УДК 004.056

ЦИФРОВЕ КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ РЕЄЄСТРУ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS

Павленко В.С., Агасов С.М.
e-mail: vladyslav.pavlenko3@nure.ua, salman.agasov@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
ім. В. В. Поповського
м. Харків, Україна

The study presents the results of systematization and own research of the Windows operating system registry. The storage locations of artifacts for the registry section "HKEY_LOCAL_MACHINE", which may be of interest for forensic investigations, as well as their brief description are given. The most informative are the "\SOFTWARE" and "\SYSTEM" subsections. For these subsections, the artifacts stored in them and which can be used for forensics are analyzed in detail.

Реєстр операційної системи (ОС) Windows – це центральна, ієрархічна база даних, яка зберігає інформацію, необхідну для налаштування системи, програм та апаратних пристроїв. Проведення цифрової криміналістичної експертизи в інтересах розслідування злочинів дозволяє отримати великий об’єм інформації о діяльності зловмисника. Реєстр ОС Windows містить п'ять розділів: HKEY_CLASSES_ROOT; HKEY_CURRENT_USER; HKEY_LOCAL_MACHINE; HKEY_USERS; HKEY_CURRENT_CONFIG.

З точки зору цифрової криміналістики найбільш інформативним є розділ HKEY_LOCAL_MACHINE. Він складається з п'яти основних підрозділів: "\HARDWARE", "\SAM", "\SECURITY", "\SOFTWARE" та "\SYSTEM". Підрозділ \HARDWARE містить інформацію про те, яке обладнання встановлено на комп'ютері. Підрозділ "\SAM" містить інформацію про локальні облікові записи користувачів та їхню приналежність до локальних груп. Також у цьому підрозділі можна знайти інформацію про привілеї, надані користувачам, та стосовно яких системних ресурсів. Підрозділ "\SECURITY" зберігає інформацію про локальні системні політики (наприклад, політики автентифікації користувачів та інші), про набори прав доступу та привілеїв для користувачів, про організацію аудиту дій суб'єктів у системі тощо. Підрозділ "\SOFTWARE" містить налаштування всіх програмних застосунків, встановлених на системному диску комп'ютера. Підрозділ "\SYSTEM" містить налаштування самої ОС Windows. Також у цьому підрозділі можна знайти налаштування системного програмного забезпечення.

Необхідно відмітити, що цифрова криміналістична експертиза реєстру ОС Windows проводиться з його образом. Образ створюється за допомогою різних програм, наприклад, AccessData FTK Imager та інші. Для зчитування образу реєстру можуть бути використані різні інструменти, наприклад, Windows Registry Recovery (WRR).

Для прикладу наведемо результати аналізу інформації, яка зберігається в підрозділі "\SYSTEM".

Таблиця – Перелік артефактів підрозділу SYSTEM

Ключ реєстру	Опис артефакту
system\ControlSet001\ Control\ ComputerName»	Ім'я локального комп'ютера
system\ControlSet001\ Enum\ACPI	Інформація про процесор (тип, ідентифікатор, тип драйвера)
system\ControlSet001\ Enum\PCI	Інформація про роз'єми материнської плати (для кожного роз'єму можна дізнатися його ідентифікатор та версію системного драйвера)
system\ControlSet001\ Enum\ROOT\VMBus	Можна отримати інформацію про ідентифікатор обладнання, пов'язаного з Hyper-V, а також версію системного драйвера та багато іншого
system\ControlSet001\ Enum\SCSI»	Інформація про фізичні диски комп'ютера (модель фізичного диска, ідентифікатор його обладнання, версія системного драйвера тощо)
system\ControlSet001\ Enum\ USBSTOR	Можна знайти інформацію про всі знімні носії, підключені до локального комп'ютера протягом певного часу
SYSTEM \ ControlSet00x \ Services \ Tcpip \ Parameters \ Interfaces; SYSTEM \ ControlSet00x \ Control \ Class \ {4D36E972-E325-11CE-BFC1-08002bE10318} \ {00nn}	Інформація про мережні інтерфейси. Це встановлені мережеві карти, мережі, до яких було підключено комп’ютер, список бездротових мереж. Існує багато випадків використання анонімних бездротових мереж для вчинення незаконних дій

Список використаних джерел:

1. Harlan Carvey, Windows Registry Forensics. Advanced Digital Forensics Analisis of the Windows Registry. 2011., 206 p.

2. Nagendar Rao Koppolu, A Importance of Registry Forensics in Digital Crime Investigations Involving Windows Machines, IJCST Vol. 12, Issue 2, April - June 2021, pp. 9 – 18.

3. Raihana Md Saidi, Siti Arpah Ahmad, Noorhayati Mohamed Noor, Rozita Yunos. Windows Registry Analysis for Forensic Investigation. Faculty of Computer and Mathematical Sciences Universiti Teknologi MARA, Malaysia, 2021, pp. 1-6.