ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ АНАЛІЗУ РЕЄСТРУ ТА ЖУРНАЛУ ПОДІЙ»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Клименко М. Н.
(прізвище та ініціали)
Керівник Собчук А.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

APIs – Application Programming Interfaces

APT – Advanced Persistent Threat

BIOS – Basic Input/Output System

CFTT – Computer Forensics Tool Testing

DFIR – Digital Forensics and Incident Response

FOX – Free Objects for X

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPsec – IP security

LGPL – Library GNU Public License

NIST – National Institute of Standards and Technology

NTFS – New Technology File System

RAID – Redundant Array of Independent Disks

RDS – Reference Data Set

XML – eXtensible Markup Language

ВСТУП

Актуальність дослідження. Протягом останнього десятиліття кількість злочинів, пов'язаних із використанням комп'ютерів, зросла, що призвело до зростання компаній та продуктів, які мають на меті допомогти правоохоронним органам використовувати комп'ютерні докази для визначення того, хто, що, де, коли і як вчинив злочин. В результаті комп'ютерна та мережева криміналістична експертиза вдосконалювалася, щоб гарантувати належне представлення даних, що є доказами комп'ютерного злочину, до суду.

Зростаюча різноманітність джерел даних в інформаційних системах організацій сприяла розробці та вдосконаленню різноманітних інструментів і методів криміналістики.

Криміналістичні інструменти та методи найчастіше розглядаються в контексті кримінальних розслідувань та обробки інцидентів комп'ютерної безпеки – використовуються для реагування на подію шляхом розслідування підозрілих систем, збору та збереження доказів, реконструкції подій та оцінки поточного стану події. Однак інструменти та методи розслідувань інцидентів також корисні для багатьох інших типів завдань, які мають за мету підтримання інформаційних систем організацій у робочому стані.

Вищесказане визначає актуальність теми даної бакалаврської роботи, основний зміст якої становлять дослідження методів та засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу реєстру та журналу подій.

Об'єкт дослідження – розслідування інцидентів в інформаційній системі організації.

Предмет дослідження – методи та засоби розслідування інцидентів в інформаційній системі організації з використанням аналізу реєстру та журналу подій.

Мета роботи – розробити рекомендації щодо розслідування інцидентів в

інформаційній системі організації з використанням аналізу реєстру та журналу подій.

Наукові завдання:

дослідити проблему розслідування інцидентів в інформаційних системах;

визначити зміст розслідування інцидентів в інформаційних системах;

дослідити існуючі методи та засоби розслідування інцидентів в інформаційних системах;

визначити порядок застосування методів та засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу реєстру та журналу подій;

розробити рекомендації щодо застосування методів та засобів розслідування інцидентів в інформаційній системі організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування методів та засобів розслідування інцидентів в інформаційній системі організації.

1 АНАЛІЗ ПРОБЛЕМИ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

1.1. Дослідження проблеми розслідування інцидентів в інформаційних системах

Необхідно відмітити, що сьогодні кількість інцидентів в інформаційних системах організацій та кількість даних, пов'язаних з ними, постійно зростає. Це ускладнює виконання покладених завдань фахівцями з кібербезпеки.

Без сучасного набору інструментів для розслідування інцидентів та реагування на них, який використовує підхід і автоматизацію на основі артефактів, командам DFIR (Digital forensics and incident response, DFIR) виконати поставлені перед ними завдання буде дуже важко [1].

Цілком зрозуміло, що чим більше даних, тим більше часу потрібно для їх ретельного аналізу. На додаток до проблеми обсягу, існує також різноманітність даних, яка зараз існує. Комп'ютери більше не є єдиним джерелом доказів. Є мобільні пристрої, хмарні програми та сервіси, а також сфера пристроїв Інтернету речей (IoT), що експоненціально зростає [1].

Коли об'єм і різноманітність даних збільшуються, проблеми, з якими стикаються команди DFIR, стають чітко зрозумілими. Фахівці DFIR повинні мати інструменти, які полегшують їх роботу.

Близько 25% організацій щотижня повідомляють про зараження програмами-вимагачами. У міру розвитку зловмисного програмного забезпечення ці окремі події об'єднуються в окремі атаки: зловмисне програмне забезпечення спочатку ексфільтрує дані, а потім шифрує їх, дозволяючи зловмисникові отримати викуп за вивільнення ключів зашифрованих даних, а також вимагати організацію, щоб запобігти оприлюдненню даних [1].

Це особливо складно для спеціалістів DFIR, оскільки вони повинні швидко пом'якшити дію програми-вимагача, перш ніж вона зможе поширюватися та

завдати шкоди. Програми-вимагачі важче пом’якшити за допомогою технологій безпеки, які потребують більше аналізу та часу [1].

На рис. 1.1 показано оцінку найбільших подій, які відбулися за останній рік і які події будуть докучати в наступні два роки.

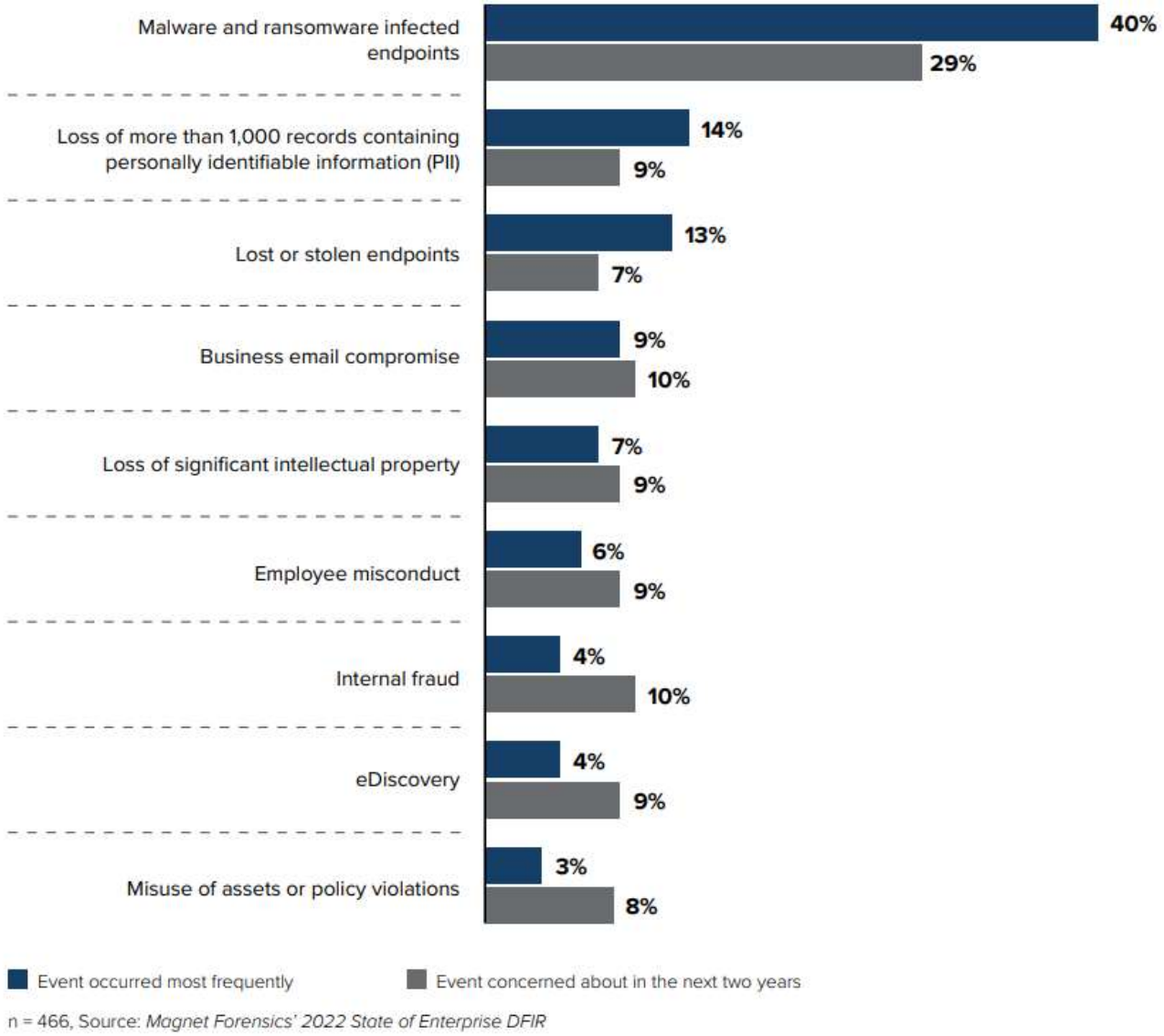
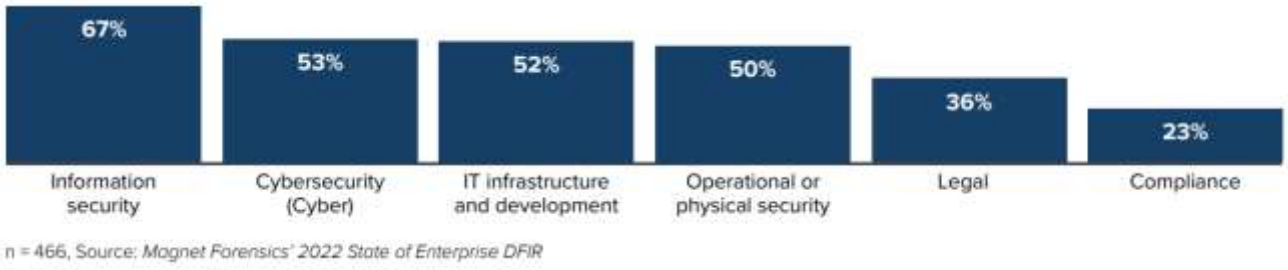


Рис. 1.1. Оцінка основних загроз за 2021 рік за даними [1]

За даними [1] розслідування інцидентів проводять фахівці інформаційної та кібербезпеки, що показано на рис. 1.2. Фахівці DFIR мають завдання реагувати на інциденти, розслідувати проблеми та надавати підтримку в судовому розгляді. Виклик цих завдань стає експоненціально складнішим, оскільки світ переходить до гібридної роботи, а дані збільшуються в розмірі та різноманітності.



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Рис. 1.2. Які фахівці розслідують інциденти [1]

Хоча відділи DFIR, як правило, невеликі, їхній список завдань великий, і в міру того, як світ розвивається, вони також повинні розвиватися. Особам, які приймають рішення, і практикам DFIR потрібні інвестиції, і ці інвестиції мають бути вдосконалені технології. Командам DFIR потрібні уніфіковані рішення, які забезпечують спрощені робочі процеси та збір із різних джерел даних, а також технології, які можуть синтезувати дані в один файл справи для зручності використання. Це інструменти, які забезпечать успіх зараз і в майбутньому [1].

Отже, дослідження методів та засобів розслідування інцидентів в інформаційній системі організації є актуальним завданням.

1.2. Аналіз змісту розслідування інцидентів в інформаційних системах

Багато експертів вважають криміналістичну науку застосуванням широкого спектру знань і технологій для розслідування та встановлення фактів, що становлять інтерес у зв'язку з кримінальним правом, цивільним правом чи нормативними питаннями [2].

Швидкий розвиток IT вимагає розробки кращих інструментів криміналістичної експертизи, щоб не відставати від можливостей зловмисників. Однак отримані методи та засоби розслідування інцидентів можуть також використовуватися для інших цілей, ніж юридичні та нормативні питання, *для реконструкції події, що сталася*.

Для цифрової криміналістичної експертизи розроблено різні моделі процесів, включаючи наступні вісім відмітних кроків і атрибутів [2]:

1. Пошук органу. Для проведення пошуку та/або вилучення даних необхідні

юридичні повноваження.

2. Ланцюг опіки. У правовому контексті необхідне хронологічне документування доступу та роботи з доказами, щоб уникнути звинувачень у підробці доказів або неправомірній поведінці.

3. Функція зображення/хешування. При виявленні елементів, що містять потенційні цифрові докази, кожен слід ретельно продублювати, а потім хешувати, щоб перевірити цілісність копії.

4. Перевірені інструменти. Якщо можливо, інструменти, що використовуються для криміналістичної експертизи, повинні бути перевірені для забезпечення надійності та правильності.

5. Аналіз. Криміналістичний аналіз – це виконання слідчих та аналітичних прийомів для дослідження, аналізу та інтерпретації вилучених доказових артефактів.

6. Повторюваність і відтворюваність (гарантія якості). Процедури та висновки криміналістичного аналізу мають бути повторюваними та відтворюваними тими ж чи іншими судовими аналітиками.

7. Звітність. Аналітик з розслідування повинен задокументувати свою аналітичну процедуру та висновки для використання іншими.

8. Презентація. У більшості випадків судовий аналітик представляє свої докази та висновки суду чи іншій аудиторії.

Також NIST (National Institute of Standards and Technology, NIST) визначає цифрову криміналістику як область криміналістики, яка займається пошуком, зберіганням та аналізом електронних даних, які можуть бути корисними в кримінальних розслідуваннях. Це включає інформацію з комп’ютерів, жорстких дисків, мобільних телефонів та інших пристроїв зберігання даних [3].

Останніми роками стали важливими більш різноманітні джерела даних, включаючи автомобілі, дрони та хмари. Цифрові криміналістичні слідчі стикаються з такими проблемами, як вилучення даних із пошкоджених або знищених пристроїв, визначення місцезнаходження окремих доказів серед величезної кількості даних і забезпечення надійного отримання даних, не

змінюючи їх жодним чином.

NIST допомагає спільноті цифрових криміналістів вирішувати ці проблеми. Так, Національна довідкова бібліотека програмного забезпечення (National Software Reference Library) містить регулярно оновлюваний архів відомих програмних програм, які можна відстежувати, зібраних NIST. NIST створює цифрові підписи з усіх файлів у цьому архіві та випускає їх у щоквартальному наборі довідкових даних (Reference Data Set, RDS). Коли правоохоронна організація вилучає комп'ютер або мобільний пристрій у рамках кримінального розслідування, вони можуть використовувати RDS, щоб швидко ідентифікувати відомі файли на цьому пристрої. Це зменшує зусилля, необхідні для визначення, які файли важливі як докази, а які ні.

У правоохоронних органах існує критична потреба у забезпеченні надійності комп'ютерних інструментів криміналістики. Програма комп'ютерного криміналістичного тестування інструментів встановлює методологію для тестування програмних засобів комп'ютерної криміналістичної експертизи шляхом розробки загальних специфікацій інструментів, процедур тестування, критеріїв тестування, наборів тестів та тестового обладнання. Результати допомагають виробникам інструментів удосконалювати свої продукти, дозволяють користувачам робити обґрунтований вибір щодо того, які інструменти використовувати, а також надають інформацію всім зацікавленим сторонам про можливості різних комп'ютерних інструментів, які використовуються в криміналістичних розслідуваннях.

Цифрові докази представляють собою дані на комп'ютерах і мобільних пристроях, включаючи аудіо, відео та файли зображень, а також програмне та апаратне забезпечення. Цифрові докази можуть бути частиною розслідування більшості злочинів, оскільки матеріали, що мають відношення до злочину, можуть бути записані в цифровій формі. Методи безпечного отримання, зберігання та аналізу цифрових доказів швидко й ефективно мають вирішальне значення [4].

Мета проекту тестування інструментів комп'ютерної криміналістичної

експертизи (Computer Forensics Tool Testing, CFTT) у NIST полягає в тому, щоб створити методологію для тестування інструментів комп'ютерної криміналістичної експертизи шляхом розробки загальних специфікацій інструментів, процедури тестування, критерії тестування, тестові набори та тестове обладнання.

NIST розробляє набори довідкових даних комп'ютерної криміналістичної експертизи (Computer Forensic Reference Data Sets, CFReDS) для цифрових доказів. Ці набори довідкових даних (CFReDS) надають досліднику задокументовані набори змодельованих цифрових доказів для дослідження.

