Modifying event log files in operating systems

S Markova¹, T Ya Druzhinina² and A A Zinoviev³

¹ Financial University under the Government of the Russian Federation, Moscow
² Irkutsk National Research Technical University, 83, Lermontova str., Irkutsk, 664074, Russia
³ Bratsk state university, Makarenko str., 40, Bratsk, 6656709, Russia

E-mail: SVMarkova@fa.ru

Abstract. This section is devoted to studying log files by working with the Windows event log. The practical examples will have one common goal: to find features of the Windows Logging Service that can be exploited by cybercriminals to commit computer crimes. Identification of such features will make the system more secure and increase the level of event registration.

1. Introduction
The experiments presented in this article are solutions to simple problems that arise when working with the event log. Windows computers were used to conduct the experiments [1, 2].

2. Terminating and resuming Windows event log
This experiment demonstrates the administrator’s ability to stop and resume the Windows Event Logging service. This experiment is quite simple but its significance is very great since it is fundamental for carrying out other actions. It is worth noting that while the Windows event log is running, the files it creates are read-only and cannot be modified [3].

There are two possible ways to carry out an experiment. Both of them give the same result.

The first is to use the services.msc command to select the Event Log service and stop it. You can also select the startup type to disable it and then the logging service will be disabled (Fig. 1).

![Figure 1. Pop-up window “services”](image-url)
The second is to change the Start DWORD parameter from 2 to 4 in the ‘HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog’ registry key as shown in Fig. 2.

After restarting the computer, there appears a message stating that at least one service has failed to start. This is a kind of warning to the user. This message will no longer appear after closing.

The logging service operation is resume by selecting the appropriate option in the pop-up box “services” or changing the parameter value in the registry.

3. Copying the event log
The experiment demonstrates whether it is possible to copy the files of the logging service while it is running. Specifically, it answers the following question: Is it possible to create an event log file that will be used on another computer afterwards?

In order to make a copy of the event log for subsequent work with it in another system, you just need to open the directory with the «System.evtx» (C:\Windows\System32\winevt\Logs) and copy it, for example, to the same folder [4, 5]. It is worth noting that you must also have administrator rights to copy. This operation can be performed while the logging service is running (Fig. 3).
The important feature of the two examples is the following: you can replace one event log with another if you know how to stop the event log on the computer and have the ability to copy it.

4. Replacing the event log from one computer to another
The following experiment shows the possibility of replacing one event log with another, as well as the possible errors that occur during this operation [6, 7].

This experiment is a combination of the first two operations. There are 2 different accounts on 2 different computers (or one, since the operation of the event log is bound to a specific isolated system created by the account). The logging service on Computer A stops and the system reboots. Next, you need to copy the event log from computer B and move it to computer A (Fig. 4).
After being restarted, computer A successfully receives a new event log without any error. Thus, you can formally change the events that occur on the computer by simply moving the event logs.

5. Changing the login code
This experiment is carried out using the WinHex program. The binary data contained in the Windows event log enables to identify a specific user who logged on to the system. The goal of the experiment is to change the input code for the entry about a specific user to appear in the event log regardless of whether he/she is logged in or not.

To change the contents of the event log files, we will use the editor “WinHex”. The data in the log file is a code that can be read using an ASCII table.

When modifying the account name and computer name, you should choose names having the same number of characters, specifically, if a computer name consists of 4 characters, then a new name must also have 4 characters. After restarting the system, the event log accepts the data change without error.

The importance of this experiment is that it shows that the data contained in the event log can be changed, and these changes will be accepted by the system.

6. Mechanism for assigning time to event in Windows OS logging service
This experiment considers how the event log timestamps and where it stores the specified entry. The used time format will also be analyzed.

We used the hex editor WinHex for this experiment. It was used to analyze the contents of the security log. In the event viewer, the date and time of a specific event were selected. The diligent search through the bytes has resulted in finding those that correspond to the date and time of the selected event. You could find out about this by changing the bytes to “0000-0000”, which was interpreted in the event log as “00:00:00 01/01/1970”, a so-called UNIX time being a system for describing moments in time adopted in UNIX; it is defined as the number of seconds since midnight, January 1, 1970.

Thus, the time entry in the event log consists of two repeating combinations of 8 bytes. For example, the time and date “18:47:24 01/11/2007” in hex will be “3C1F 2A47”. In the event log, you can find such an area that repeats twice, which indicates a time stamp (Figure 6).
7. Changing events chronology

The experiment attempts to change the time stamp of a specific event using WinHex.

This experiment is a direct extension of the previous one. Its essence is to detect any deviations in the operation of the event log when the log file content is altered. The alterations concern the temporal characteristics of the events. It is worth recalling that the time entry in the event log consists of two repeating combinations of 8 bytes. For example, the time and date “18:47:24 01/11/2007” in hexadecimal form, and, therefore, in the event log it will be “3C1F 2A47” (Fig. 7).

To change the time value for at least one second, it is necessary to replace the second byte with the next value in increments of 1. Thus, the record “3C1F 2A47” becomes “3D1F 2A47”. After restarting the system, the event time is changed to a new one. In this case, the event log does not issue any errors.
8. Conclusion
From the experiments presented in the article and carried out by the authors, a number of conclusions can be drawn: replacing one event log with another is possible when knowing how to stop the event log on a computer and have the ability to copy it. The data contained in the event log can be changed, and these changes will be accepted by the system. The time of events in the editor can be changed almost completely.

References
[1] Sysoev I A, Kondrat’ev V V, Zimina T I and Karlina A I 2018 Simulation of the Energy States of Electrolyzers with Roasted Anodes at Elevated Currents Metallurgist 61(11–12) 943–949
[2] Nemarov A A, Lebedev N V, Kondrat’ev V V, Korneyakov M V and Karlina A I 2016 Theoretical and experimental research of parameters of pneumatic aerators and elementary cycle flotation International Journal of Applied Engineering Research 11(20) 10222–10226
[3] Gura D A, Gura A Y, Volkova T A and Lipilin D A 2020 Recreational space as a factor of sustainable development of coastal ecosystems of the Krasnodar region IOP Conference Series: Earth and Environmental Science 579(1) 012007 doi:10.1088/1755-1315/579/1/012007
[4] Suslov K V, Solonina N N and Smirnov A S 2011 Smart meters for distributed filtering of high harmonics in Smart Grid International Conference on Power Engineering, Energy and Electrical Drives 6036552
[5] Suslov K V, Solonina N N and Smirnov A S 2014 Distributed power quality monitoring Proceedings of International Conference on Harmonics and Quality of Power pp 517–520 6842882
[6] Balanovskiy A E, Karlina A I, Kolosov A D, Karlina Y I 2021 Study of the effect of nanomodifiers from silicon production wastes on morphological form of gray cast iron graphites. CIS Iron and Steel Review 21 64–69
[7] Sivtsov A V, Elkin K S, Pan’kov V A, Karlina A I 2021 Specific Features of the Electric Mode of the Technological Process of Smelting of Commercial Silicon. Metallurgist 64(9-10) 923–930