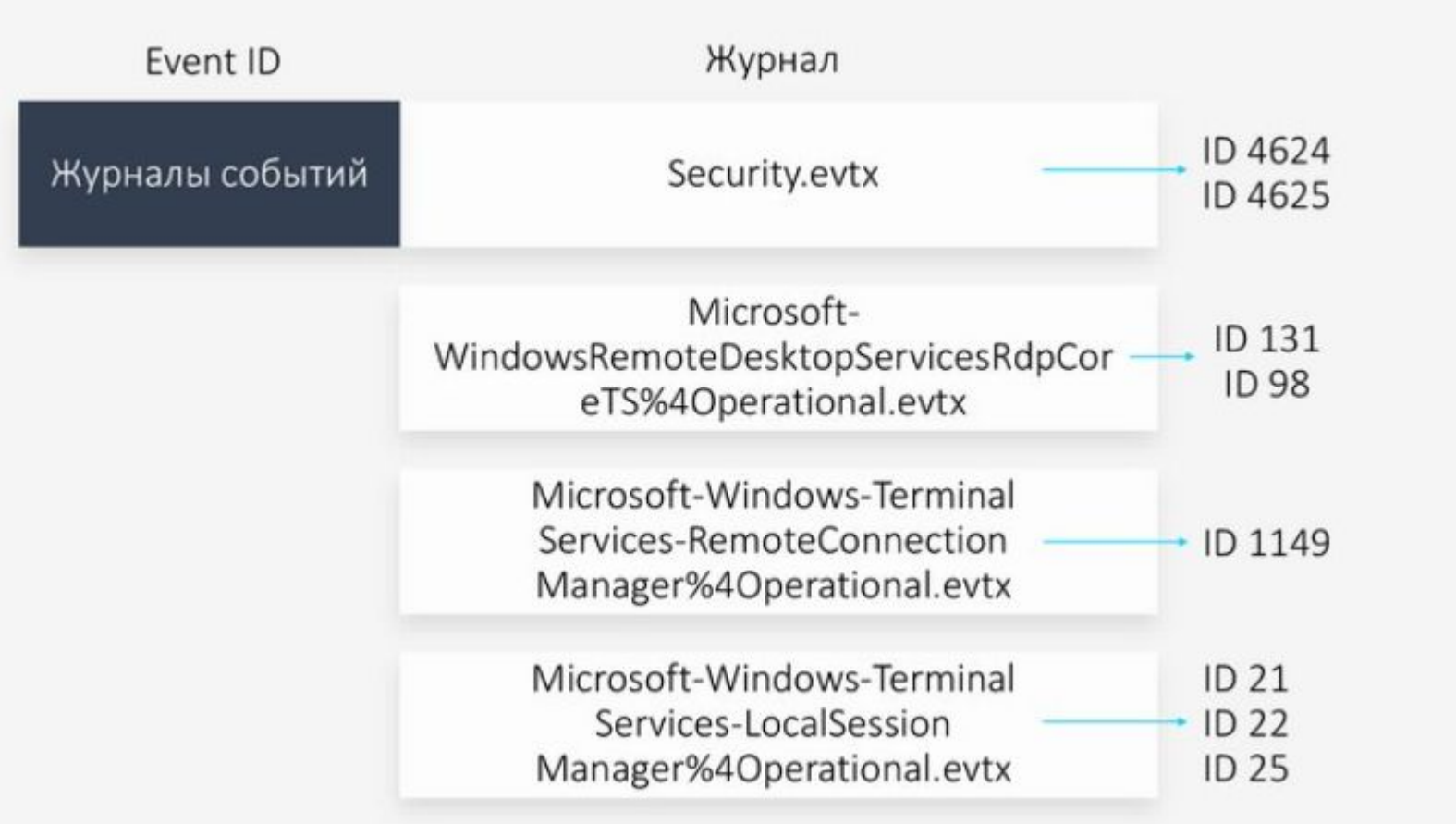
Код	Описание
131	прием RDP соединения (с IP)
98	установление соединения

Подключения по RDP



Код	Описание
1149	Успешный вход по RDP на компьютер

Подключения по RDP



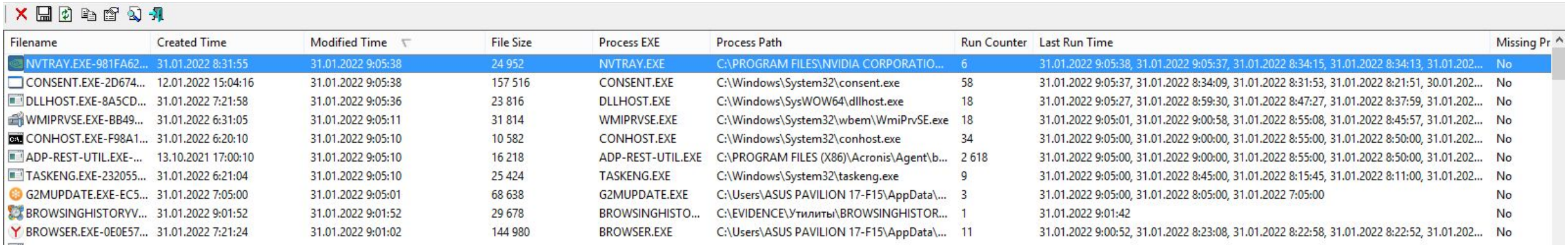
Код	Описание
21	Успешный вход в текущую сессию
22	Открытие GUI в RDP
25	Выход из сессии