Цифрова криміналістична експертиза, також відома як комп'ютерна та мережева експертиза, має багато визначень. Як правило, це вважається застосуванням науки для ідентифікації, збору, дослідження та аналізу даних, зберігаючи цілісність інформації та підтримуючи суворий ланцюг зберігання даних. Дані – це окремі фрагменти цифрової інформації, які були відформатовані певним чином. Організації мають постійно зростаючий обсяг даних з багатьох джерел. Наприклад, дані можуть зберігатися або передаватися стандартними комп'ютерними системами, мережевим обладнанням, комп'ютерною периферією, персональними цифровими помічниками (PDA), споживчими електронними пристроями та різними типами носіїв, серед інших джерел [5].

Через різноманітність джерел даних цифрові криміналістичні методи можуть використовуватися для багатьох цілей, наприклад, для розслідування злочинів і порушень внутрішньої політики, відновлення інцидентів безпеки, усунення несправностей у роботі та відновлення після випадкових пошкоджень системи.

Зазначається, що практично кожна організація повинна мати можливість виконувати цифрову криміналістичну експертизу. Без такої можливості організації буде важко визначити, які події відбулися в її системах і мережах, наприклад розкриття захищених, конфіденційних даних [5].

Розглянемо основні етапи криміналістичного процесу: збір, експертиза, аналіз та звітність відповідно до [5]. Основні етапи криміналістичного процесу

показано на рис. 1.3.

Під час збору дані, пов’язані з певною подією, ідентифікуються, маркуються, записуються та збираються, а їх цілісність зберігається. На другому етапі виконується експертиза, інструменти та методи криміналістичної експертизи, що відповідають типам зібраних даних, щоб ідентифікувати та витягти відповідну інформацію із зібраних даних, одночасно захищаючи їх цілісність. Експертиза може використовувати комбінацію автоматизованих інструментів і ручних процесів. Наступна фаза, аналіз, передбачає аналіз результатів експертизи для отримання корисної інформації, яка вирішує питання, які послужили поштовхом для проведення збору та експертизи. Останній етап включає звіт про результати аналізу, який може включати опис виконаних дій, визначення інших дій, які необхідно виконати, і рекомендації щодо покращення політики, керівних принципів, процедур, інструментів та інших аспектів процесу криміналістичної експертизи.

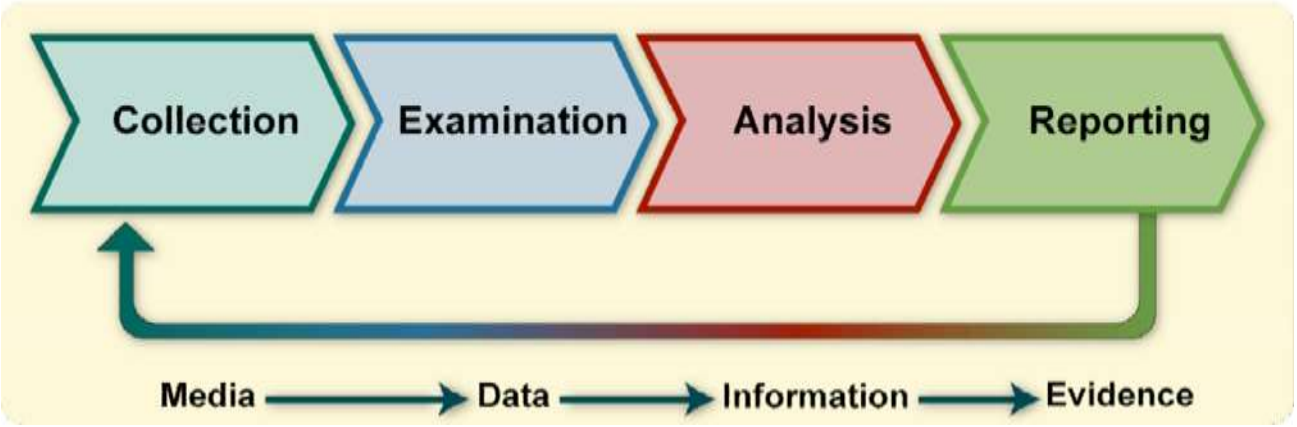


Рис. 1.3. Складові криміналістичного процесу [5]

Як показано в нижній частині рисунка 1.3, криміналістичний процес перетворює медіа на докази, незалежно від того, чи потрібні докази для правоохоронних органів чи для внутрішнього використання організації.

Зокрема, перше перетворення відбувається, коли зібрані дані перевіряються, що витягує дані із носіїв і перетворює їх у формат, який може бути оброблений інструментами криміналістики.

По-друге, дані перетворюються в інформацію за допомогою аналізу. Нарешті, перетворення інформації в докази аналогічно передачі знань у дію – використання інформації, отриманої в результаті аналізу, одним або кількома способами під час фази звітування. Наприклад, це може бути використано як докази, щоб допомогти притягнути до відповідальності конкретну особу, інформація, яка може діяти, щоб допомогти зупинити або пом'якшити певну діяльність, або знання для створення нових потенційних клієнтів для справи.

Першим кроком у процесі розслідування інцидентів є визначення потенційних джерел даних та отримання даних з них – *збір даних (Collection)*.

Визначення можливих джерел даних. Все більш широке використання цифрових технологій як для професійних, так і для особистих цілей призвело до великої кількості джерел даних. Найочевиднішими та поширеними джерелами даних є комп'ютери, сервери, мережеві пристрої зберігання даних та ноутбуки. Ці системи зазвичай мають внутрішні накопичувачі, а також мають кілька типів портів (наприклад, USB, PCMCIA), до яких можна підключити медіа та пристрої, на яких зберігаються зовнішні дані. Прикладами зовнішніх форм зберігання даних, які можуть бути джерелами даних, є флеш-накопичувачі, картки пам'яті та флеш-карти, оптичні диски та магнітні диски.

Стандартні комп'ютерні системи також містять дані, які доступні тимчасово (тобто, поки система не буде вимкнена або перезавантажена). На додаток до пристроїв, пов'язаних з комп'ютером, багато типів портативних цифрових пристроїв (наприклад, КПК, мобільні телефони, цифрові камери, цифрові рекордери, аудіоплеєри) також можуть містити дані. Аналітики повинні вміти оглядати фізичну територію, наприклад офіс, та розпізнавати можливі джерела даних.

Аналітики також повинні подумати про можливі джерела даних, розташовані в інших місцях. Наприклад, зазвичай в організації існує багато джерел інформації про мережеву діяльність і використання програм. Інформація також може бути записана іншими організаціями, наприклад журнали мережевої активності для постачальника послуг Інтернету (ISP). Аналітики повинні

пам’ятати про власника кожного джерела даних і вплив, який це може мати на збір даних. Наприклад, для отримання копій записів провайдера зазвичай потрібне рішення суду.

Аналітики також повинні знати про політику організації, а також юридичні міркування щодо майна, що перебуває у зовнішній власності на об’єктах організації (наприклад, персональний ноутбук співробітника або ноутбук підрядника). Ситуація може стати ще складнішою, якщо задіяні місця поза контролем організації, наприклад інцидент із комп’ютером у домашньому офісі дистанційного працівника. Іноді зібрати дані з первинного джерела даних просто неможливо. Тому аналітики повинні знати про альтернативні джерела даних, які можуть містити деякі або всі ті самі дані, і повинні використовувати ці джерела замість недосяжного джерела.

Організації можуть вживати постійних активних заходів для збору даних, які можуть бути корисними для криміналістичних цілей. Наприклад, більшість ОС можна *налаштувати на аудит і запис певних типів подій*, таких як спроби автентифікації та зміни політики безпеки, як частина звичайних операцій. Записи аудиту можуть надавати цінну інформацію, включаючи час, коли відбулася подія, і походження події.

Ще одна корисна дія – *запровадити централізоване ведення журналів*, що означає, що певні системи та програми пересилають копії своїх журналів на захищені центральні сервери журналів. Централізоване ведення журналів запобігає неавторизованим користувачам від втручання в журнали та використання методів для перешкоджання аналізу.

Регулярне резервне копіювання систем дозволяє аналітикам переглядати вміст системи таким, яким він був у певний час. Крім того, засоби контролю безпеки, такі як програмне забезпечення для виявлення вторгнень, антивірусне програмне забезпечення та утиліти виявлення та видалення шпигунських програм, можуть створювати журнали, які показують, коли і як відбулася атака або вторгнення.

Іншим проактивним заходом збору даних є *моніторинг поведінки*

користувачів, наприклад моніторинг натискання клавіш, який фіксує використання клавіатури певною системою. Хоча цей захід може забезпечити цінний запис діяльності, він також може бути порушенням конфіденційності, якщо користувачі не повідомлені через організаційну політику та банери входу, що такий моніторинг може здійснюватися. Більшість організацій не використовують такі методи, як моніторинг натискання клавіш, за винятком випадків збору додаткової інформації про підозрюваний інцидент. Повноваження для здійснення такого моніторингу мають бути обговорені з юридичними радниками та чітко зафіксовані в політиці організації.

Експертиза (Examination). Після того як дані були зібрані, наступним етапом є перевірка даних, яка включає оцінку та вилучення відповідної інформації із зібраних даних. Ця фаза також може включати обхід або пом'якшення функцій ОС або програм, які приховують дані та код, наприклад механізми стиснення даних, шифрування та контролю доступу. Придбаний жорсткий диск може містити сотні тисяч файлів даних; визначення файлів даних, які містять інформацію, що цікавить, включаючи інформацію, приховану за допомогою стиснення файлів і контролю доступу, може бути складним завданням. Крім того, файли даних, що представляють інтерес, можуть містити сторонню інформацію, яку слід відфільтрувати. Наприклад, вчорашній журнал брандмауера може містити мільйони записів, але лише п'ять записів можуть бути пов'язані з подією, що цікавить.

На щастя, можна використовувати різні інструменти та методи, щоб зменшити кількість даних, які необхідно просіяти. Пошук тексту та шаблону можна використовувати для визначення відповідних даних, наприклад, для пошуку документів, у яких згадується певна тема чи особа, або для ідентифікації записів журналу електронної пошти для певної адреси електронної пошти.

Іншим корисним методом є використання інструмента, який може визначити тип вмісту кожного файлу даних, наприклад текст, графіка, музика або стиснутий файловий архів. Знання типів файлів даних можна використовувати для визначення файлів, які потребують подальшого вивчення, а також для

виключення файлів, які не представляють інтересу для перевірки. Існують також бази даних, що містять інформацію про відомі файли, які також можна використовувати для включення або виключення файлів з подальшого розгляду.

Аналіз (Analysis). Після отримання відповідної інформації аналітик повинен вивчити та проаналізувати дані, щоб зробити з них висновки.

Основою криміналістики є використання методичного підходу для досягнення відповідних висновків на основі наявних даних або визначення того, що висновки ще не можуть бути зроблені.

Аналіз повинен включати визначення людей, місць, предметів і подій, а також визначення того, як ці елементи пов’язані, щоб можна було зробити висновок. Часто ці зусилля включатимуть кореляцію даних із кількох джерел. Наприклад, журнал системи виявлення вторгнення в мережу (IDS) може пов’язувати подію з хостом, журнали аудиту хосту можуть пов’язувати подію з певним обліковим записом користувача, а журнал IDS хоста може вказувати, які дії виконував цей користувач. Такі інструменти, як централізоване ведення журналів і програмне забезпечення для керування подіями безпеки, можуть полегшити цей процес шляхом автоматичного збору та співвіднесення даних. Порівнюючи характеристики системи з відомими базовими лініями, можна визначити різні типи змін, внесених у систему.

Звітність (Reporting). Завершальним етапом є звітність, яка є процесом підготовки та представлення інформації, отриманої в результаті фази аналізу. На звітування впливає багато факторів, зокрема такі:

альтернативні пояснення. Якщо інформація про подію є неповною, неможливо отримати остаточне пояснення того, що сталося. Якщо подія має два або більше правдоподібних пояснень, кожне з них має бути належним чином розглянуто в процесі звітування. Аналітики повинні використовувати методичний підхід, щоб спробувати довести або спростувати кожне можливе пояснення, яке пропонується;

розгляд аудиторії. Важливо знати аудиторію, якій будуть показані дані чи інформація. Інцидент, що вимагає залучення правоохоронних органів, вимагає

дуже детальних звітів про всю зібрану інформацію, а також може вимагати копій усіх отриманих доказових даних. Системний адміністратор може захотіти детально ознайомитися з мережевим трафіком і пов’язаною статистикою. Вище керівництво може просто захотіти отримати детальний огляд того, що сталося, наприклад, спрощене візуальне уявлення про те, як сталася атака, і що потрібно зробити, щоб запобігти подібним інцидентам;

діюча інформація. Звітність також включає визначення отриманої інформації, яка може бути використана з даних, які можуть дозволити аналітику збирати нові джерела інформації. Наприклад, список контактів може бути складений на основі даних, які можуть привести до додаткової інформації про інцидент або злочин. Крім того, може бути отримана інформація, яка може запобігти майбутнім подіям, наприклад бекдор у системі, який може бути використаний для майбутніх атак, планований злочин, хробак, який заплановано почати поширюватися в певний час, або вразливість, яка може бути експлуатованим.

У рамках процесу звітності аналітики повинні визначити будь-які проблеми, які, можливо, потрібно буде виправити, наприклад, недоліки політики або процедурні помилки. Багато криміналістичних експертів та груп реагування на інциденти проводять офіційні огляди після кожної великої події. Такі огляди, як правило, включають серйозне розгляд можливих покращень керівних принципів і процедур, і зазвичай принаймні деякі незначні зміни затверджуються та впроваджуються після кожного перегляду.

Наприклад, одна поширена проблема полягає в тому, що багато організацій вважають, що ведення поточних списків персоналу, з яким можна зв’язатися з кожним різним типом інциденту, що може статися, є ресурсномістким. Інші поширені проблеми полягають у тому, що робити з гігабайтами або терабайтами даних, зібраних під час розслідування, і як можна змінити засоби контролю безпеки (наприклад, аудит, журналювання, виявлення вторгнень) для запису додаткових даних, які будуть корисні для майбутніх розслідувань.

1.3. Аналіз існуючих методів та засобів розслідування інцидентів в інформаційних системах

Зростання кількості злочинів, пов’язаних із використанням комп’ютерів, призвело до зростання компаній та продуктів, які мають на меті допомогти правоохоронним органам використовувати комп’ютерні докази для визначення того, хто, що, де, коли і як вчинив злочин. В результаті комп’ютерна та мережева криміналістична експертиза вдосконалювалася, щоб гарантувати належне представлення даних, що є доказами комп’ютерного злочину, до суду. Криміналістичні інструменти та методи найчастіше розглядаються в контексті кримінальних розслідувань та обробки інцидентів комп’ютерної безпеки – використовуються для реагування на подію шляхом розслідування підозрілих систем, збору та збереження доказів, реконструкції подій та оцінки поточного стану події [5].

Однак інструменти та методи розслідувань інцидентів також корисні для багатьох інших типів завдань, наприклад [5]:

операційне усунення несправностей. Багато інструментів і методів криміналістичної експертизи можуть бути застосовані для усунення несправностей операційних проблем, таких як пошук віртуального та фізичного розташування хоста з неправильною конфігурацією мережі, вирішення функціональної проблеми з програмою, а також запис і перегляд поточних параметрів конфігурації ОС і прикладних програми;

моніторинг журналу. Різні інструменти та методи можуть допомогти в моніторингу журналів, наприклад, аналіз записів журналу та співвіднесення записів журналу в кількох системах. Це може допомогти в обробці інцидентів, виявленні порушень політики, аудиті та інших зусиллях;

відновлення даних. Існують десятки інструментів, які можуть відновити втрачені дані з систем, у тому числі дані, які були випадково чи навмисно видалені чи іншим чином змінені. Обсяг даних, які можна відновити, варіюється в кожному окремому випадку;

збір даних. Деякі організації використовують інструменти криміналістичної експертизи для отримання даних від хостів, які перерозгортаються або вилучаються. Наприклад, коли користувач залишає організацію, дані з робочої станції користувача можуть бути отримані та збережені, якщо вони знадобляться в майбутньому. Потім носій робочої станції можна очистити, щоб видалити всі вихідні дані користувача;

дотримання нормативних вимог. Існуючі та нові норми вимагають від багатьох організацій захищати конфіденційну інформацію та підтримувати певні записи для цілей аудиту.

