Analiza rejestru systemów z rodziny Windows za pomocą programu X-Ways Forensics. Informacje podstawowe

Wprowadzenie i cel pracy

Niniejsza publikacja stanowi wstęp do cyklu artykułów poświęconych możliwościom analizy systemów operacyjnych z rodziny NT. Przeprowadzone badania oraz przedstawione przykłady w znacznej mierze będą opierać się na pracy w programie X-Ways Forensics, jednak autor przedstawi również programy niekomercyjne, które mogą wspomóc analizę cyfrowego materiału dowodowego. Pierwsza część artykułu to wgląd w podstawowe informacje o rejestrze Windows oraz omówienie poszczególnych jego gałęzi. Następnie poruszone zostaną zagadnienia dotyczące m.in. ostatniej aktywności użytkownika, analizy działalności internetowej, konfiguracji sprzętu, identyfikacji podłączanych urządzeń.

Nawiązanie współpracy pomiędzy Komendą Wojewódzką Policji w Łodzi a Politechniką Łódzką, przy wsparciu oddziału łódzkiego Polskiego Towarzystwa Informatycznego, zaowocowało pracami nad oprogramowaniem wspomagającym ekspertów z dziedziny informatyki. Dlatego też w dalszych częściach zostaną przedstawione narzędzia, będące wynikiem tej współpracy. Służyć one mogą do analizy danych znajdujących się na dysku twardym (m.in. program do analizy plików z popularnych przeglądarek internetowych takich jak: FireFox, Opera, Chrome, IE), konwertowania formatów plików multimedialnych, pomagają tworzyć różnego rodzaju raporty.

Pracując z cyfrowymi nośnikami danych, nie można zapomnieć o prawidłowym postępowaniu z materiałem dowodowym. Dlatego też autor zaproponuje procedury, które powinny być stosowane w laboratoriach kryminalistycznych. Wypracowanie dobrych praktyk wydaje się konieczne, bowiem do tej pory pomimo ich stosowania w poszczególnych laboratoriach, nie zostały one usystematyzowane i rekomendowane przez wszystkie pracownie.

Celem starań podjętych przez autora jest zarówno zapoznanie kandydatów na ekspertów pracowni komputerowych z obecnie stosowanymi metodami ujawniania informacji z elektronicznych nośników danych, jak i ugruntowanie wiadomości doświadczonych inżynierów z zakresu informatyki śledczej. Poniższe opracowanie może wydawać się istotne ze względu na fakt, iż w resorcie brak jest specjalistycznych szkoleń podnoszących kwalifikacje ekspertów w dziedzinie informatyki. Dlatego też wypracowywane i przedstawione metody bazują na doświadczeniach ekspertów z terenu całego kraju.

Informacje podstawowe – rejestr Windows

Rejestr ustawień w systemach operacyjnych z rodziny Windows to baza danych zawierająca, zestawione hierarchicznie, informacje konfiguracyjne. W tej bazie przechowywane są liczne dane opisujące: system operacyjny (w tym datę instalacji[1]), konta użytkowników, urządzenia zarządzane przez system operacyjny z wykorzystaniem kontrolerów IDE/ATA/ATAPI, SCSI, RAID, stacje dysków, karty sieciowe, przenośne urządzenia magazynujące, zainstalowane oprogramowanie oraz wiele innych. Z uwagi na fakt, że działanie systemu zależy w znacznej mierze od ustawień zapisanych w rejestrze, z punktu widzenia informatyki śledczej jest to bardzo cenny zbiór informacji przydatnych w czasie przeprowadzanych badań, jak chociażby zapisy o odinstalowanych programach.

Struktura rejestru składa się z pięciu kluczy głównych przedstawionych w tabeli 1.

W starszych systemach takich jak Windows 98 pliki rejestru zlokalizowane były w dwóch plikach *system.dat* i *user.dat*. Systemy operacyjne z rodziny NT mają kilka pojedynczych plików zawierających tematycznie zorganizowane informacje tzw. gałęzie[2]. Informacja o miejscu ich przechowywania znajduje się w kluczu HKEY_LOCAL_MACHINE\System\ControlSet001\Control\hivelist (ryc. 1) i może przedstawiać się następująco:

- HKEY_LOCAL_MACHINE\SAM
- HKEY_LOCAL_MACHINE\Security
- HKEY_LOCAL_MACHINE\Software
- HKEY_LOCAL_MACHINE\System
- HKEY_USER\.Default
- HKEY_USER\S-1-5-21-220523388-492894223-1343024091
- HKEY_USER\S-1-5-21-220523388-492894223-1343024091-Classes

W skład jednej gałęzi np. *HKLM* wchodzą pliki główne zapisane na dysku twardym. Posiadają one pliki dodatkowe, np. *C:\windows\system32\config*. zawiera m.in. pliki[3]:

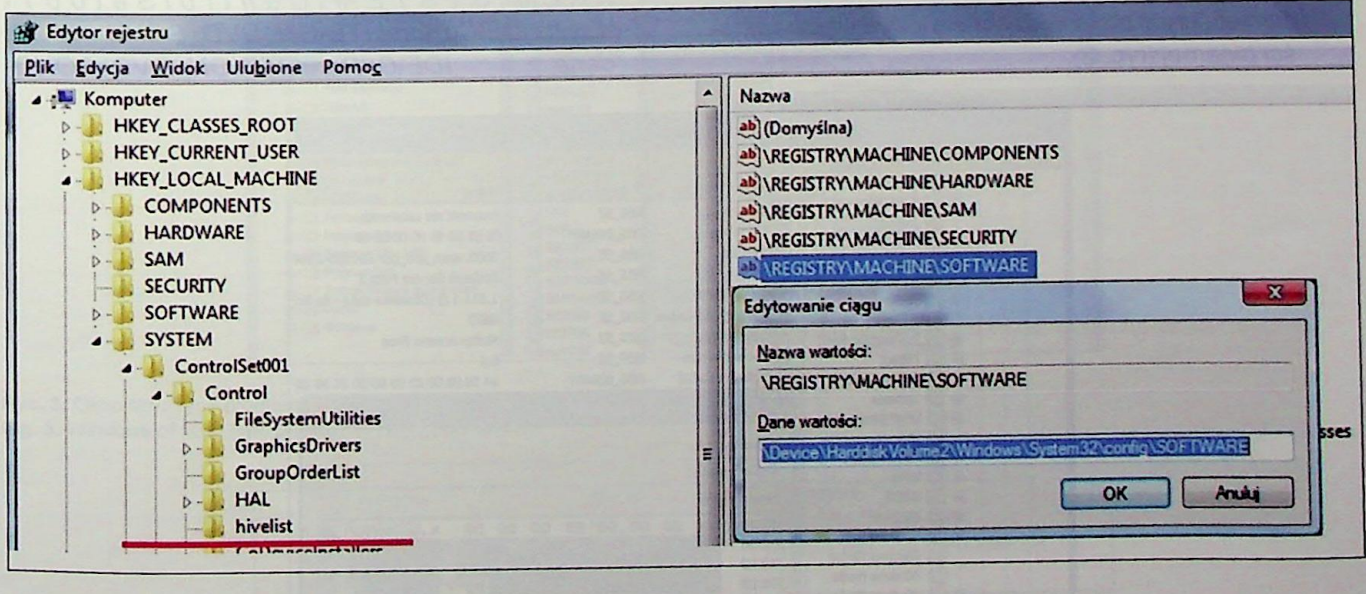
Tabela 1

Struktura rejestru Windows

Structure of Windows register

Nazwa klucza głównego	Opis
HKEY_LOCAL_MACHINE HKLM	Zawiera informacje o systemie komputera lokalnego, włączając w to dane dotyczące sprzętu i systemu operacyjnego, takie jak typ magistrali, pamięć systemowa, sterowniki urządzeń i dane kontroli uruchamiania.
HKEY_CLASSES_ROOT HKCR	Zawiera informacje wykorzystywane przez różnego rodzaju technologie OLE i dane skojarzeń klas plików. Dany klucz lub wartość występuje w kluczu *HKEY_CLASSES_ROOT*, jeśli odpowiadający mu klucz lub wartość występuje w kluczu *HKEY_LOCAL_MACHINE\SOFTWARE\Classes* bądź kluczu *HKEY_CURRENT_USER\SOFTWARE\Classes*. Jeżeli klucz lub wartość występuje w obydwu miejscach, to wersja *HKEY_CURRENT_USER* jest tą, która występuje w kluczu *HKEY_CLASSES_ROOT*.
HKEY_CURRENT_USER HKCU	Zawiera profil użytkownika, który jest aktualnie zalogowany interaktywnie (jako przeciwieństwo zalogowania zdalnego), w tym zmienne środowiskowe, ustawienia pulpitu, połączenia sieciowe, drukarki i preferencje programów. To poddrzewo jest aliasem poddrzewa *HKEY_USERS* i wskazuje na *HKEY_USERS\identyfikator_zabezpieczeń_bieżącego_użytkownika*.
HKEY_USERS HKU	Zawiera informacje o aktualnie załadowanych profilach użytkowników i profilu domyślnym. Część tych informacji pojawia się także w kluczu *HKEY_CURRENT_USER*. Użytkownicy uzyskujący zdalny dostęp do serwera nie mają profili pod tym kluczem na serwerze; ich profile są załadowane do rejestru ich własnych komputerów.
HKEY_CURRENT_CONFIG HKCC	Zawiera informacje o profilu sprzętowym używanym podczas uruchamiania komputera lokalnego. Te informacje są używane między innymi do konfiguracji ustawień, takich jak sterowniki urządzeń do załadowania i dostępne rozdzielczości wyświetlania. To poddrzewo wchodzi w skład poddrzewa *HKEY_LOCAL_MACHINE* i wskazuje klucz *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current*.

źródło: opracowanie własne na podstawie http://technet.microsoft.com



Ryc. 1. Okno *Edytor rejestru* widok klucza hivelist
źródło (ryc. 1–9): autor
Fig. 1. *Windows Registry editor hivelist key view*

Tabela 2

Pliki zapisane na dysku twardym oraz ich powiązania z odpowiednimi gałęziami w rejestrze Windows
Files recorded on hard disk and connected with Windows register hives

Nazwa pliku	Opis zawartości
system, system.sav, system.log	HKLM\SYSTEM
sam, sam.log	HKLM\SECURITY\SAM
software, software.sav, software.log	HKLM\SOFTWARE, HKCR
security, security.log	HKLM\SECURITY
default	HKU\.DEFAULT
C:\Documents and settings-\Nazwa użytkownika-\ntuser.datuser.dat.log	HKCU, HKU\-identyfikator użytkownika (SID)-