Следы запуска программного обеспечения

WinPrefetch

Путь: C:\Windows\Prefetch

- Утилита: https://www.nirsoft.net/utils/win_prefetch_view.html



Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Pr
NVTRAY.EXE-981FA62...	31.01.2022 8:31:55	31.01.2022 9:05:38	24 952	NVTRAY.EXE	C:\PROGRAM FILES\NVIDIA CORPORATIO...	6	31.01.2022 9:05:38, 31.01.2022 9:05:37, 31.01.2022 8:34:15, 31.01.2022 8:34:13, 31.01.202...	No
CONSENT.EXE-2D674...	12.01.2022 15:04:16	31.01.2022 9:05:38	157 516	CONSENT.EXE	C:\Windows\System32\consent.exe	58	31.01.2022 9:05:37, 31.01.2022 8:34:09, 31.01.2022 8:31:53, 31.01.2022 8:21:51, 30.01.202...	No
DLLHOST.EXE-8A5CD...	31.01.2022 7:21:58	31.01.2022 9:05:36	23 816	DLLHOST.EXE	C:\Windows\SysWOW64\dllhost.exe	18	31.01.2022 9:05:27, 31.01.2022 8:59:30, 31.01.2022 8:47:27, 31.01.2022 8:37:59, 31.01.202...	No
WMIPRVSE.EXE-BB49...	31.01.2022 6:31:05	31.01.2022 9:05:11	31 814	WMIPRVSE.EXE	C:\Windows\System32\wbem\WmiPrvSE.exe	18	31.01.2022 9:05:01, 31.01.2022 9:00:58, 31.01.2022 8:55:08, 31.01.2022 8:45:57, 31.01.202...	No
CONHOST.EXE-F98A1...	31.01.2022 6:20:10	31.01.2022 9:05:10	10 582	CONHOST.EXE	C:\Windows\System32\conhost.exe	34	31.01.2022 9:05:00, 31.01.2022 9:00:00, 31.01.2022 8:55:00, 31.01.2022 8:50:00, 31.01.202...	No
ADP-REST-UTIL.EXE-...	13.10.2021 17:00:10	31.01.2022 9:05:10	16 218	ADP-REST-UTIL.EXE	C:\PROGRAM FILES (X86)\Acronis\Agent\b...	2 618	31.01.2022 9:05:00, 31.01.2022 9:00:00, 31.01.2022 8:55:00, 31.01.2022 8:50:00, 31.01.202...	No
TASKENG.EXE-232055...	31.01.2022 6:21:04	31.01.2022 9:05:10	25 424	TASKENG.EXE	C:\Windows\System32\taskeng.exe	9	31.01.2022 9:05:00, 31.01.2022 8:45:00, 31.01.2022 8:15:45, 31.01.2022 8:11:00, 31.01.202...	No
G2MUPDATE.EXE-EC5...	31.01.2022 7:05:00	31.01.2022 9:05:01	68 638	G2MUPDATE.EXE	C:\Users\ASUS PAVILION 17-F15\AppData\...	3	31.01.2022 9:05:00, 31.01.2022 8:05:00, 31.01.2022 7:05:00	No
BROWSINGHISTORYV...	31.01.2022 9:01:52	31.01.2022 9:01:52	29 678	BROWSINGHISTO...	C:\EVIDENCE\Утилиты\BROWSINGHISTOR...	1	31.01.2022 9:01:42	No
BROWSER.EXE-0E0E57...	31.01.2022 7:21:24	31.01.2022 9:01:02	144 980	BROWSER.EXE	C:\Users\ASUS PAVILION 17-F15\AppData\...	11	31.01.2022 9:00:52, 31.01.2022 8:23:08, 31.01.2022 8:22:58, 31.01.2022 8:22:52, 31.01.202...	No

UserAssist

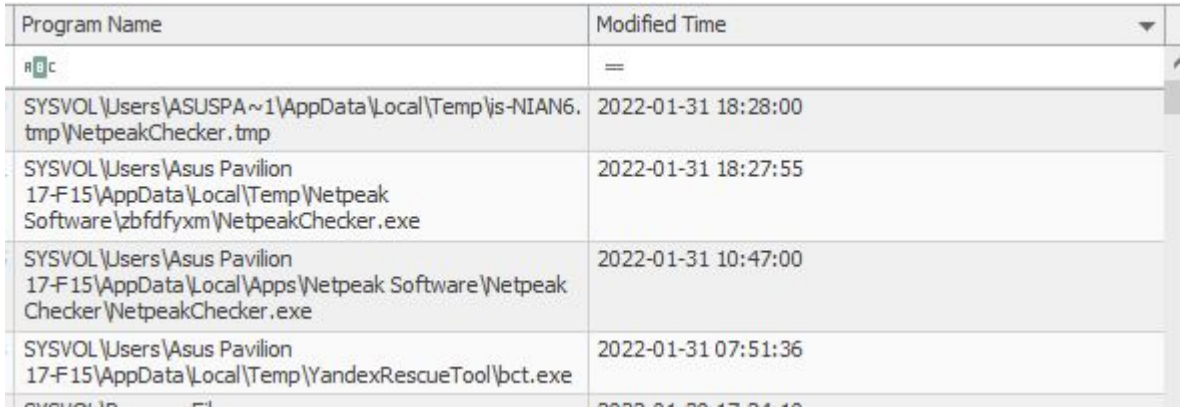
- Путь: NTUSER.DAT |

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

	Program Name	Run Counter	Focus Count	Focus Time	Last Executed
	UEME_CTLSESSION	138	2001	0d, 23h, 30m, 01s	
	Microsoft.Windows.RemoteDesktop	0	0	0d, 0h, 00m, 00s	2020-03-24 04:05:52
	UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s	
	Microsoft.Windows.ControlPanel	0	1	0d, 0h, 01m, 14s	
	Microsoft.InternetExplorer.Default	0	0	0d, 0h, 00m, 00s	2022-01-18 13:05:14

