A Computer Abusive Access Case Study Solved with Windows Registry Analysis

Dr. Pierluigi PERRONE PhD[1], Dr. Antonio SILVESTRE[2], Dr. Giuseppe TARASCHI[2]
[1]LUISS University, Rome, Italy
pperrone@luiss.it
[2]Technical Investigation Unit, Arma dei Carabinieri, Naples, Italy
antonio1.silvestre@carabinieri.it, giuseppe.taraschi@carabinieri.it

Abstract

This article has the aim to describe a real forensics investigation case. An employee is accused of revealing confidential company information related to a project he was working on using a company computer registered to the company domain. The accused defends himself, insinuating the doubt that it could have been anyone because his office is always open. After the seizure and acquisition of a company hard drive, the investigators want to find some evidences related the Windows system registry. In particular, the analysis will be aimed at identifying what were the energy and standby settings at the time of the seizure and if upon reactivation of the screen, the password was requested and needed to access the system.

Index terms: Cybersecurity, Digital Forensics, Digital Investigation

1. Introduction

The recent technological evolutions have led to the birth of various electronic devices that until a few years ago were present only in the collective imagination. Just think of the so-called wearable devices (smartwatches, fitness bands), drones, modern sensor-rich smartphones and infotainment systems in vehicles. All these devices have the ability to generate/store data and this last aspect has assumed a role of primary importance in the judicial field. In fact, it is increasingly common to find their presence at the crime scene, which is why the need to apply a scientific methodology, the so-called. Digital Forensics so that the aforementioned data can represent evidence that can be used in the trial for the resolution of cases.

The purpose of this article is to show how it is possible to trace information of investigative interest by analyzing the Windows system registry (hierarchical database) through a forensic copy.
An employee is accused of revealing confidential company information related to a project he was working on using a company computer registered to the company domain.
The accused defends himself, insinuating the doubt that it could have been anyone because his office is always open.

In particular, we will look for any traces left by those who would have violated the device and in particular we want to understand if the computer automatically went into protection when left unattended. The version of the operating system in question is Windows 10 Pro. Specifically, the analysis will be aimed to identify:

- what were the energy and standby settings at the time of the seizure;
- if upon reactivation of the screen the password was requested and needed to access the system.

2. Windows registry structure

Before proceeding with the identification of what is of interest, it is necessary to mention the structure of the Windows registry [1].

"The registry is a hierarchical database that contains data critical to the operation of Windows, the applications and services it runs. The structure is of the tree type in which each node is called a key. Each key can contain both subkeys and data items called values. The presence or absence of a key in the configuration registry tells a specific application how to operate. A key can have any number of values, and the values can be in any format. Each key has a name consisting of one or more printable characters that are not case sensitive, they cannot include the back slash (\) character, but you can use any other printable character. While the names of the values and data can include the aforementioned character. Also, the name of each subkey is unique with respect to the hierarchically superior key. Finally, a registry tree can be 512 levels long, and up to 32 levels can be created at a time through a single registry API call."

3. Analysis of personal computer energy and standby settings

As far as the operations to be carried out, first of all a forensic copy of the hard disk contained in the PC will be acquired, in compliance with the **ISO/IEC 27037:2012** [2], which provides a guide to identifying, collecting, acquiring, managing and retaining digital evidence.

Subsequently, the examiner will continue to identify what is of interest in compliance with the **ISO/IEC 27042:2015** [3]; in this specific case, since the examiner is looking for data within the Windows system registry, they can be identified in the following path: ***C:\Windows\System32\config***.

For the identification and interpretation of the data contained in the aforementioned path, the Magnet Axiom software was used, but other different software for forensic use with both free and commercial licenses could be used.

The Windows component for managing energy plans analyzes the system registry to know the configuration parameters set by the user. There are a few predefined combinations that the user can choose from, each identified by unique alphanumeric keys (GUID). To find out the value of these keys and which of these has been chosen for Windows operation, it is possible to run the command *powercfg.exe /list* (Fig.1):

```
C:\Users\Administrator>powercfg.exe /list

Combinazioni risparmio energia esistenti (* attive)
-----------------------------------
GUID combinazione risparmio energia: 21d7866e-c0d2-44cd-b659-9c6656d25187  (Massimo risparmio energetico)
GUID combinazione risparmio energia: 381b4222-f694-41f0-9685-ff5bb260df2e  (Bilanciato)
GUID combinazione risparmio energia: 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c  (Prestazioni elevate) *
GUID combinazione risparmio energia: a1841308-3541-4fab-bc81-f71556f20b4a  (Risparmio di energia)
GUID combinazione risparmio energia: eac52e11-9bcc-44e4-8877-1d45575e9a6b  (Riproduzione video)
GUID combinazione risparmio energia: ebc794ee-dc6a-479d-ae56-d8210598cb2c  (Prestazioni massime)
GUID combinazione risparmio energia: f43d1b91-33aa-4006-987e-11408ac763f0  (Origine alimentazione ottimiz)
GUID combinazione risparmio energia: fb7defd7-548e-46d6-98a9-e44d25599e7e  (Timer disattivati (Presentaz))

C:\Users\Administrator>
```

