

Министерство образования республики Молдова
Технический Университет Молдовы
Департамент Программной Инженерии и Автоматики

О т ч ё т

Лабораторная работа №5

По предмету: Infractioni informatice si tehnici de investigare

Выполнил студ. гр. SI-202

Абабий Эдуард

Проверил

Масютин Максим

Кишинёв – 2023

Scopul acestui laborator este de a-i învăța pe studenți despre artefactele încorporate în fișierele Prefetch și despre modul de a utiliza aceste fișiere pentru a identifica malware și circumstanțele de infectare.

Sarcina:

1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!
2. Pentru primele 3 întrebări, de mai jos, creați un writeup (descrieți pe pași cum ați aflat răspuns la întrebările selectate, obligatoriu includeți și capturi de ecran).

Rezolvarea sarcinilor:

1. Care fișier a fost executat de cele mai multe ori?

SEARCHFILTERHOST.EXE

Filename	Run ...	La:
SEARCHFILTERHOST.EXE-AA7A1FDD.pf	885	02.
SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf	838	02.

- a. Din ce cale a fost executat acest fișier?

\\VOLUME{01d2f5bc8f23c7b32c8f7692}\\WINDOWS\\SYSTEM32\\SEARCHFILTERHOST.EXE



- b. Când a fost pornit acesta pentru prima și ultima dată?

Первый раз был запущен - 05.07.2017 17:43:31

Последний раз был запущен - 02.08.2017 21:13:42

Filename:	SEARCHFILTERHOST.EXE-AA7/
Created Time:	05.07.2017 17:43:31
Modified Time:	02.08.2017 21:14:08
File Size:	4 372
Process EXE:	SEARCHFILTERHOST.EXE
Process Path:	\\VOLUME{01d2f5bc8f23c7b3-2c
Run Counter:	885
Last Run Time:	02.08.2017 21:13:42, 01.08.201
Missing Process:	No

c. Ce zonă de timp reprezintă?

UTC

2. Când a fost instalat Thunderbird?

Был установлен 6 июля 2017 года

Filename:	THUNDERBIRD SETUP 52.2.1.EXE-5480B4EC.pf
Created Time:	06.07.2017 18:50:37
Modified Time:	06.07.2017 18:50:37
File Size:	12 604
Process EXE:	
Process Path:	
Run Counter:	1
Last Run Time:	06.07.2017 18:50:26
Missing Process:	No

a. Când a fost folosit acesta pentru prima oară?

Первый раз был использован 7 июля 2017 года

Filename:	THUNDERBIRD.EXE-D7BDD9EA.pf
Created Time:	07.07.2017 17:38:08

3. A fost vreo operațiune executată din medii detașabile? Ce anume și când? (Sugestie: Referință la Internet Lab.)

SETUP.EXE-E589C2EE.pf Из диска, с другим id по сравнению с остальными

INSTALL.EXE-70929234.pf	\VOLUME{01021D0C023C-03-2C01-092} \VOLUME{039AA9703B00C0D7AD3AC1D043} \...	1
INSTALL.EXE-BADEBC8F.pf	\VOLUME{01d2f5bc8f23c7b3-2c8f7692} \6681009D9942B5A3FDC06E4E94A05E \INS...	1
SETUP.EXE-E589C2EE.pf	\VOLUME{0000000000000000-c173bfcf} \SETUP.EXE	2
INSTUP.EXE-0428A795.pf		0
LIVTCD EXE 76D16D15 .pf		0

*** Vă rugăm să treceți peste următoarele întrebări până după laboratorul Windows Event Log.**

4. Mergeți înapoi la Laboratorul Event Log, când a fost ultima acțiune de RDP?

Последний раз использование RDP было замечено в 20:55:29 в 01.08.2017

Type	Date	Time	Event	Source
Information	01.08.2017	20:55:29	1149	Microsoft-Windows-TerminalServices-RemoteConnectionManager
Information	01.08.2017	20:49:04	1149	Microsoft-Windows-TerminalServices-RemoteConnectionManager
Information	01.08.2017	20:40:42	1149	Microsoft-Windows-TerminalServices-RemoteConnectionManager

- a. Există careva fișiere Prefetch de potențial interes în jurul acestui interval de timp?