Крім того, коли захищена інформація стає доступною для інших сторін, організації можуть вимагати сповістити інші установи або осіб, яких це стосується. Криміналістична експертиза може допомогти організаціям проявити належну обачність і дотримуватися таких вимог.

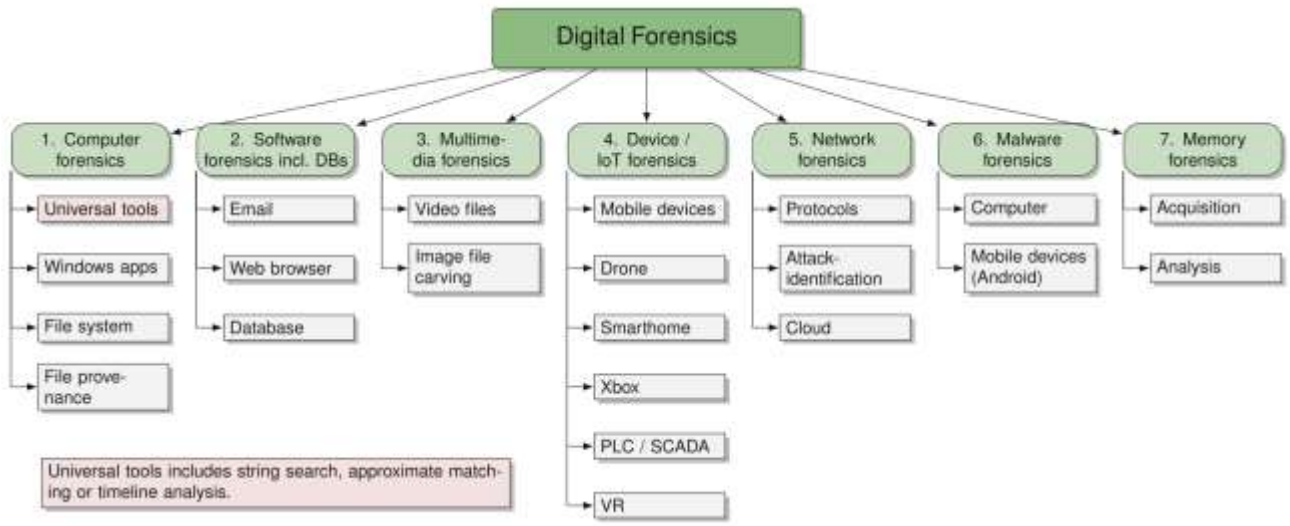


Рис. 1.4. Напрямки цифрової криміналістики, які визначають види методів та засобів її проведення [6]

Аналітики повинні використовувати методичний підхід до вивчення даних. Основою криміналістики є використання методичного підходу до аналізу наявних даних, щоб аналітики могли зробити відповідні висновки на основі наявних даних або визначити, що висновки ще не можуть бути зроблені. Якщо можуть знадобитися докази для юридичних або внутрішніх дисциплінарних заходів,

аналітики повинні ретельно задокументувати висновки та всі вжиті кроки [5].

Одним із основних джерел аналітичних даних є файли даних.

Файл даних (також званий файлом) – це набір інформації, логічно згрупований в одну сутність і на який посилається унікальне ім’я, наприклад ім’я файлу. Файл може мати багато типів даних, включаючи документ, зображення, відео або програму. Успішна криміналістична обробка комп’ютерних носіїв залежить від здатності збирати, досліджувати та аналізувати файли, які зберігаються на носіях.

Перш ніж намагатися збирати або досліджувати файли, аналітики повинні мати достатньо вичерпне розуміння файлів і файлових систем. По-перше, аналітики повинні знати про різноманітність носіїв, які можуть містити файли.

Широке використання комп’ютерів та інших цифрових пристроїв призвело до значного збільшення кількості різних типів носіїв, які використовуються для зберігання файлів.

Перш ніж використовувати носії для зберігання файлів, їх зазвичай потрібно розділити на розділи та відформатувати в логічні томи. Розбиття це логічний поділ носія на частини, які функціонують як фізично окремі одиниці. Логічний том це розділ або набір розділів, що діють як єдиний об’єкт, відформатований у файловій системі. Формат логічних томів визначається вибраною файловою системою.

Файлова система визначає спосіб іменування, зберігання, упорядкування та доступу до файлів на логічних томах.

Існує багато різних файлових систем, кожна з яких надає унікальні функції та структури даних. Проте всі файлові системи мають деякі спільні риси. По-перше, вони використовують концепції каталогів і файлів для організації та зберігання даних. Каталоги це організаційні структури, які використовуються для групування файлів разом.

Крім файлів, каталоги можуть містити інші каталоги, які називаються підкаталогами. По-друге, файлові системи використовують деяку структуру даних, щоб вказати на розташування файлів на носіях. Крім того, вони зберігають

кожен файл даних, записаний на носій, в одній або кількох одиницях розміщення файлів. Деякі файлові системи називають їх кластерами (наприклад, таблиця розміщення файлів [FAT], файлова система NT [NTFS]), а інші файлові системи (наприклад, UNIX і Linux) називають блоками. Одиниця розміщення файлів це просто група секторів, які є найменшими одиницями, до яких можна отримати доступ на носіях.

Аналітики повинні мати доступ до різних інструментів, які дають їм змогу проводити експертизу та аналіз даних, а також певну діяльність зі збору даних. Багато криміналістичних продуктів дозволяють аналітику виконувати широкий спектр процесів для аналізу файлів і програм, а також збирати файли, читати образи дисків і витягувати дані з файлів. Більшість продуктів аналізу також мають можливість створювати звіти та реєструвати всі помилки, що виникли під час аналізу. Хоча ці продукти є неоціненними для виконання аналізу, важливо зрозуміти, які процеси слід запустити, щоб відповісти на конкретні запитання про дані. Аналітику може знадобитися надати швидку відповідь або просто відповісти на просте запитання про зібрані дані.

У цих випадках повна криміналістична експертиза може бути непотрібною або навіть можливою. Інструментарій криміналістичної експертизи повинен містити програми, які можуть виконувати перевірку та аналіз даних багатьма способами і які можна швидко й ефективно запускати з носіїв інформації або робочої станції криміналістичної експертизи.

Серед тих процесів, які аналітик повинен вміти виконувати за допомогою різноманітних інструментів, є [5]:

використання програм для перегляду файлів. Використання засобів перегляду замість вихідних програм для відображення вмісту певних типів файлів є важливою технікою для сканування або попереднього перегляду даних і є більш ефективним, оскільки аналітику не потрібні власні програми для перегляду кожного типу файлів.

Доступні різні інструменти для перегляду поширених типів файлів, а також спеціалізовані інструменти виключно для перегляду графіки. Якщо доступні

засоби перегляду файлів не підтримують певний формат файлу, слід використовувати початкову програму; якщо це недоступне, то може знадобитися дослідити формат файлу та вручну витягти дані з файлу;

використання програм для розпакування файлів. Стислі файли можуть містити файли з корисною інформацією, а також інші стислі файли. Тому важливо, щоб аналітик знаходив та витягував стислі файли. Розпакування файлів слід виконувати на початку процесу криміналістики, щоб переконатися, що вміст стиснутих файлів буде включено в пошук та інші дії. Однак аналітикам слід пам'ятати, що стислі файли можуть містити шкідливий вміст, наприклад бомби стиснення, які є файлами, які багаторазово стискалися, як правило, десятки чи сотні разів. Компресійні бомби можуть призвести до несправності інструментів експертизи або споживати значні ресурси; вони також можуть містити зловмисне програмне забезпечення та інші шкідливі корисні навантаження. Хоча не існує певного способу виявлення бомб стиснення перед розпакуванням файлу, є способи мінімізувати їх вплив. Наприклад, система іспиту повинна використовувати сучасне антивірусне програмне забезпечення та бути автономною, щоб обмежити вплив лише цією системою. Крім того, слід створити образ системи обстеження, щоб у разі потреби можна було відновити систему;

використання програм для графічного відображення структур каталогів. Така практика полегшує та пришвидшує аналітикам збір загальної інформації про вміст медіа, наприклад, тип встановленого програмного забезпечення та ймовірні технічні здібності користувача(-ів), які створили дані. Більшість продуктів можуть відображати структури каталогів Windows, Linux та UNIX, тоді як інші продукти специфічні для структур каталогів Macintosh;

використання програм для ідентифікація відомих файлів. Перевага пошуку файлів, що цікавлять, очевидна, але також часто буває корисно виключити з розгляду неважливі файли, такі як відомо, що ОС і файли програм. Аналітики повинні використовувати перевірені набори хешів, наприклад створені проектом Національної бібліотеки програмного забезпечення (NSRL) NIST, або особисто створені набори хешів, які були перевірені, як основу для ідентифікації відомих

доброякісних і шкідливих файлів. Набори хешів зазвичай використовують алгоритми SHA-1 і MD5 для встановлення значень дайджесту повідомлень для кожного відомого файлу;

використання програм для виконання пошуку рядків і відповідності шаблону. Пошук рядків допомагає переглядати великі обсяги даних для пошуку ключових слів або рядків. Доступні різні інструменти пошуку, які можуть використовувати булеву логіку, нечітку логіку, синоніми та поняття, стемування та інші методи пошуку. Приклади поширених пошуків включають пошук кількох слів в одному файлі та пошук версій певних слів з помилкою. Розробка стислих наборів пошукових термінів для поширених ситуацій може допомогти аналітику зменшити обсяг інформації для перегляду.

Таким чином, аналітики повинні мати набір криміналістичних інструментів для дослідження та аналізу даних. Набір інструментів повинен містити різні інструменти, які забезпечують можливість швидкого перегляду даних, а також поглибленого аналізу. Набір інструментів повинен дозволяти швидко й ефективно запускати його програми зі знімних носіїв або робочої станції криміналістичної експертизи.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ АНАЛІЗУ РЕЄСТРУ ТА ЖУРНАЛУ ПОДІЙ

2.1. Використання даних реєстру ОС Windows під час розслідування інцидентів

Розглянемо можливості використання даних з операційних систем під час розслідування інцидентів.

Операційна система (ОС) це програма, яка виконується на комп'ютері та забезпечує програмну платформу, на якій можуть працювати інші програми. Крім того, ОС відповідає за обробку вхідних команд від користувача, відправку виводу на дисплей, взаємодію з пристроями пам'яті для зберігання та отримання даних, а також керування периферійними пристроями, такими як принтери та модеми. Деякі поширені ОС для робочих станцій або серверів включають різні версії Windows, Linux, UNIX і Mac OS тощо. Деякі мережеві пристрої, такі як маршрутизатори, мають власні ОС. На КПК часто працюють спеціалізовані ОС. Багато вбудованих систем, таких як мобільні телефони, цифрові камери та аудіоплеєри, також використовують ОС [5].

Дані ОС існують як у енергонезалежному, так і в непостійному стані. Енергонезалежні дані – це дані, які зберігаються навіть після вимкнення комп'ютера, наприклад, файлова система, що зберігається на жорсткому диску. Непостійні дані – це дані про діючу систему, які втрачаються після вимкнення комп'ютера, наприклад поточні мережеві підключення до системи та з неї. Багато типів енергонезалежних і непостійних даних можуть представляти інтерес з точки зору криміналістики.

Основним джерелом енергонезалежних даних в ОС є файлова система. Файлова система також зазвичай є найбільшим і найбагатшим джерелом даних в ОС, що містить більшість інформації, відновленої під час типової

криміналістичної події. Файлова система забезпечує зберігання ОС на одному або кількох носіях.

Файлова система зазвичай містить багато типів файлів, кожен з яких може бути корисним для аналітиків у різних ситуаціях. Крім того, важливі залишкові дані можна відновити з невикористаного простору файлової системи. Нижче наведено кілька *типів даних, які зазвичай зустрічаються в файлових системах ОС*:

Конфігураційні файли. ОС може використовувати файли конфігурації для зберігання налаштувань ОС і програми. Наприклад, файли конфігурації можуть перелічувати служби, які автоматично запускаються після завантаження системи, і вказувати розташування файлів журналів і тимчасових файлів. Користувачі також можуть мати окремі файли конфігурації ОС і програми, які містять конкретну інформацію та параметри користувача, такі як параметри, пов’язані з обладнанням (наприклад, роздільна здатність екрана, параметри принтера) та асоціації файлів.

Особливий інтерес представляють такі файли конфігурації:

Користувачі та групи. ОС веде записи облікових записів і груп користувачів. Інформація про обліковий запис може включати членство в групі, назву та опис облікового запису, дозволи облікового запису, статус облікового запису (наприклад, активний, вимкнений) і шлях до домашнього каталогу облікового запису.

Файли паролів. ОС може зберігати хеші паролів у файлах даних. Різні утиліти для злому паролів можуть використовуватися для перетворення хешу пароля в його еквівалент чистого тексту для певних ОС.

Планові роботи. ОС підтримує список запланованих завдань, які мають виконуватися автоматично в певний час (наприклад, щотижня перевіряти віруси). Інформація, яку можна отримати з цього, включає назву завдання, програму, яка використовується для виконання завдання, перемикачі та аргументи командного рядка, а також дні та час виконання завдання.

Журнали. Файли журналу ОС містять інформацію про різні події ОС, а

також можуть містити інформацію про події, специфічні для програм. Залежно від ОС журнали можуть зберігатися в текстових файлах, бінарних файлах власного формату або базах даних. Деякі ОС записують записи журналу в два або більше окремих файлів. Типи інформації, які зазвичай містяться в журналах ОС:

Системні події. Системні події – це оперативні дії, які виконуються компонентами ОС, наприклад, вимкнення системи або запуск служби. Зазвичай реєструються невдалі події та найважливіші успішні події, але багато ОС дозволяють системним адміністраторам вказувати, які типи подій будуть реєструватися. Деталі, які реєструються для кожної події, також сильно відрізняються. Кожна подія зазвичай має мітку часу; інша допоміжна інформація може включати коди подій, коди статусу та ім’я користувача.

Аудиторські записи. Записи аудиту містять інформацію про події безпеки, наприклад успішні та невдалі спроби автентифікації та зміни політики безпеки. ОС зазвичай дозволяють системним адміністраторам вказувати, які типи подій слід перевіряти. Адміністратори також можуть налаштувати деякі ОС для реєстрації успішних, невдалих або всіх спроб виконання певних дій.

Події застосування. Події програми – це значні операційні дії, які виконуються програмами, наприклад запуск і завершення програми, збої програми та основні зміни конфігурації програми.

Історія команд. Деякі ОС мають окремі файли журналу (як правило, для кожного користувача), які містять історію команд ОС, які виконує кожен користувач.

Нещодавно доступні файли. ОС може реєструвати останні звернення до файлів або інше використання, створюючи список останніх доступних файлів.

Файли програми. Програми можуть складатися з багатьох типів файлів, включаючи виконувані файли, сценарії, документацію, файли конфігурації, файли журналів, файли історії, графіку, звуки та значки.

Файли даних. Файли даних зберігають інформацію для програм. Прикладами поширених файлів даних є текстові файли, документи для обробки текстів, електронні таблиці, бази даних, аудіофайли та графічні файли. Крім того,

коли дані друкуються, більшість ОС створюють один або кілька тимчасових файлів для друку, які містять готову для друку версію даних.

Обмін файлами. Більшість ОС використовують файли підкачки разом з оперативною пам’яттю, щоб забезпечити тимчасове зберігання даних, які часто використовуються програмами. Файли підкачки по суті розширюють обсяг пам'яті, доступної для програми, дозволяючи переміщати сторінки (або сегменти) даних в оперативну пам'ять і виключати її. Файли підкачки можуть містити широкий спектр інформації про ОС і програми, наприклад імена користувачів, хеші паролів та контактну інформацію.

Дамп файлів. Деякі ОС мають можливість автоматично зберігати вміст пам’яті під час виникнення помилки, щоб допомогти в подальшому усуненні несправностей. Файл, який містить збережений вміст пам'яті, відомий як файл дампа.

Файли режиму глибокого сну. Файл режиму глибокого сну створюється для збереження поточного стану системи (як правило, ноутбука) шляхом запису пам’яті та відкритих файлів перед вимкненням системи. При наступному ввімкненні системи стан системи відновлюється.

