AIM:

Extract the **SYSTEM** and **SOFTWARE** hives from your Windows system. (*Hint:  look in* ***/Windows/System32/Config***). You can use any Registry parser (E.g.  Registry Ripper/Registry Explorer) and then select the appropriate hive file to answer these questions (put a snapshot for each answer)

I had used Registry Ripper 3.0 for this assignment and cross checked the information from the Registry Editor. Following are the screenshot of Registry Ripper and hive files that I used in this assignment.

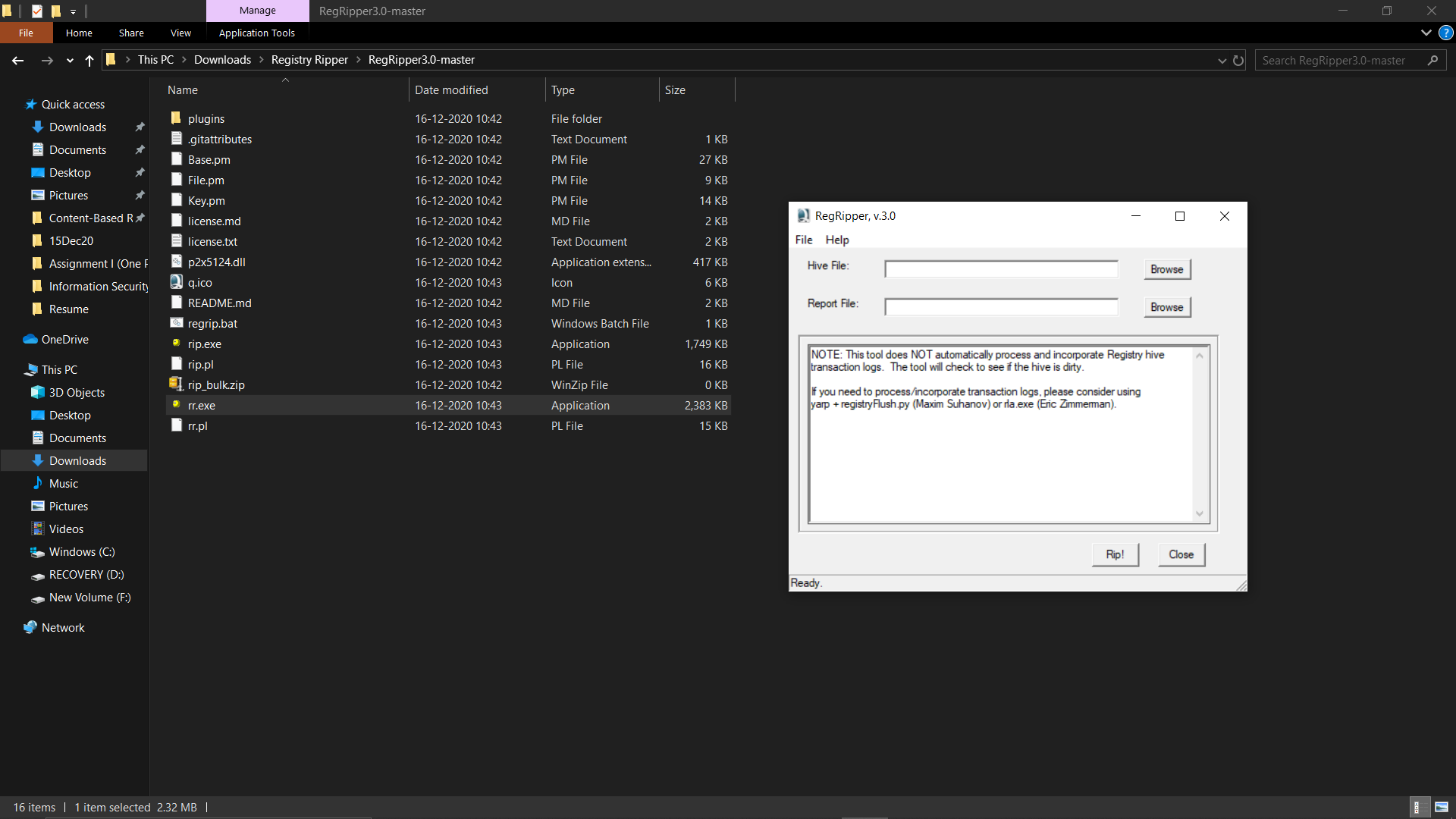


Fig 0.1: Registry Ripper 3.0

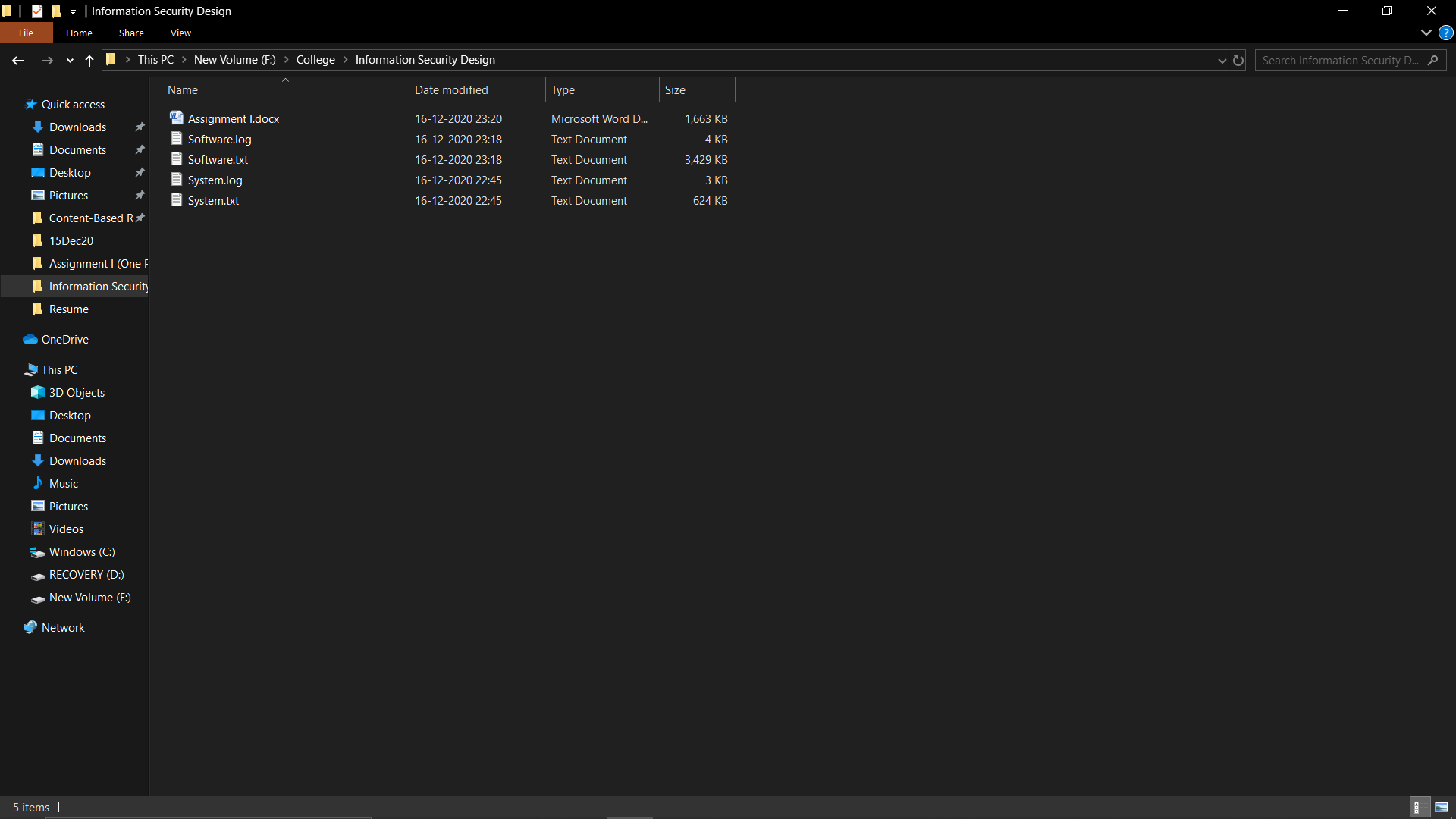


Fig 0.2: Software and System hive files.

