УДК 004.056
DOI: 10.31673/2409-7292.2022.022229

Гончаренко М.Ф., Стежко М.В.

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА ОСНОВІ РІШЕНЬ AUTOPSY ТА VOLATILITY

У даній статті наведено відомості про основні методи проведення розслідувань для будь-якої організації на основі рішень рішень Autopsy та Volatility. Проаналізовано можливі джерела даних, та складність виокремлення певної інформації з них. Запропоновано загальні рекомендації щодо проведення розслідувань. Розглянуті інструменти та процес аналізу отриманих даних.

Ключові слова: кіберінцидент, загроза, аналіз, безпека, форензика, пошук доказів, зловмисник, розслідування.

Вступ

Сучасне суспільство все більше залежить від комунікаційних мереж, мобільних пристроїв, рішень Інтернету, технологій, різного роду систем і хмарних сервісів. Використовуючи переваги найсучасніших інформаційно-комунікаційних технологій (ІКТ), комерційна діяльність, ділові операції та державні послуги зросли, змінивши спосіб життя майже всіх людей. Тісний зв'язок фізичного світу з ІКТ-технологіями привів до безсумнівних переваг. У той же час, це пояснює поширення нових загроз і проблем кібербезпеки, таких як кібер-залякування, витік даних із використанням соціальної інженерії або приховування інформації, шкідливе програмне забезпечення, яке перетворює вузли Інтернету речей на «зомбі», організовані за допомогою бот-мереж і зловмисного програмного забезпечення, націленого на конкретні пристрої, такі як пристрої VoIP та розумні транспортні засоби. Як наслідок, кіберінциденти можуть мати значний соціально-економічний вплив на глобальні підприємства та фізичні особи [1]. Це призвело до зростання компаній та продуктів, які мають на меті допомогти приватним компаніям та правоохоронним органам використовувати цифрові докази для визначення того, хто, що, де, коли і як зробив.

Ціль статті: дослідження джерел інформації та її обробки для проведення розслідувань на основі рішень рішень Autopsy та Volatility.

Відомості про використовуване ПЗ

Volatility Framework – це ПЗ яке використовується для пошуку артефактів та аналізу вже зібраних даних з відкритим вихідним кодом для реагування на інциденти та аналізу шкідливих програм. Написане на Python і пропонує засоби для аналізу даних з Microsoft Windows, MacOS X і Linux.

Autopsy – це платформа для цифрової криміналістики та графічний інтерфейс для Sleuth Kit та інших інструментів для цифрової криміналістики.

The Sleuth Kit – це набір інструментів командного рядка та бібліотеки C, які дозволяють аналізувати образи дисків та відновлювати з них файли. Він використовується за лаштунками в Autopsy та багатьох інших відкритих та комерційних криміналістичних інструментах.

Інсталяція необхідного ПЗ

Для інсталяції Autopsy необхідно перейти за посиланням https://www.autopsy.com/download/ та завантажити програму. Процес інсталяції є інтуїтивно зрозумілим, тому розглядати його не будемо.

Для інсталяції Volatility перш за все, нам необхідно завантажити та встановити Microsoft C++ Build Tools та Python Snappy для подальшої роботи з Volatility Framework. Для цього завантажуємо інсталятор та за допомогою нього завантажуємо та встановлюємо автономний компілятор MSVC, необхідні бібліотеки та скрипти. Також завантажуємо та встановлюємо Python версії 3. Далі необхідно інсталювати та пакет Snappy, це реалізація алгоритму стиснення написана виключно на мові Python. Далі завантажуємо код Volatility безпосередньо з сторінки проекту на GitHub. Це можна зробити встановивши Git на робочу

станцію та зклонувавши репозиторій, чи просто завантажити zip файл з стисненим кодом ПЗ. Наступним кроком необхідно запустити Windows Powershell та перейти в директорію з завантаженим кодом й інсталювати файл requirements.txt виконавши команду pip install –r requirements.txt. Далі ми будемо використовувати дамп оперативної пам'яті ОС Windows 10 x64 розміром в 4 Гб. Дамп було зроблено програмним засобом FTK Imager, та буде використовуватись для розгляду функціональних можливостей та методів аналізу даних запропонованих в Volatility Framework. Volatility містить в собі плагіни які безпосередньо і використовуються для аналізу. Далі використаємо деякі з них для аналізу даних ОС Windows.