Тимчасові файли. Під час встановлення ОС, програми чи ОС або оновлення та оновлення програми часто створюються тимчасові файли. Хоча такі файли зазвичай видаляються в кінці процесу встановлення, це відбувається не завжди. Крім того, при запуску багатьох програм створюються тимчасові файли; знову ж таки, такі файли зазвичай видаляються після завершення роботи програми, але це відбувається не завжди. Тимчасові файли можуть містити копії інших файлів у системі, дані програми або іншу інформацію.

Хоча файлові системи є основним джерелом енергонезалежних даних, іншим джерелом інтересу є BIOS.

BIOS містить багато типів інформації, пов'язаної з апаратним забезпеченням, наприклад, підключені пристрої (наприклад, CDROM-диски, жорсткі диски), типи з'єднань і призначення лінії запиту переривання (IRQ) (наприклад, послідовний порт, USB, мережева карта), материнська плата

компоненти (наприклад, тип і швидкість процесора, розмір кешу, інформація про пам'ять), параметри безпеки системи та гарячі клавіші. BIOS також взаємодіє з драйверами RAID і відображає інформацію, надану драйверами. Наприклад, BIOS розглядає апаратний RAID як один диск, а програмний RAID як кілька дисків. BIOS зазвичай дозволяє користувачеві встановлювати паролі, які обмежують доступ до налаштувань BIOS і можуть перешкоджати завантаженню системи, якщо пароль не вказано. BIOS також зберігає системну дату і час.

Слід звернути увагу на деякі моменти. Під час збору нестабільних даних ОС усі інструменти криміналістики, які можуть знадобитися, повинні бути розміщені на носії інформації, з якого ці інструменти мають виконуватися. Це дає змогу аналітикам збирати дані ОС із найменшими перешкодами для системи. Крім того, слід використовувати лише інструменти криміналістики, оскільки користувач міг замінити системні команди шкідливими програмами, наприклад, для форматування жорсткого диска або повернення неправдивої інформації. Однак використання криміналістичних інструментів не є гарантією того, що отримані дані будуть точними.

Якщо система була повністю скомпрометована, можливо, були встановлені руткіти та інші шкідливі утиліти, які змінюють функціональність системи на рівні ядра. Це може призвести до повернення неправдивих даних до інструментів на рівні користувача.

При створенні колекції інструментів криміналістики слід використовувати статично пов’язані двійкові файли. Такий виконуваний файл містить усі функції та бібліотечні функції, на які він посилається, тому окремі бібліотеки динамічних посилань (DLL) та інші допоміжні файли не потрібні. Це усуває необхідність розміщення відповідних версій DLL на носіях інструментів і підвищує надійність інструментів. Перш ніж збирати мінливі дані, аналітик повинен знати, як кожен інструмент впливає на систему або змінює її.

Дайджест повідомлень кожного інструменту має бути обчислений і безпечно збережений для перевірки цілісності файлу. Інформація про ліцензування та версію також має бути задокументована для кожного інструмента

криміналістики. Крім того, слід задокументувати точні команди, які використовувалися для запуску кожного інструмента криміналістики (тобто аргументи командного рядка та перемикачі). Може бути корисним розмістити сценарій на носій інструментів, який можна запустити, щоб фіксувати, які команди були запущені, в який час і з яким результатом.

Як зазначається в [7] *реєстр Windows є основним компонентом операційних систем Windows*, але коли справа доходить до цифрового аналізу систем Windows, це, мабуть, найменш зрозумілий компонент системи Windows. Ця може бути пов'язана з тим, що більшість комерційних програм криміналістичного аналізу роблять трохи більше, ніж відкривають реєстр Windows у програмі типу переглядача і не передбачають застосування раніше розроблених (з останнього випадку аналітика або надані іншими аналітиками) розвідку до наявних даних [7].

Реєстр Windows зберігає велику кількість конфігураційної інформації про систему, підтримуючи параметри для різних функціональних можливостей системи (тобто може бути ввімкнено або вимкнено). Крім того, реєстр зберігає історичну інформацію про діяльність користувачів для того, щоб забезпечити користувача «кращим» загальним враженням, відомості про встановлені програми та доступ до них, а також положення та розміри вікон зберігаються так само, як у файлі журналу. Вся ця інформація може бути надзвичайно цінною для судового експерта, особливо коли він намагається встановити часову шкалу діяльності системи та/або користувача.

Інформація, отримана з реєстру, мала б значну користь у багатьох випадках, якби аналітик був обізнаний про інформацію та про те, як найкраще використати її для цілей перевірки.

Що є в реєстрі? Перше, що слід пам'ятати, проводячи аналіз реєстру, це те, що там не все можна знайти. Системи Windows не записують операції копіювання файлів. Реєстр Windows є неймовірно цінним криміналістичним ресурсом. Інформація в реєстрі може мати набагато більший вплив на експертизу. Існує багато значень реєстру, які можуть мати значний вплив на поведінку різних компонентів системи. Наприклад, є значення реєстру, яке наказує операційній

системі припинити оновлення часу останнього доступу до файлу, тому щоразу, коли файл відкривається (хоча нічого не змінено) для перегляду або пошуку, мітка часу не оновлюється відповідно. Це ввімкнено за замовчуванням, починаючи з Windows Vista, і все ще ввімкнено за замовчуванням у системах Windows 7 та Windows 8. З огляду на це, як експерти визначають, коли було здійснено доступ до файлу [7].

Існують інші ресурси, як у реєстрі, так і без нього (наприклад, списки переходів), які можуть надати цю інформацію, особливо залежно від типу файлу, до якого здійснюється доступ, та програми, яка використовується для доступу до файлу. Кілька прикладів значень реєстру, які можуть вплинути на перевірку, включають (але не обмежуються) [7]:

зміни тунелювання файлової системи;

поведінка або оновлення часу останнього доступу до файлів і папок;

видалення файлів, які користувач автоматично видаляє, минаючи кошик;

зміни аварійного дампу системи, функції попереднього вибору та поведінки точки відновлення;

очищення файлу підкачки під час вимкнення системи;

увімкнення або вимкнення аудиту журналу подій;

увімкнення або вимкнення брандмауера Windows;

переспрямування веб-браузеру Internet Explorer на певну початкову сторінку або проксі-сервер;

автоматичний запуск програм без будь-яких вказівок від користувача, крім завантаження системи та входу.

Усі ці параметри реєстру можуть суттєво вплинути на напрямок розслідування. У ряді випадків у файлі сторінки є цінні дані (наприклад, відповіді на запити веб-сервера), яких там не було б, якби файл підкачки було очищено під час вимкнення. При перевірці системи Windows, може бути дуже важливо визначити, чи очистив користувач кошик, чи систему було налаштовано на видалення. файли автоматично в обхід кошика. Використання попередньої вибірки програм, яка ввімкнена за замовчуванням у версіях Windows для робочих

станцій (але не на серверних версіях, таких як Windows 2008 R2), може надати цінні підказки під час вторгнення та виявлення шкідливих програм.

Це лише кілька прикладів. Існує ряд інших ключів і значень реєстру, які можуть мати значний вплив (можливо, навіть згубно) на те, що бачить аналітик під час аналізу диска та файлової системи. Деякі з цих значень фактично не існують у реєстрі за замовчуванням і їх потрібно додати, щоб вплинути на систему. Принаймні, розуміння цих параметрів і того, як вони впливають на загальну систему, може додати контекст до того, що аналітик спостерігає в інших областях свого дослідження.

Реєстр Windows містить ряд значень, які суттєво впливають на поведінку системи. Наприклад, аналітик може отримати зображення для аналізу і визначити, що каталог попередньої вибірки не містить файлів попередньої вибірки (*.pf). Значення реєстру, що представляють інтерес у такому випадку, включатимуть ті, які ідентифікують операційну систему та версію; за замовчуванням Windows XP, Vista і Windows 7 виконуватимуть попередню вибірку програми (і створюють файли *.pf); однак Windows 2003 не виконує попередню вибірку програми (хоча її можна налаштувати на це) за замовчуванням [7].

Коли зловмисне програмне забезпечення заражає систему, воно зазвичай потрапляє в систему за допомогою певних засобів, наприклад, зараження браузером «проїздом», через спільну мережу, USB-накопичувач або вкладення електронної пошти.

Коли зловмисник отримує доступ до системи, виникає певний артефакт, такий як мережеве з’єднання або діяльність у цільовій системі. При цьому цільова система міститиме деяку інформацію про систему, з якої походить зловмисник. Частина цієї інформації може бути надзвичайно мінливою, що означає, що вона залишається видимою для операційної системи (а отже, і для аналітика) лише протягом короткого періоду часу. Однак залишки цього артефакту можуть зберігатися протягом значної кількості часу. Будь-яка взаємодія з системою Windows, зокрема через графічний інтерфейс, залишає сліди.

Коли користувач, навіть зловмисник, який отримав доступ до системи,

взаємодіє з системою, і особливо з інтерфейсом користувача Windows Explorer (він же «оболонка»), створюються деякі досить стійкі артефакти. Якщо зловмисник увійшов у систему та підключив USB-накопичувач, відбувається обмін інформацією, і деякі з цих артефактів зберігаються в реєстрі (те саме стосується підключення до пристроїв через Bluetooth).

Якщо зловмисник потім запускає програми, будуть створені додаткові артефакти. Коли користувач підключає свою систему до точки безпроводового доступу (WAP), інформація про WAP зберігається в системі.

Коли зловмисне програмне забезпечення заражає систему, створюється кілька файлів (і, можливо, ключів/значень реєстру), і можуть також деякі мережеві з'єднання, оскільки зловмисне програмне забезпечення зв'язується поза системою. Коли зловмисник отримує доступ до системи через віддалений робочий стіл завдяки легко вгадуваному паролю, може бути створено кілька записів журналу подій, деякі ключі реєстру створені або змінені, і залежно від дій, які вони виконують, можливо, деякі файли створені, змінені або видалені в цій системі.

Багато вторгнень залишаються непоміченими протягом тривалого періоду часу, оскільки зловмисник буде використовувати дуже прості методи, щоб максимально звести до мінімуму артефакти, залишені в системі.

Реєстр Windows є центральною ієрархічною базою даних, що використовується в Windows 98, Windows CE, Windows NT і Windows 2000, що використовується для зберігання інформації, необхідної для налаштування системи для одного або кількох користувачів, програм і апаратних пристроїв [8].

Реєстр містить інформацію, на яку Windows постійно посилається під час роботи, таку як профілі для кожного користувача, програми, встановлені на комп’ютері, і типи документів, які кожен може створювати, параметри таблиць властивостей для папок і піктограм програм, яке обладнання існує в системі, і порти, які використовуються.

Реєстр замінює більшість текстових файлів .ini, які використовуються у файлах конфігурації Windows 3.x і MS-DOS, таких як Autoexec.bat і Config.sys.

Хоча реєстр є загальним для кількох операційних систем Windows, між ними є деякі відмінності. Гілка реєстру – це група ключів, підключів і значень у реєстрі, яка має набір допоміжних файлів, що містять резервні копії його даних.

Допоміжні файли для всіх гілок, крім HKEY_CURRENT_USER, знаходяться в %SystemRoot%\System32\Configпапці Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 і Windows Vista. Допоміжні файли для HKEY_CURRENT_USER знаходяться в%SystemRoot%\Profiles\Usernameпапку. Розширення імен файлів у цих папках вказують на тип даних, які вони містять. Крім того, відсутність розширення іноді може вказувати на тип даних, які вони містять.

Registry hive	Supporting files
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Рис. 2.1. Гілки реєстру та допоміжні файли [8]

Реєстр Windows містить велику кількість інформації, яка може забезпечити значний контекст для широкого кола досліджень. Якщо користувач отримує доступ до файлу або встановлює та запускає програму, ознаки цих дій (та інших) залишаться довго після видалення файлу або програми і більше не доступні. Це пов’язано з тим, що велика частина «відстеження», яке відбувається в системах Windows, є функцією операційної системи, середовища або екосистеми, в якій функціонує програма або користувач.

Папка / попередньо визначений ключ	Опис
HKEY_CURRENT_USER	Містить корінь інформації про конфігурацію користувача, який наразі ввійшов у систему. Тут зберігаються папки користувача, кольори екрана та налаштування панелі керування. Ця інформація пов'язана з профілем користувача. Цей ключ іноді скорочується як *HKCU* .
HKEY_USERS	Містить усі активно завантажені профілі користувачів на комп'ютері. HKEY_CURRENT_USER є підключом HKEY_USERS. HKEY_USERS іноді скорочується як *HKU* .
HKEY_LOCAL_MACHINE	Містить інформацію про конфігурацію комп'ютера (для будь-якого користувача). Цей ключ іноді скорочується як *HKLM* .
HKEY_CLASSES_ROOT	Є підключом `HKEY_LOCAL_MACHINE\Software`. Інформація, що зберігається тут, гарантує, що правильна програма відкривається, коли ви відкриваєте файл за допомогою Провідника Windows. Цей ключ іноді скорочується як *HKCR* . Починаючи з Windows 2000, ця інформація зберігається під ключами HKEY_LOCAL_MACHINE і HKEY_CURRENT_USER. Ключ `HKEY_LOCAL_MACHINE\Software\Classes` містить налаштування за замовчуванням, які можуть застосовуватися до всіх користувачів на локальному комп'ютері. The `HKEY_CURRENT_USER\Software\Classes` ключ містить налаштування, які замінюють налаштування за замовчуванням і застосовуються лише до інтерактивного користувача. Ключ HKEY_CLASSES_ROOT забезпечує перегляд реєстру, який об'єднує інформацію з цих двох джерел. HKEY_CLASSES_ROOT також забезпечує це об'єднане представлення для програм, розроблених для попередніх версій Windows. Щоб змінити налаштування інтерактивного користувача, зміни потрібно внести під HKEY_CLASSES_ROOT, `HKEY_CURRENT_USER\Software\Classes` а не під HKEY_CLASSES_ROOT. Щоб змінити налаштування за замовчуванням, зміни необхідно внести в розділі `HKEY_LOCAL_MACHINE\Software\Classes`. Якщо ви пишете ключі до ключа під HKEY_CLASSES_ROOT, система зберігає інформацію під `HKEY_LOCAL_MACHINE\Software\Classes`. Якщо ви запишете значення в ключ під HKEY_CLASSES_ROOT, а ключ уже існує під `HKEY_CURRENT_USER\Software\Classes`, система збереже інформацію там, а не під `HKEY_LOCAL_MACHINE\Software\Classes`.
HKEY_CURRENT_CONFIG	Містить інформацію про профіль обладнання, який використовується локальним комп'ютером під час запуску системи.

Рис. 2.2. Попередньо визначені ключі, які використовуються системою [8]

Таким чином, велика частина цієї діяльності відбувається без чіткого відома користувача чи програми – це просто відбувається. Розуміння цього, а також розуміння його обмежень може відкрити для аналітика нові перспективи щодо даних.

2.2. Призначення та можливості засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу реєстру

Американська компанія TZWorks спеціалізується на розробці технологій комп'ютерної криміналістики/моніторингу. Вона надає передові інструменти, які

(а) спрощують процес розслідування, (б) надають нові автоматизовані можливості там, де були доступні тільки ручні методи, або (в) реконструюють новий аспект операційної системи, щоб надати нові можливості аналізу артефактів, де їх не було.

Yet Another Registry Utility (yaru) – це незалежний від платформи засіб перегляду реєстру Windows. Задля ознайомлення з метаданими реєстру Windows, щоб краще криміналістично проаналізувати гілки реєстру, yaru було розроблено з урахуванням портативної та розширюваної архітектури, щоб її можна було зібрати для роботи в різних операційних системах. Механізм аналізу реєстру написаний на стандартному C/C++ і не має залежностей від функцій API реєстру Windows. Це означає, що синтаксичний аналіз може мати проблеми з певними неперевіреними граничними умовами [9].