1. What is the computer name of the system?

Ans: LAPTOP-ON9LBPEU

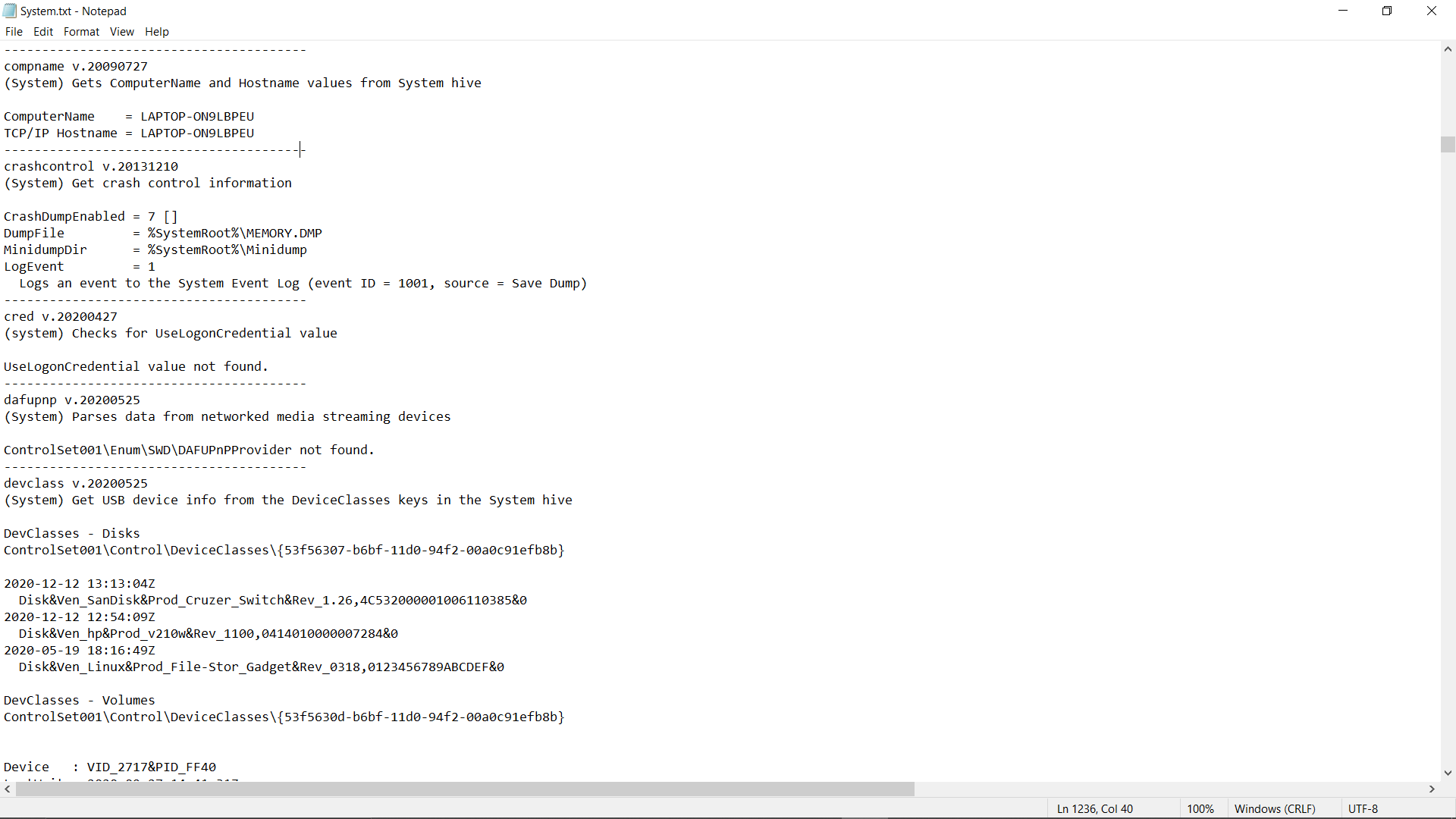


Fig 1.1: Computer Name from System hive file

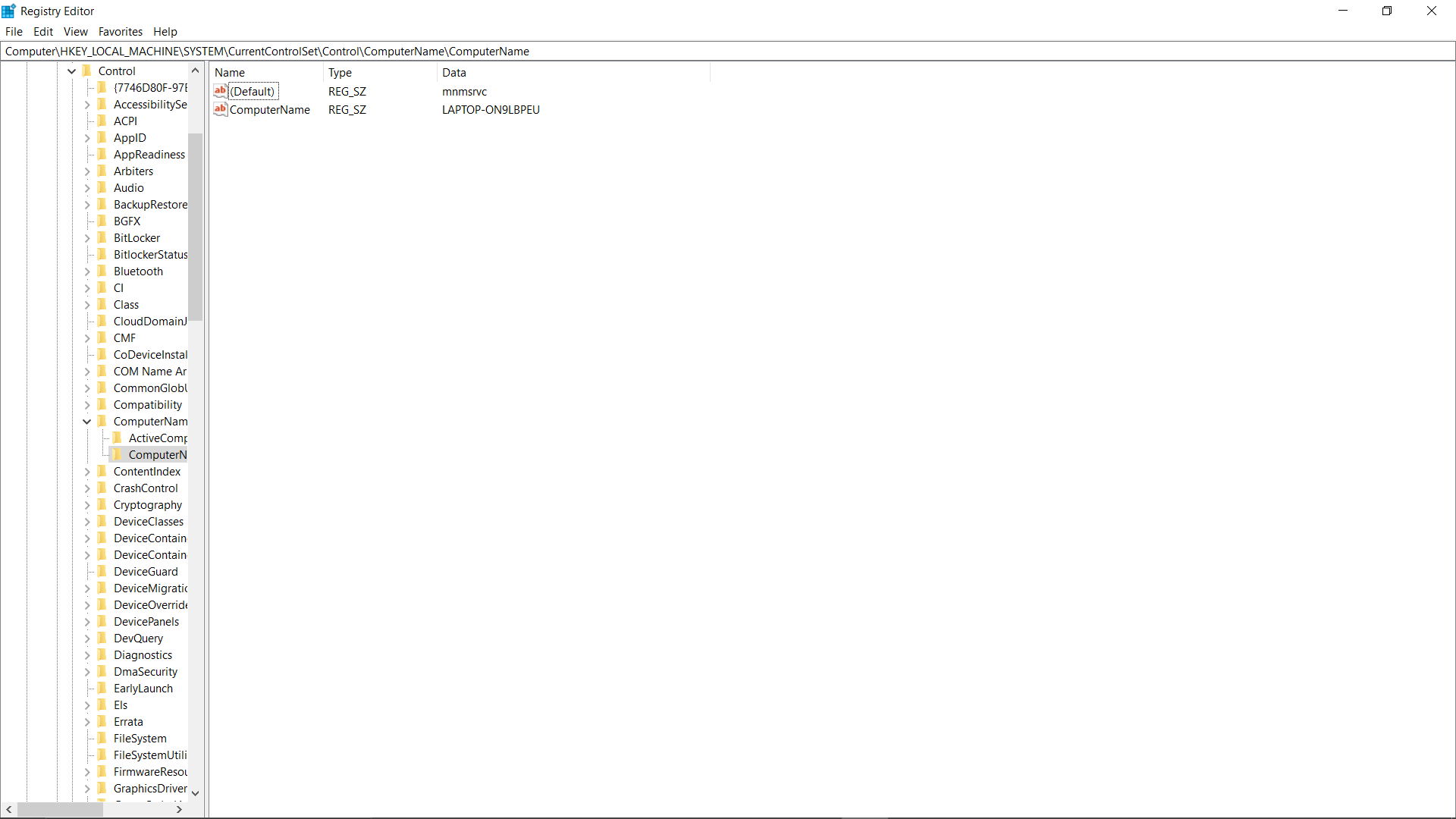


Fig 1.2: Computer Name from Registry Editor

\*\*Just follow the link in Registry Editor and you will get your output\*\*

---------------------------------------------------------------------------------------------------------------------------------------------------------