Аналіз дампу оперативної пам'яті за допомогою Volatility Framework

Першим кроком переглянемо загальну інформацію про наявний дамп оперативної пам'яті. Для цього ми використаємо файл дампу оперативної пам'яті [2]. Також одним із перших кроків під час аналізу дампу оперативної пам'яті з яких зазвичай варто починати це перелік запущених процесів. Для перегляду переліку ми використали програму more для поетапного відображення результату. Першочерговий інтерес становлять поля PID, PPID, ImageFileName, Handles та іноді Threads. Поле ImageFileName дозволяє фільтрувати список за назвою та зосереджувати увагу на одному або декількох процесах. Поля PID, PPID вказують на те який процес був запущений першим, та який є материнським, а який є дочірнім. Поле Handles вказує на те які файли використовує процес. Threads вказує на кількість потоків використовуваних процесом (рис. 1).

```
PS C:\Users\38073\Desktop\volatility3> py vol.py -f C:\Users\38073\Downloads\ram_dump\case1\20210430-Win10Home-20H2-64bi
t-memdump.mem windows.pslist | more
Volatility 3 Framework 2.2.0

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime
File output

4       0       System  0xbf0f64a63080  132     -       N/A     False   2021-04-30 12:39:40.000000      N/A     Disabled
108     4       Registry        0xbf0f64bc6040  4       -       N/A     False   2021-04-30 12:39:38.000000      N/A
Disabled
396     4       smss.exe        0xbf0f66967040  2       -       N/A     False   2021-04-30 12:39:40.000000      N/A
Disabled
492     484     csrss.exe       0xbf0f6adb6080  13      -       0       False   2021-04-30 12:39:44.000000      N/A
Disabled
568     484     wininit.exe     0xbf0f6b67a080  1       -       0       False   2021-04-30 12:39:44.000000      N/A
```

Рис. 1. Перелік процесів

Фільтруємо процеси за назвою chrome. Select-String не є частиною Volatility, а програмою PowerShell. В системах Linux аналогом слугує grep. Заглибимось в дослідження процесу chrome.exe з PID 1328 та дослідимо до яких файлів мав доступ цей процес. Для цього використаємо плагін windows.handles та вкажемо PID. Переглядаючи перелік знаходимо файл, з шляхом до нього. Нас цікавлять файли тому фільтруємо результати пошуку по ключовому слову File. Знаючи що браузери зберігають історію, встановлюємо ключове слово History для фільтрації результатів пошуку файлів (рис. 2).

```
PS C:\Users\38073\Desktop\volatility3> py vol.py -f C:\Users\38073\Downloads\ram_dump\case1\20210430-Win10Home-20H2-64bi
t-memdump.mem windows.handles --pid 1328 | Select-String File | Select-String  history | more

1328    chrome.exe      0xbf0f6abe9740  0x89c   File    0x12019f        \Device\HarddiskVolume2\Users\John
Doe\AppData\Local\Google\Chrome\User Data\Default\History
1328    chrome.exe      0xbf0f6abe95b0  0x8c4   File    0x12019f        \Device\HarddiskVolume2\Users\John
Doe\AppData\Local\Google\Chrome\User Data\Default\Media History
1328    chrome.exe      0xbf0f6aca1e90  0x1478  File    0x12019f        \Device\HarddiskVolume2\Users\John
Doe\AppData\Local\Google\Chrome\User Data\Default\History-journal
```

Рис. 2. Файли історії браузера

В результаті отримуємо перелік файлів історії процесу chrome.exe. Ці файли можуть містити важливу для розслідування інформацію. Тому наступним кроком ми скопіюємо

вміст файлу History та переглянемо його. Для цього вказуємо директорію для дампу, встановивши параметр «–o», назву директорії, куди буде скопійований файл, назву плагіну, номер PID, та значення virtual address для цього файла, інакше буде створено дампи для всіх файлів процесу з PID 1328.

Перейшовши в менеджер файлів та обравши необхідну директорію відкриваємо дамп файл за допомогою HxD редактора. HxD – це Hex редактор, який, крім редагування даних диску та модифікації основної пам'яті (RAM), обробляє файли будь-якого розміру (рис. 3).

Рис. 3. Відкритий дамп файлу History через HxD редактор

Після відкриття ми бачимо заголовок SQLite format 3. Прогорнувши далі ми бачимо що це дійсно файл історії хром браузеру. Далі для зручності аналізу варто використати програми для перегляду SQL формату (рис. 4).