Частина графічного інтерфейсу yaru використовує бібліотеку FOX (Free Objects for X), яку було розроблено як кросплатформна. Бібліотека FOX є у вільному доступі та поширюється у вихідній формі під публічною ліцензією бібліотеки GNU (LGPL). Наразі існують скомпільовані версії yaru, які працюватимуть на Windows, Linux та OS-X.

Версія yaru для Windows має можливість зробити знімок будь-якої з активних гілок реєстру і вивчити внутрішню структуру гілки реєстру. Оскільки операційна система Windows блокує активні гілки реєстру від інших процесів, які їх читають, yaru може вдатися до необроблених читань з диска NTFS, щоб прочитати будь-який із бажаних гілок реєстру. Отже, це вимагає від користувача запуску цього інструмента з правами адміністратора. Хоча цей підхід додає складності yaru, він гарантує, що всі метадані будуть доступні для аналізу, а також гарантує, що під час аналізу активна гілка реєстру не буде пошкоджено або не зміниться [9].

Деякі інші елементарні функції включають [9]:

показ виділеного (але невикористаного) простору даних значень ключа (тут згадується простір кластера);

показ нерозподіленого простору гілки реєстру (тут згадується як простір

гілки);

можливість переміщення простору гілки реєстру та перерахування видалених ключів;

можливість створення звітів. Для звичайних артефактів криміналістичної експертизи реєстру доступний ряд параметрів для створення звітів із активних гілок, копій гілок або гілок із немонтованих файлів розділів. Для останнього необхідна побітна (нестиснена) копія зображення розділу;

додаткова можливість ведення журналу, який записує вибір користувача разом із значеннями даних в окремий файл XML для подальшого перегляду. Для кожного сеансу створюється окремий файл XML;

можливість експортувати будь-який ключ у гілці, який оцінюється, у реєстраційний файл (.reg), який буде використовуватися для аналізу. Формат намагається імітувати версію 5.00 редактора реєстру Windows з деякими додатковими метаданими у формі коментарів;

можливість обробки будь-якої гілки реєстру за допомогою шаблонів, визначених користувачем. Ці шаблони дозволяють налаштувати, які дані потрібно витягти. Хоча ці шаблони мають дуже примітивний набір команд, вони можуть бути корисними для повторюваних завдань;

можливість простого пошуку: (а) назви ключів, (б) назви значень, (в) діапазони дат і (г) рядків (більше 4 символів);

можливість перевірити, чи всі виділені фрагменти мають дійсні посилання на реєстр.

Говорячи про артефакти криміналістичної експертизи в реєстрі Windows, слід обговорити архітектуру реєстру. Відповідно до набору ресурсів сервера Windows 2000, реєстр «є ієрархічною базою даних, яка містить значення змінних у Windows… а також у програмах та службах, які працюють у Windows… Реєстр складається з вкладених контейнерів, відомих як піддерева, ключі і підключі. Це як папки. Дані… зберігаються в записах реєстру, найнижчому елементі реєстру. Записи схожі на файли... Запис складається з імені, типу даних, який визначає довжину та формат даних, які запис може зберігати, і поля, відомого як значення

запису реєстру» [9].

На жаль, внутрішні елементи реєстру Windows є власністю Microsoft. Тому знайти документ з відкритим вихідним кодом, який точно документує внутрішні елементи без помилок, важко, і будь-які відкриті дані, швидше за все, отримані з емпіричних результатів перегляду шістнадцятирозрядних дампів необроблених гілок реєстру. Перша спроба задокументувати внутрішні елементи реєстру була з документа, написаного багато років тому (близько 1998 року), який був поширений в Інтернеті від автора, ідентифікованого лише ініціалами «BD». На рисунку наведено знімок екрана використаної діаграми в документі BD. Хоча рисунок мав назву «Дуже спрощена структура реєстру NT», виявляється, він точно показує основні компоненти ключ/значення/дані та їх взаємозв'язки. Поряд зі схемою містяться деякі визначення структур для кожного з блоків [9].

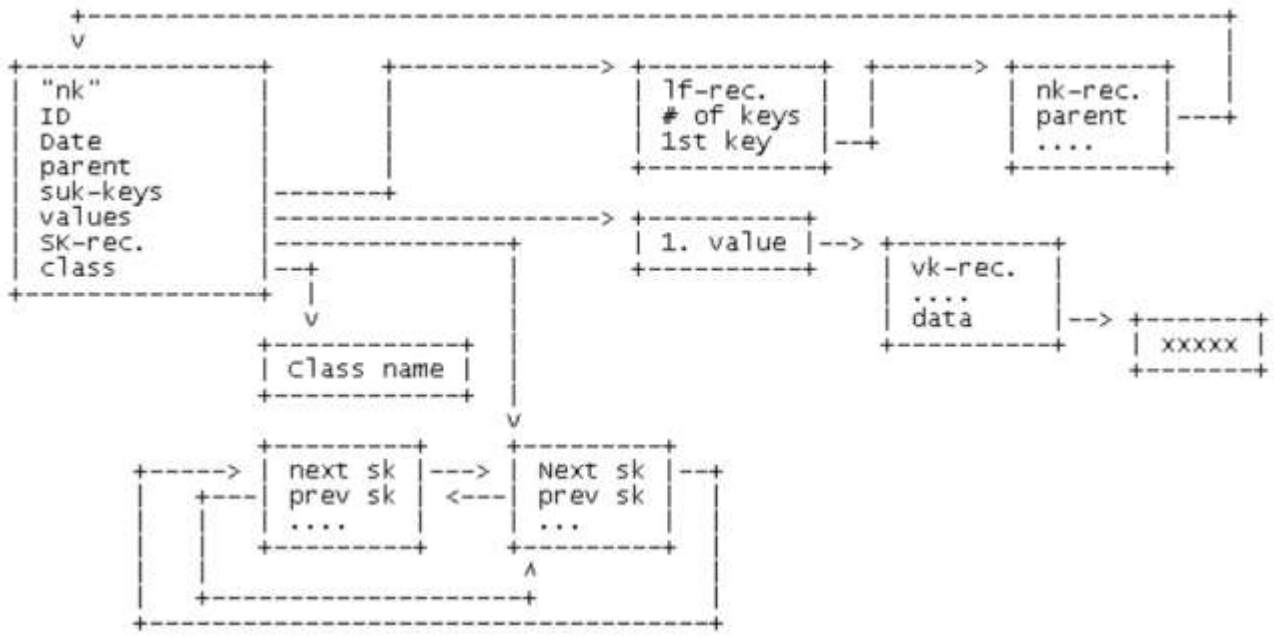


Рис. 2.3. «Дуже спрощена структура реєстру NT» [9]

На діаграмі BD структури імен ключів реєстру називають «nk», а структури значень ключа – «vk». Ключ безпеки, пов'язаний з кожним розділом реєстру, відображається як «sk». Ця номенклатура була заснована на відповідній сигнатурі кожної структури під час перегляду двійкового дампу кожного типу (наприклад, «nk», «vk», «sk»). Взявши результати з усіх відкритих джерел і озброївшись

шістнадцятковим редактором, можна використовувати структури, задокументовані до цього моменту, щоб вручну обстежити весь реєстр з достатньою точністю [9].

Гілки реєстру знаходяться в різних місцях, залежно від того, пов’язані вони з системою чи обліковими записами користувача.

Hive	Location
Ntuser.dat	%userprofile%\ntuser.dat
UsrClass.dat	(xp) %userprofile%\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat (vista and later) %userprofile%\AppData\Local\Microsoft\Windows\UsrClass.dat
System	%systemroot%\system32\config\system
Sam	%systemroot%\system32\config\sam
Software	%systemroot%\system32\config\software
Security	%systemroot%\system32\config\Security
Components	(vista and later) %systemroot%\system32\config\Components
BCD	(vista and later) %systemdrive%\boot\bcd
Syscache.hive	(vista and later) System Volume Information\ Syscache.hive
Schema.dat	%systemroot%\System32\SMI\Store\Machine\schema.dat
AmCache.hve	(win 8 and later) %systemroot%\AppCompat\Programs\AmCache.hve
ELAM	(win8 and later) %systemroot%\system32\config\elam
BBI	(win8 and later) %systemroot%\system32\config\bbi
DRIVERS	(win8 and later) %systemroot%\system32\config\drivers

Рис. 2.4. Розташування гілок реєстру [9]

2.3. Використання даних журналу подій ОС Windows під час розслідування інцидентів

Журнали подій ОС Windows – це спеціальні файли, в яких система та програми записують значущі для вашого комп'ютера події, такі як події входу користувачів до системи або помилки, що виникають під час роботи програм. Коли виникають такі типи подій, Windows створює записи в журналах подій. У детальних описах подій користувачі можуть знайти інформацію, корисну для усунення несправностей, виявлення причин проблем із системою, програмами, обладнанням комп'ютера [10].

Журнали подій Windows це не текстові файли (не як UNIX syslog) і їх не можна переглядати та досліджувати простими текстовими редакторами. Журнали подій Windows – це бінарні файли спеціального формату, схожі на файли баз

даних, що складаються зі спеціальних записів – подій Windows.

Microsoft Windows запускає спеціальну службу (сервіс) Журнал подій Windows для обслуговування завдань, пов'язаних з журналами подій – управління журналами подій, записом нових подій у журнали, обслуговуванням запитів на читання даних із журналів тощо. Служба Журнал подій Windows надає спеціальне API, яке дозволяє програмам працювати з журналами подій.

Реєстрація подій як стандартний системний механізм забезпечення безпеки та стійкості до відмови з'явилася у версії Microsoft Windows NT 3.1 в 1993 році. Починаючи з цієї версії в будь-якій Windows присутні 3 основні журнали - журнал Програми, журнал Система та журнал Безпека. У сучасних версіях Windows та Windows Server кількість журналів може перевищувати сотню, оскільки тепер і програми можуть створювати власні журнали, інтегровані в систему реєстрації подій Windows [10].

Переглядати та досліджувати події Windows можна стандартною програмою *Перегляд подій* або спеціальними програмами, що постачаються незалежними розробниками.

Служба (сервіс) "Журнал подій Windows" – це спеціальна служба (сервіс) для керування подіями та журналами подій. Вона підтримує виконання операцій запису нових подій, читання подій додатками, передплати подій, резервного копіювання та архівування журналів подій тощо. За замовчуванням, після інсталяції Windows служба "Журнал подій Windows" увімкнена та запускається автоматично. Не варто зупиняти або вимкнути цю службу. Зупинка служби журналу подій Windows може погіршити стабільність та безпеку системи.

Журнали подій Windows зберігаються у спеціальних файлах із системним каталогом Windows. Служба (сервіс) Журнал подій Windows дозволяє користувачам зберігати журнали та робити резервні копії журналів у файли. Windows NT, 2000 та XP/Server 2003 зберігають журнали подій у файлах EVT формату. Windows Vista/Server 2008 та новіші системи зберігають журнали подій в EVTX форматі. *Аналіз файлів журналів подій та їх резервна копія є основою розслідування різних інцидентів*.

Робочі версії файлів журналів подій Windows зазвичай заблоковані системою, точніше службою "Журнал подій Windows" і їх неможливо відкрити безпосередньо на живій, працюючій системі. Але якщо комп'ютер буде завантажений іншою системою з іншого диска, робочі файли журналів системи можна відкрити або скопіювати. Також їх можна скопіювати або відкрити, якщо підключити системний диск до іншого комп'ютера. За промовчанням файли журналів подій Windows Vista/Server 2008 зберігаються в каталозі "C:\Windows\System32\winevt\Logs\" [10].

Відкрити файл журналу подій у програмі Перегляд подій Windows можна за допомогою таких дій:

Запустіть програму Перегляд подій.

Натисніть "Відкрити збережений журнал" на панелі "Дії", розташованій у правій частині вікна.

Знайдіть і виберіть потрібний файл у списку файлів, натисніть кнопку "Відкрити" і його вміст відобразиться в області перегляду подій у програмі.

Журнал подій Програми містить події, створені програмами, а не системою. Наприклад, сервер бази даних може записувати помилки, що виникають під час його роботи в журналі програм. Розробники програм самі вирішують, які події має сенс протоколювати в журналі подій Програми. Наприклад, Microsoft SQL Server протоколює докладну інформацію про важливі аварійні ситуації, що виникають при роботі SQL-сервера, таких як "недостатньо пам'яті", "збій при резервному копію" При цьому події, згенеровані різними додатками, потрапляють у єдиний журнал додатків. Програми ідентифікуються як різні "джерела" в базовій властивості подій. Тому нескладно виділити події конкретного додатка. Також варто враховувати що ID події (код події) також визначається додатком, що згенерував подію та коди можуть дублюватися для різних джерел.

Журнал подій Система містить події, створені системними компонентами. Наприклад, відмови драйверів або інших системних компонентів під час запуску системи записуються в журнал журналу подій. Типи та коди подій системних компонентів визначені розробниками операційної системи Windows. Аналогічно

журналу додатків, системний журнал містить події з різних джерел (системних компонентів) і слід враховувати, що конкретні події ідентифікуються не тільки кодом, але джерелом. *Журнал подій Система – важливе джерело інформації при пошуку причин відмов та проблем системними адміністраторами та технічними фахівцями.*

Журнал подій Безпека містить події, що впливають на безпеку системи. Це спроби (і вдалі та невдалі) входу в акаунти системи, використання ресурсів (файлів, реєстру, пристроїв), управління обліковими записами, зміни прав та привілеїв акаунтів, запуск та зупинення процесів (програм) тощо. Адміністратор може конфігурувати, які категорії подій необхідно реєструвати. Наприклад, за замовчуванням система налаштована реєструвати події керування обліковими записами, події входу в систему, а аудит доступу до об'єктів не увімкнено. Варто бути обережним при настроюванні аудиту доступу до файлів, це може призвести до появи великої кількості подій, що в свою чергу може негативно позначитися на загальній продуктивності системи та швидкому переповненню журналу безпеки.

Запис до журналу безпеки виконується лише системними компонентами, коди подій однозначно ідентифікують події. *Журнал подій Безпека є важливим джерелом інформації при розслідуванні інцидентів порушення безпеки та його аналіз актуальний для адміністраторів безпеки, спеціалістів з інформаційної безпеки та фахівців з цифрової криміналістичної експертизи.*

Розглянемо аудит безпеки у ОС Windows.

Аудит безпеки ОС Windows – це технічні засоби та заходи, спрямовані на реєстрацію та систематичний регулярний аналіз подій, що впливають на безпеку інформаційних систем підприємства. Технічно, аудит безпеки в ОС Windows реалізується через налаштування політик аудиту та налаштування аудиту об'єктів [11].

Політика аудиту визначає, які події та для яких об'єктів будуть генеруватися в журнал подій Безпека. Регулярний аналіз даних журналу безпеки відноситься до організаційних заходів, для підтримки яких може застосовуватись різне програмне забезпечення. У найпростішому випадку можна використовувати

програму Перегляд подій. Для автоматизації завдань аналізу подій безпеки можуть застосовуватися більш просунуті програми та системи управління подіями безпеки (SIEM), що забезпечують постійний контроль журналів безпеки, виявлення нових подій, їх класифікацію, оповіщення фахівців при виявленні критичних подій.

Як встановити та настроїти аудит безпеки у Windows? Аудит безпеки Windows включається через Групову політику (Group Policy) у Active Directory або локальну політику безпеки. Щоб настроїти аудит на окремому комп'ютері, без Active Directory, виконайте такі дії [11]:

Відкрийте Панель керування Windows, виберіть пункт Адміністрація, а потім запустіть Локальна політика безпеки (Local Security Policy).

Відкрийте гілку Локальні політики та виберіть Політика Аудиту.

У правій панелі вікна Локальна політика безпеки (Local Security Policy) ви побачите список політик аудиту. Подвійним кліком на політиці, що вас цікавить, відкрийте параметри і встановіть прапорці Аудит успіхів або Аудит відмов (Success or Failure).

Так налаштовуються базові політики аудиту.

Починаючи з Windows 2008 R2/Windows 7, ви можете використовувати розширені політики (Advanced Security Audit Policy):

Local Security Policy -> Advanced Audit Policy Configuration -> System Audit Policies.

