3. Інструкція про призначення та проведення судових експертиз та експертних досліджень Міністерства юстиції України від 08.10.98 р. №53/5. [Електронний ресурс]. — Режим доступу: URL: http://zakon3.rada.gov.ua/laws/show/z0705-98.
4. Кримінальний процесуальний кодекс України від 05.07.2012. [Електронний ресурс]. — Режим доступу: URL: http://zakon4.rada.gov.ua/laws/show/4651-17.
5. *Нарижный А.В.* Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: дис. ... канд. юрид. наук: 12.00.09 / А.В. Нарижный; Кубан. гос. ун-т. — Краснодар, 2009. — 270 с.

Резюме

Проводится анализ новой законодательной базы, регулирующей вопросы относительно судебных экспертиз, в частности процедуру их назначения. В этом контексте рассматриваются особенности назначения судебной компьютерно-технической экспертизы.

Summary

The analysis of new legislative base, which regulates the forensic examinations issues, in particular the order procedure, is provided. In this context, the features of forensic computer-technical examination order are observed.

Ю.Ю. Нізовцев

Інститут спец. техніки та суд. експертиз СБУ

КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ, ЩО ПІДДАВАЛИСЯ ВІДДАЛЕНІЙ АТАЦІ НА ВІДМОВУ В ОБСЛУГОВУВАННІ: ЛОГ-ФАЙЛИ СЕРВІСІВ ТА ФАЙЛИ-ЗВІТИ ДІАГНОСТИЧНИХ УТИЛІТ, ЯК БЕЗПОСЕРЕДНІ ОБ'ЄКТИ ДОСЛІДЖЕННЯ

Одним з різновидів втручання в роботу автоматизованих систем є атака на відмову в обслуговуванні (або просто атака на відмову), яка полягає в заблокуванні доступу користувачів до сервісу, що надається атакованою системою, або у примушуванні атакованої системи функціонувати потрібним зловмисникові чином. Криміналістичне дослідження автоматизованих систем, що піддавалися атакам на відмову, зазвичай є невід'ємною складовою процесу розкриття та розслідування таких правопорушень.

Основними безпосередніми об'єктами таких досліджень є лог-файли роботи певних сервісів, які були піддані атаці (наприклад, access-log web-серверу) та/або проміжних вузлів (маршрутизаторів,

мостів тощо), а також файли-звіти роботи певних діагностичних утиліт (наприклад — tcpdump).

Лог-файл або просто лог (англ. *Log file*, від грец. *logos* — слово, смисл, думка, мова) — спеціальний файл реєстрації подій, в якому накопичується зібрана службова та статистична інформація про події в системі (програмі) у хронологічному порядку. Операційні системи (особливо це стосується серверних ОС) та серверне програмне забезпечення зазвичай мають розвинуту систему ведення логів.

Інформація з лог-файлів надалі використовується адміністраторами для аналізу подій, виявлення помилок, збоїв, зведення статистики, звітування, відстеження дій підозрілих користувачів, вузлів тощо.

Саме за допомогою аналізу логів можна встановити, що відбувається чи відбулося на комп'ютері або в мережі.

У випадку, якщо автоматизована система функціонує не штатним чином (різко знижується продуктивність роботи, спостерігається певна нестабільність в роботі тощо) або є збої в роботі мережі, можуть бути запущені спеціалізовані діагностичні утиліти. Результати роботи цих утиліт можуть бути виведені як на екран, так і в спеціальний файл-звіт. Аналіз цих файлів-звітів може допомогти вірно локалізувати та діагностувати проблему.

Задля того, щоб грамотно витягти корисну інформацію з лог-файлів або файлів-звітів іноді досить простого текстового редактора. В інших випадках необхідне спеціалізоване програмне забезпечення для інтерпретації зафіксованої у цих файлах інформації. Але у будь-якому разі необхідно знати особливості структури різних лог-файлів і файлів-звітів та інформації, що в них зафіксована.

В залежності від способу подання інформації лог-файли можна розділити на наступні типи:

- логіювання у текстовий файл з простою структурою;
- логіювання у текстовий файл із складною структурою;
- логіювання у бінарний файл;
- логіювання до бази даних.

Наступним важливим параметром, який слід враховувати під час дослідження лог-файлів, є конфігурування логіювання.

Найчастіше використовуються наступні налаштування (їх можна з'ясувати, переглянувши конфігурацію програмного забезпечення):

- ім'я лог-файлу, директорія (папка) або повний шлях до файлу, в який здійснюється запис логів;
- параметри заміни лог-файлів, або ротація логів (Log Rotation);

- частота скидання інформації до лог-файлу;
- перелік подій, що підлягають логіюванню.