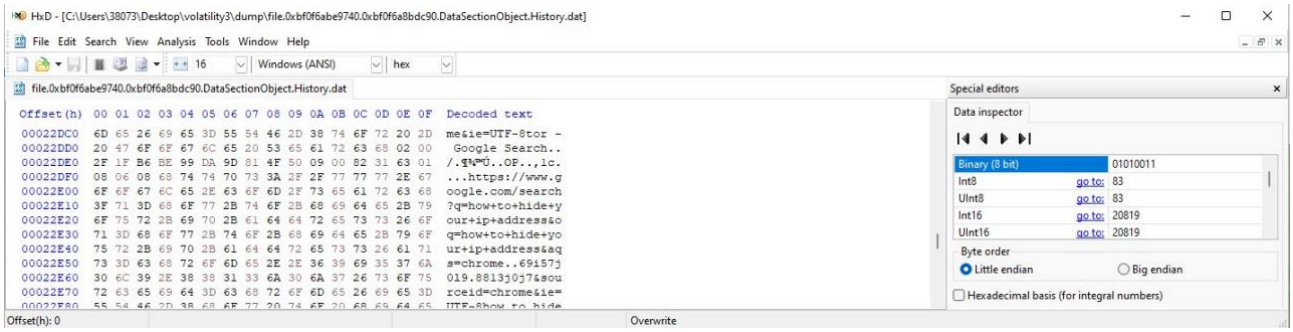

Рис. 4. Аналіз дампу файлу історії

На цьому прикладі ми розглянули як можна знаходити та досліджувати файли в середині процесів, робити дамп і досліджувати окремо. Також ми можемо зробити дамп усіх фалів процесу просто вказавши PID не вказуючи адресу пам’яті.

Далі розглянемо плагін який дозволяє переглядати використання командного інтерфейсу з усіма встановленими параметрами. Плагін дозволяє відобразити наявну інформацію про те що і де було запущене та приховані параметри. Наприклад в цьому переліку також присутній запис про зняття дампу оперативної пам’яті програмою FTK Imager, також вказано що її було запущено з диску E, що свідчить про те що цей диск є зовнішнім і може бути USB носієм, або флеш накопичувачем.

Перегляд мережевої активності також є одним із важливих джерел інформації. Дані про мережеву активність містять внутрішню IP та IP адреси отримувача, порти, назву процесу який використовує мережеві з’єднання. Це джерело надає вагому інформацію про дії користувача або шкідливого програмного забезпечення, як воно могло бути завантажене чи його комунікацію. Ми також можемо переглядати які процеси були запущені, які файли ними запускалися, які мережеві з’єднання встановлювалися. Також якщо ми зацікавлені конкретним процесом можна відфільтровувати дані про всі інші, як зображено на рис. 5.

Попередньо зібрані дані дають нам можливість заглиблюватись і далі шукати додаткову інформацію цікаву для подальшого розслідування. Для пошуку хешів паролів використовується хешдамп. Він відображає всі хеші в системі Windows. Це дає уявлення про паролі які використовуються в даній системі чи в інших. Визначення паролю з хешу може нести суттєвий вплив на кількість та вичерпність зібраної інформації.

```
PS C:\Users\38073\Desktop\volatility3> py vol.py -f C:\Users\38073\Downloads\ram_dump\case1\20210430-Win10Home-20H2-64bi
t-memdump.mem windows.netstat |Select-String chrome | more

0xbf0f6d8a1010  TCPv4   10.0.2.15       49771   185.70.41.35    443     CLOSE_WAIT      1840    chrome.exe      2021-04-
30 17:44:57.000000
0xbf0f6cbb9530  TCPv4   10.0.2.15       49772   185.70.41.35    443     FIN_WAIT2       1840    chrome.exe      2021-04-
30 17:44:58.000000
0xbf0f6ca71a20  TCPv4   10.0.2.15       49769   142.250.190.14  443     CLOSE_WAIT      1840    chrome.exe      2021-04-
30 17:44:55.000000
0xbf0f6cfd17f0  TCPv4   10.0.2.15       49777   35.186.220.63   443     CLOSE_WAIT      1840    chrome.exe      2021-04-
30 17:44:58.000000
0xbf0f6c85bb20  TCPv4   10.0.2.15       49775   185.70.41.35    443     FIN_WAIT2       1840    chrome.exe      2021-04-
30 17:44:58.000000
```

Рис. 5. Netstat

Іншим джерелом даних є дані з реєстру. Плагін windows.registry.userassist пропонує детальну інформацію щодо діяльності користувачів в системі. Містить такі дані як Name Hive(назва «куща»), Path, Last Write Time, це час останньої дії відносно ключа або останній раз коли програма запускалася, Count вказує на кількість разів запуску, Focus Count вказує на кількість разів коли користувач використовував програму, Time Focused вказує на кількість часу загального користування програмою. Далі розглянемо на прикладі.