Аудит безпеки Windows дозволяє контролювати події входу в систему та виявляти невдалі спроби входу. Система Windows генерує такі події не тільки під час безпосередньої спроби входу в систему, але й при віддаленому доступі з іншого комп'ютера до ресурсів із загальним доступом. *Аудит подій входу допомагає виявляти підозрілу активність або потенційні атаки при адмініструванні та розслідуванні інцидентів.*

Для окремого комп'ютера (без Active Directory) аудит подій входу налаштовується так [11]:

Відкрийте гілку Локальні політики (Local Policies) у Локальна політика

безпеки (Local Security Policy)

Виберіть Audit Policy.

Подвійним кліком відкрийте Аудит подій входу (Audit logon events) та увімкніть опції аудиту успіхів та відмов (Success та Failure).

Після цього всі спроби входу - успішні та невдалі протоколюватимуться в журнал подій.

Список кодів важливих подій входу до системи:

4624 Вхід з обліковим записом успішно виконано;

4625 Не вдалося виконати вхід з обліковим записом;

4648 Спроба входу в систему за допомогою явних облікових даних;

4675 Ідентифікатори безпеки були відфільтровані.

Засоби Аудиту безпеки Windows дозволяють контролювати доступ до файлів, папок, ключів реєстру та інших об'єктів та інших системних об'єктів, у яких є SACL. Моніторинг доступу до файлів для файл-сервера може бути важливим завданням і засоби аудиту безпеки Windows допомагають адміністраторам у цьому. *Аудит доступу до файлів та реєстру дозволяє виявляти спроби несанкціонованого доступу до файлів та запобігати або відстежувати зміни конфігурацій системи та програм.*

2.4. Призначення та можливості засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу журналу подій

Розглянемо інструмент перегляду журналу подій Windows компанії TZWorks *Windows Event Log Viewer (evtx_view).*

evtx_view інструмент на основі графічного інтерфейсу, який може аналізувати журнали подій Windows з усіх версій Windows, починаючи з Windows XP. Це включає в себе Vista, Windows 7, Windows 8 і серверні частини.

Вихід представлений у вигляді дерева, де можна вибрати компоненти журналу подій і відобразити їх внутрішню структуру. Інструмент дозволяє створювати звіти для певних конкретних категорій журналу подій, таких як події

USB plug-n-play, зміни облікових даних, зміни пароля тощо. Якщо один із доступних звітів не відповідає потребам аналітика, є можливість налаштувати та створити звіт для використання та обробки.

Спочатку при введенні формату журналу подій Microsoft Vista, evtx_view був спробою реалізувати незалежний механізм аналізу Windows API. Повністю написаний на C++, механізм розбору evtx_view був перенесений на Windows, Linux і Mac OS-X [12].

Інструмент evtx_view використовує механізм аналізу журналу подій. evtx_view також використовує набір інструментів FOX. FOX – це набір інструментів на основі C++ для розробки програм із графічним інтерфейсом, які можуть легко працювати на різних платформах шляхом компіляції вихідного коду для відповідної ОС. FOX поширюється під ліцензією GNU Lesser General Public License (LGPL) з додатком до ліцензії FOX Library License [12].

Вихід представлений у вигляді дерева, де можна вибрати компоненти журналу подій і відобразити їх внутрішню структуру. Інструмент дозволяє створювати звіти для певних конкретних категорій журналу подій, таких як події USB plug-n-play, зміни облікових даних, зміни пароля тощо. Якщо один із доступних звітів не відповідає потребам аналітика, є можливість створити користувацький звіт, який буде використовуватися та оброблятися.

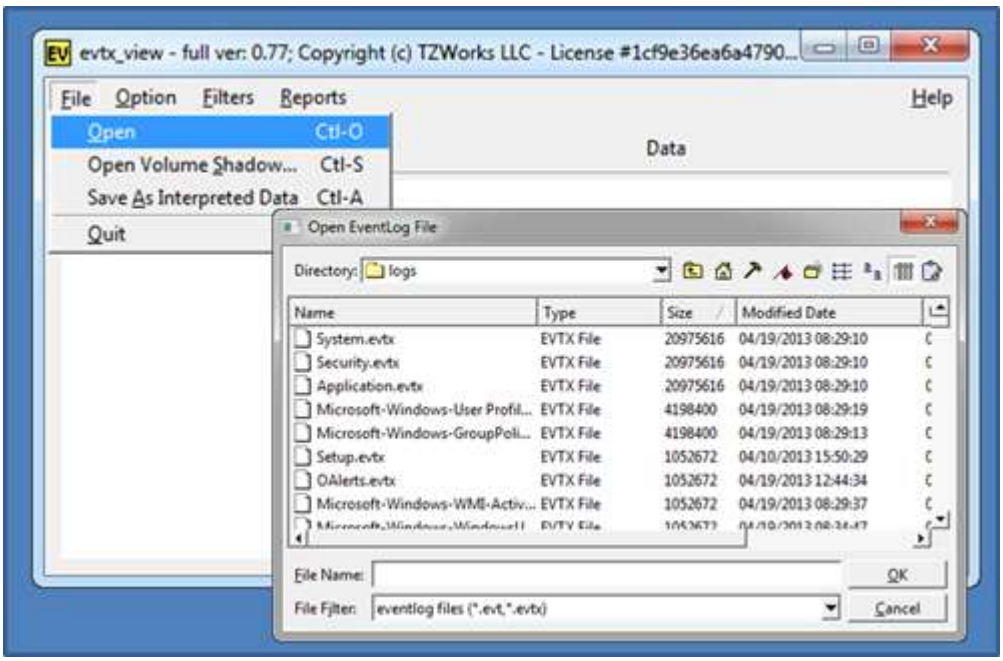


Рис. 2.5. Інтерфейс інструмента перегляду журналу подій Windows *evtx_view*

Журнали подій ОС Windows зберігаються в різних місцях залежно від того, чи знаходиться це на коробці Windows XP чи Windows 7 тощо. На додаток до відмінностей у розташуваннях, існують також (а) відмінності в іменах у самому файлі журналу подій і (б) значно більше журналів подій, починаючи з Vista та пізніших операційних систем. Наприклад, Windows 7 може мати понад 70 унікальних журналів подій проти трьох, наявних у Windows XP. Нижче наведено розташування журналів подій у різних операційних системах Windows [12].

Windows XP і раніше:

%windir%\system32\config\[AppEvent.Evt | SecEvent.Evt | SysEvent.Evt]

Windows Vista і новіші (Windows 7 і Windows 8, …)

%windir%\system32\winevt\logs\[Application.evtx | Security.evtx | System.evtx | ...].

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ АНАЛІЗУ РЕЄСТРУ ТА ЖУРНАЛУ ПОДІЙ

3.1. Порядок застосування засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу реєстру

Коли гілка реєстру завантажується в *yaru*, вона розбивається на 4 основні сегменти: (a) звичайні дані гілки, які можуть переглядати звичайні редактори реєстру, (b) нерозподілений простір у гілці, (c) будь-який виділений простір який повинен мати батьківський ключ, але його немає, і (d) будь-які видалені ключі та пов’язані з ними значення, які не були перезаписані [9].

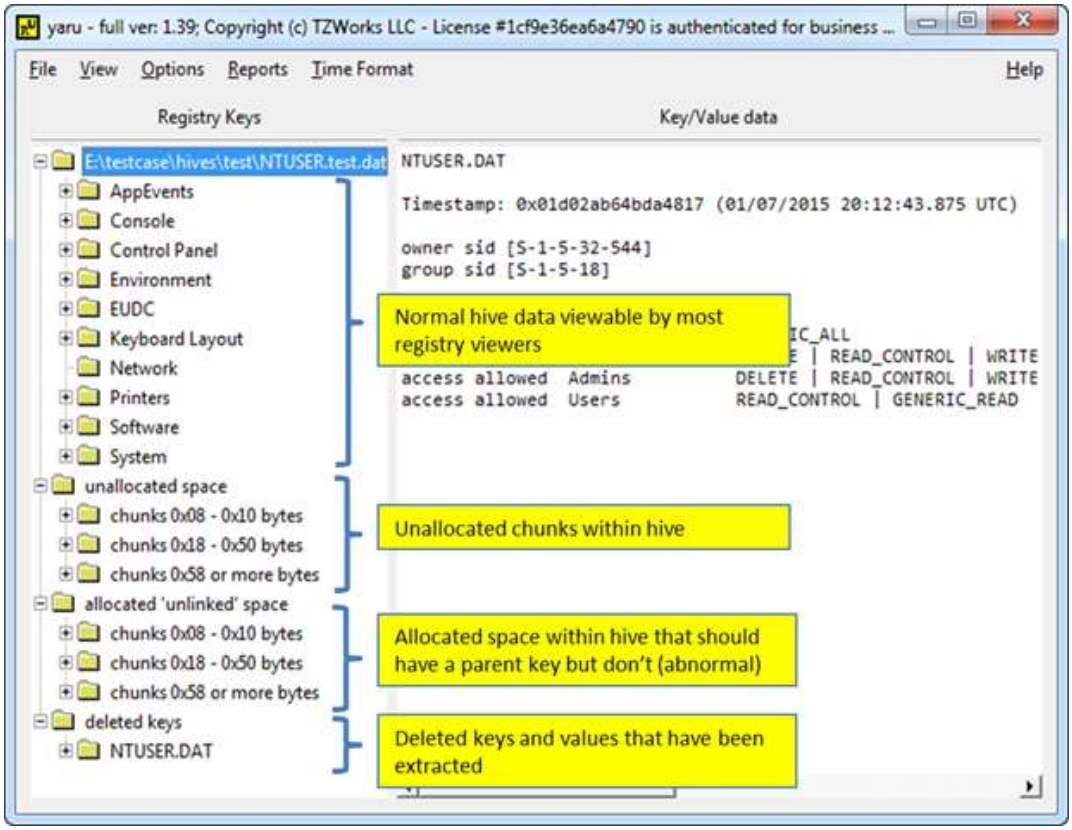


Рис. 3.1. Сегменти гілки реєстру в yaru

Під час обходу будь-якого з ключів або пов’язаних значень відображаються всі метадані без урахування дозволів користувача, який запускає *yaru*. Однак, залежно від ліцензії, деяка інформація може не відображатися.

Для відновлення видалених ключів/значень *yaru* робить усе можливе, щоб помістити видалені записи у відповідний контекст, де вони були в загальній ієрархії гілки реєстру. Іноді це неможливо, коли один із вузлів ієрархії був перезаписаний під час повторного використання простору. *yaru* чітко показує, коли він не може завершити весь шлях до батьківського кореневого ключа, згрупувавши ці записи в папці "unk_path", як показано нижче.

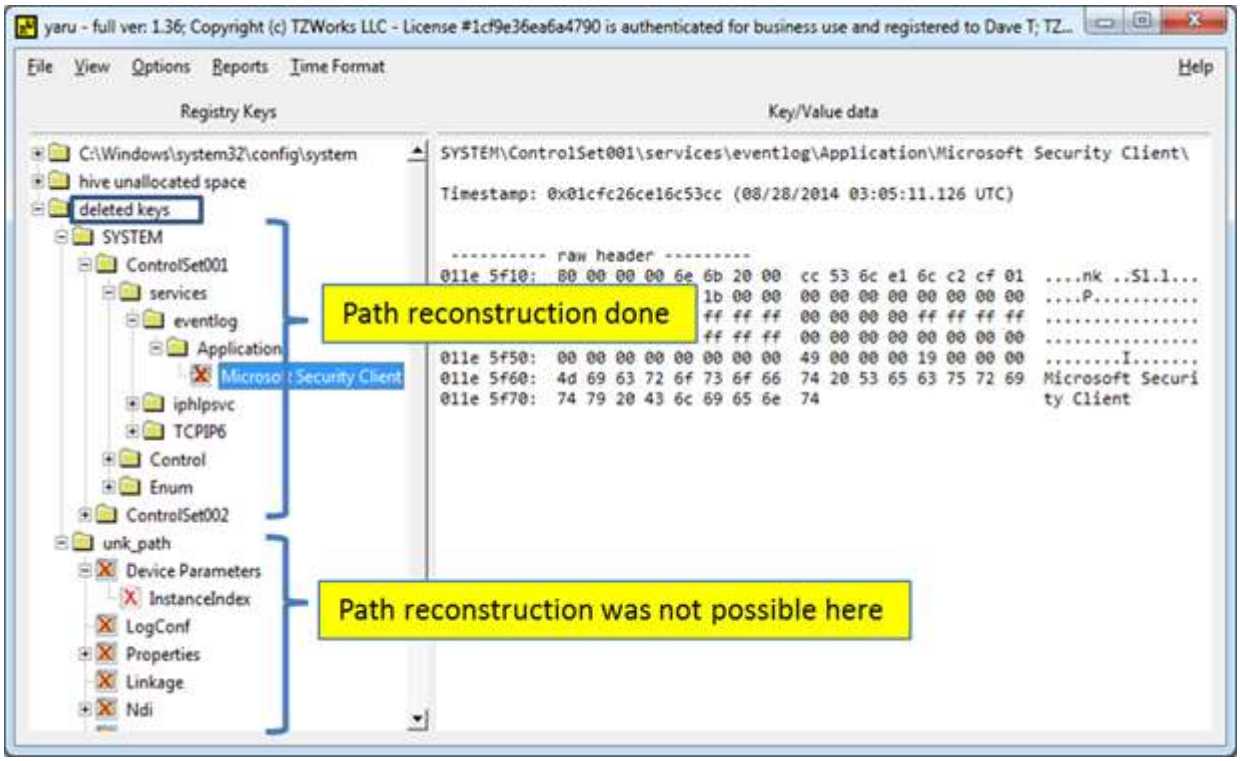


Рис. 3.2. Шлях до батьківського кореневого ключа реєстра

Можна експортувати будь-який із видалених ключів разом із пов’язаними з ними батьками, які не були видалені, але клацнути правою кнопкою миші на папці та вибрати один із параметрів «Експортувати ключі».

Експортовані ключі та значення відображаються у форматі редактора реєстру Windows версії 5.00. Якщо видалений ключ має батьківський ключ в ієрархії, який не видаляється, вони також відображаються. Нижче наведено фрагмент видаленого ключа та те, як виглядає результат.

