Література

1. Белкин Р. С. История отечественной криминалистики. — М.: НОРМА, 1999. — 496 с.
2. Буринский Е. Судебная экспертиза документов, производство ее и пользование ею. — С.Пб., 1903. — 352 с.
3. Князев А. Необходимо расширить сеть криминалистических учреждений // Социалистическая законность. — М., 1941. — № 4. — С. 50–51.
4. Краткая записка прокурора Одесского окружного суда в Министерство юстиции от 24 ноября (7 декабря) 1912 р. с предложением о необходимости учреждения Кабинета научно-судебной экспертизы при прокуроре Одесской судебной палаты // РДІА. — Ф. 1405. — Оп. 532. — Спр. 131. — А. 45–50.
5. Криминалистика: Техника и тактика расследования преступлений. — М.: Юриздат НКЮ СССР, 1938. — 540 с.
6. Митричев С. П. Задачи советской криминалистической экспертизы // Труды первой научной сессии Всесоюзного института юридических наук (27 января — 3 февраля 1939 г.). — М., 1940. — С. 425–431.
7. Об устройстве судебно-фотографической лаборатории при прокуроре Петербургской судебной палаты: Закон Российской империи от 9(21) ноября 1892 г. // Собрание узаконений и распоряжений правительства. — С.Пб., 1892. — № 144. — Ст. 1254.
8. Об учреждении Кабинета научно-судебной экспертизы: Закон одобренный Государственным Советом и Государственною Думою 28 июня (11 июля) 1912 г. // Собрание узаконений и распоряжений правительства. — 1912. — Отд. 1., № 142. — Ст. 1237.
9. Об учреждении кабинетов научно-судебной экспертизы в городах Москве, Киеве и Одессе: Закон одобренный Государственным Советом и Государственною Думою 4(17) июля 1913 г. // Собрание узаконений и распоряжений правительства. — 1913. — Отд. 1, № 158. — Ст. 1441.
10. Положение о кабинетах научно-судебной экспертизы: Постановление СНК УССР от 10 июля 1923 г. // Собрание узаконений и распоряжений рабоче-крестьянского правительства Украины. — 1923. — Отд. 1, № 26. — Ст. 384.
11. Положение о судоустройстве УССР, утвержденное 2-й сессией ВУЦИКа IX созыва 23 октября 1925 г. // Собрание узаконений и распоряжений рабоче-крестьянского правительства Украины. — 1925. — Отд. 1, № 92–93. — Ст. 522.
12. Bertillon A. La Phofographie Judiciaire. — Paris, 1890. — 115 p.
13. Bertillon A. La Phofographie Judiciaire de la prefecture de Police // La Nature. — Paris, 1913. — An. 41, N 2086. — P. 393–397.
14. Bertillon A. Sur le fonctionnement du service d'identification par les signalements anthropometriques donnee le 22 novembre 1885 // Actes du Congres penitentiaire snternational de Rom. Novembre 1885. — Rome, 1887. — Vol. 1. — P. 687–705.
15. Reiss R.-A. Die Entwicklung der photographischen Bromsilbert — Ockenplatte und die Entwickler. — Halle, 1902. — 156 S.
16. Paul F. Handbuch der kriminalistischen Photographie fur Beamte der Gerichte, der Staatsanwaltschaften und der Sicherheitsbehorden. — Berlin, 1900. — 93 S.

УДК 340.6:004.63

М. В. Полякова, В. С. Рукавішников, А. М. Шабля

СУДОВА КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА: ПІДХІД ДО ДОСЛІДЖЕННЯ ФАЙЛОВИХ СИСТЕМ

На сучасному етапі розвитку персональних комп'ютерів (ПК) і програмного забезпечення (ПЗ) існує декілька конкуруючих операційних систем (ОС), які використовують більш десятка різних файлових систем (ФС).

Узагальнюючи більш ніж десятирічну практику експертів ОНДІСЕ, можна

констатувати, що найбільш поширеними є ОС родини Windows [3, 5]: досі використовуються Windows 98/Me/NT; багато користувачів вже перейшли на Windows XP; зараз впроваджується Windows Vista.

Windows 98/Me орієнтовані на роботу з ФС FAT 12, FAT16, FAT32. Для Windows NT була спеціально розроблена ФС NTFS, у подальшому вдосконалена для Windows 2000 і яка використовується у ОС Windows XP та Windows Vista.

Окрім ОС родини Windows використовуються ОС з відкритим програмним кодом. Це Unix-подібні ОС, з яких найбільш популярні ОС родини Linux (Mandriva (раніше Mandrake), Red Hat, Slackware, Debian тощо) та ОС родини BSD, зокрема FreeBSD [1; 2; 4; 6–8]. В ОС родини Linux найбільш поширеними є ФС ext2, ext3, raiserfs.

Одним з основних питань, які ставлять на вирішення комп'ютерно-технічної експертизи, є питання пошуку інформації, у тому числі і серед видалених файлів. Для вирішення цього питання необхідно визначитися з ОС, яка буде коректно працювати з ФС на накопичувачі на жорстких магнітних дисках (НЖМД), що підлягає дослідженню.