Fig. 1. Example command to display energy plans on Windows

In the case of the analyzed disk, the energy plan with GUID **8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c** corresponding to that of **high performance** was set (the asterisk * means active).

The Windows system registry, indeed, highlighted in the subkey Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\User\PowerSchemes that the value with name "ActivePowerScheme" is set to **8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c** (Fig.2):

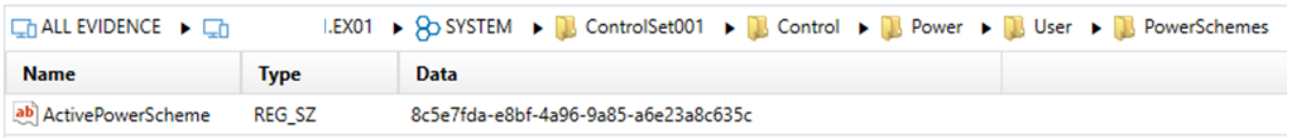

Fig. 2. Windows identification key for the high-performance energy plan

It should be noted that this energy plan has this default values:

– turns off the screen after 15 minutes of inactivity;

– never puts the PC to sleep.

All the different possible energy combinations are reported in the configuration register as subkeys of "PowerSchemes" (Fig. 3).

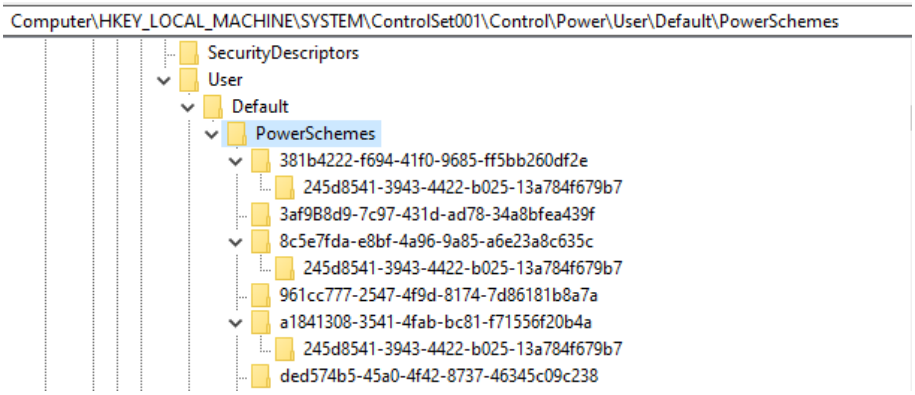

Fig. 3. Windows default energy plan keys

If the default values of the selected energy plan are changed, additional subkeys will be created in the system registry with the resulting value edited. Possible subkeys are listed in the path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\PowerSettings (Fig. 4):