źródło (tab. 2–17): opracowanie własne

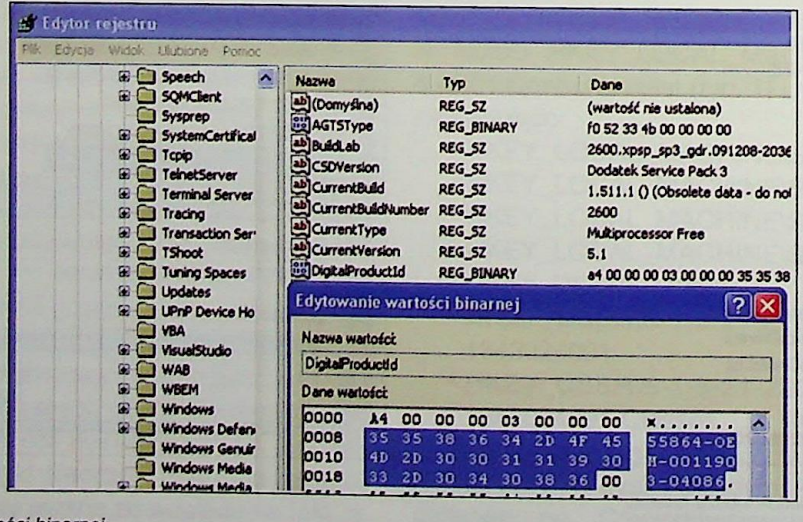
- software – plik główny,
- software.log – wprowadzane zmiany,
- software.sav – kopia.

Powiązanie plików zapisanych na dysku twardym z kluczami rejestru przedstawia tabela 2.

Każdy klucz lub podklucz może zawierać kilka wpisów (lub być pusty). Wszystkie wpisy składają się z trzech członów: nazwy, typu i danych.

Przykładowe typy danych używanych w rejestrze[4]:

- *REG_BINARY* – wartość binarna[5] wyświetlana przez edytor rejestru w notacji heksadecymalnej[6], np. klucz *HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\DigitalProductId*; dane *a4 00 00 00 03 00 00 00 38 39 35 38 33 2d (...)*[7]. Wartość binarną można jednak w niektórych przypadkach podejrzeć, uruchamiając zakładkę *Edytowanie wartości binarnej* (ryc. 2).
- *REG_DWORD* – dane zapisane w postaci liczby o długości 4 bajtów (32 bity), wyświetlane przez edytor rejestru w notacji binarnej, szesnastkowej lub dziesiętnej[8], np. klucz *HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\InstallDate*; dane szesnastkowe *4ac3906f*, dziesiętne *1254330479*.
- *REG_EXPAND_SZ* – ciąg danych o zmiennej długości obliczany, gdy program bądź usługa z nich korzysta, np. klucz *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*; dane *%USERPROFILE%\Desktop*.
- *REG_MULTI_SZ* – ciąg wielokrotny. Wartości przedstawione są w formie możliwej do odczytania przez użytkowników. Wpisy są oddzielone spacjami, przecinkami lub innymi znacznikami, np. klucz *HKLM\SYSTEM\ControlSet001\Enum\IDE\CdRomLITE-ON_DVD_SOHD-16P9S*; dane *IDE\CdRomLITE-ON_DVD_SOHD-*



Ryc. 2. Okno *Edytowanie wartości binarnej*
Fig. 2. *Windows Editing of the binary value*

-16P9S_____FS09____IDE\LITE-ON_DVD_SOHD-16P9S (...).

- *REG_SZ* – ciąg tekstowy o stałej długości, np. klucz: *HKLM\SOFTWARE\Symantec\SymNetDrv\SymIM*; dane *C:\Program Files(x86)\Norton AntiVirus\Engine64\16.7.2.11*.

Informacje podstawowe – X-Ways Forensics

X-Ways Forensics jest zaawansowanym środowiskiem pracy dla specjalistów z zakresu informatyki śledczej, oferującym duże możliwości analizy danych. Za pomocą programu można m.in.: powielać cyfrowy materiał w postaci klonów lub obrazów, odzyskiwać dane, analizować zawartość nośników, w tym również dokonywać podglądu poszczególnych plików np. obrazów graficznych, archiwów, kluczy systemowych[9].

Raportowanie oraz analiza rejestru Windows za pomocą programu X-Ways Forensics

Analizę klucza systemowego MS Windows za pomocą X-Ways Forensics można przeprowadzić na dwa sposoby:

- manualne wskazanie konkretnego pliku (istnieje niebezpieczeństwo pominięcia informacji zapisanych w innych niż standardowa lokalizacja),
- wykorzystanie trybu automatycznego z filtrem Typ/Windows Registry i opcją Explore Recursively (ryc. 3), który pozwala ujawniać wszystkie (widoczne, skasowane, w tym wyeksportowane) pliki rejestru na danej partycji.