Кущ у реєстрі Windows — це ім'я, яке є основним розділом реєстру, який містить розділи реєстру, підрозділи реєстру та значення реєстру. Всі ключі, які вважаються кущами, починаються з HKEY і знаходяться в корені або на вершині ієрархії в реєстрі, тому їх також іноді називають кореневими ключами або кущами основної системи [3].

У першому результаті з переліку бачимо що mspaint.exe запускався 7 разів, але час роботи з програмою становить 1 хвилину, що вказує на те що програма запускалася, але справді не була використовувана. У останньому результаті бачимо програму MSEdge яка запускалася тричі та була у роботі 16 разів, що вказує на перемикання між вікнами і користувач то виходив то повертався, загального користування програмою склав 1 год. 50 хв. 56 сек.

Коли постає необхідність відобразити всі наявні «кущі» у системі, ми можемо використати наступний команду. Даний перелік можна фільтрувати по ключових словах використовуючи опцію – filter. Якщо деякий ключ становить інтерес є можливість дослідити його детальніше зробивши дамп, для подальшого аналізу (рис. 6).

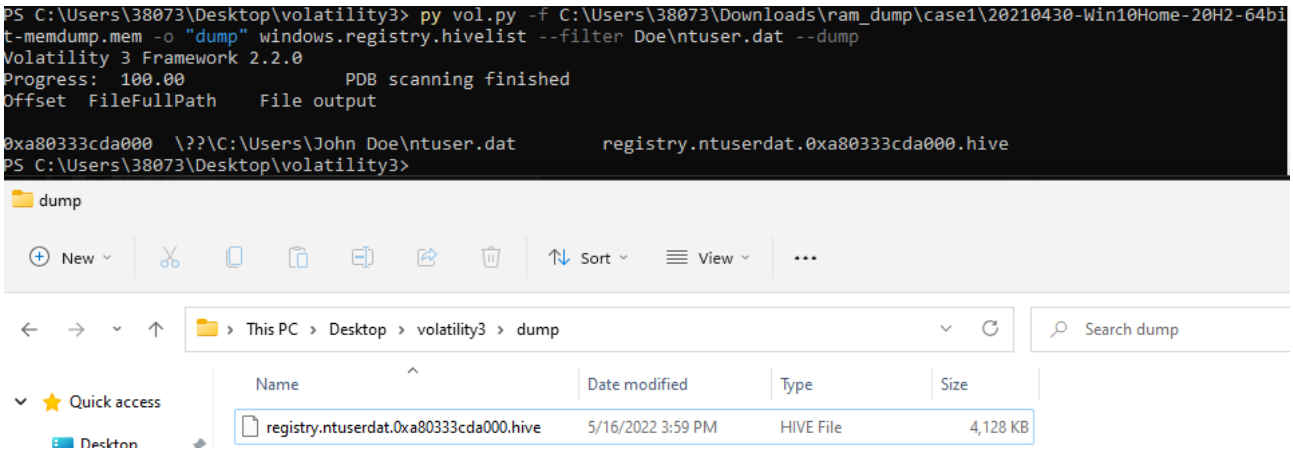

Рис. 6. Створення дампу «ключа»

Дослідження функціональних можливостей Autopsy

Перш за все варто пам’ятати, що будь-які дії у ході розслідування, збору та аналізу доказів, усі виконані дії з файлами, даними та інформацією, що досліджуються, необхідно ретельно документувати. Тому створюємо текстовий файл для нашого розслідування та починаємо документувати (рис. 7).