ShimCache

- Списки переходов, панель задач Windows 7-10 (список переходов) спроектирована таким образом, чтобы пользователи могли быстро получить доступ к элементам, которые они часто или недавно использовали.
- SYSTEM|ControlSet001\Control\Session Manager\AppCompatCache



Program Name	Modified Time
SYSVOL\Users\ASUSPA~1\AppData\Local\Temp\js-NIAN6.tmp\NetpeakChecker.tmp	2022-01-31 18:28:00
SYSVOL\Users\Asus Pavilion 17-F15\AppData\Local\Temp\Netpeak Software\zbfdfyxm\NetpeakChecker.exe	2022-01-31 18:27:55
SYSVOL\Users\Asus Pavilion 17-F15\AppData\Local\Apps\Netpeak Software\Netpeak Checker\NetpeakChecker.exe	2022-01-31 10:47:00
SYSVOL\Users\Asus Pavilion 17-F15\AppData\Local\Temp\YandexRescueTool\bct.exe	2022-01-31 07:51:36

Следы закрепления в системе

Ключи реестра RUN

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

Startup Folders

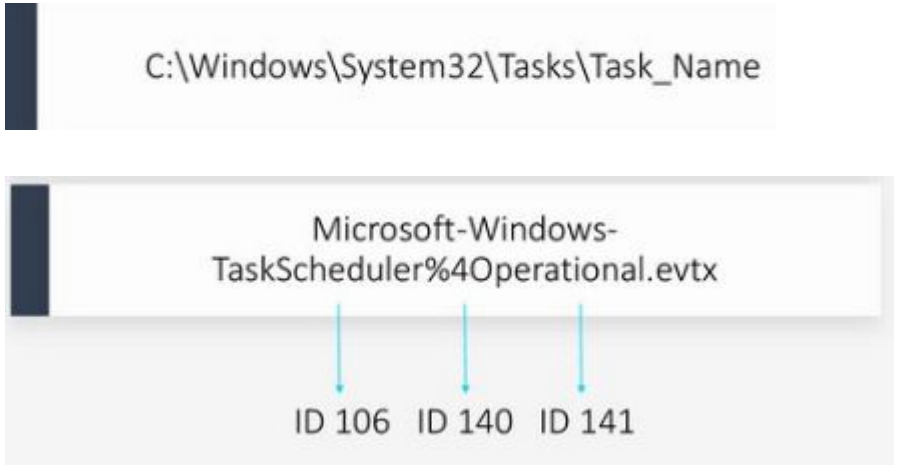
Пользователь	Путь
Current user	C:\Users\<profile>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
All users	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Запланированные задания

- Популярный путь – создание запланированных заданий

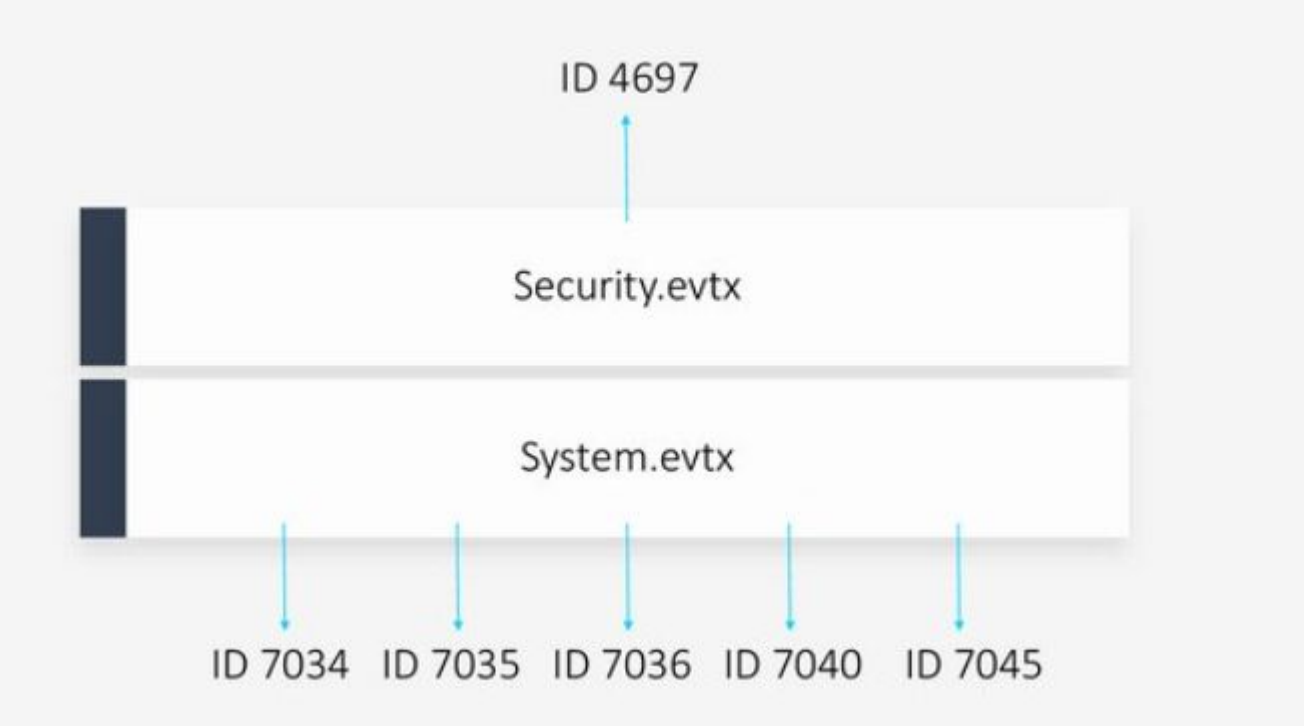
```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.4" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2021-07-07T07:18:27.0218058</Date>
    <Author>УДАЛЕНО</Author>
    <URI>\ УДАЛЕНО</URI>
  </RegistrationInfo>
  <Triggers>
    <SessionStateChangeTrigger>
      <Enabled>true</Enabled>
      <StateChange>SessionLock</StateChange>
      <Delay>PT3M</Delay>
    </SessionStateChangeTrigger>
    <IdleTrigger>
      <Enabled>true</Enabled>
    </IdleTrigger>
    <BootTrigger>
      <Enabled>true</Enabled>
      <Delay>PT5M</Delay>
    </BootTrigger>
    <EventTrigger>
      <Enabled>true</Enabled>
      <Subscription>&lt;QueryList&gt;&lt;Query Id="0" Path="Security"&gt;&lt;Select
Path="Security"&gt;*[System[EventID=4647]]&lt;/Select&gt;&lt;/Query&gt;&lt;/QueryList&gt;</S
ubscription>
      <Delay>PT3M</Delay>
```

