Министерство образования республики Молдова

Технический Университет Молдовы

Департамент Программной Инженерии и Автоматики

Отчёт

Лабораторная работа №5

По предмету: Infractiuni 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:**

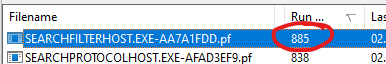
1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!

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



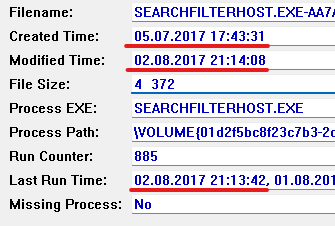
* 1. Din ce cale a fost executat acest fișier?

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



* 1. 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

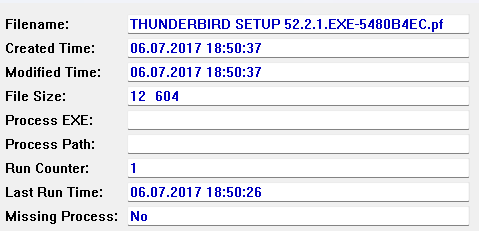


* 1. Ce zonă de timp reprezintă?

UTC

1. Când a fost instalat Thunderbird?

Был установлен 6 июля 2017 года



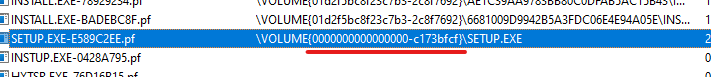
* 1. Când a fost folosit acesta pentru prima oară?

Первый раз был использован 7 июля 2017 года



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

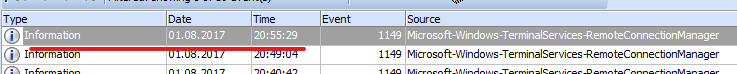
SETUP.EXE-E589C2EE.pf Из диска, с другим id по сравнению с остальными

****

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

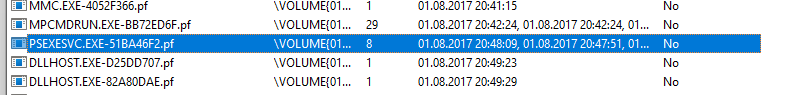
1. Mergeți înapoi la Laboratorul Event Log, când a fost ultima acțiune de RDP?

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



* 1. Există careva fișiere Prefetch de potențial interes în jurul acestui interval de timp?

Да, был найден PSEXESVC.exe



* 1. Ce este psexesvc.exe? De câte ori a fost executat acesta?

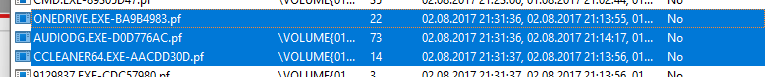
Он был запущен 8 раз.

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

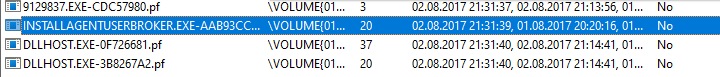
* 1. Ce a fost executat cu exact 10 secunde înainte de 9129837.exe? Ce ar putea însemna acest lucru?

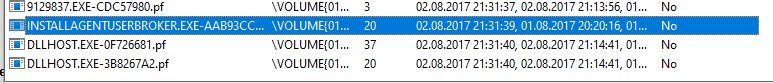
ONEDRIVE.EXE/ AUDIODG.EXE / CCLEANER64.EXE

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 )



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

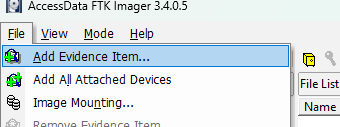
В первых 10 секундах после запуска файла 9129837.exe мы замечаем, что был запущен установщик посредника, затем 2 dllhost.exe файла  
Связи как таковой не вижу, возможно каким-то образом через установщика посредника злоумышленник смог скачать какой-то нужный софт.

