УДК 343.9

А.М. Гаркуша, *начальник сектору*
Науково-дослідного експертно-криміналістичного
центру при УМВС України в Херсонській області

ПИТАННЯ ВИЗНАЧЕННЯ ЧАСОВИХ МІТОК ФАЙЛІВ У ФАЙЛОВИХ СИСТЕМАХ «FAT» І «NTFS»

Розглянуто загальні положення формування шкали часу, визначено особливості роботи операційних систем із файловими системами «FAT» і «NTFS» при виконанні дій з файлами в частині фіксації хронометричних даних.
Ключові слова: мітка часу, файлова система, NTFS, FAT.

Рассмотрены общие положения формирования шкалы времени, определены особенности работы операционных систем с файловыми системами «FAT» и «NTFS» при выполнении действий с файлами в части фиксации хронометрических данных.

The paper gives outline of formation of the time scale. It studies the specific features of work of operation systems with «FAT» and «NTFS» in terms of time stamping.

Відповідно до положень частини першої ст. 91 Кримінального процесуального кодексу України у кримінальному провадженні серед інших обставин підлягає доказуванню подія кримінального правопорушення: час, місце, спосіб, інші обставини вчинення кримінального правопорушення.

Розслідування кримінальних правопорушень часто потребує дослідження носіїв цифрових даних, для чого призначають судову комп'ютерно-технічну експертизу. Одним із важливих питань при цьому є визначення часу вчинення певних дій користувачами або часу настання подій в інформаційній системі. Вирішення цих питань часто потребує від експерта встановлення фактів створення та зміни певних файлів, а також доступу до них, що неможливо без відповідної фахової його обізнаності щодо порядку інтерпретації отриманих даних про час. З огляду на широке розповсюдження операційних систем, які використовують для зберігання файлів файлові системи «FAT» і «NTFS», у цій статті запропоновано розглянути, крім загальних положень формування часу, особливості функціонування цих операційних систем з файловими системами при виконанні дій з файлами.

Насамперед слід нагадати, що з 1964 року використовують систему всесвітнього координованого часу UTC (від англ. «Coordinated Universal Time») [1].

З метою подолання однієї з перешкод на шляху до міжнародного співробітництва у 1884 році на підставі рішення Міжнародної меридіанної конференції у Вашингтоні про всесвітній час, за який мав правити середній сонячний час на меридіані Гринвіча, було прийнято поясну систему обліку часу [2; 3]. Згідно з такою системою обліку земну кулю було поділено на 24 пояси, кожний приблизно по 15° [4] з проходженням початкового меридіана нульового пояса через обсерваторію

м. Гринвіча (Великобританія). Час першого пояса відрізняється від часу нульового пояса рівно на 1 год. Різність поясних часів дорівнює різності номерів їх часових поясів (за винятком окремих країн).

Згідно з відповідними нормативно-правовими актами на території України запроваджено час другого часового пояса (київський час) [5]. Алгоритм визначення часу на території України виглядає так: UTC(UA)= UTC + 2.

Багато держав Європи та Америки, у тому числі й Україна, запроваджують так званий «літній час», тобто місцевий час, який встановлюють на певній території на літній період року. Зазвичай такий час різниться на годину від стандартного часу, прийнятого на цій території (наприклад, для України літній час визначають за формулою «поясний час + 1 год.» — (UTC+2) + 1 = UTC+3).

Національна шкала координованого часу UTC(UA) формується з використанням Державного первинного еталону одиниць часу та частоти України. Забезпечення безперервного функціонування державного первинного еталона одиниці часу і національної шкали координованого часу України UTC(UA) покладено на Український метрологічний центр Державної служби єдиного часу і еталонних частот (далі — ДСЧЧ), який діє на базі Національного наукового центру «Інститут метрології» (м. Харків).

Як відомо, з метою обліку часу сучасні електронні пристрої оснащено годинниками. Кожний комп'ютер має у своєму складі годинник реального часу RTC (від англ. «real-time clock»), представлений електронною схемою, призначеною для обліку хронометричних даних (час, дата, день тижня тощо). До схеми входять автономне джерело живлення та обліковий пристрій. Вперше RTC було представлено у складі IBM PC/AT у 1984 році [6].