Під час досліджень дані на НЖМД повинні оставатися у первинному стані, тобто на досліджуваний накопичувач не повинна записуватися нова інформація. Це обумовлено тим, що видалення файлів з НЖМД означає позначення дискового простору, де ці файли були фізично розташовані, як вільного. Таким чином, якщо ОС чи користувач буде виконувати запис даних на НЖМД, існує імовірність запису на місце видаленого файлу, що відповідно унеможливлює відновлення раніше записаного.

Для ОС MS Windows існують програмні засоби для читання даних з ФС ext2, однак ФС ext3, raiserfs і біля десятку інших ФС (менш поширених серед користувачів Linux) для Windows недоступні.

У будь-якій базовій конфігурації ОС Linux є драйвери для роботи з ФС FAT12, FAT16, FAT32. Для роботи з ФС NTFS існують декілька драйверів, які не включені у дистрибутиви ОС Linux, але вони вільно розповсюджуються, і будь-який користувач за бажанням може їх встановити і використовувати, отримуючи повний доступ до ФС NTFS.

Для забезпечення неушкодженості даних на досліджуваному носії можна використовувати апаратні засоби, які фізично переривають сигнали запису даних, тим самим гарантуючи їх цілісність. Однак апаратні рішення вельми дорогі, до того ж існує більш дешевий спосіб, який дає таку ж надійну гарантію захисту від запису у розділи НЖМД, який досліджується. Мова йде про використання функції ОС Linux монтування розділів НЖМД у режимі «лише читання». При цьому користувач отримує повний доступ для копіювання і відновлення даних з НЖМД, але не має можливості вносити будь-які зміни в них.

Як найбільш оптимальний вибір для подолання зазначених проблем пропонується використовувати Linux Live CD дистрибутив. Це спеціальна версія дистрибутиву ОС Linux, яка завантажується з оптичного носія (CD або DVD) і існує майже для всіх дистрибутивів Linux. Linux на Live CD має всі функціо-

нальні можливості, притаманні звичайному дистрибутиву Linux, який встановлюється на НЖМД. Але для цього варіанта ОС розділи за умовчанням монтуються у режимі «читання». Окрім того такий Live CD може бути використаний як портативний засіб діагностики і дослідження ПК.

Серед дистрибутивів Linux Live CD особливе місце займає дистрибутив Knoppix, який оснований на дистрибутиві Debian — найбільш великому і найбільш «вільному» дистрибутиві Linux (дистрибутив Debian розміщується на 14 CD і містить декілька тисяч програм, які розповсюджуються з їх первинними кодами). Із всіх Linux Live CD, що існують на сьогодні, Knoppix має засоби для найбільш повного і найбільш коректного визначення апаратних засобів ПК і роботи з ними. Knoppix стабільно працює як з вже застарілими ПК, так і з новітніми, визначаючи практично всі пристрої і забезпечуючи користувачу комфортне робоче середовище. На базі дистрибутиву Knoppix створюються різноманітні спеціалізовані Linux Live CD дистрибутиви. Зокрема у ОНДІСЕ був розроблений Linux Live CD дистрибутив, призначений саме для проведення комп'ютерно-технічних експертиз.

Серед ПЗ, що входить у розроблений Linux Live CD, слід відмітити такі утиліти:

Chntpw — дозволяє змінити паролі користувача у файлі userdatabase Windows NT/2000/XP. Обнуляє пароль облікового запису у NT-системі, модифікуючи зашифрований пароль у SAM-файлі.

Dar (Disk Archive) — програма резервного копіювання дерев директорій і файлів. Dar — простий, але гнучкий і потужний інструмент. Дозволяє створювати вибіркові і специфічні резервні копії, розбивати архів на частини (для розміщення на декількох зовнішніх носіях, таких як CD/DVD чи Zip), проводити шифрування і стиснення інформації. Dar може зберігати каталог кожної резервної копії у базі даних. При цьому можна легко знайти в серії резервних копій останню версію (чи необхідну) видаленого файлу і відновити його.

Dd_rescue копіює дані з одного файлу (чи пристрою) в інший. Можливості *dd_rescue* дозволяють відновити дані з НЖМД, на якому є дефектні сектори.

Foremost — консольна програма для відновлення файлів, яка основана на визначені їх заголовків, нижніх зносок і внутрішньої структури даних. Foremost може працювати з образами файлів, якщо вони створені програмами Safeback, Encase тощо, чи безпосередньо з носієм. Наявність вбудованих типів файлів дозволяє надійно і швидко відновити файл відповідного формату. Працює з ФС FAT, FAT32, NTFS, ext2, ext3.

Gpart — інструмент, який дозволяє розпізнати, а потім відновити первинну таблицю розділів НЖМД у випадку, якщо вона у секторі 0 пошкоджена, некоректна чи видалена. ФС чи типи розділів, які розпізнає gpart: BeOS ФС; FreeBSD/NetBSD/386BSD підрозділи, які використовуються на платформах Intel; Linux second extended filesystem — ext2; MS-DOS FAT12/16/32 ФС; IBM OS/2 High Performance filesystem; Linux LVM physical volumes; Linux swap partitions (версії 0 і 1); ФС ОС Minix; MS Windows NT/2000 ФС; QNX 4.x ФС; Reiser ФС (версії 3.5.X, X > 11); Sun Solaris на платформах Intel використовує схему

підрозділів на НЖМД подібну до BSD, ФС с журналом Silicon Graphics для Linux. Інші типи можуть бути додані відносно легко, як окремо скомпільовані модулі.