Запланированные задания



Код	Описание
106	Задача создана
140	Задача изменена
141	Задача удалена

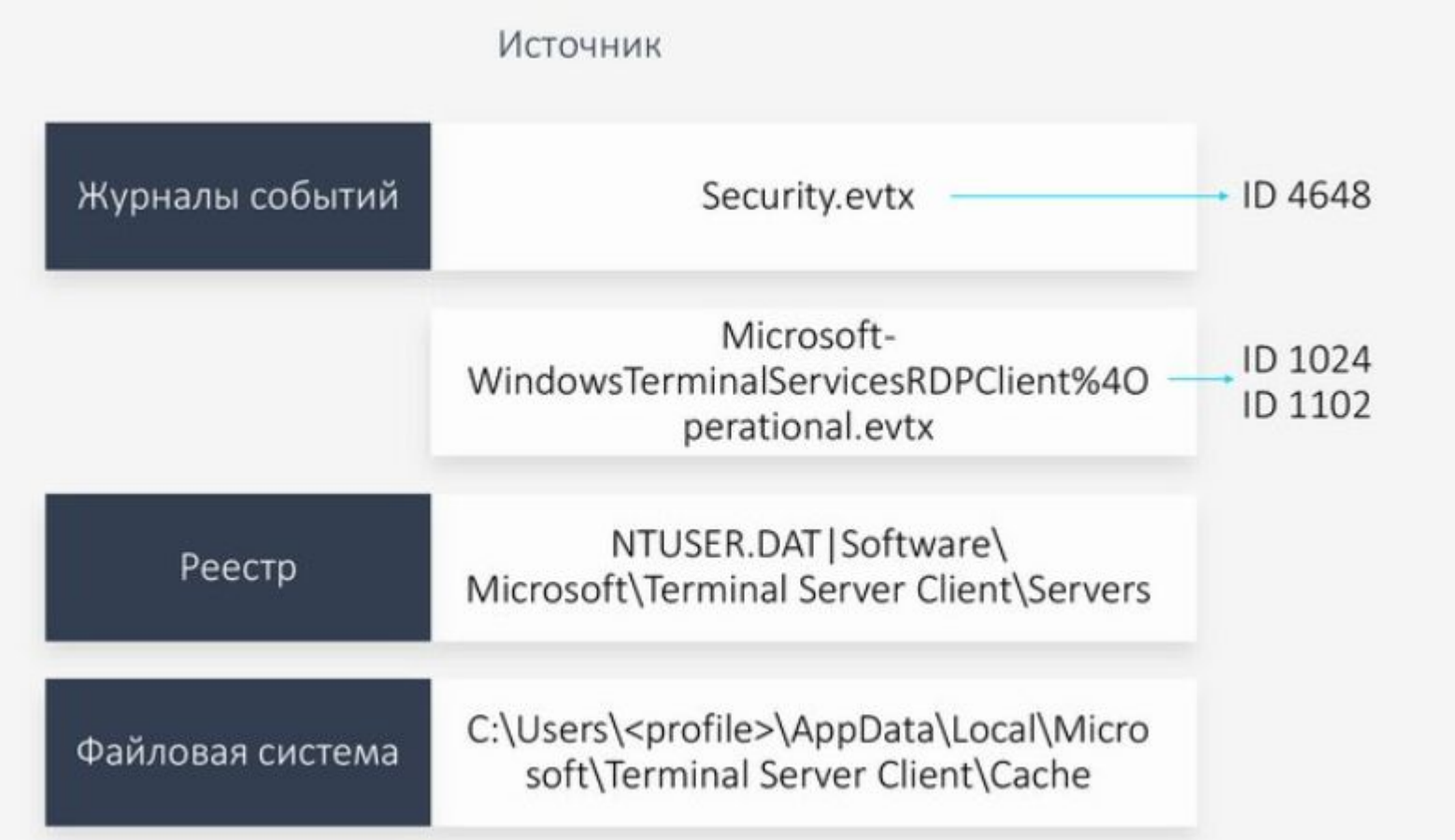
Создание служб



Код	Описание
7034	Служба неожиданно остановлена
7035	Служба остановлена пользователем (как правило возникает при отключении логирования событий) https://attack.mitre.org/techniques/T1562/002/
7036	Служба начинает остановку
7040	Изменение параметров старта службы
7045	В системе создана служба
4697	В системе создана служба