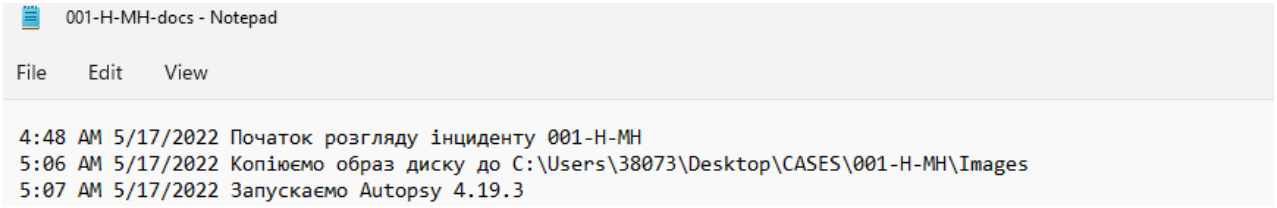

Рис. 7. Приклад документування дії аналітика

Запускаємо встановлене ПЗ. Після запуску нам необхідно визначити обрати чи це вже існуюче чи нове розслідування. Обираємо параметр для створення нового. Далі необхідно буде вказати назву розслідування та директорію яка буде містити файли розслідування. Наступним кроком вказуємо номер розслідування, контакти аналітика та організацію для якої проводимо розслідування. Далі необхідно вказати ім'я комп'ютера або іншого джерела даних що має один або більше носіїв інформації [4]. Після завершення цієї фази Autopsy проводить сканування згідно налаштованими нами параметрами (рис. 8).

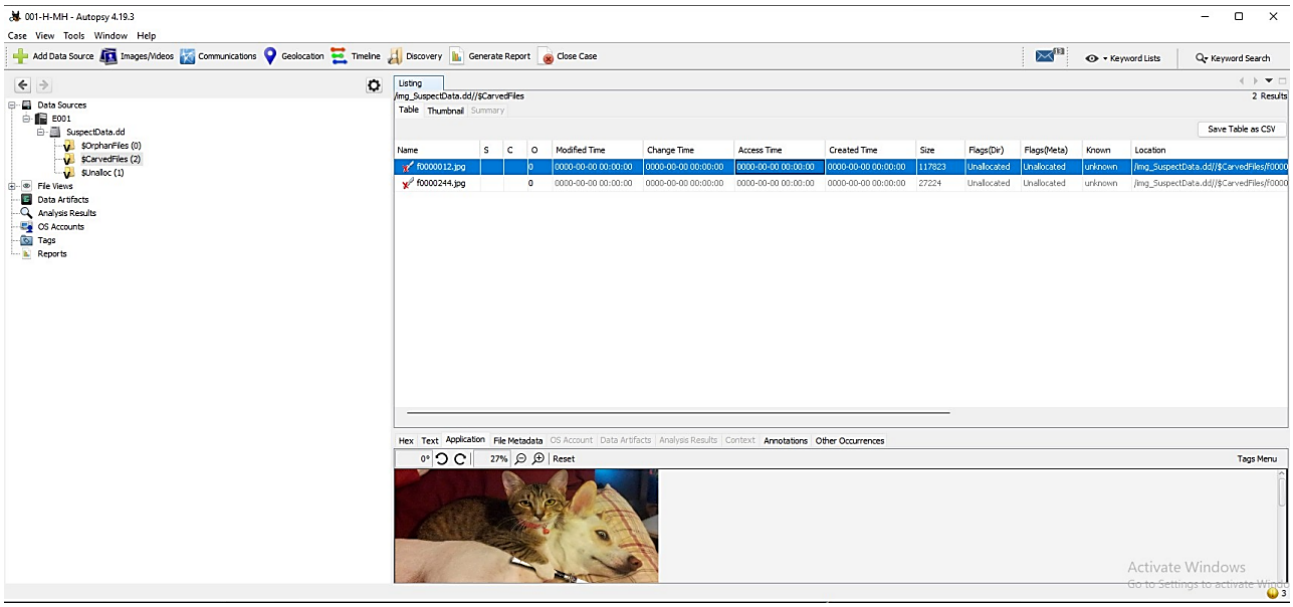

Рис. 8. Робочий інтерфейс Autopsy

Обробка джерела даних може коливатися від двох хвилин до 24 годин, в залежності від обсягу даних. Після завершення обробки ми бачимо ієрархічну структуру ліворуч, вікно перегляду директорій та вікно перегляду вмісту файлів праворуч. Ми бачимо в джерелах даних назву пристрою яку ми вказували перед додаванням образу диску. Ми можемо переглянути вміст диску, директорії, файли та їх вміст. Також ми маємо можливість переглядати додаткові дані, такі як, час створення, зміни, доступу, розмір, хеш-функції, розташування. Перегляд вмісту файлів дозволяє нам їх проглядати у HEX вигляді, що містить інформацію про індексування та файл, метадані, та чи фігурував даний файл раніше у інших процесах.