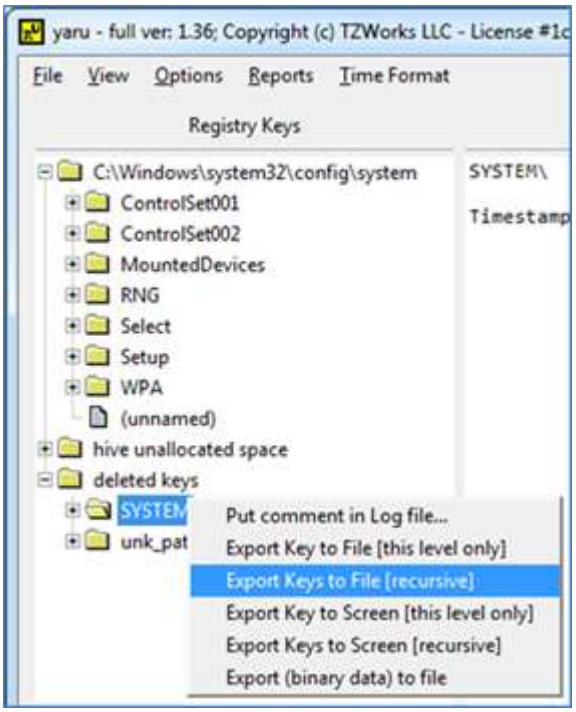


Рис. 3.3. Експорт видалених ключів

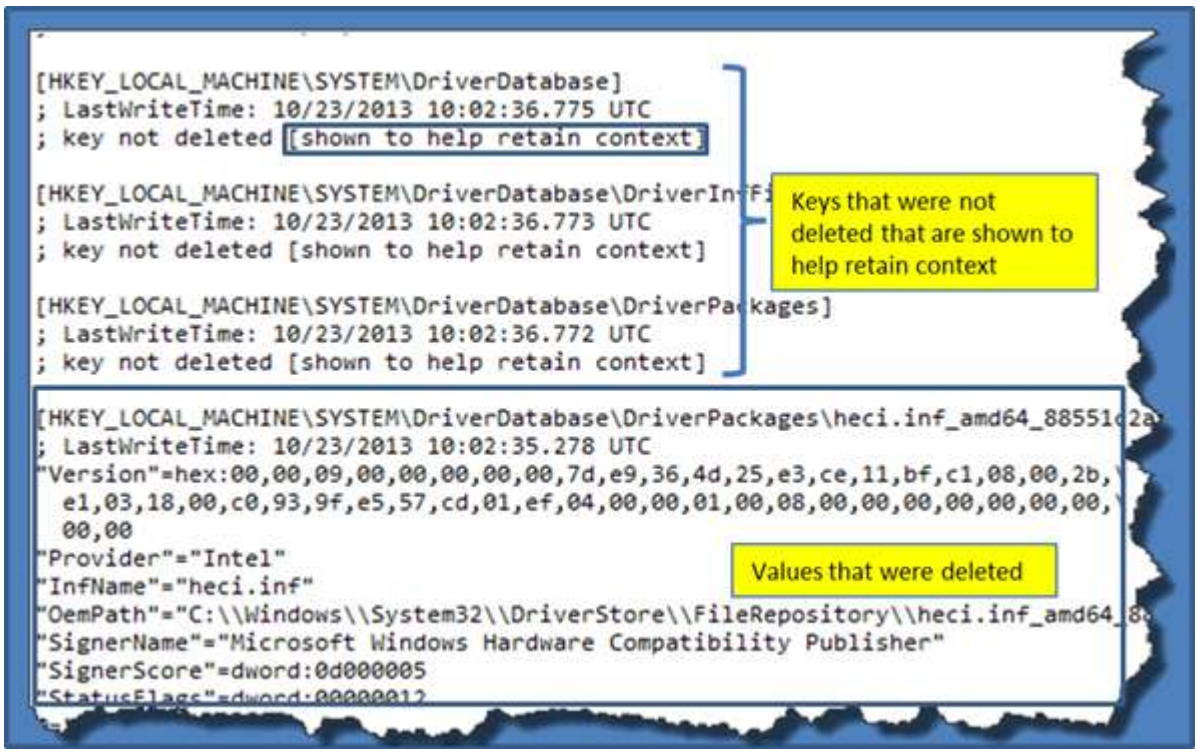


Рис. 3.4. Фрагмент видаленого ключа

Однією з найбільш корисних можливостей *yaru* є можливість генерувати звіти. Ці звіти можуть орієнтуватися на діючу системну гілку реєстра або гілку, яку було явно завантажено в yaru.

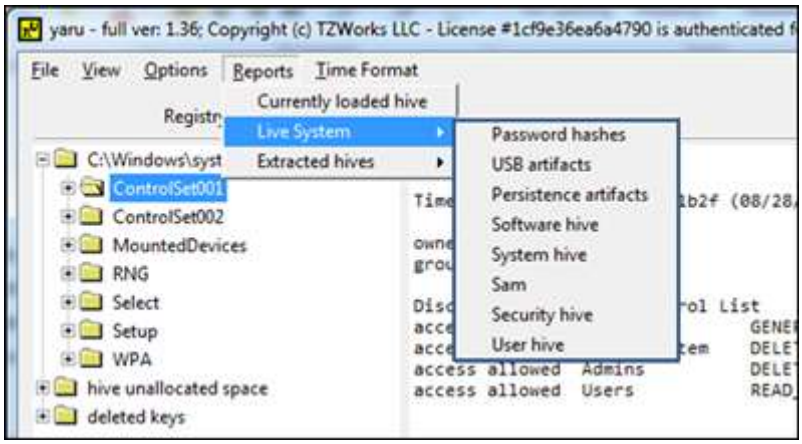


Рис. 3.5. Формування звіту

3.2. Порядок застосування засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу журналу подій

Після запуску *evtx_view* інструмент спробує встановити права адміністратора. Це дозволить йому отримати доступ до каталогу журналу подій Windows на хості.

Щоб проаналізувати журнал подій, потрібно просто перейти до потрібного журналу, і *evtx_view* спробує проаналізувати кожен запис у журналі. Оскільки *evtx_view* використовує FOX як механізм графічного інтерфейсу, головна панель графічного інтерфейсу та діалогові вікна відрізняються від звичайних операційних систем Windows. Хоча відмінності незначні, набір інструментів FOX дозволяє розробникам відносно легко переносити інструменти GUI з однієї операційної системи в іншу.

Після аналізу даних можна перейти до кожного запису або структури з панелі перегляду дерева. Залежно від того, який тип файлу журналу аналізується, ця частина графічного інтерфейсу розбивається на блоки записів для журналів Windows 7 або окремих записів подій для Windows XP. Нижче наведено знімок екрана того, як Windows XP відтворюється замість Windows 7 (рис. 3.6). Різниця у відображенні полягає в тому, як дві операційні системи внутрішньо структурують свій відповідний журнал подій. Windows XP – це лише послідовність записів, тоді як Windows 7 інкапсулює частину записів у так званий ElfChnk. *evtx_view* зберігає

це, відображаючи внутрішні елементи кожного журналу.

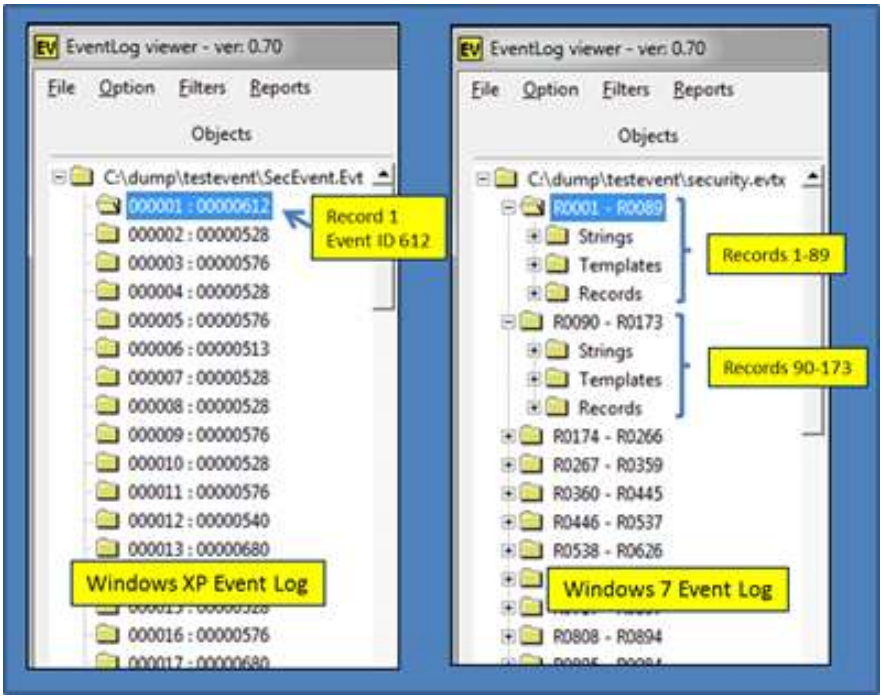


Рис. 3.6. Блоки записів для журналів Windows 7 або окремих записів подій для Windows XP

У перегляді дерева можна вибрати окремі записи для відображення, або у випадку Window 7 відобразити пов’язаний ElfChnk. Нижче наведено приклад перегляду вибраної Windows 7 ElfChnk. Як бачимо, відображаються всі внутрішні елементи структури, а також зміщення файлу. Це, зазвичай, не використовується аналітиком, він корисний для реверс-інженера.

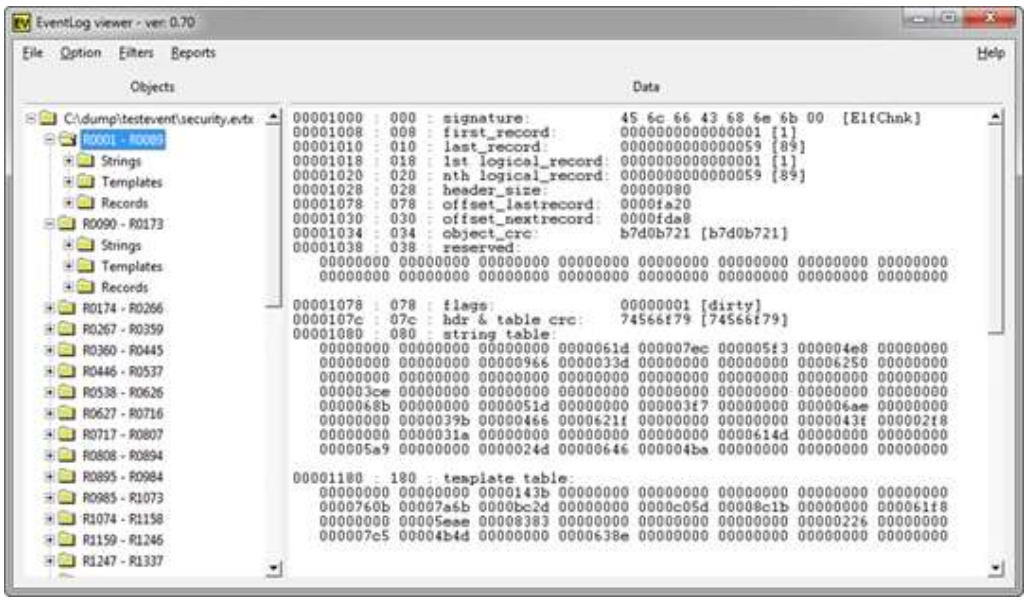


Рис. 3.7. Перегляду вибраної гілки ElfChnk Windows 7

Переходячи вниз до окремого запису, можна відобразити пов’язані дані для цього запису. На відміну від даних для Windows XP, для Windows 7 метадані журналу подій виражаються як двійковий XML. На знімку екрана нижче показано повторно згенеровані дані XML для запису Windows 7.

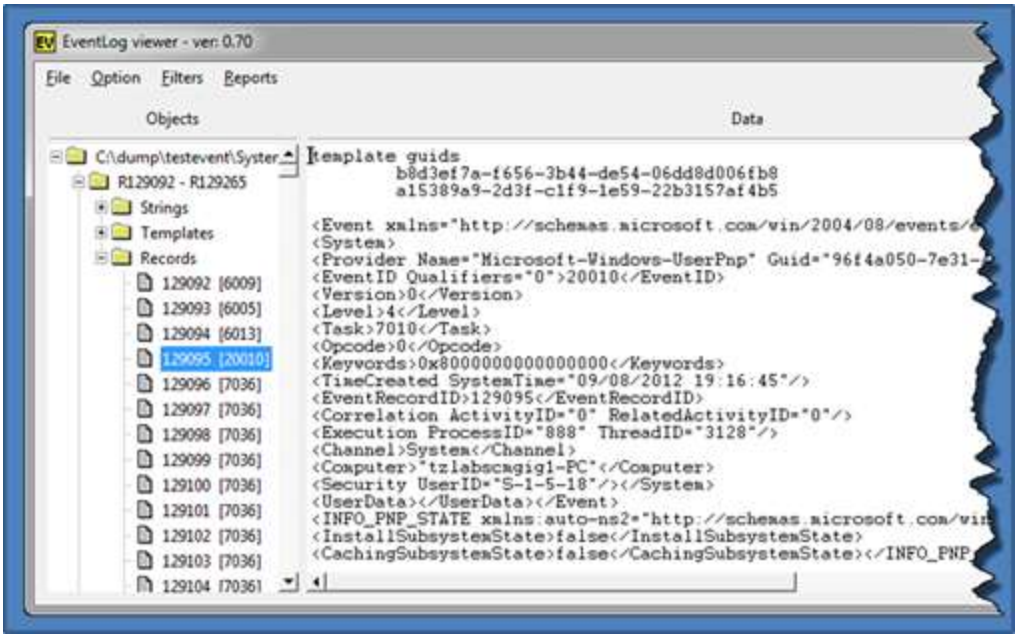


Рис. 3.8. Повторно згенеровані дані XML для запису Windows 7

Звіти про категорії подій. Хоча перегляд даних запису є корисним, витягування конкретних подій і направлення хронології подій у звіт зазвичай корисніше для аналітика. Для цього випадку використання *evtx_view* має кілька опцій для отримання конкретних подій на основі типу категорії. Різниця між «Завантаженим журналом» і «Діючим журналом» полягає в тому, що перший націлений на журнал подій, який завантажується в графічний інтерфейс, а другий – на відповідний журнал(и) подій на діючому хості.

Вилучення записів за допомогою фільтрів. Можна використовувати доступні фільтри, щоб знайти певні записи, що цікавлять. Наразі меню фільтра *evtx_view* має параметри для: (a) діапазону дат, (b) ідентифікатора(ів) події або (в) шаблону рядка. У наведеному нижче прикладі виконується пошук рядка «usb» у даних запису. Результат також показаний. Кожен тип запису "подібний" групується разом у вихідних даних, тому кожен конкретний заголовок ідентифікатора події може бути включено як частину групування.

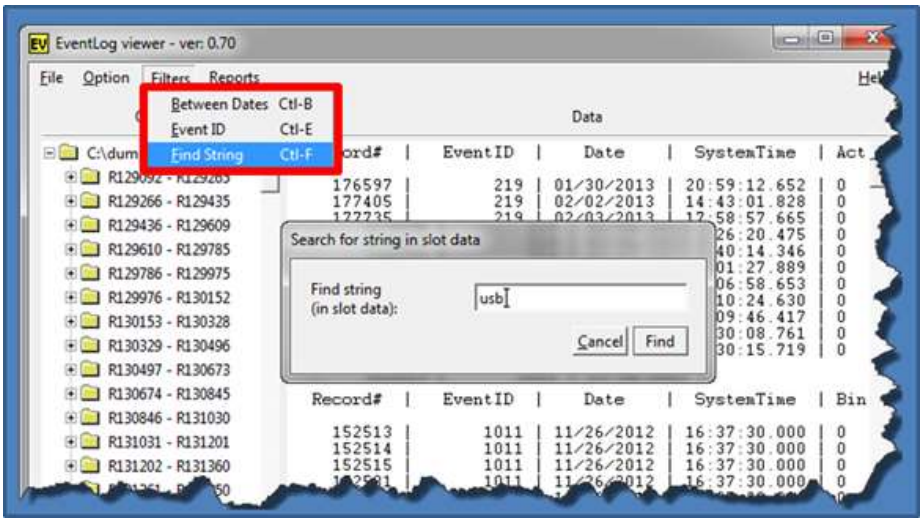


Рис. 3.9. Вилучення записів за допомогою фільтрів

Іноді необхідно перевіряти вихідні дані запису події, щоб перевірити правильність створених записів XML. Щоб переглянути вихідні дані, є два варіанти: (a) або переглянути запис із пов’язаними шістнадцятковими даними, або (b) переглянути запис із необробленими даними про слот (Vista та новіші). Нижче наведено скріншот останнього варіанту. У нижній частині правої панелі відображаються дані слота, пов’язані із записом.