Більшість RTC використовують кварцовий резонатор на частоті 32768 Гц (таку саму частоту використовують у кварцових годинниках; вони не відрізняються особливою точністю, тому потребують періодичного контролю).

Контроль часу здійснюють особисто користувачі під час звіряння зі стороннімиими годинниками або «службою часу Windows» в автоматичному чи ручному режимах шляхом синхронізації по мережі з одним із серверів часу (локальним або в мережі Інтернет), який може бути заданий користувачем. Факт успішної або неуспішної синхронізації відображається у журналі «Система» операційної системи. Для отримання значень точного часу слід рекомендувати користуватися національним сервером Державної служби єдиного часу і еталонних частот — ntpd.metrology.kharkov.ua.

У кожному випадку порядок фіксації або відображення інформації про час комп'ютер здійснює індивідуально залежно від конкретної версії операційної системи, від файлової системи тощо.

Файлові системи «FAT» і «NTFS» передбачають зберігання часових міток (time stamp) відносно файлів і каталогів (у спеціалізованій літературі мітки розглядають як частину метаданих файлових систем [7]).

За загальним правилом файлова система «FAT» зберігає часові мітки, базуючись на локальному часі комп'ютера, а файлова система «NTFS», зберігаючи часові мітки в UTC-форматі, враховує не тільки локальний час, а й поправку на часовий пояс і літній час. Наприклад, якщо упродовж однієї хвилини зберегти той самий файл на флеш-накопичувачі (FAT32) та жорсткому диску (NTFS), то значення часо-

вих міток буде різним. Так, у файловій системі «FAT32» дата створення файлу фіксується як 23.02.2012 10:00, а у файловій системі «NTFS» — як 23.02.2012 08:00 у випадку налаштувань часового пояса «UTC+02:00 Київ».

Крім формату зберігання, файлові системи також мають відмінності в обсязі та кількості міток часу, які характеризують файл. Особливості файлових систем щодо фіксації часових міток наведено в таблиці.

Таблиця

Часові мітки файлів у файлових системах «FAT» і «NTFS»

№ з/п	Назва часової мітки	Реальний час	FAT (UTC+02:00)	NTFS (UTC)
1	Дата створення	05.09.2012 9:47:51	05.09.2012 9:47:51	05.09.2012 7:47:51
2	Дата змін	03.09.2012 4:55:23	03.09.2012 4:55:23	03.09.2012 2:55:23
3	Дата останнього доступу	05.09.2012 9:47:51	05.09.2012	05.09.2012 7:47:51
4	Дата змін запису MFT (тільки для NTFS)	05.09.2012 9:47:51	—	05.09.2012 7:47:51

Існують також особливості утворення та змін часових міток файлів при їх копіюванні або переміщенні (описані в документації підтримки компанії Microsoft [8]), а саме:

– якщо файл копіюється з C:\fat16 в C:\fat16\sub, дата змін зберігається, а дата створення файлу змінюється на поточну;

– якщо файл переміщується з C:\fat16 до C:\fat16\sub, дата змін і дата створення файлу зберігаються;

– якщо файл копіюється з C:\fat16 в D:\NTFS, дата змін зберігається, а дата створення файлу змінюється на поточну;

– якщо файл переміщується з C:\fat16 до D:\NTFS, дата змін і дата створення файлу зберігаються;

– якщо файл копіюється з D:\NTFS в D:\NTFS\SUB, дата змін зберігається, а дата створення файлу змінюється на поточну;

– якщо файл переміщується з D:\NTFS до D:\NTFS\SUB, дата змін і дата створення файлу зберігаються.

У всіх випадках дата змін зберігається доти, доки файл не будуть редагувати, а дата створення змінюється залежно від того, копіюють файл чи переміщують.

Також слід мати на увазі, що, якщо файл копіюють з файлової системи «NTFS» у файлову систему «FAT», часові мітки округлюються до повних секунд [9].