Перегляд файлів (Files Views) автоматично групує усі файли знайдені на диску за такими категоріями як типи файлів, видалені файли, та за розміром. Це дозволяє сконцентруватись на окремих типах файлів, залежно від інтересів розслідування. Перше з чого можна почати з пошуку за певними ключовими словами. Встановлені нами параметри пошуку безпосередньо впливають на кількість результатів. Після перегляду результатів пошуку ми переглядаємо які файли є підозрілими і помічаємо їх. Після того як ми

переглянули усі файли ми переходимо до розділу Tags у лівій частині та продовжуємо роботу з ними, за потреби використовуємо сторонні інструменти для їх подальшого аналізу.

Зараз ми додали ще одне джерело даних “E002”[5] та розглянемо “Analysis Results” і “Data Artifacts ”. Data Artifacts містить результати обробки образу диску кожним вибраним нами модулем, якщо відповідні дані до цих модулів були знайдені.

Першим підрозділом Data Artifacts є Встановлені програми. Цей підрозділ дозволяє аналітикам швидко переглядати всі встановлені програми на досліджуваній системі (рис. 9).

SOFTWARE			0	FileZilla Client 3.53.1 v.3.53.1	2021-04-29 16:03:58 EEST	001Win10.E01
SOFTWARE			0	Angry IP Scanner v.3.7.6	2021-04-29 16:03:13 EEST	001Win10.E01
SOFTWARE			0	Google Chrome v.90.0.4430.93	2021-04-29 14:23:39 EEST	001Win10.E01
SOFTWARE			0	Wireshark 3.4.5 64-bit v.3.4.5	2021-04-28 17:33:15 EEST	001Win10.E01
SOFTWARE			0	Npcap v.1.10	2021-04-28 17:32:55 EEST	001Win10.E01
SOFTWARE			0	Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14...	2021-04-28 17:28:01 EEST	001Win10.E01
SOFTWARE			0	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729...	2021-04-28 17:15:55 EEST	001Win10.E01
SOFTWARE			0	Nmap 7.91 v.7.91	2021-04-28 17:15:20 EEST	001Win10.E01

Рис. 9. Частина переліку встановлених програм

Ми бачимо програму FileZilla, FTP кілєнт, що дозволяє завантажувати та відправляти файли з та на FTP сервер. Це може виглядати підозрілим, і цікавим буде переглянути параметри, якщо ця програма не є нормою для сфери роботи фахівця, наприклад якщо він не web-розробник. Також Angry IP Scanner не є однією з розповсюджених програм, як наприклад на противагу Microsoft World. Цей перелік дає нам частину уявлення як найімовірніше ця система використовувалась. Якщо аналітик вирішує, що деякі програми стосуються питань розслідування, то аналітик може досліджувати кожну таку програму безпосередньо.

Наступним підрозділом є Метадані. Ці дані містять інформацію про дату створення, зміни, власника, тобто того хто створив цей файл, версії програми які використовувалась для створення файлу. Ці данні можуть проливати світло на хронологічний порядок подій, оскільки дані часу оперативної системи можуть бути змінені зловмисником, а про дані вбудовані в файли, він може не знати, чи не мати можливості їх виправити.

Інформація операційної системи. Це загальна інформація про операційну систему(ОС), що була зібрана з реєстру Windows. Важливим моментом є можливість переглянути на якому саме диску встановлена операційна система. Розділ останні документи є цікавим оскільки вказує на поведінку користувача. Тобто ми бачимо звідки та які файли відкривалися. Проте ми не маємо змоги переглядати вміст самих файлів. Інформація в даному розділі може містити ключовий характер для розслідування (рис. 10).

10-million-password-list-top-1000000.lnk				E:\10-million-password-list-top-1000000.txt	2021-04-29 21:20:20 EEST	001Win10.E01
20210429_151510.jpg.lnk				C:\Users\John Doe\Pictures\Contact\20210429_151510.jp...	2021-04-30 03:27:52 EEST	001Win10.E01
20210429_151510.lnk				C:\Users\John Doe\Pictures\Contact\20210429_151510.jpg	2021-04-30 03:27:08 EEST	001Win10.E01
accountNum.lnk				C:\Users\John Doe\Documents\accountNum.zip	2021-04-30 04:02:30 EEST	001Win10.E01
bettercap_windows_amd64_v2.31.0.lnk				C:\Users\John Doe\Downloads\bettercap_windows_amd64...	2021-04-28 20:16:49 EEST	001Win10.E01

Рис. 10. Частина переліку відкриття файлів

Корзина містить видалені файли. Вікно попереднього перегляду дозволяє нам переглядати їх вміст та видобувати за потреби. Дані в розділі Запущені програми зібрані з prefetch-файлів. Ці файли створюються за замовчуванням щоразу, коли виконуваний файл запускається у Windows. Prefetch-файли містять інформацію про файли, що завантажуються виконуваним файлом, та використовується для оптимізації виконання програми [6].