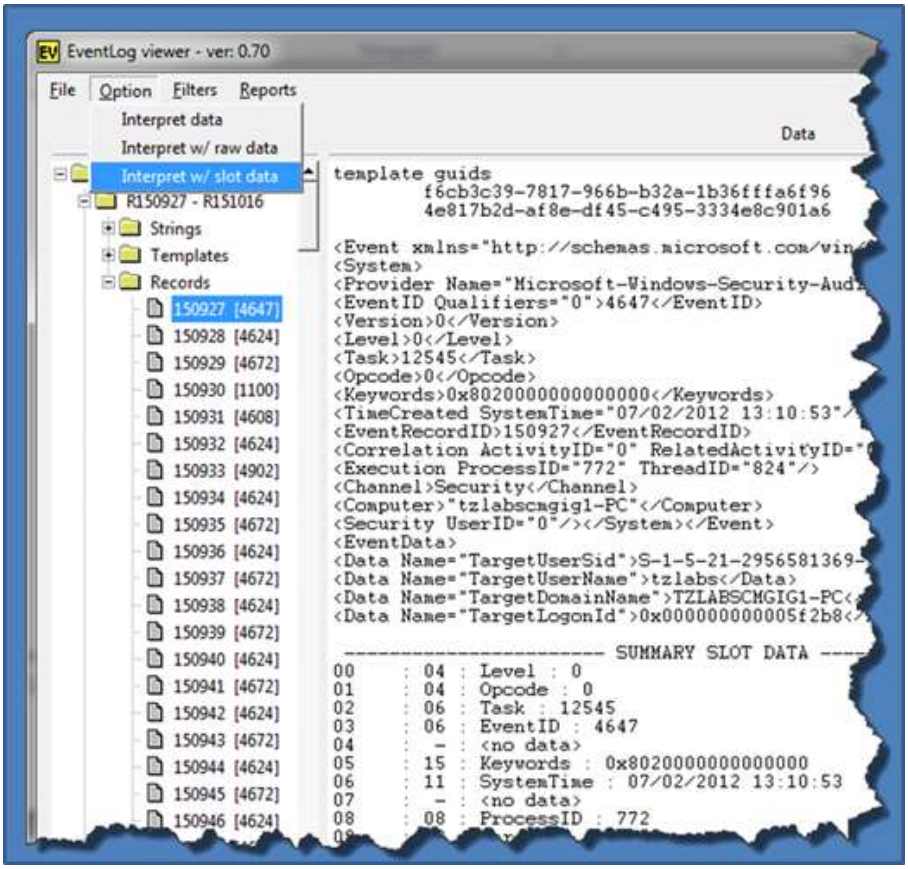


Рис. 3.10. Перевірка внутрішніх записів

3.3. Рекомендації щодо застосування методів та засобів розслідування інцидентів в інформаційній системі організації

Криміналістична експертиза має бути в центрі уваги будь-якої організації, яка серйозно ставиться до захисту своїх активів. Щоб мати найкращі можливості криміналістичної експертизи, існує кілька ключових рекомендацій, які забезпечать групу криміналістів необхідними інструментами [1]:

простота використання має першорядне значення. Час для доказів є ключовим показником і потребою для практиків-криміналістів. Складність заважає часу на докази, і, таким чином, практики – незалежно від того, наскільки вони просунуті – отримують переваги від інструментів, які прості у використанні та спрощують робочі процеси;

необхідно використовувати інструменти, сумісні з усіма технологіями. Підприємства мають різноманітні пристрої, операційні системи, бази коду та місця розташування. Розширюваність інструмента повинна відповідати широті джерел даних підприємства та розташування. Загрози надходять звідусіль, а також необхідна здатність проводити розслідування скрізь;

необхідно використовувати інструменти з можливістю збору з мережі. Гібридна робота залишиться. Технології підприємства та складність даних з часом будуть лише зростати. Фахівці-криміналісти повинні мати можливість збирати з кінцевих точок у мережі та поза межами мережі, щоб гарантувати, що вони можуть швидко та легко отримати доступ до потрібних цифрових доказів;

необхідно використовувати інструменти, які борються з втомою агентів і дозволяють приховані колекції. Неможливо переоцінити необхідність проведення таємних операцій при проведенні тих чи інших розслідувань. Організації розгортають занадто багато агентів і вичерпують системні ресурси. Дуже важливо обмежити вплив збору на суб’єктів безагентним підходом, щоб уникнути виявлення.

Організації повинні створювати та підтримувати процедури та інструкції для виконання завдань криміналістичної експертизи на основі політики

організації та всіх застосовних законів і нормативних актів [5].

Інструкції та процедури повинні сприяти послідовним, ефективним і точним діям, що особливо важливо для інцидентів, які можуть призвести до кримінального переслідування або внутрішніх дисциплінарних заходів.

Оскільки електронні журнали та інші записи можна змінювати або іншим чином маніпулювати, організації повинні бути готові, використовуючи свою політику, інструкції та процедури, продемонструвати цілісність таких записів. Інструкції та процедури слід періодично переглядати, а також коли в політику та процедури команди вносяться значні зміни [5].

Політика та процедури організацій повинні чітко пояснювати, які дії з розслідування інцидентів слід, а які не повинні виконуватися за різних обставин, а також описувати необхідні запобіжні заходи для конфіденційної інформації, яка може бути записана за допомогою криміналістичних інструментів, таких як паролі, особисті дані (наприклад, номери соціального страхування), а також вміст електронних листів.

Необхідна підтримка криміналістики в життєвому циклі інформаційної системи. Багато інцидентів можна обробляти ефективніше, якщо криміналістичні міркування були включені в життєвий цикл інформаційної системи. Нижче наведено приклади таких міркувань [5]:

регулярне резервне копіювання систем і підтримка попередніх резервних копій протягом певного періоду часу;

проведення аудиту на робочих станціях, серверах та мережевих пристроях;

пересилання записів аудиту на захищені централізовані сервери журналів;

налаштування критично важливих програм для виконання аудиту, включаючи запис усіх спроб автентифікації;

підтримка бази даних хешів файлів для файлів поширених операційних систем і програм, а також використання програмного забезпечення для перевірки цілісності файлів для особливо важливих активів;

ведення записів (наприклад, базових даних) про конфігурації мережі та системи;

встановлення політики збереження даних, яка підтримує виконання історичних оглядів системної та мережевої активності, виконання запитів або вимог щодо збереження даних, що стосуються поточних криміналістичних процесів і розслідувань, а також знищення даних, які більше не потрібні.

Більшість із цих міркувань є розширенням існуючих положень політики та процедур організації, тому вони зазвичай вказуються у відповідних окремих документах замість централізованої політики криміналістики.

Організації повинні мати можливість проводити комп'ютерну та мережеву експертизу. Групи з розгляду інцидентів повинні мати потужні криміналістичні можливості. Більш ніж один член команди повинен мати можливість виконувати кожну типову криміналістичну діяльність. Практичні вправи та навчальні курси з IT та криміналістичної експертизи можуть бути корисними для формування та підтримки навичок, а також демонстрації нових інструментів і технологій.

Тобто, криміналістична політика повинна чітко визначати ролі та відповідальність усіх людей, які виконують криміналістичну діяльність організації або допомагають їй. Політика повинна включати всі внутрішні та зовнішні сторони, які можуть бути залучені, і повинна чітко вказувати, хто з якими сторонами має контактувати за різних обставин.

Криміналістична експертиза необхідна для виконання різних завдань в організації, включаючи розслідування злочинів і неадекватної поведінки, відновлення інцидентів з комп'ютерною безпекою, усунення несправностей в роботі, підтримку належної перевірки для ведення записів аудиту та відновлення після випадкових пошкоджень системи. Без такої можливості організації буде важко визначити, які події відбулися в її системах і мережах, наприклад розкриття захищених, конфіденційних даних. Крім того, обробка доказів у судово обґрунтований спосіб ставить осіб, які приймають рішення, у положення, де вони можуть впевнено вживати необхідних дій.

Аналітики повинні мати набір криміналістичних інструментів для збору, дослідження та аналізу даних. Він повинен містити різноманітні інструменти, які забезпечують можливість збирати й досліджувати нестабільні та енергонезалежні

дані та виконувати швидкий огляд даних, а також поглиблений аналіз. Набір інструментів повинен дозволяти швидко й ефективно запускати його програми зі знімних носіїв або робочої станції криміналістичної експертизи.

Організації повинні забезпечити достатнє сховище для журналів, пов'язаних із мережевою активністю. Організації повинні оцінити типове та пікове використання журналів, визначити, скільки годин або днів потрібно зберігати дані на основі політик організації, і переконатися, що системи та програми мають достатній обсяг доступного місця. Журнали, пов'язані з інцидентами комп'ютерної безпеки, можливо, потрібно буде зберігати значно довше, ніж інші журнали.

Організації повинні проводити криміналістичну експертизу, використовуючи послідовний процес: чотири етапний процес криміналістичної експертизи з етапами збору, експертизи, аналізу та звітності. Точні деталі етапів можуть відрізнятися залежно від потреби в криміналістичній експертизі.

Організації повинні бути активними у зборі корисних даних. Налаштування аудиту в ОС, впровадження централізованого ведення журналів, виконання регулярного резервного копіювання системи та використання засобів контролю безпеки може створювати джерела даних для майбутніх криміналістичних заходів.

Аналітики повинні здійснювати збір даних, використовуючи стандартний процес. Рекомендовані кроки: визначення джерел даних, розробка плану отримання даних, отримання даних і перевірка цілісності даних. У плані слід визначати пріоритети джерел даних, встановлюючи порядок, у якому дані мають бути отримані, на основі ймовірної цінності даних, мінливості даних та кількості необхідних зусиль. Перед початком збору даних аналітик або керівництво має прийняти рішення щодо необхідності збирання та збереження доказів у спосіб, який підтверджує їх використання в майбутніх юридичних або внутрішніх дисциплінарних провадженнях. У таких ситуаціях слід дотримуватися чітко визначеного ланцюга опіки, щоб уникнути звинувачень у неправильному поводженні чи підробці доказів.

Аналітики повинні використовувати методичний підхід до вивчення даних. Основою криміналістики є використання методичного підходу до аналізу наявних даних, щоб аналітики могли або зробити відповідні висновки на основі наявних даних, або визначити, що висновки ще не можуть бути зроблені. Якщо можуть знадобитися докази для юридичних або внутрішніх дисциплінарних заходів, аналітики повинні ретельно задокументувати висновки та вжиті кроки.

Аналітики повинні об'єднувати дані з різних джерел. Аналітик повинен переглянути результати дослідження та аналізу окремих джерел даних, таких як файли даних, операційні системи та мережевий трафік, і визначити, як інформація поєднується разом, щоб виконати детальний аналіз подій, пов'язаних із застосуванням, та реконструкції подій.

Аналітики повинні досліджувати копії файлів, а не оригінальні файли. На етапі збирання аналітик повинен зробити кілька копій потрібних файлів або файлових систем, як правило, головну та робочу копію. Потім аналітик може працювати з робочою копією файлів, не впливаючи на оригінальні файли чи головну копію. Зображення бітового потоку слід виконувати, якщо можуть знадобитися докази для притягнення до відповідальності чи дисциплінарних заходів, або якщо важливо зберегти час файлу.

Аналітики повинні зберігати та перевіряти цілісність файлів. Використання блокувальника запису під час резервного копіювання та створення образів запобігає запису комп'ютера на носій даних. Цілісність скопійованих даних має бути перевірена шляхом обчислення та порівняння дайджестів повідомлень файлів. Доступ до резервних копій та зображень має бути доступним лише для читання, коли це можливо. Блокувальники запису також можна використовувати для запобігання запису в резервну копію або файл образу або відновлену резервну копію або образ.

Аналітики повинні покладатися на заголовки файлів, а не на розширення файлів, щоб визначити типи вмісту файлів.

Оскільки користувачі можуть призначати будь-яке розширення файлу, аналітики не повинні вважати, що розширення файлів точні. Аналітики можуть

визначити тип даних, що зберігаються в багатьох файлах, дивлячись на заголовки їхніх файлів. Хоча люди можуть змінювати заголовки файлів, щоб приховати фактичні типи файлів, це набагато рідше, ніж зміна розширень файлів.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми розслідування інцидентів в інформаційних системах. Відмічається, що сьогодні кількість інцидентів в інформаційних системах організацій та кількість даних, пов’язаних з ними, постійно зростає. Це ускладнює виконання покладених завдань фахівцями з кібербезпеки. Тому, без сучасного набору методів та засобів для розслідування інцидентів та реагування на них, фахівцями з кібербезпеки виконати поставлені перед ними завдання буде дуже важко.

Визначено зміст розслідування інцидентів в інформаційних системах. Організації повинні проводити криміналістичну експертизу, використовуючи послідовний процес, який складається з чотирьох основних етапів збору, експертизи, аналізу та звітності.

Досліджено існуючі методи та засоби розслідування інцидентів в інформаційних системах. Аналітики безпеки мають доступ до різних інструментів, які дають їм змогу проводити експертизу та аналіз даних, а також певну діяльність зі збору даних. Багато криміналістичних продуктів дозволяють аналітику виконувати широкий спектр процесів для аналізу файлів і програм, а також збирати файли, читати образи дисків і витягувати дані з файлів. Більшість продуктів аналізу також мають можливість створювати звіти та реєструвати всі помилки, що виникли під час аналізу.

Визначено порядок застосування методів та засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу реєстру та журналу подій. Реєстр ОС Windows містить велику кількість інформації, яка може забезпечити значний контекст для широкого кола досліджень. Розглянуто можливості інструмента *yaru*, який є незалежним від платформи засіб перегляду реєстру ОС Windows.

Журнали подій ОС Windows – це спеціальні файли, в яких система та програми записують значущі для даного комп'ютера події, такі як події входу

користувачів до системи або помилки, що виникають під час роботи програм. Дані з журналів подій ОС Windows містять багато корисної інформації під час розслідування інцидентів безпеки. Розглянуто можливості інструмента *evtx_view*, який побудований на основі графічного інтерфейсу та може аналізувати журнали подій ОС Windows.

Розглянуто порядок застосування методів та засобів розслідування інцидентів в інформаційній системі організації з використанням аналізу реєстру та журналу подій.

Розроблено рекомендації керівникам організацій та фахівцям з кібербезпеки щодо застосування методів та засобів розслідування інцидентів в інформаційних системах організацій.

Набір програмних засобів для розслідування інцидентів та реагування на них має вирішальне значення, особливо враховуючи нестачу кваліфікованих фахівців з кібербезпеки. Правильне програмне забезпечення може закрити розрив у навичках і дозволити практикам бути більш ефективними. Команди з безпеки повинні бути максимально ефективними, щоб вирішувати завдання, які стоять перед ними.

Таким чином, запропоновані в роботі рекомендації мають сприяти ефективному розслідуванню та реагуванню на інциденти в інформаційних системах організацій, а також запобіганню їх повторенню в майбутньому.

ПЕРЕЛІК ПОСИЛАНЬ

1. State Of Enterprise DFIR: 2023 Report. An IDC eBook, sponsored by Magnet Forensics [Електронний ресурс] – Режим доступу: https://www.magnetforensics.com/2023-state-of-enterprise-dfir/#form.

2. NIST Cloud Computing Forensic Science Challenges. NISTIR 8006. Date Published: August 2020. [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/nistir/8006/final.

3. DIGITAL EVIDENCE [Електронний ресурс] – Режим доступу: https://www.nist.gov/digital-evidence.

4. Digital Forensics [Електронний ресурс] – Режим доступу: https://www.nist.gov/programs-projects/digital-forensics.

5. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang. Guide to Integrating Forensic Techniques into Incident Response. SP 800-86. Date Published: August 2006. [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf.

6. Tina Wu, Frank Breitinger, Stephen O'Shaughnessy. Digital forensic tools: Recent advances and enhancing the status quo. Forensic Science International: Digital Investigation.Volume 34, September 2020, 300999 [Електронний ресурс] – Режим доступу: https://doi.org/10.1016/j.fsidi.2020.300999.

7. Harlan Carvey. Windows Registry Forensics. Advanced Digital Forensic Analysis of the Windows Registry. Second Edition. 2016, 2011 Elsevier Inc. 204 pp. http://dx.doi.org/10.1016/B978-0-12-803291-6.00002-4

8. Windows registry information for advanced users. Article 06/04/2023. [Електронний ресурс] – Режим доступу: https://docs.microsoft.com/en-gb/troubleshoot/windows-server/performance/windows-registry-advanced-users.

9. TZWorks Yet Another Registry Utility (yaru). Users Guide. Updated: Dec 7, 2021. [Електронний ресурс] – Режим доступу: https://tzworks.com/prototypes/yaru/yaru.users.guide.pdf.

10. Журналы событий Windows. [Електронний ресурс] – Режим доступу: https://eventlogxp.com/rus/essentials/windowseventlog.html#SecurityEventLog.

11. Аудит безпеки у Windows. [Електронний ресурс] – Режим доступу: https://eventlogxp.com/rus/essentials/securityauditing.html.

12. TZWorks Windows Event Log Viewer (evtx_view). Users Guide. Document applies to v1.15 of evtx_view. Updated: Dec 7, 2021. [Електронний ресурс] – Режим доступу: https://tzworks.com/prototypes/evtx_view/evtx_view.users.guide.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)