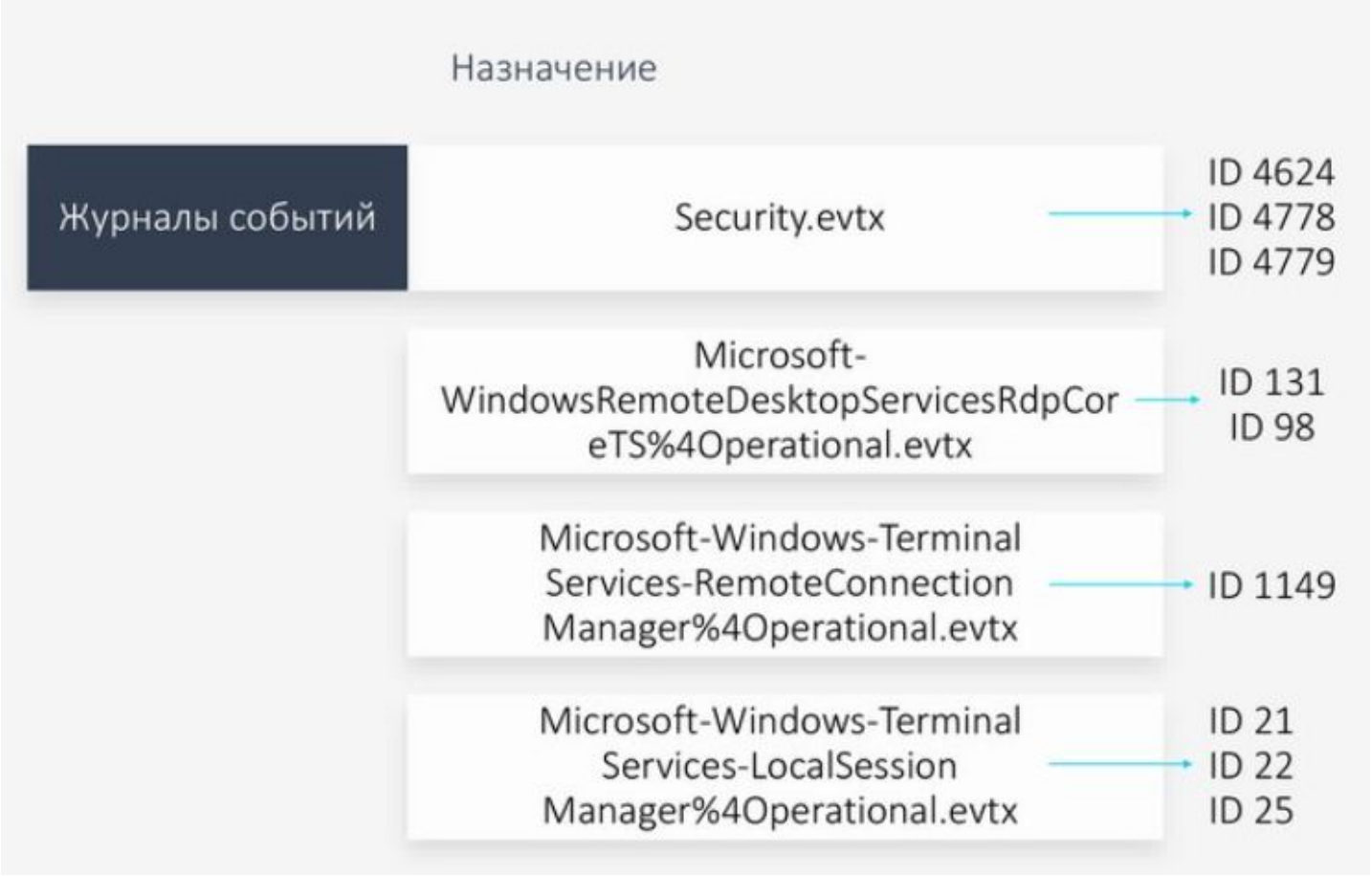
Поиск следов горизонтального продвижения

RDP



Код	Описание
4648	Использование других реквизитов в текущей сессии (Runas)
1024	Пользователь инициирует соединение RDP с помощью клиента RDP MSTSC.exe в Windows, нажав "подключиться". Записи о событиях 1024 будут созданы независимо от того, подключен сеанс или нет.
1102	Успех события 1024