Ротація лог-файлів може бути налаштована наступним чином:

- заміна лог-файлу з настанням певного часу (через певні проміжки часу).
- заміна лог-файлу при досягненні ним певного об'єму.
- заміна лог-файлу під час перезапуску сервісу.

Під час аналізу лог-файлів та файлів-звітів слід встановити, чи зафіксована у цих файлах інформація стосовно подій, які цікавлять слідство чи суд. Для цього з'ясовується наступна інформація:

- Яка програма згенерувала файл?
- Які були налаштування логіювання чи формування звіту при генерації файлу?
- Події стосовно якого ресурсу зафіксовані у файлі?
- Події за який проміжок часу зафіксовані у файлі?
- Чи є файл оригіналом, або отриманий шляхом вибірки з оригінального? Якщо отриманий шляхом вибірки, то за якими параметрами здійснювалася ця вибірка?
- Події якого рівня мережевої моделі "TCP/IP" зафіксовані у файлі?

Як бачимо, лог-файли сервісів та файли-звіти діагностичних утиліт бувають різних типів, формуються з різними параметрами та можуть містити різну статистично-діагностичну інформацію щодо подій в роботі сервісу, в роботі автоматизованої системи в цілому чи в мережі. Задля коректного витягування цієї інформації та ефективного її використання необхідно досконало знати особливості генерації зазначених файлів, а також з'ясувати при отриманні їх на дослідження ряд питань щодо походження цих файлів.

Список використаної літератури

1. Видеозапись отключения Solaris-сервера, проработавшего без перезапуска более 10 лет. [Електронний ресурс]. — Режим доступу: www.opennet.ru/opennews/art.shtml?num=36401
2. Лог-файлы (логи) / "Энциклопедия хостинга" [Електронний ресурс]. — Режим доступу: http://book.majordomo.ru/
3. *Сидоров В.* Что такое лог-файлы сайта и зачем их нужно анализировать? / В. Сидоров [Електронний ресурс]. — Режим доступу:
4. http://netler.ru/pc/log-file.htm
5. Логи: разбираемся с понятием лог файл / Зеркало рунета [Електронний ресурс]. — Режим доступу: http://thelocalhost.ru/log/
6. Что такое лог-файлы. Анализ лог-файлов / HTML — это просто [Електронний ресурс]. — Режим доступу:
7. http://on-line-teaching.com/site/lsn022.html

8. Логирование информации /.hostinfo [Електронний ресурс]. — Режим доступу: http://hostinfo.ru/articles/security/rubric157/1062/
9. Лог / wikipedia [Електронний ресурс]. — Режим доступу:
10. http://uk.wikipedia.org/wiki/Лог
11. Файл регистрации / wikipedia [Електронний ресурс]. — Режим доступу: http://ru.wikipedia.org/wiki/Файл_регистрации

Резюме

В статье раскрывается понятие лог-файлов сервисов, приводятся их типы. Раскрывается понятие файлов-отчетов диагностических утилит. Также в статье рассмотрены параметры логирования. В конце статьи приводятся основные моменты, которые необходимо уточнить при получении на исследование лог-файла или файла-отчета для эффективного исследования этих файлов.

Summary

In the paper notion of log-files of services is disclosed, their types are specified. Notion of diagnostic report files is disclosed. Also log parameters are considered in the paper. At the end of the paper basic points are given, which need to be clarified, when a log-file or a report file is received for examination in order to examine them efficiently.

С.Д. Прокопенко, нач. лаборатории

ООО "ЕПОС"

ПРОБЛЕМЫ КОПИРОВАНИЯ ДАННЫХ С НАКОПИТЕЛЕЙ С ДЕФЕКТНЫМИ СЕКТОРАМИ ПРИ ПРОИЗВОДСТВЕ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

В соответствии с Криминальным процессуальным кодексом Украины [1] в обязанности эксперта входит обеспечение сохранности объекта экспертизы. При производстве компьютерно-технических экспертиз это требование фактически означает необходимость предотвращения внесения изменений в данные на исследуемых носителях информации.

В большинстве случаев, как свидетельствует практика, для выполнения этого требования эксперты создают побитовую копию исследуемого накопителя на жестких магнитных дисках (НЖМД) и в дальнейшем проводят исследование именно копии, не работая с оригиналом. Поэтому от целостности и полноты копии зависят все последующие этапы экспертного исследования.

Одной из наиболее распространенных проблем при копировании данных является разрушение рабочих поверхностей НЖМД, которое