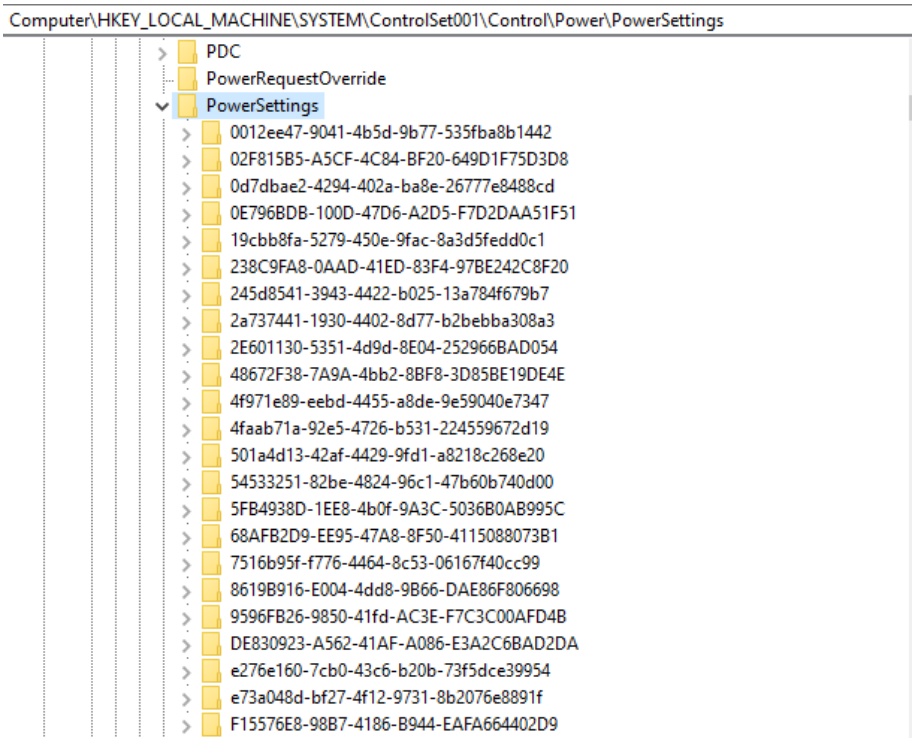

Fig. 4. Possible energy plans subkeys

For the forensic case in argument, it is therefore necessary to examine the registry key "Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\User\PowerSchemes". For a better understanding, we will show two different cases:

1. the default settings of the high-performance energy plan are set;
2. high-performance energy plan has its standard values edited.

First case:

Energy plan **8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c** - High performance – with default settings (Fig. 5).

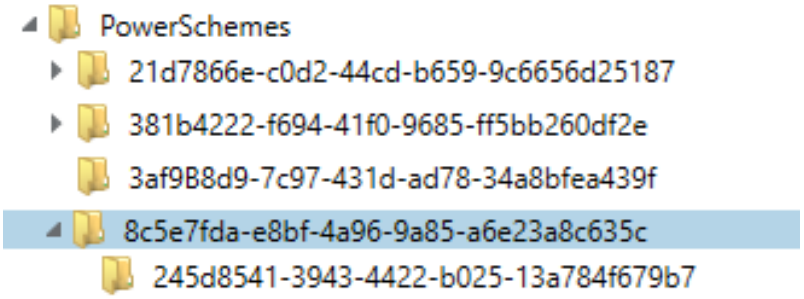

Fig. 5. High performance energy plan default settings

In Figure 5, there is only one subkey named **245d8541-3943-4422-b025-13a784f679b7** that references the default settings.

Second case:

Energy plan **8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c** - High performance - with default settings edited. To emulate these settings another PC was used with the same Windows 10 Pro operating system as the PC under examination and the following values were set (Fig. 6):

– screen deactivation (10 minutes – 600 seconds);
– computer suspension (15 minutes – 900 seconds).

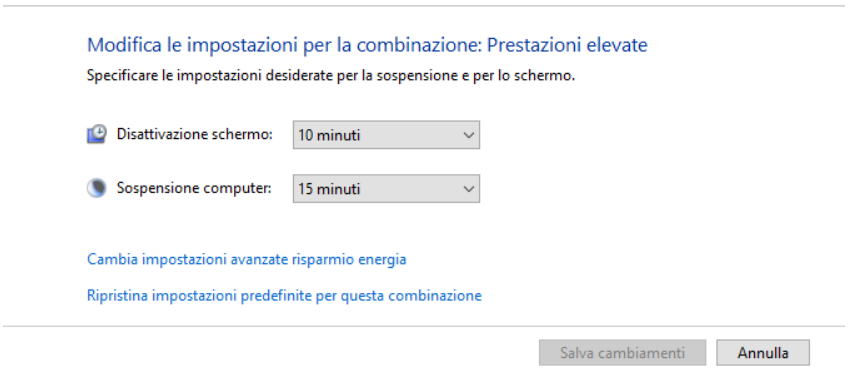

Fig. 6. High performance energy plan set values (different from default)

Below we report the changes that take place in the Windows registry (Fig. 7):

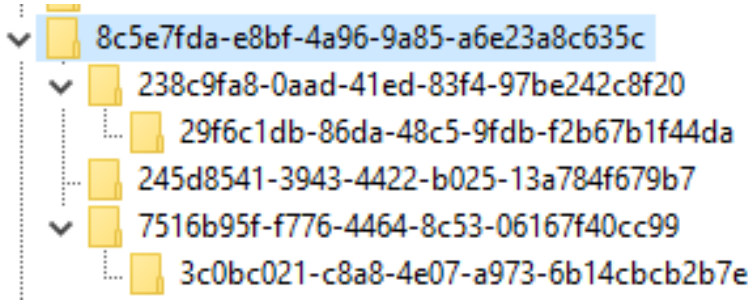

Fig. 7. Additional subkeys for the high-performance energy plan

The above settings lead to the creation of the:

– **238c9fa8-0aad-41ed-83f4-97be242c8f20** key with the **29f6c1db-86da-48c5-9fdb-f2b67b1f44da** subkey (which refers to the computer suspension settings) in which the time expressed in seconds (900) is reported in the ACSettingIndex item of suspending the computer (Fig. 8);

Fig. 8. Value expressed in seconds for computer suspension

– **7516b95f-f776-4464-8c53-06167f40cc99** key with the **3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e** subkey (which refers to the screen off setting) in which the time expressed in seconds (600) is reported in the ACSettingIndex item screen deactivation (Fig. 9).

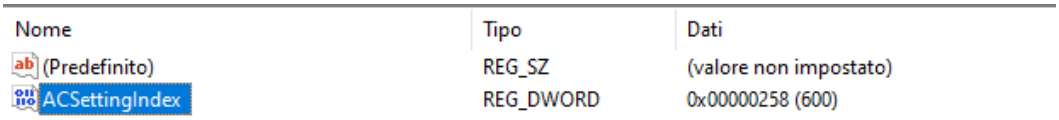

Fig. 9. Value expressed in seconds for screen deactivation

The settings on the PC under examination were the default ones due to the absence of the aforementioned additional keys. The default values for High performance plan are **15 minutes** (**900 second**) for screen deactivation and **never** for computer suspension.

We report for comparison:

– the system registry where the default settings of the High-performance energy plan are visible:

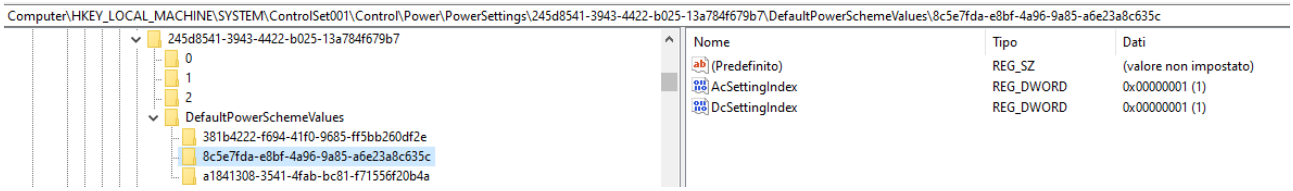

Fig. 10. Default setting of the high-performance energy plan

– the excerpt from the system registry extrapolated using the analysis software, and in which the registry key for the default settings on the PC under examination are visible:

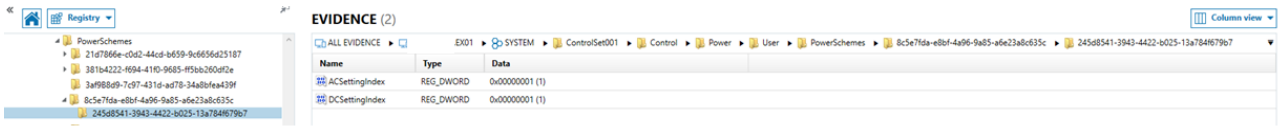

Fig. 11. Default high performance energy plan of the PC under test

4. Analysis to find if the password was required to enter the system when the screen was reactivated

We proceeded to verify whether, after the period of screen deactivation (15 minutes – 900 seconds), the password for accessing the system was requested.

For Windows 10 Pro system, the password prompt setting, after screen off period, is done by default after a password is associated with an account. All this occurs through the following option accessible from the *Settings / Account / Access options* menu (Fig. 12):