Також ми можемо перевірити завантаження і дізнатися чи був завантажений nmap, таким чином вибудовуючи хронологічну послідовність дій. З файлів попередньої вибірки ми отримуємо таке значення як кількість, яке вказує на кількість разів запуску програми.

Оскільки nmap це програма командного рядка ми можемо дослідити його історію. Для цього переглянемо вміст файлу ConsoleHost_history.txt. Ми з'ясували що nmap запускався тричі, його параметри та цільові хости сканування. Помічаємо цей файл. Зараз ми вже маємо більш чітку картину як і коли використовувалась дана програма.

Наступний підрозділ Shell Bags. Це набір ключів реєстру, які містять відомості про папку, що переглядається користувачем; таких як його розмір, положення та значок. Це означає, що всі обходи каталогів відстежуються та зберігаються у реєстрі [7]. Вони цікаве тим що дозволяє визначити чи користувач знав про певні директорії. Аналогічно до розділу останніх документів, але для директорій. Під'єднані USB пристрої часто э першим на що звертають увагу аналітики (рис. 11).

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			0	2021-04-29 22:58:36 EEST		ROOT_HUB30	4&14c8cfa78&0&0	001Win10.E01
SYSTEM			0	2021-04-30 03:46:25 EEST	LG Electronics USA, Inc.	Product: 70D6	AA00000000000873	001Win10.E01
SYSTEM			0	2021-04-30 03:46:46 EEST	LG Electronics, Inc.	LM-X420xxx/G2/G3 Android Phone (MTP/download mode)	LMQ725K2c1b72a	001Win10.E01
SYSTEM			0	2021-04-29 22:58:36 EEST	VirtualBox	USB Tablet	5&d788e138&0&1	001Win10.E01

Рис. 11. Перелік під'єднаних USB пристроїв

Локальні акуанти використовувані на досліджуваній робочій станції відображаються в розділі Web-акаунти. Ми можемо бачити час останнього доступу, але для детальної інформації необхідно переглянути історію. Web-кеш використовується для перегляду доменів, та часу доступу до цих доменів. Web-кукі, по суті пропонують таку ж саму інформацію як і web-кеш, в розслідуваннях вони використовуються для визначення часу доступу до доменів, та побудови хронологічної послідовності дій. Web-завантаження вказує на джерело завантажених даних. Це може бути доволі інформативно під час дослідження зараження робочої станції шкідливим програмним забезпеченням. Також ми бачимо завантаження nmap, мітка часу вказує на те, що він був завантажений та через хвилину був запущений файл інсталяції. Автозаповнення вказує нам на дані браузеру які є часто використовуваними. Web історія є глибоким джерелом щодо того чим людина інтересується, яким чином вона досліджує предмет інтересу. Web пошук дає нам уявлення про те що шукає людина, які браузери використовує (рис. 12).

History				google.com	messaging app with no login	Brave	2021-04-30 03:20:34 EEST	001Win10.E01
History				google.com	nmap	Google Chrome	2021-04-28 20:13:44 EEST	001Win10.E01
History				google.com	nmap	Google Chrome	2021-04-28 20:13:44 EEST	001Win10.E01
History				google.com	apr spoof windows	Google Chrome	2021-04-28 20:14:54 EEST	001Win10.E01
History				google.com	apr spoof windows	Google Chrome	2021-04-28 20:14:54 EEST	001Win10.E01

Рис. 12. Web пошук

Analysis Results зберігає висновки певної методики аналізу, наприклад пошуку у файлі ключових слів або хеш-значень. EXIF метадані це дані з .jpg файлів такі як дата створення, координати, пристрій. Розділ «Підозрілі файли користувачів» збирає файли які Autopsy рахує за підозрілі. Зазвичай це зображення чи документи з метаданими. Розділ «Тип акаунтів» відображає локальні акаунти які можна пов'язувати з сутністю, наприклад користувачем, номером кредитної карти. Розділ «web категорії» сортує файли за доменами.