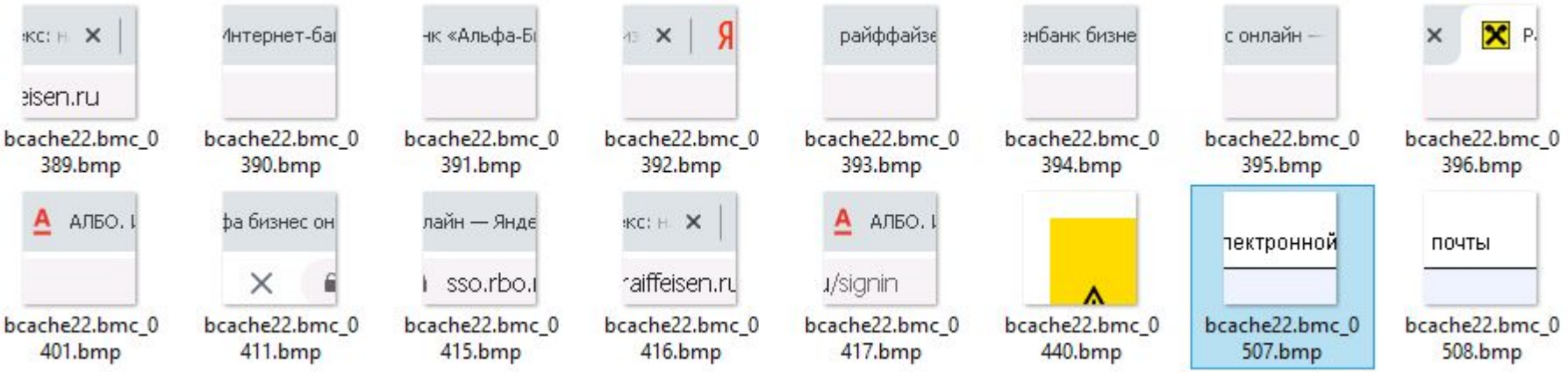
RDP


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

См. ранее

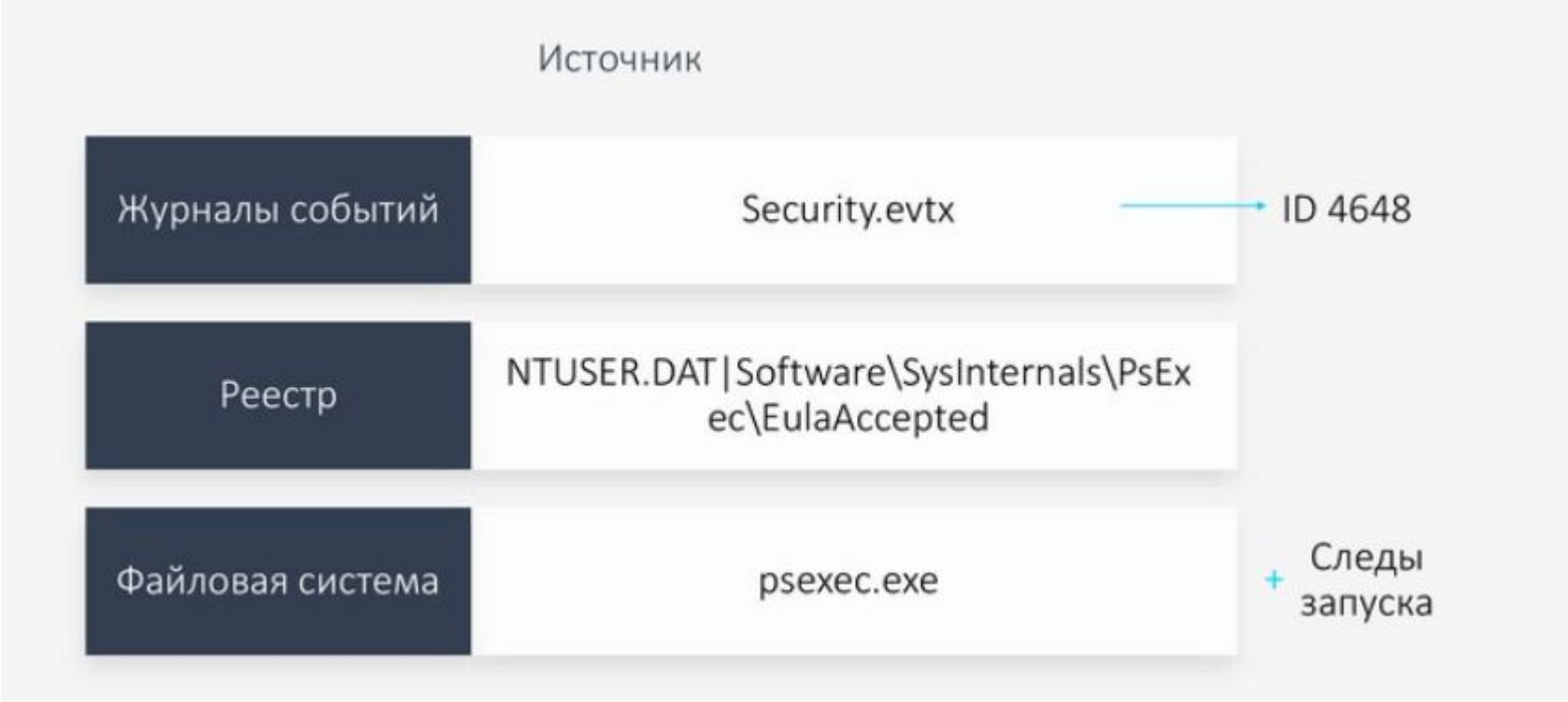
Реконструкция BMC-кэша

- Инструмент: https://github.com/ANSSI-FR/bmc-tools