2. When was the Operating System installed?

Ans:

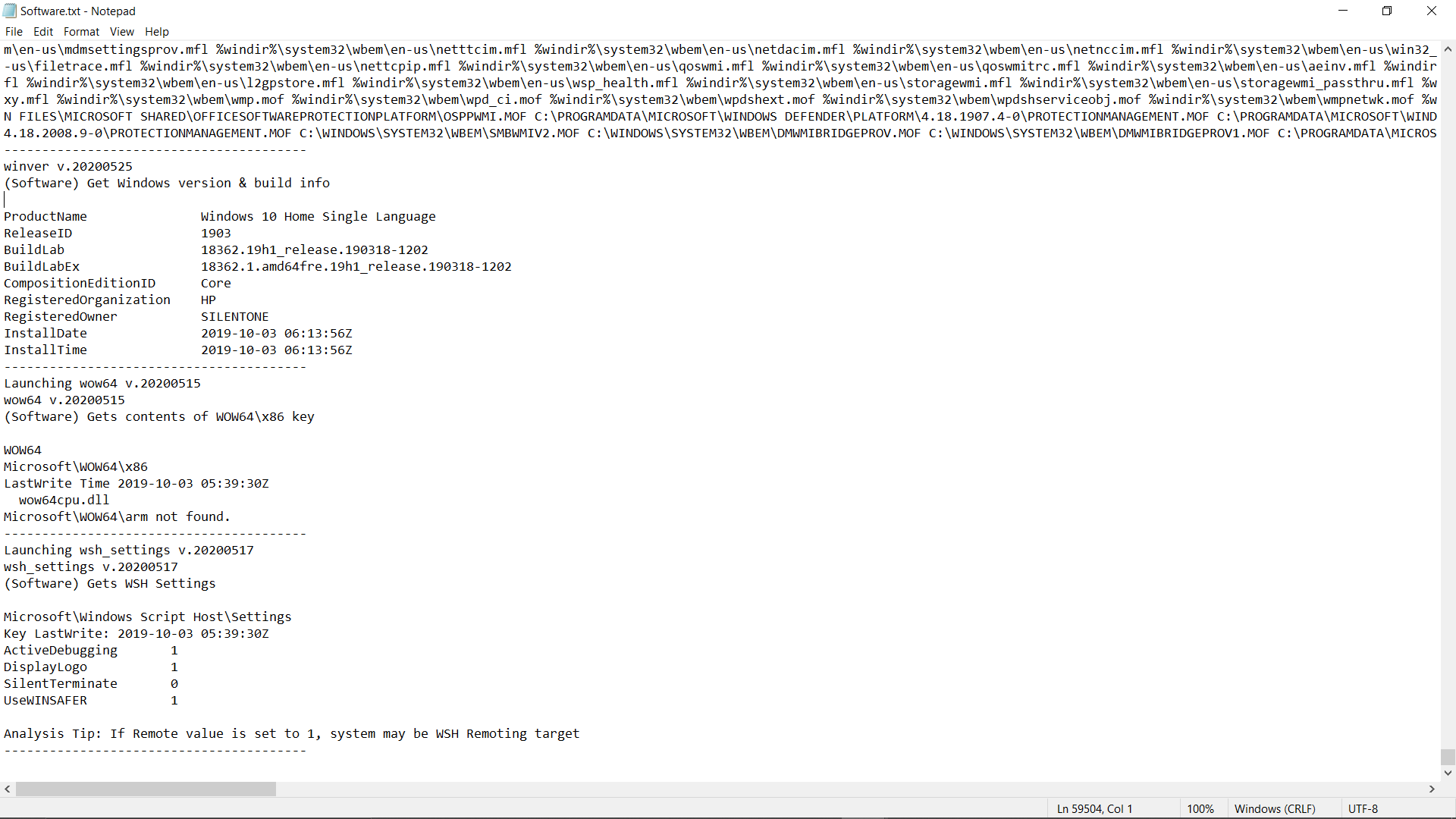


Fig 2.1: OS install date and time from Software hive file

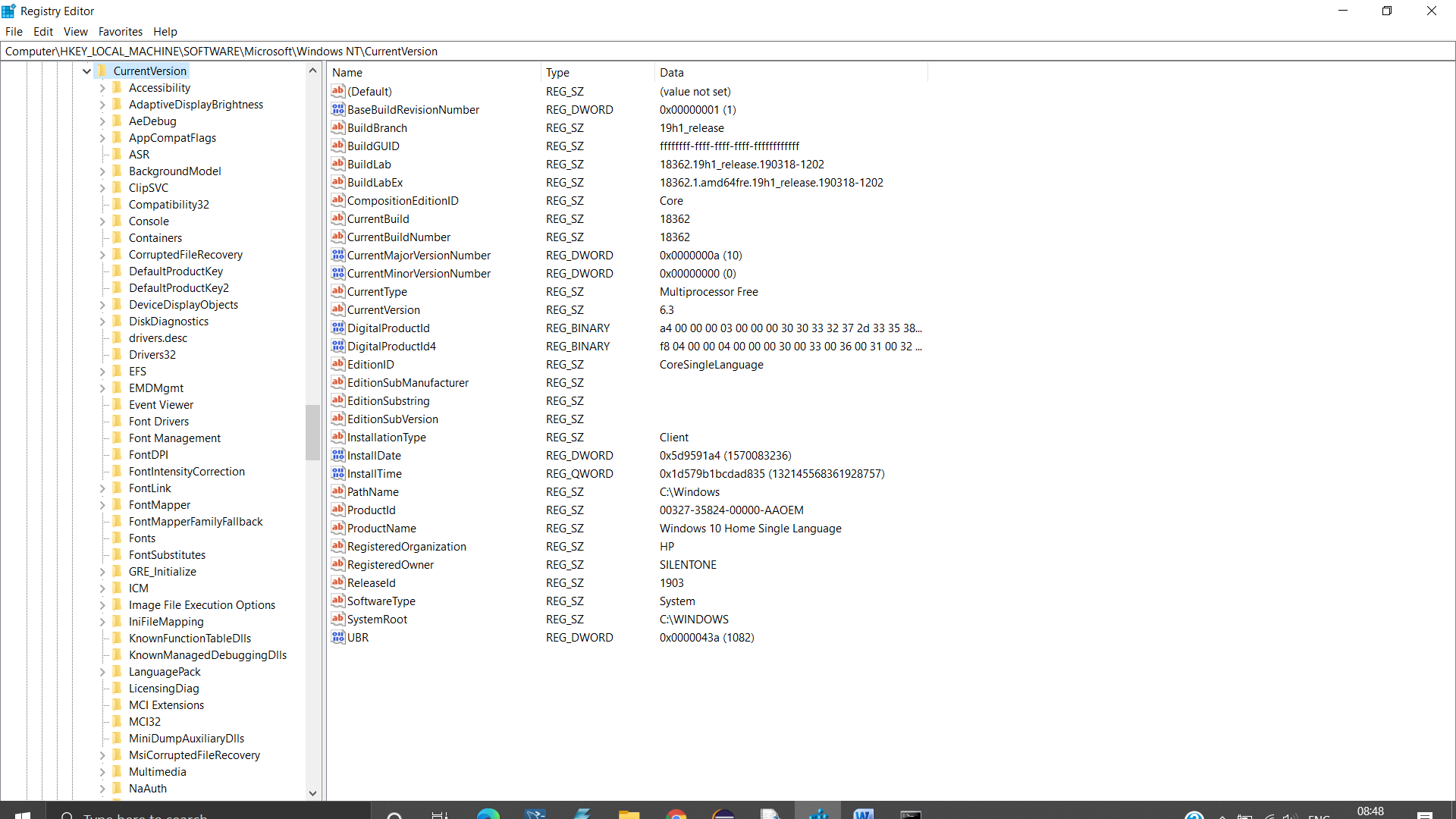


Fig 2.2: Install Date from Registry Editor

\*\*Just follow the link in Registry Editor and you will get your output\*\*

---------------------------------------------------------------------------------------------------------------------------------------------------------