Да, был найден PSEXESVC.exe

MMC.EXE-4052F366.pf	\VOLUME{01...	1	01.08.2017 20:41:15	No
MPCCMDRUN.EXE-BB72ED6F.pf	\VOLUME{01...	29	01.08.2017 20:42:24, 01.08.2017 20:42:24, 01...	No
PSEXESVC.EXE-51BA46F2.pf	\VOLUME{01...	8	01.08.2017 20:48:09, 01.08.2017 20:47:51, 01...	No
DLLHOST.EXE-D25DD707.pf	\VOLUME{01...	1	01.08.2017 20:49:23	No
DLLHOST.EXE-82A80DAE.pf	\VOLUME{01...	1	01.08.2017 20:49:29	No

- b. Ce este psexesvc.exe? De câte ori a fost executat acesta?

Он был запущен 8 раз.

Он нужен для выполнения команд на удаленном компьютере — задача довольно распространенная. Это может быть необходимо для изменения настроек системы, установки или удаления программ и много еще для чего

- c. Ce a fost executat cu exact 10 secunde înainte de 9129837.exe? Ce ar putea însemna acest lucru?

ONEDRIVE.EXE/ AUDIODG.EXE / CCLEANER64.EXE

Я думаю, что изначально был запущен процесс AUDIODG.exe, который отвечает за изоляцию аудио устройств, дабы отключить его и чтобы звук на компьютере не проигрывался, а это значит, что при выводе каких-то окон с уведомлением, сами уведомления не будут проигрываться. Затем возможно был запущен CCLEANER64.exe для отключения проверки системы на файлы вирусы (это моё предположение)

CMD.EXE-03303D47.pf	\\VOLUME{01...	33	02.08.2017 21:13:36, 01.08.2017 21:02:44, 01...	No
ONEDRIVE.EXE-BA9B4983.pf	\\VOLUME{01...	22	02.08.2017 21:31:36, 02.08.2017 21:13:55, 01...	No
AUDIODG.EXE-D0D776AC.pf	\\VOLUME{01...	73	02.08.2017 21:31:36, 02.08.2017 21:14:17, 01...	No
CCLEANER64.EXE-AACDD30D.pf	\\VOLUME{01...	14	02.08.2017 21:31:37, 02.08.2017 21:13:56, 01...	No
9129837.EXE-CDC57980.pf	\\VOLUME{01...	3	02.08.2017 21:31:37, 02.08.2017 21:13:56, 01...	No

- d. Uitați-vă la panoul de jos al fișierelor accesate în primele 10 secunde după executarea 9129837.exe. Observați altceva anormal?

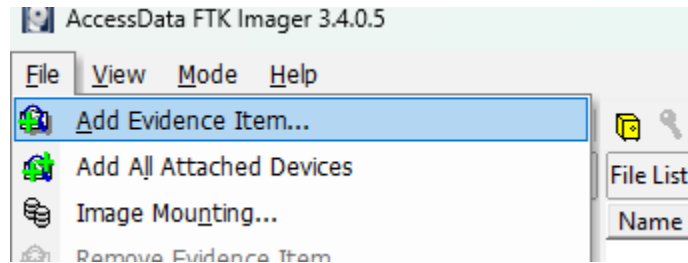
В первых 10 секундах после запуска файла 9129837.exe мы замечаем, что был запущен установщик посредника, затем 2 dllhost.exe файла
Связи как таковой не вижу, возможно каким-то образом через установщика посредника злоумышленник смог скачать какой-то нужный софт.

9129837.EXE-CDC57980.pf	\\VOLUME{01...	3	02.08.2017 21:31:37, 02.08.2017 21:13:56, 01...	No
INSTALLAGENTUSERBROKER.EXE-AAB93CC...	\\VOLUME{01...	20	02.08.2017 21:31:39, 01.08.2017 20:20:16, 01...	No
DLLHOST.EXE-0F726681.pf	\\VOLUME{01...	37	02.08.2017 21:31:40, 02.08.2017 21:14:41, 01...	No
DLLHOST.EXE-3B8267A2.pf	\\VOLUME{01...	20	02.08.2017 21:31:40, 02.08.2017 21:14:41, 01...	No