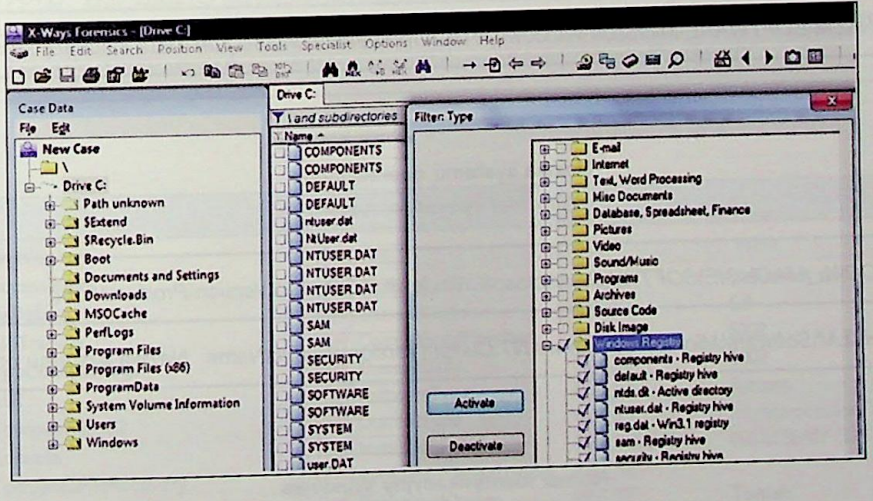
Kolejny krok to wskazanie odpowiedniego pliku zawierającego klucz rejestru. Po tej czynności za pomocą prawego przycisku myszy należy otworzyć podręczne *Menu* i wybrać opcję *Create Raport*. Wzorzec raportu Rejestru Windows ma nazwę *Reg Report.txt*. Jest to edytowalny plik tekstowy. Następnie należy wskazać nazwę oraz miejsce, w którym ma być zapisany raport w formacie HTML. Program, tworząc zestawienie na podstawie zdefiniowanego pliku *Reg Report.txt*, zwraca wartości zadeklarowanych kluczy w postaci:

HKLM\SOFTWARE\Microsoft\Windows NT\
\CurrentVersion\ProductName
2009-10-14 03:13:40 Operating system: Name
Windows Vista (TM) Home Premium

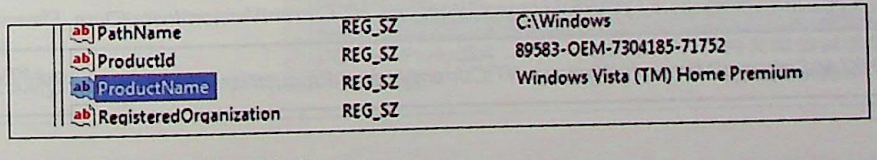
W przypadku wystąpienia *n* wartości danego podklucza zostanie on umieszczony *n* razy w raporcie.

Poniżej przedstawiono klucz *HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion* zawierający informacje o systemie Windows możliwe do odczytania z poziomu programu *Edytor rejestru* (ryc. 4).

Jak już wspomniano, plik wzorca raportu może być edytowany. Funkcjonalność ta może okazać się przydatna, gdy poszukuje się informacji fragmentarycznych np. tylko danych typu: nazwa systemu operacyjnego, data instalacji itp. lub danych pierwotnie nieprzewidzianych w raporcie przez producentów oprogramowania.



Ryc. 3. Okno filtru Type programu X-Ways Forensics
Fig. 3. *Windows of filter Type program X-Ways Forensics*

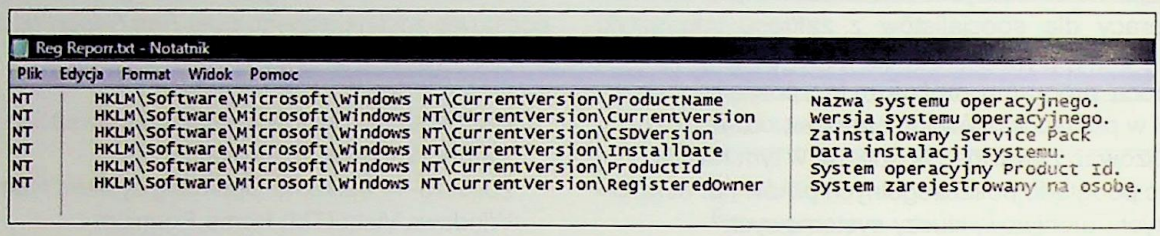


Ryc. 4. Rejestr Windows – podgląd z programu *Edytor rejestru*
Fig. 4. *Windows register of preview from program Register Viwer*

W tym celu należy odszukać plik *Reg Report.txt* w folderze *C:\Program Files\X-Ways Forensics*. Składa się on z następujących trzech elementów. Pierwsza część określa system operacyjny NT, druga część to wartość klucza z rejestru, który będzie wyświetlony, trzecia część to opis (ryc. 5).

Zmieniając oraz dodając elementy do tego pliku, można dowolnie modyfikować późniejszy raport tak, aby dostosować go do własnych potrzeb.

Poniżej przedstawiono przykłady modyfikacji oraz korelacji poszczególnych kluczy w rejestrze z informacjami, które można uzyskać poprzez tradycyjne przeglądanie działającego systemu Windows[10]. W celu łatwiejszego zrozumienia, dane odnośnie do kluczy rejestru będą podawane w tabelkach w oryginalnym brzmieniu – wiersz „Rejestr" oraz zmodyfikowane gotowe do użycia w programie X-Ways Forensics – wiersz „X-Ways" (tab. 3–17).



Ryc. 5. Fragment pliku *Reg Report.txt* z zamienionymi na język polski opisami
Fig. 5. *Fragment of file Reg Report.txt with descriptions converted into Polish*

Podstawowe informacje o systemie operacyjnym

Tabela 3

Data instalacji systemu operacyjnego
Date of operation system installation

Rejestr	*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate*
X-Ways	NT *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate* Data instalacji systemu operacyjnego

Tabela 4

Nazwa systemu operacyjnego
Name of operation system

Rejestr	*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName*
X-Ways	NT *HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProductName* Nazwa systemu operacyjnego

Tabela 5

Numer identyfikacyjny Windows
Windows ID number

Rejestr	*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate*
X-Ways	NT *HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProductName* Numer identyfikacyjny Windows

W doprecyzowaniu wersji produktu Windows XP można również przeanalizować zawartość pliku szablonu domyślnych uprawnień systemu plików NTFS *defltkw.inf* znajdującego się w folderze *WINDOWS\inf*.