GtkRecover — GUI версія консольної утиліти recover. Відновлює файли в розділах НЖМД з ФС ext2. Дозволяє виконувати пошук видаленого файлу по таких параметрах: назві; року видалення; місяцю видалення; дню тижня видалення; першим/останнім можливим днем місяцю; мінімально/максимально можливим розміром файлу; мінімально/максимально можливим часом видалення; мінімально/максимально можливою хвилиною видалення; ідентифікатором користувача видаленого файлу; по послідовності символів у файлі.

Magicrescue відкриває пристрої (*devices*) для читання, переглядає, шукає файли відомих їй типів і викликає зовнішню програму для відновлення. Утиліту можна використовувати і для відновлення видалених файлів, і для відновлення пошкодженого розділу. Дозволяє працювати з багатьма ФС, але на дуже фрагментованих розділах може відновити лише перший фрагмент кожного файлу (іноді ці фрагмент досягають 50МБ).

Ncurses_Hexedit — редактор файлів, який дозволяє редагувати і переглядати файл у шістнадцятковому представлені, разом з його ASCII чи еквівалентним текстом розширеного двійкового-десяткового коду (EBCDIC).

НАБІР УТИЛІТ *ntfsprogs* — набір утиліт для роботи з ФС NTFS. Цей набір дозволяє:

– створювати ФС NTFS (утиліта *Mkntfs*);

– читати файл чи потік з тому NTFS, виводити вміст файлу (потоку) на стандартний пристрій виводу (утиліта *Ntfscat*);

– ефективно клонувати NTFS розділ, створювати образ, відновлювати видалені чи пошкоджені файли, розділи ФС NTFS, а також створювати резервні копії (утиліта *Ntfsclone*);

– перевіряти і фіксувати деякі загальні помилки, очищати файл журналу (LogFile) NTFS (утиліта *Ntfsfix*);

– отримувати інформацію про NTFS чи одного з файлів, чи директорій у межах ФС (утиліта *Ntfsinfo*);

– монтувати розділи з NTFS за допомогою драйвера простору користувача для читання/запису у ФС (утиліта *Ntfsmount*);

– змінювати розміри ФС NTFS у ОС Windows XP, Windows Server 2003, Windows 2000, Windows NT4 і Longhorn без втрати даних (утиліта *Ntfsresize*);

– відновлювати видалені файли на томі з ФС NTFS (утиліта *Ntfsundelete*).

Таким чином, створений Live-CD дистрибутив на основі Knoppix дозволяє експертові у галузі судових комп'ютерно-технічних досліджень виконувати пошук та відновлення видалених і пошкоджених файлів, розділів НЖМД з файловими системами FAT12, FAT16, FAT32, NTFS, ext2, ext3, raiserfs з можливістю подальшого копіювання інформації на інший носій, а також створення резервних копій розділів НЖМД і файлів, аналізувати файли-журналів. Можливо також виконання деяких операцій по відновленню інформації ФС: BeOS, FreeBSD/NetBSD/386BSD, IBM OS/2, LVM, ОС Minix, MS Windows NT/2000;

QNX 4.x, Reiser (версії 3.5.X, X > 11), Sun Solaris на платформах Intel, Silicon Graphics для Linux.

Описаний програмний продукт є відкритим, що дозволяє у подальшому розширювати його функціональні можливості шляхом доповнення новими утилітами.

Література

1. Вахалия Ю. UNIX изнутри. — С.Пб.: Питер, 2003.
2. Дупаев С. Unix. System V. Release 4.2. — М.: Диалог МИФИ, 1996.
3. Кастер Х. Основы Windows NT и NTFS. — М.: Рус. ред., 1996.
4. Керниган Б. В., Пайк Р. UNIX — универсальная среда программирования. — М.: Финансы и статистика, 1992.
5. Соломон Д., Руссинович М. Внутреннее устройство Microsoft Windows 2000. — С.Пб.: Питер; М.: Рус. ред., 2001.
6. Стивенс У. UNIX: Взаимодействие процессов. — С.Пб.: Питер, 2002.
7. Робачевский А. Операционная система UNIX. — С.Пб.: BHV, 1999.
8. Інтернет-ресурси: http://computerlibrary.info/, http://www.redhat.com/, http://www.debian.org, http://www.slackware.com/, http://www.suse.com/, http://www.mandriva.com, http://www.altlinux.ru/, http://www.asplinux.ru/, http://www.gentoo.org/, http://www.knoppix.ru/, http://www.archlinux.org/, http://mirrors.fedoraproject.org/, http://www.ubuntu.com/, http://wiki.freespire.org/, http://www.sun.com/software/solaris/, http://www.xandros.com/