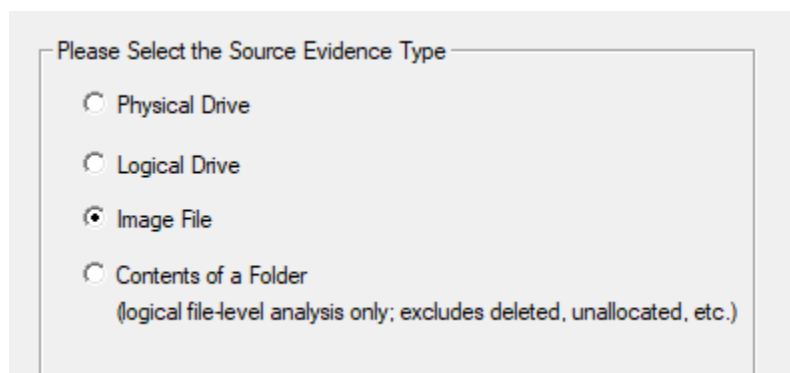
2. Writeup: Întrebarea 1, 2, 3.

Для начала мы должны были сгенерировать Prefetch файлы для их последующего анализа

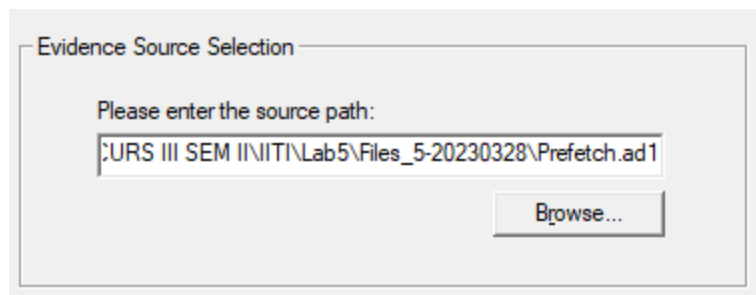
Открыл файл FTK Manager и выбрал опцию Add Evidence Item



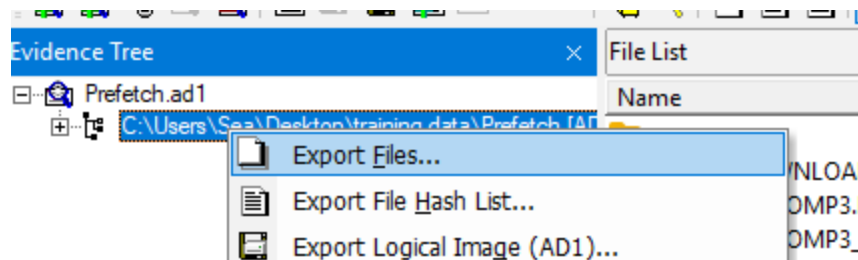
после чего выбрал исходный тип файла Image File