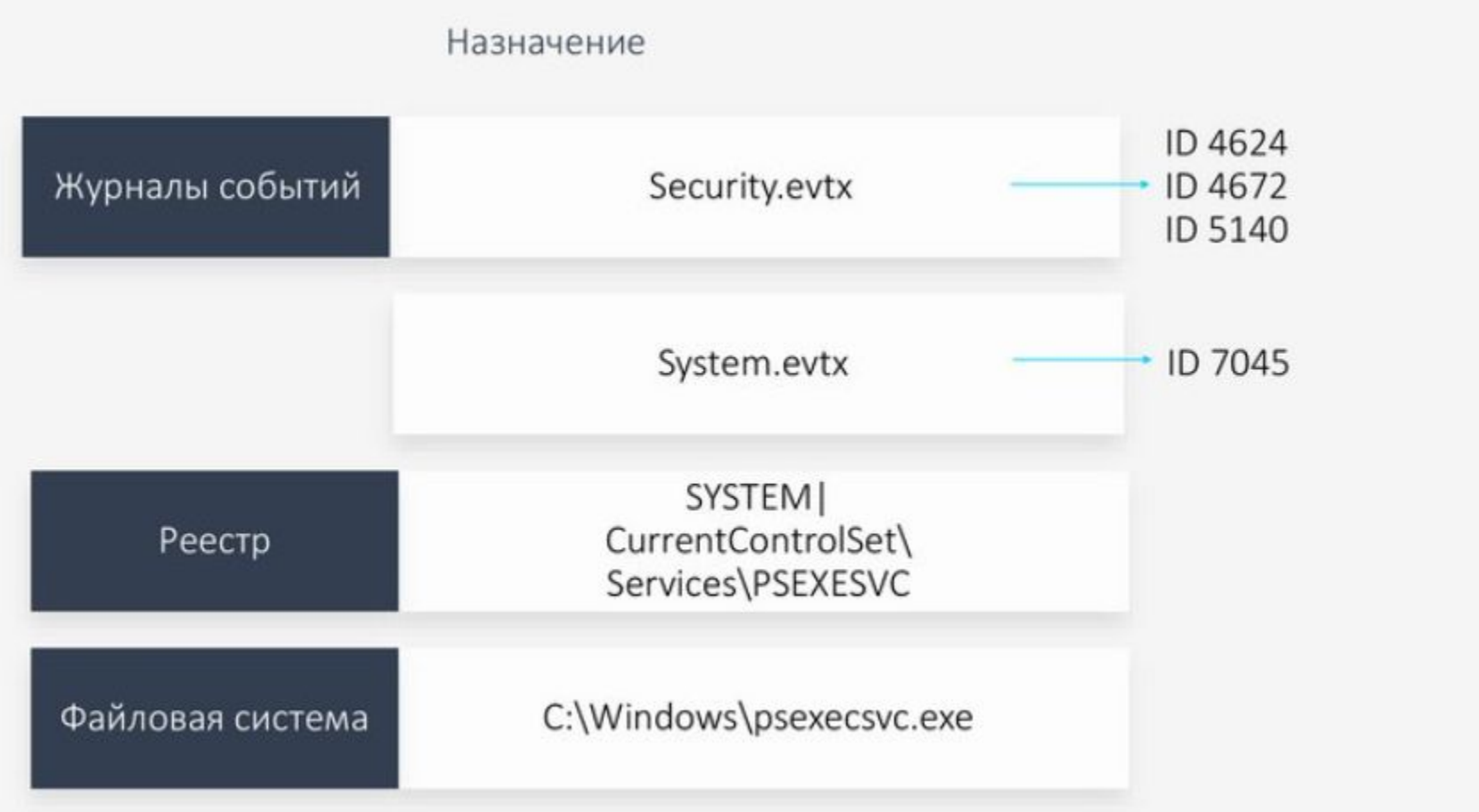
- Пример: https://codeby.net/threads/rdp-cache-forensics-na-storone-klienta.64854/

PsExec



Код	Описание
4648	Использование других реквизитов в текущей сессии (Runas)