У спеціальній літературі також описано правила змін часових міток для каталогів [8]. Серед них є такі:

– якщо створити нові каталоги у томі NTFS з іменами D:\NTFS1 та D:\NTFS2, дата створення та дата змін ідентичні;

– якщо каталог D:\NTFS2 переміщують до каталогу D:\NTFS1 і при цьому створюють D:\NTFS1\NTFS2, тоді для:

D:\NTFS1 дата створення зберігається, а дата змін змінюється;

D:\NTFS1\NTFS2 обидві мітки як щодо дати створення, так і щодо дати змін залишаються незмінними;

– якщо каталог D:\NTFS2 копіюють у D:\NTFS1, утворюючи D:\NTFS1\NTFS2, тоді для:

D:\NTFS1 дата створення залишається незмінною, а дата змін змінюється;

D:\NTFS2 жодних змін у часових мітках не відбувається;

D:\NTFS1\NTFS2 часові мітки щодо дати створення та дати змін змінюються на час, коли відбулося переміщення.

При цьому слід мати на увазі певні особливості, які стосуються файлової системи «FAT», зокрема те, що дата змін каталогу не зміниться, якщо навіть зміниться зміст каталогу.

Дослідження часових міток файлової системи «NTFS» слід проводити з використанням спеціального криміналістичного програмного забезпечення, наприклад, програм «AccessData FTK Imager», «AccessData FTK» тощо. Застосування програм, які використовують для визначення часових міток програмні засоби операційної системи, слід вважати обмежено допустимим, оскільки існує велика ймовірність похибки під час визначення часу через ігнорування часового пояса операційної системи, яка оперувала даними на досліджуваному носії. У такому випадку слід зробити окрему помітку, в якій визначити поточний часовий пояс (за необхідності і літній час), встановлений в операційній системі експерта.

На завершення слід зазначити, що встановлення часу дії чи події є одним з важливих завдань слідства під час встановлення факту та механізму вчинення правопорушення. Визначення показань часу, що фіксуються на носіях даних комп'ютерів відносно дій користувачів і програм, сприятимуть встановленню винних осіб, з'ясуванню механізму вчинення правопорушення тощо.

Крім того, для повного розуміння механізму формування точного часу слід взяти до уваги, що точний час є величиною умовною, яка породжується довіреними установами, утвореними міжнародною спільнотою: Міжнародним бюро мір і ваг та Міжнародною службою обертання Землі. Проте кожна держава має свої уповноважені органи, які обліковують еталонний час і поширюють його серед населення та організацій. В Україні цю функцію покладено на Державну службу єдиного часу і еталонних частот.

Файли як продукт діяльності програм мають певні властивості, в тому числі й ті, які вказують на час їх створення, змін, доступу до них. Файлові системи, призначені для зберігання файлів, розраховані на фіксацію часових параметрів за певним алгоритмом, який виконує операційна система. Широко розповсюджені файлові системи «FAT» і «NTFS» мають лише їм властиві правила щодо фіксації часу, отриманого від годинника реального часу комп'ютера. Отже, у процесі дослідження при визначенні часових міток слід підходити до інтерпретації результатів індивідуально в кожному випадку.

Список використаної літератури

1. *Всемирное* координированное время [Электронный ресурс]. — Режим доступа : http://ru.wikipedia.org/wiki/.

2. *Клищенко А.П.* Астрономия : учеб. пособ. / А.П. Клищенко, В.И. Шупляк. — М. : Новое знание, 2004. — 224 с.

3. *Корсунь А.* Паризький хранитель часу з Одеси [Електронний ресурс] / А. Корсунь // Вісник НАН України. — 2001. — № 8. — Режим доступу : http://www.nbuv.gov.ua/portal/all/herald/2001-08/11.htm.

4. *Жаров В.Е.* Сферическая астрономия / В.Е. Жаров. — Фрязино : Век-2, 2006. — 480 с.

5. *Постанова* Верховної Ради Української РСР від 11 червня 1990 року № 15-XII «Про зміну порядку обчислення часу на території Української РСР» // Відомості Верховної Ради УРСР. — 1990. — № 26. — Ст. 400.

6. *Часы* реального времени [Электронный ресурс]. — Режим доступа : http://ru.wikipedia.org/wiki/.

7. *Кэрриэ Б.* Криминалистический анализ файловых систем / Б. Кэрриэ. — СПб. : Питер, 2007. — 480 с.

8. *Description* of NTFS date and time stamps for files and folders [Electronic resource]. — Access mode : http://support.microsoft.com/kb/299648/.

9. *Time* Stamps Change When Copying From NTFS to FAT [Electronic resource]. — Access mode : http://support.microsoft.com/kb/127830.