Затем вписал путь к файлу Prefetch.ad1

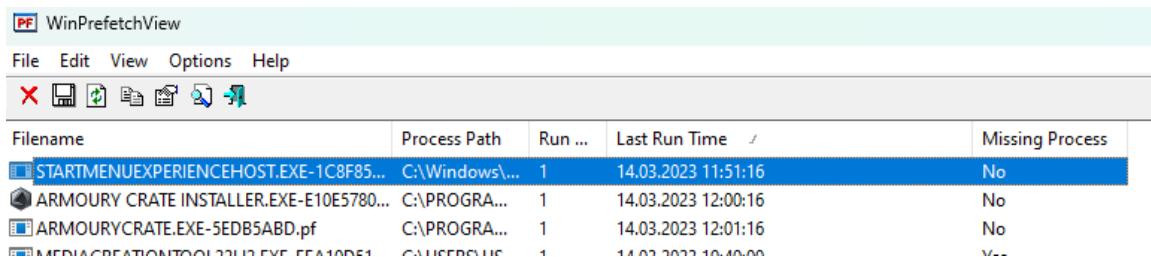


При нажатии на кнопку Finish у нас появляется древовидное отображение файлов



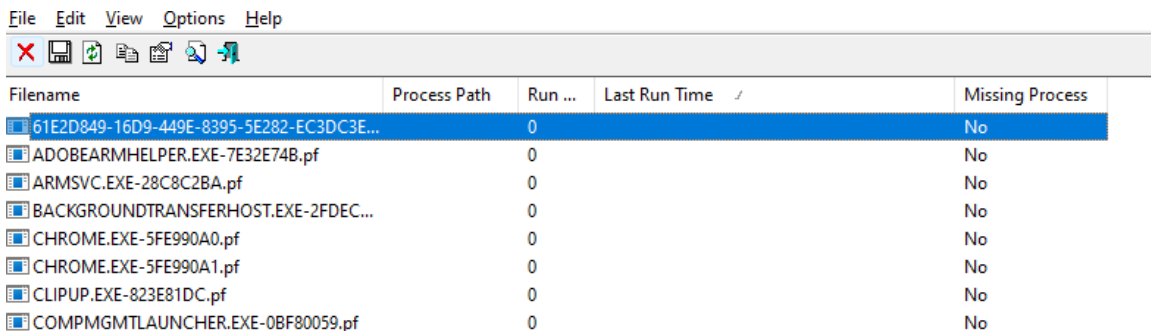
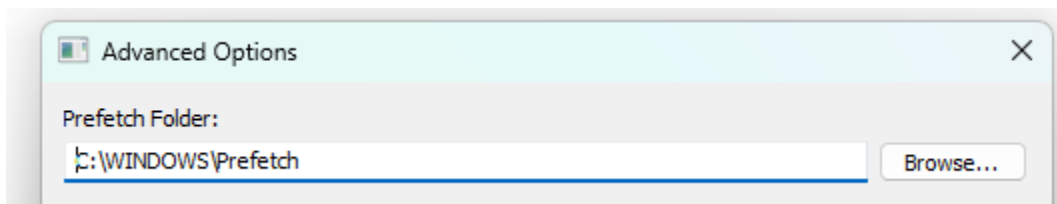
И делаем Export Files

Затем запускаем программу WinPrefetchView



Filename	Process Path	Run ...	Last Run Time	Missing Process
STARTMENUEXPERIENCEHOST.EXE-1C8F85...	C:\Windows\...	1	14.03.2023 11:51:16	No
ARMOURY CRATE INSTALLER.EXE-E10E5780...	C:\PROGRA...	1	14.03.2023 12:00:16	No
ARMOURYCRATE.EXE-5EDB5ABD.pf	C:\PROGRA...	1	14.03.2023 12:01:16	No
MEDIA CREATION TOOL 2013 EXE-5FA10D51...	C:\USERS\...	1	14.03.2023 12:40:00	Yes

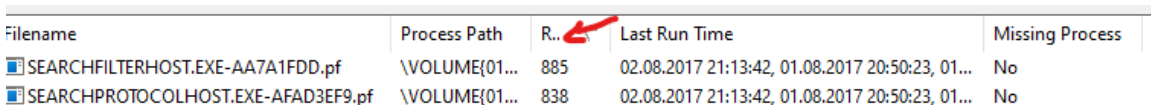
По умолчанию стоит путь к Prefetch файлам нашей системы, но мы должны поменять путь к файлам, которые мы экспортировали



Filename	Process Path	Run ...	Last Run Time	Missing Process
61E2D849-16D9-449E-8395-5E282-EC3DC3E...		0		No
ADOBEARMHELPER.EXE-7E32E74B.pf		0		No
ARMSVC.EXE-28C8C2BA.pf		0		No
BACKGROUNDTRANSFERHOST.EXE-2FDEC...		0		No
CHROME.EXE-5FE990A0.pf		0		No
CHROME.EXE-5FE990A1.pf		0		No
CLIPUP.EXE-823E81DC.pf		0		No
COMPMGMTLAUNCHER.EXE-0BF80059.pf		0		No

Затем мы можем просмотреть все наши Prefetch файлы.

Сортируем их по количеству запуска и находим ответ на вопрос, какой файл больше всего запускался



Filename	Process Path	Run ...	Last Run Time	Missing Process
SEARCHFILTERHOST.EXE-AA7A1FDD.pf	\VOLUME{01...	885	02.08.2017 21:13:42, 01.08.2017 20:50:23, 01...	No
SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf	\VOLUME{01...	838	02.08.2017 21:13:42, 01.08.2017 20:50:23, 01...	No

Два раза на него нажав и мы находим ответ на другой вопрос, какой путь к запуску

этого файла

Process EXE:	SEARCHFILTERHOST.EXE
Process Path:	\VOLUME{01d2f5bc8f23c7b3-2c8f7692}\WINDOWS\S
Run Counter:	885