PsExec

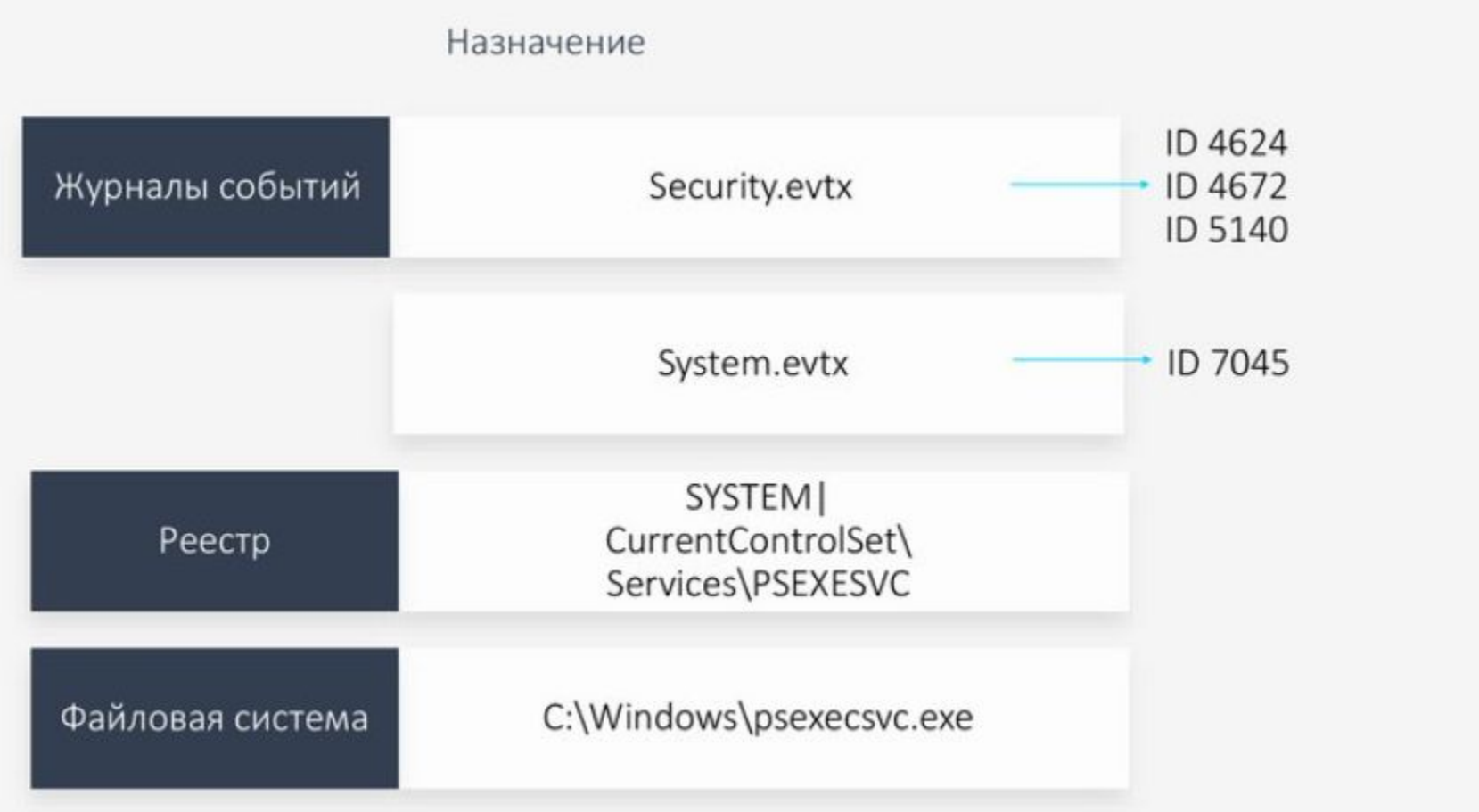


Код	Описание
4624	Вход в систему

Interpretation

Logon Type	Explanation
2	Logon via console
3	Network Logon
4	Batch Logon
5	Windows Service Logon
7	Credentials used to unlock screen
8	Network logon sending credentials (cleartext)
9	Different credentials used than logged on user
10	Remote interactive logon (RDP)
11	Cached credentials used to logon
12	Cached remote interactive (similar to Type 10)
13	Cached unlock (similar to Type 7)

PsExec



Код	Описание
4672	Вход с правами суперпользователя (администратора)
5140	Доступ к сетевой папке
7045	В системе создана служба

Поиск следов доступа к информации

Получение реквизитов доступа

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 новых аккаунтов

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

Удаленный доступ

Следы создания / исполнения файлов, предназначенных для инсталляции программ для удаленного управления

Следы запуска программ для удаленного управления

Анализ журналов программ для удаленного управления

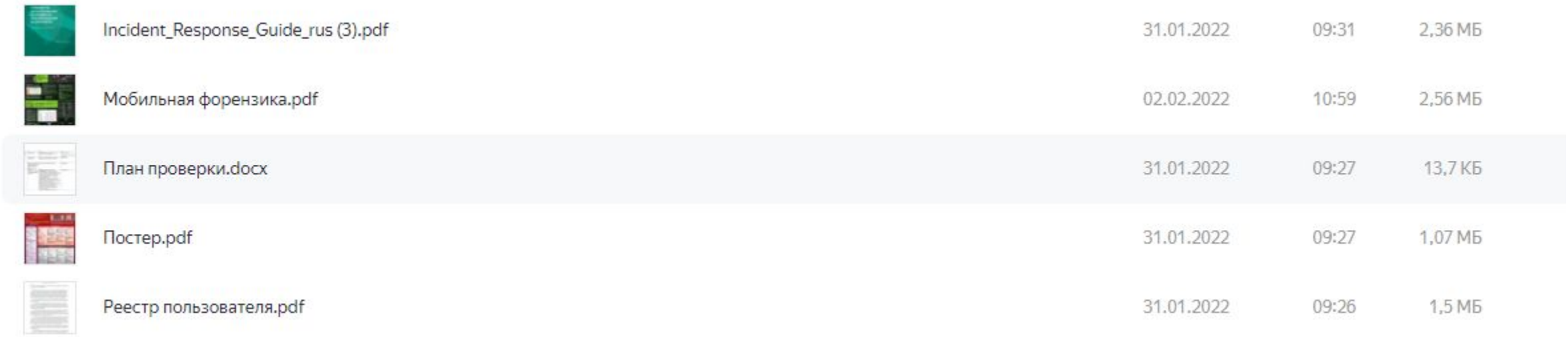
Использование прикладного ПО

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

Создание / модификация файлов средствами имеющегося на скомпрометированных хостах программного обеспечения

Дополнительные материалы

- https://disk.yandex.ru/d/idU3lCef5JLbtQ



СПАСИБО ЗА ВНИМАНИЕ!

Почта – evgeny.komotsky@urfu.ru
Телефон – 8-965-518-55-30
Вконтакте:
https://vk.com/id4172702