Dla wersji Windows Home Edition widnieje w nim zapis NT 5.1 Personal Edition

(c) Microsoft Corporation 1997–2000
Security Configuration Template for Security Configuration Manager
Template Name: DefltWK.INF
Template Version: 05.10.DP.0000
Default Security for NT 5.1 Personal Edition.

Potwierdza to również plik *eula.txt* znajdujący się w folderze *WINDOWS\system32*, w którym znajduje się zapis Microsoft(r) Windows(r) XP Home Edition.

W przypadku wersji Windows Professional zapisy będą wyglądać odpowiednio:

Plik *defltkw.inf*:
(c) Microsoft Corporation 1997–2000
Security Configuration Template for Security Configuration Editor
Template Name: DefltWK.INF
Template Version: 05.10.DW.0000
Default Security for Windows NT 5.1 Professional
Plik *eula.txt*: Microsoft Windows XP Professional.

Przykładowe oznaczenia Windows Product ID[11]:
xxxxx-OEM-xxxxxxx-xxxxx – wersja OEM,
xxxxx-640-xxxxxxx-xxxxx – wersja BOX,
xxxxx-647-xxxxxxx-xxxxx – wersja VLK.

Tabela 6

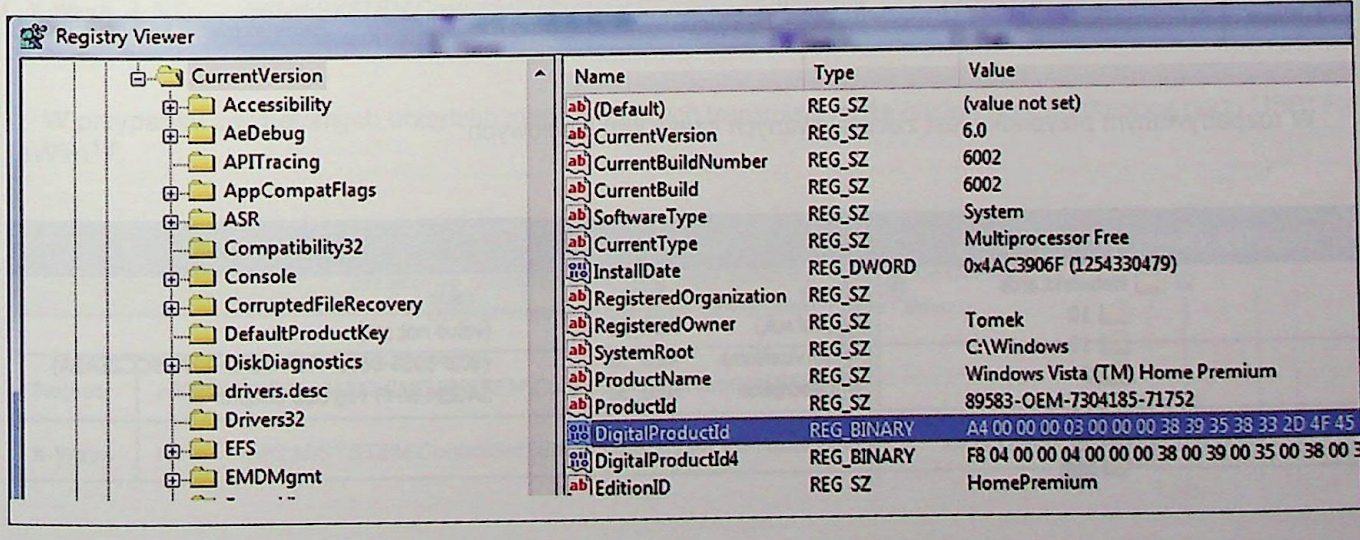
Windows Product ID

Rejestr	*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProductID*	
X-Ways	NT *HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProductId*	Windows Product ID

Tabela 7

Klucz Windows
Key Windows

Rejestr	*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductID*	
X-Ways	NT *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductID*	Klucz Windows



Ryc. 6. Klucz produktu Windows zapisany w rejestrze
Fig. 6. *Windows Key recorded in register*

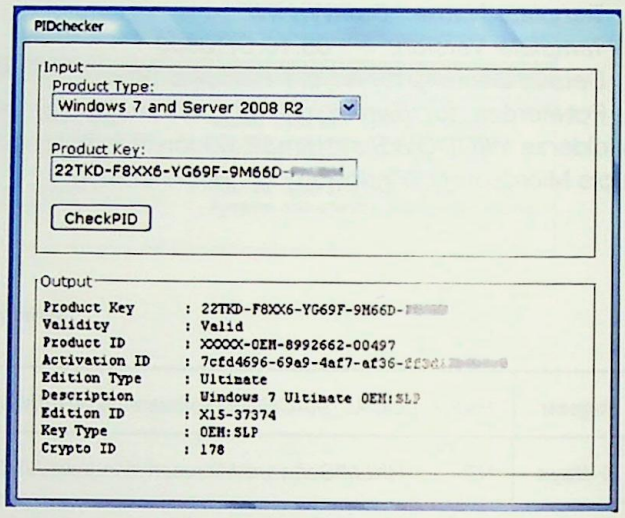
Tabela 8

Zainstalowane oprogramowanie
Installed software

Rejestr	*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*
X-Ways	NT *HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall*\DisplayName* Local machine: installed programs: name

W rejestrze klucz produktu Windows widnieje jako wartość binarna, natomiast w raporcie otrzymujemy przekonwertowane dane[12] (ryc. 6).