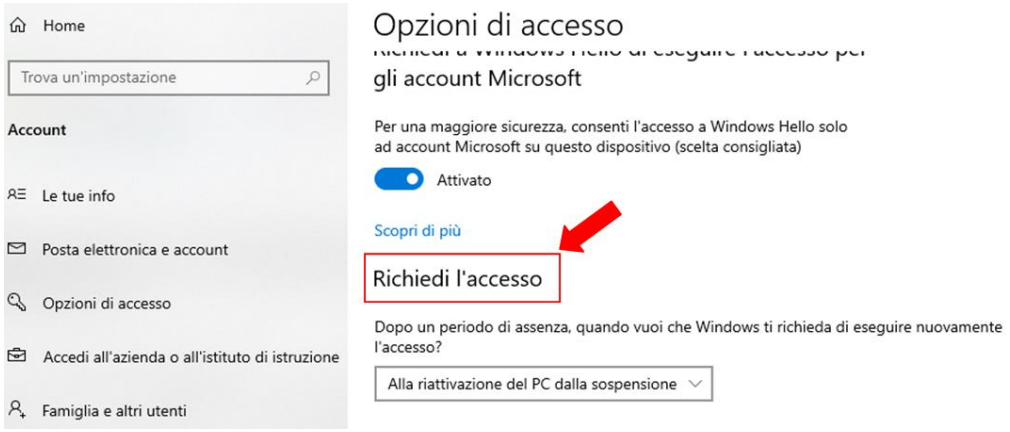

Fig. 12. Default high performance energy plan of the PC under examination

The drop-down menu in access request has two options (Fig. 12): the default one called "When the PC wakes up from suspension" and the one with "Never".

The first option, a few seconds after the screen has been deactivated, requires the user password upon reactivation, while the second option "Never", even after the screen has been deactivated, no longer shows the password entry screen. Also, in this case it is possible to verify this setting, by analyzing the Windows system registry.

In fact, if the default settings for the energy plan in argument, identified by the key **8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c**, are not changed, no subkey will be created; otherwise if the default settings are modified the subkey **0e796bdb-100d-47d6- a2d5-f7d2daa51f51** will be created. This subkey, after its creation, will remain present in the system registry unless default settings are restored. Fig. 13 shows the case in which default settings have been modified: the subkey **0e796bdb-100d-47d6- a2d5-f7d2daa51f51** is created with the "ACSettingIndex" item set to "Never" (value equal to 0); if it had been set to 1 it would have had the meaning of “When PC wakes up from sleep”.

Fig. 13. Access request set to “Never”

The settings on the PC under examination were the default ones (When PC wakes up from sleep) due to the absence of the aforementioned additional subkey. Therefore, password entry was required after the screen off period.

To know the default values relating to the access request, you need to examine the values of the key **0e796bdb-100d-47d6-a2d5-f7d2daa51f51** which we find under the path "Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\User\PowerSchemes".

The values found in the PC under examination extrapolated by the analysis software are reported:

– in the path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\User\PowerSchemes\8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c" only one subkey named **245d8541-3943-4422-b025-13a784f679b7** is visible without the aforementioned **0e796bdb-100d-47d6-a2d5-f7d2daa51f51**. All to demonstrate that no changes have been made;

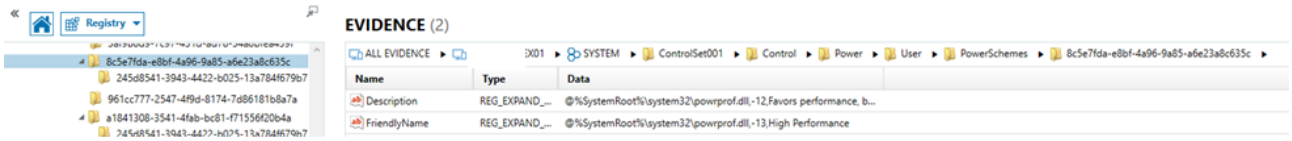

Fig. 14. Password request when target PC wakes up

– to find out the default values, analyze the path "Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51" where for the settings relating to the **high-performance** energy plan, it is set the value (1) of ACSettingIndex and then Request access/When PC wakes up from suspension:

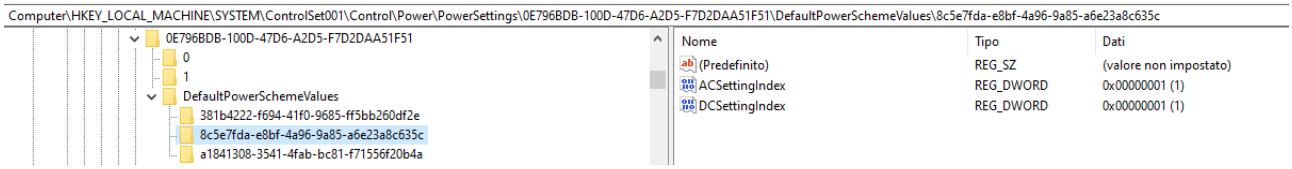

Fig. 15. Default setting for the password request when restarting the PC

5. Conclusion

In conclusion, it has been demonstrated that the possible execution of operations on the PC under examination could only be carried out by those in possession of the access password of the account in argument.

References

[1]. https://docs.microsoft.com/it-it/windows/win32/sysinfo/structure-of-the-registry.
[2]. Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO/IEC 27037:2012.
[3]. Guidelines for the analysis and interpretation of digital evidence. ISO/IEC 27042:2015.