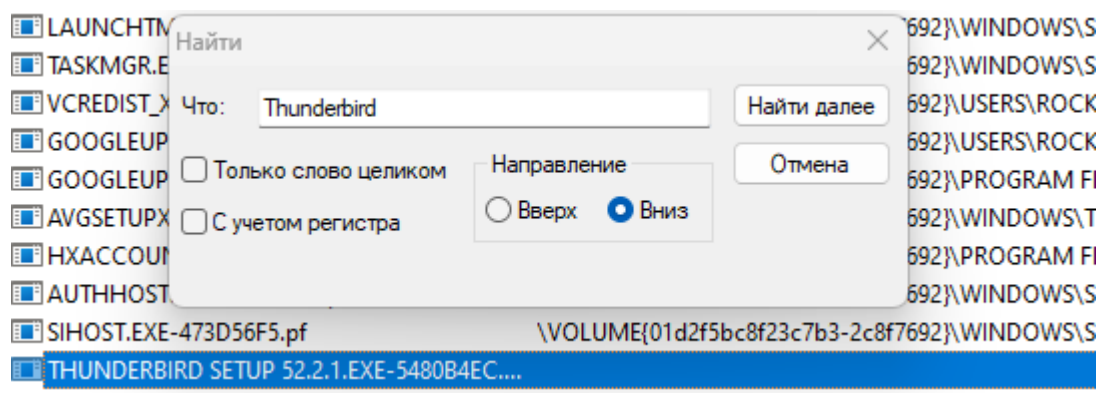
И смотрим, когда он был запущен в первый и последний раз

Filename:	SEARCHFILTERHOST.EXE-AA7A1FDD.pf
Created Time:	05.07.2017 17:43:31
Modified Time:	02.08.2017 21:14:08
File Size:	4 372
Process EXE:	SEARCHFILTERHOST.EXE
Process Path:	\VOLUME{01d2f5bc8f23c7b3-2c8f7692}\WINDOWS\S
Run Counter:	885
Last Run Time:	02.08.2017 21:13:42, 01.08.2017 20:50:23, 01.08.20
Missing Process:	No

Задание 2:

Нам нужно было найти время, когда был установлен Thunderbird

Воспользовавшись поиском мы нашли файл установки Thunderbird



И находим дату его установки

Filename:	THUNDERBIRD SETUP 52.2.1.EXE-5480B4EC.pf
Created Time:	06.07.2017 18:50:37
Modified Time:	06.07.2017 18:50:37

Затем снова воспользовавшись поиском находим его exe файл и видим, когда он был запущен в первый раз

Filename:	THUNDERBIRD.EXE-D7BDD9EA.pf
Created Time:	07.07.2017 17:38:08 
Modified Time:	01.08.2017 17:46:21

Задание 3 было немного сложнее, потому что не так было просто найти exe файл какого-то iso

Но немного просмотрев, мы видим, что почти все файлы были запущены с определенного диска и только один был запущен с другого места

HXMAIL.EXE-C8EC8373.pf	\VOLUME{01d2f5bc8f23c7b3-2c8f7692}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSCOMMUNICATIONSAPPS_17.7906.42257.0_
SETUP.EXE-FCABDC1C.pf	
READER11_EN_XA_INSTALL.EXE-80EA0B73.pf	\VOLUME{01d2f5bc8f23c7b3-2c8f7692}\USERS\ROCK HAMMERFIST\DOWNLOADS\READER11_EN_XA_INSTALL.EXE
SETUP.EXE-E589C2EE.pf	<u>\VOLUME{0000000000000000-c173bfcf}\SETUP.EXE</u>
SOFTWARE_REPORTER_TOOL.EXE-DE17B35...	\VOLUME{01d2f5bc8f23c7b3-2c8f7692}\USERS\ROCK HAMMERFIST\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\SWREPORTER\20.114.2
CONTROL.EXE-9459D5A0.pf	\VOLUME{01d2f5bc8f23c7b3-2c8f7692}\WINDOWS\SYSTEM32\CONTROL.EXE

Поэтому можно утверждать, что это iso образ файл

Вывод: В данной лабораторной работе я научился анализировать Prefetch файлы компьютера. Это позволит нам понять, какие файлы запускались, когда и откуда, сколько раз. Это позволит найти несостыковку или подозрительные действия.