W celu identyfikacji Windows 7, Vista, Server 2008, posiadając jedynie Klucz Windows, można posłużyć się stronami typu Windows PIDchecker (*http://d--fault.nl/pidcheck/*). Po wpisaniu klucza produktu Windows otrzymuje się takie dane jak: Windows Product ID nazwę Windows oraz rodzaj licencji (ryc. 7).



Ryc. 7. Widok Windows PIDchecker z kluczem produktu Windows i dodatkowymi informacjami na temat wersji
Fig. 7. *View of Windows PIDchecker with Windows CD Key and more information about MS version*

Informacje na temat kart sieciowych

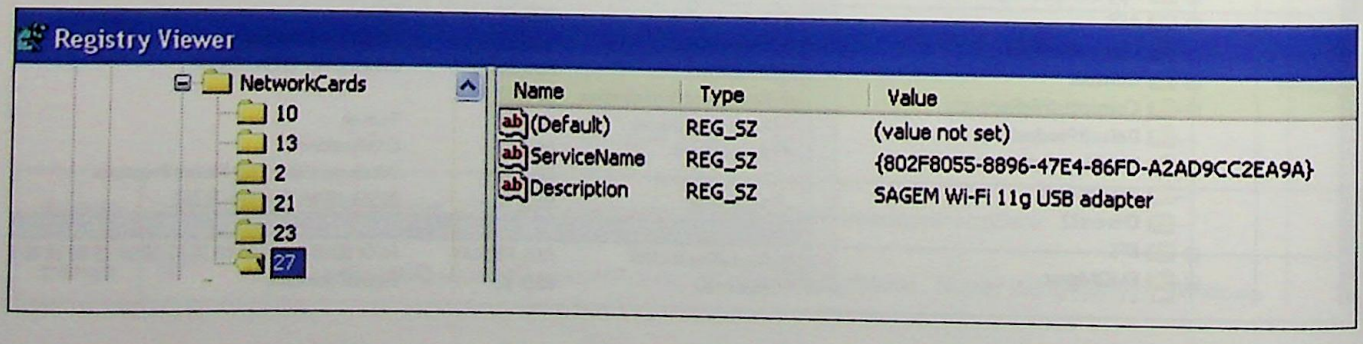
W rejestrze systemu można znaleźć informacje na temat zainstalowanych kart sieciowych. W przypadku fizycznego wyjęcia karty dane na jej temat są nadal zapisane w rejestrze. Karty sieciowe numerowane są od 1 w górę, ilość numerów oznacza liczbę zainstalowanych urządzeń. Dane te znajdują się w kluczu przedstawionym w tabeli 9 (ryc. 8).

Tabela 9

Zainstalowane karty sieciowe
Installed network cards

Rejestr	*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards*
X-Ways	NT *HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkCards* Zainstalowane karty sieciowe

W rozpatrywanym przypadku jest zainstalowanych sześć kart sieciowych.



Ryc. 8. Widok klucza rejestru z zainstalowanymi kartami sieciowymi
Fig. 8. *View of register key with network cards installed*

Raport z programu X-Ways Forensics wygląda następująco:

HKLM\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\10\Description
2007-10-10 12:09:18
Model description of installed network card Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC

HKLM\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\13\Description
2008-08-22 09:31:55
Model description of installed network card
Karta Realtek RTL8029(AS) PCI Ethernet Adapter

HKLM\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\2\Description
2007-10-10 12:10:13
Model description of installed network card
Karta sieciowa 1394

HKLM\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\21\Description
2009-10-19 09:55:06
Model description of installed network card
Sony Ericsson Device 0016 USB Ethernet Emulation (NDIS 5)

HKLM\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\23\Description
2009-06-17 10:32:27
Model description of installed network card
LGE Mobile USB WMC Ethernet (NDIS 5)

HKLM\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\27\Description
2009-11-06 10:00:43
Model description of installed network card
SAGEM Wi-Fi 11g USB adapter

Powyższe dane można uzyskać w *Panel sterowania/System/Menadżer urządzeń*, następnie wybierając właściwości kart sieciowych. Jednak nie wszystkie urządzenia sieciowe zapisują informacje o swoich sterownikach w podkluczu *NetworkCards*. Niektóre z nich (przeważnie USB) można znaleźć w innych lokalizacjach.

Dane dotyczące zainstalowanych urządzeń

Informacje o zainstalowanym sprzęcie znajdują się w podkluczu *HKLM\SYSTEM\CurrentControlSet\Enum*. W przypadku urządzeń magazynujących należy w pierwszej kolejności rozpatrzyć, za pomocą jakiego interfejsu urządzenie to zostało połączone z komputerem. W przypadku standardów ATA/SATA zainstalowane urządzenia odnajduje się w podkluczu IDE.

Tabela 10

Urządzenia typu CD, DVD, HDD (ATA/SATA)
CD, DVD, HDD (ATA/SATA) devices

Rejestr	*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\IDE*
X-Ways	NT *HKLM\SYSTEM\ControlSet*\Enum\IDE**\FriendlyNameName* Urządzenie IDE

W przypadku zewnętrznych urządzeń magazynujących transmisja może następować za pomocą portu USB/ FireWire[13].