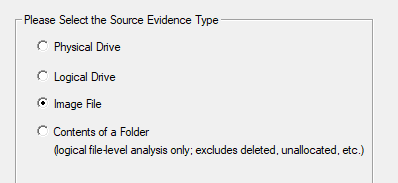
****

**2. Writeup: Întrebarea 1, 2, 3.**

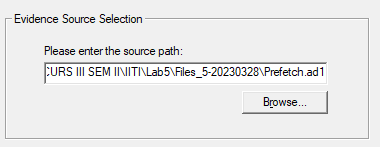
Для начала мы должны были сгенерировать Prefetch файлы для их последующего анализа

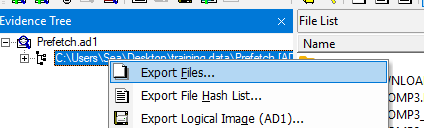
Открыл файл FTK Manager и выбрал опцию Add Evidence Item



после чего выбрал исходный тип файла Image File

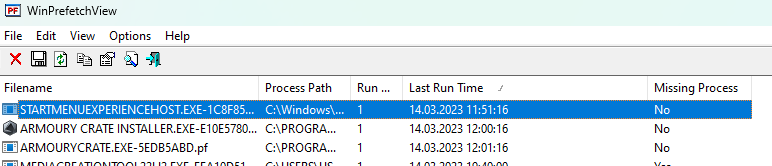
Затем вписал путь к файлу Prefetch.ad1



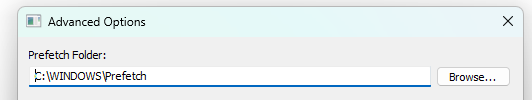
При нажатии на кнопку Finish у нас появляется древовидное отображение файлов

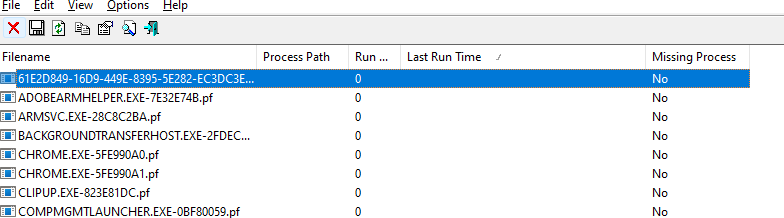
И делаем Export Files

Затем запускаем программу WinPrefetchView

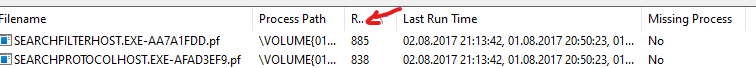


По умолчанию стоит путь к Prefetch файлам нашей системы, но мы должны поменять путь к файлам, которые мы экспортировали





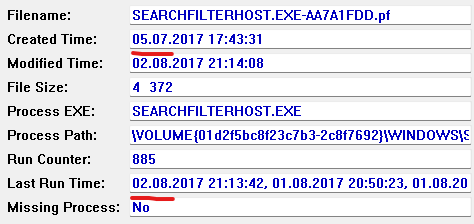
Затем мы можем просмотреть все наши Prefetch файлы.

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

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

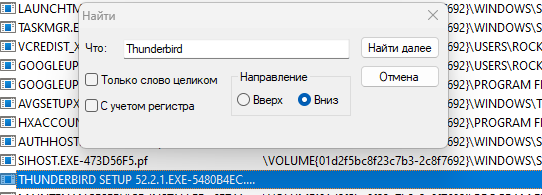


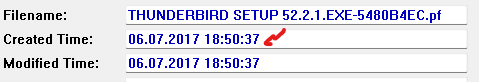
И смотрим, когда он был запущен в первый и последний раз



Задание 2:  
Нам нужно было найти время, когда был установлен Thunderbird

Воспользовавшись поиском мы нашли файл установки Thunderbird

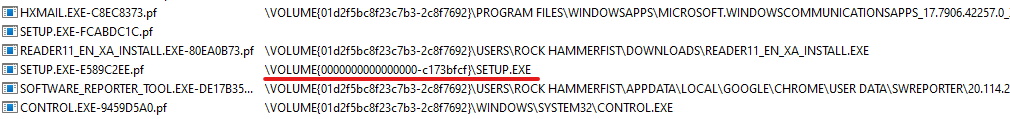


И находим дату его установки

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



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

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.