Після завершення пошуку та аналізу ми генеруємо звіт. Його можна побудувати в різних представленнях, ми обрали HTML, та на яких даних він буде базуватися, на всіх результатах, тільки помічених, чи особливо виділених. Вказали які файли буде містити звіт та згенерували його (рис. 13).

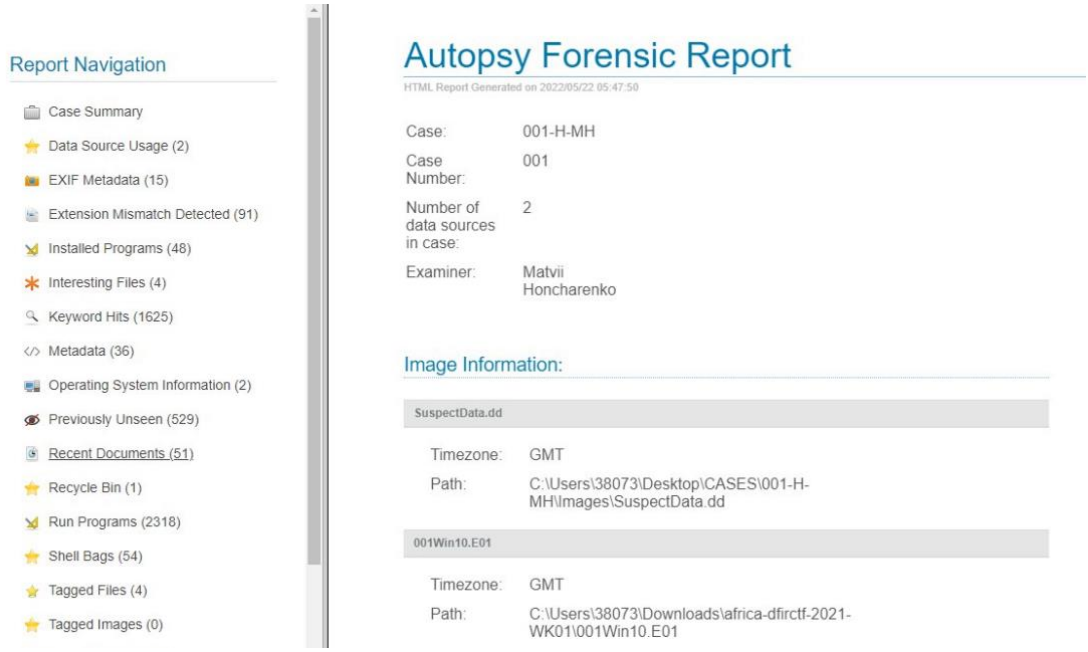

Рис. 13. Згенерований звіт

Висновок

Досліджуючи шляхи розслідування кіберінцидентів в корпоративній інформаційній системі було розглянуто процес використання засобів для аналізу зібраних даних. Було встановлено Volatility Framework та Autopsy, що є програмними засобами з відкритим вихідним кодом, що дає можливість будь яким юридичним чи фізичним особам використовувати ці засоби безкоштовно та мати можливість змінювати вихідний код за потреби. Важливим також є спільнота навколо цих продуктів яка їх підтримує та створює специфічні модулі і тим самим розширює функціональність цих засобів. Було розглянуто основні функції програм, методи їх практичного застосування та поетапні кроки необхідні для проведення аналізу.

Перелік посилань

1. The Future of Digital Forensics: Challenges and the Road Ahead. [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/319998952_The_Future_of_Digital_Forensics_Challenges_and_the_Road_Ahead.
2. Дамп ОЗУ. [Електронний ресурс] – Режим доступу до ресурсу: https://archive.org/download/Africa-DFIRCTF-2021-WK02/20210430-Win10Home-20H2-64bit-memdump.mem.7z.
3. Що таке кущ реєстру? [Електронний ресурс] – Режим доступу до ресурсу: https://www.lifewire.com/what-is-a-registry-hive-2625986.
4. Образ диску. [Електронний ресурс] – Режим доступу до ресурсу: https://dfir.science/assets/data/SuspectData.dd.zip.
5. Образ диску. [Електронний ресурс] – Режим доступу до ресурсу: https://archive.org/download/africa-dfirctf-2021-WK01/africa-dfirctf-2021-WK01_archive.torrent.
6. Prefetch файли. [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/topics/computer-science/prefetch.
7. Shellbags. [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/ce-digital-forensics/shellbag-analysis-18c9b2e87ac7.

Надійшла: 18.05.2022 Рецензент: д.т.н., професор Гайдур Г.І.