Tabela 11

Urządzenia magazynujące USB typu pendrive, dyski w kieszeniach
USB storage devices such as pendrive, pocket drive

Rejestr	*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR*
X-Ways	NT *HKLM\SYSTEM\ControlSet*\Enum\USBSTOR**\FriendlyName* Urządzenie magazynujące USB

Tabela 12

Urządzenia podłączone poprzez FireWire
Devices connected by FireWire

Rejestr	*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\1394*
X-Ways	NT *HKLM\SYSTEM\ControlSet*\Enum\1394**\HardwareID* Urządzenie magazynujące podłączone poprzez FireWire

Tabela 13

Stacja FDD
FDD station

Rejestr	*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum*
X-Ways	NT *HKLM\SYSTEM\ControlSet*\Enum\FDC**\HardwareID* Stacja dyskietek

Tabela 14

Drukarki USB
USB printers

Rejestr	*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBPRINT*
X-Ways	NT *HKLM\SYSTEM\ControlSet*\Enum\USBPRINT**\FriendlyName* Drukarki USB

Dane dotyczące użytkownika

Informacje dotyczące konta użytkownika można odnaleźć w plikach: *ntuser.dat*. Zawierają one takie dane jak ostatnio uruchomione, za pomocą Windows, programy czy też dokumenty. Istotne mogą okazać się przypisane operacjom daty systemowe, wraz z danymi o zainstalowanym oprogramowaniu (*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*\DisplayName*) można dokonać identyfikacji zainstalowanych oraz najczęściej używanych programów[14].

Tabela 15

Historia otwieranych dokumentów
History of opened documents

Rejestr	*HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*
X-Ways	NT *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs** Historia otwieranych dokumentów

Tabela 16

Programy w autostarcie
Programmes in autostart

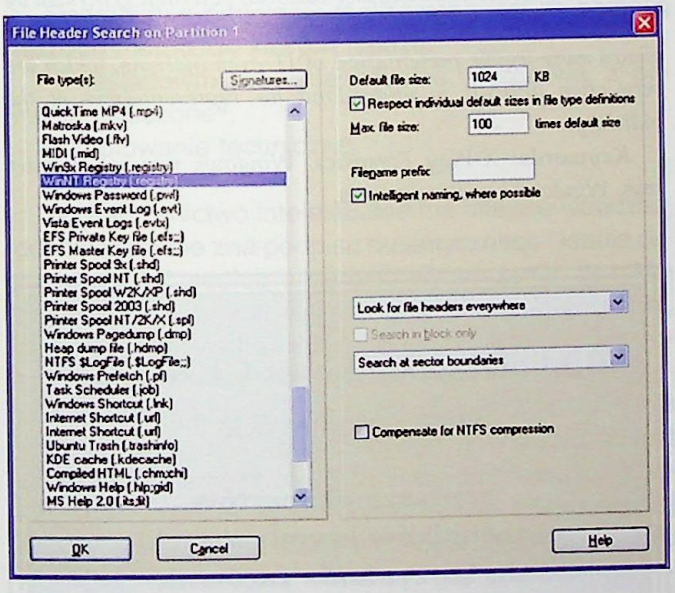
Rejestr	*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*
X-Ways	NT *HKLM\Software\Microsoft\Windows\CurrentVersion\Run** Programy uruchamiane przy starcie systemu

Tabela 17

Historia uruchamianych programów
History of launched programmes

Rejestr	*HKEY_CURRENT_USER\ SOFTWARE \ Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count*
X-Ways	NT HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count* Historia uruchamianych programów

Za pomocą X-Ways Forensics można również odzyskiwać pliki, w tym pliki rejestru. Jedną z metod jest funkcja *File header signature search*. Opcja ta ma duże możliwości konfiguracyjne polegające m.in. na ustawieniu maksymalnej wielkości odzyskiwanych plików, obszaru przeszukania (m.in. wyboru obszaru *free space*, przestrzeni zaalokowanych czy też całej powierzchni nośnika). Pliki odzyskane za pomocą tej funkcji są umieszczane w utworzonym przez program wirtualnym katalogu badanego nośnika (ryc. 9).



Ryc. 9. Okno opcji odzyskiwania *File Header Signature Search* programu X-Ways Forensics
Fig. 9. *Windows of recovery options File Header Signature Search program X-Ways Forensics*

W przypadku plików skasowanych za pomocą kosza systemowego zdołano przywrócić dane oraz odczytać z nich informacje, jednak już po szybkim (dostępnym z poziomu MS Windows) sformatowaniu nie były one czytelne dla programu.

Podsumowanie

Rejestr systemu Windows to znaczące źródło informacji o badanym sprzęcie, jego użytkowniku, systemie operacyjnym, oprogramowaniu, urządzeniach USB oraz wielu innych przydatnych, z punktu widzenia informatyki śledczej, informacjach. Dlatego też podczas interpretacji zapisanych za pomocą systemu operacyjnego Windows danych nie można pominąć dokładnej jego analizy. Natomiast elastyczny mechanizm raportowania, zaimplementowany w programie X-Ways Forensics, pozwala na tworzenie własnych przejrzystych szablonów mogących znacznie wspomóc pracę eksperta. Wzorzec raportu Rejestru Windows ma nazwę *Reg Report.txt*, w momencie zakupu programu jest zdefiniowany w języku angielskim. Programiści z X-Ways Software Technology AG przewidzieli jego rozbudowę i edycję, dzięki zapisaniu go w tekstowym pliku edytowalnym. Znajomość kluczy rejestru umożliwia dostosowanie raportów do własnych potrzeb i uwzględnienie danych nieprzewidzianych przez autorów programu.

Tomasz Pawlicki

PRZYPISY

1 Wszystkie daty/czas zapisywane w systemie Windows są pobierane z urządzenia znajdującego się na płycie głównej komputera tzw. zegara systemowego.
2 ang. *hives* – ul, gałąź (w rejestrze systemu z rodziny NT).
3 W trakcie tworzenia artykułu LK KWP Łódź nie dysponowało systemem Windows 7.
4 **J. Honeycutt**: Microsoft Windows XP Registry Guide, Washington 2003, s. 24–25 (tłumaczenie autora).
5 System binarny (dwójkowy) to system liczbowy, w którym podstawą pozycji są kolejne potęgi liczby 2. Do zapisu liczb potrzebne są więc tylko dwie cyfry: 0 i 1.
6 Heksadecymalny – szesnastkowy system liczbowy, w którym podstawą pozycji są kolejne potęgi liczby 16. Do zapisu liczb w tym systemie potrzebnych jest szesnaście cyfr. Poza cyframi dziesiętnymi od 0 do 9 używa się pierwszych sześciu liter alfabetu łacińskiego: A, B, C, D, E, F (duże i małe litery).
7 Nie wstawiono całego ciągu znaków.
8 Dziesiętny system liczbowy (decymalny) – system liczbowy, w którym podstawą pozycji są kolejne potęgi licz-

by 10. Do zapisu liczb potrzebnych jest więc w nim 10 cyfr: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

[9] Podstawowa analiza danych za pomocą programu X-Ways Forensics została opisana w pracach zaliczeniowych Błażeja Karpińskiego „Wykorzystanie programu X-Ways Forensics w opracowywaniu ekspertyz z zakresu badań sprzętu komputerowego" oraz Marka Liszkiewicza „Wykorzystanie aplikacji X-Ways Forensics w kryminalistycznych badaniach cyfrowych nośników danych – aspekty praktyczne".

[10] W przypadku analizy materiału dowodowego i konieczności pracy na uruchomionym systemie należy wykonać jego klon.

[11] Szerzej na ten temat można dowiedzieć się ze stron: http://wiki.lunarsoft.net/wiki/Product_IDs#.27xxxxx.27_—_the_Microsoft_Product_Code oraz http://www.tacktech.com/display.cfm?ttid=342.

[12] Dotyczy X-Ways Forensics od wersji 15.3.

[13] W trakcie pisania artykułu nie posiadano komputera z interfejsem eSATA.

[14] W tym celu dodatkowe informacje można uzyskać za pomocą programu Windows File Analyzer, który analizuje m.in. zawartość folderu *C:/Windows/Prefetch*.

BIBLIOGRAFIA

1. **Fleischmann S.**: X-Ways Software Technology AG X--Ways Forensics/WinHex. Manual book, Copyright © 1995-2009, X-Ways Software Technology AG.
2. **Honeycutt J.**: Microsoft Windows XP Registry Guide, Copyright (C) 2003 by Jerry Honeycutt.
3. **Chorążewski M., Zięba D.**: Rejestr Windows XP. Leksykon kieszonkowy, Helion 2004 r.
4. **Karpiński B.**: Wykorzystanie programu X-Ways Forensics w opracowywaniu ekspertyz z zakresu badań sprzętu komputerowego, praca zaliczeniowa, LK KWP Bydgoszcz, 2008 r.
5. **Liszkiewicz M.**: Wykorzystanie aplikacji X-Ways Forensics w kryminalistycznych badaniach cyfrowych nośników danych – aspekty praktyczne, praca zaliczeniowa, LK KWP Kraków, 2009 r.

Streszczenie

Praca ma na celu zapoznanie z podstawowymi informacjami na temat rejestru Windows, który może być jedynym źródłem pozwalającym na identyfikację sprzętu i aktywności użytkownika. Struktura rejestru składa się z pięciu kluczy głównych zawierających m.in.: informacje o systemie komputera lokalnego, ustawieniach pulpitu, połączeniach sieciowych, drukarkach i preferencjach programów oraz konfiguracji sprzętowej. Z uwagi na ten fakt działanie systemu zależy w znacznej mierze od ustawień zapisanych w rejestrze, a z punktu widzenia informatyki śledczej jest to bardzo cenny zbiór informacji przydatny w czasie przeprowadzanych badań. Ponieważ jednym z elementów pracy informatyka śledczego jest czytelne przedstawianie wyników, w artykule omówione są również możliwości edycyjne raportów generowanych przez program X-Ways Forensics. Takie dostosowanie programu pozwala na czytelniejszą prezentację wyników badań informatycznych, które są bardzo często niezrozumiałe dla przedstawicieli wymiaru sprawiedliwości.

Słowa kluczowe: *X-Ways Forensics, rejestr Windows, klucze rejestru, analiza rejestru Windows.*

Summary

The hereby article presents basic information on Windows register that may be the only source allowing identification of hardware and user activity. The structure of register comprises five main keys including: information on local computer system, desktop settings, network connections, printers and software preferences, as well as hardware configuration. Due to that fact, system operation largely depends on settings recorded in the register. From the point of view of IT investigations it is a very important collection of information useful in examinations. Because of the elements of IT expert it is clear presentation of results, the Article discusses also editorial potential generated by X-Way Forensics software. This adjustment of the programme allows more legible presentation of IT examinations, which are very often difficult to understand for representatives of the judiciary.

Keywords: *X-Way Forensics, Windows register, register keys, Windows register analysis.*