3. What are the applications installed on the system?

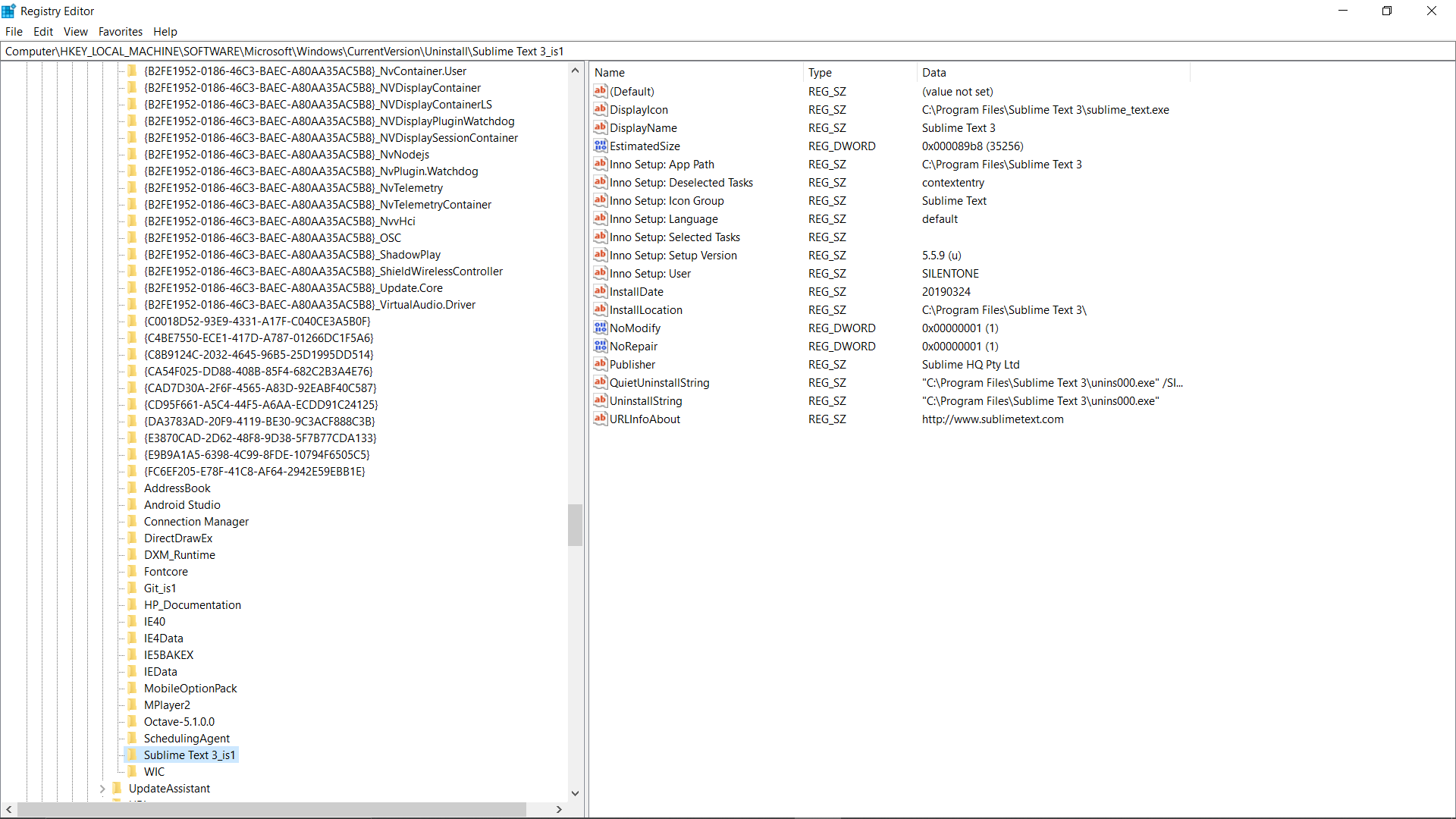


Fig 3.1: Application List from Registry Editor

\*\*Just follow the link in Registry Editor and you will get your output\*\*

---------------------------------------------------------------------------------------------------------------------------------------------------------

Q.4. What date/time (in UTC) was the Operating System installed? Hint: you may have to convert epoch time to human readable time using DCode tool.

Ans:

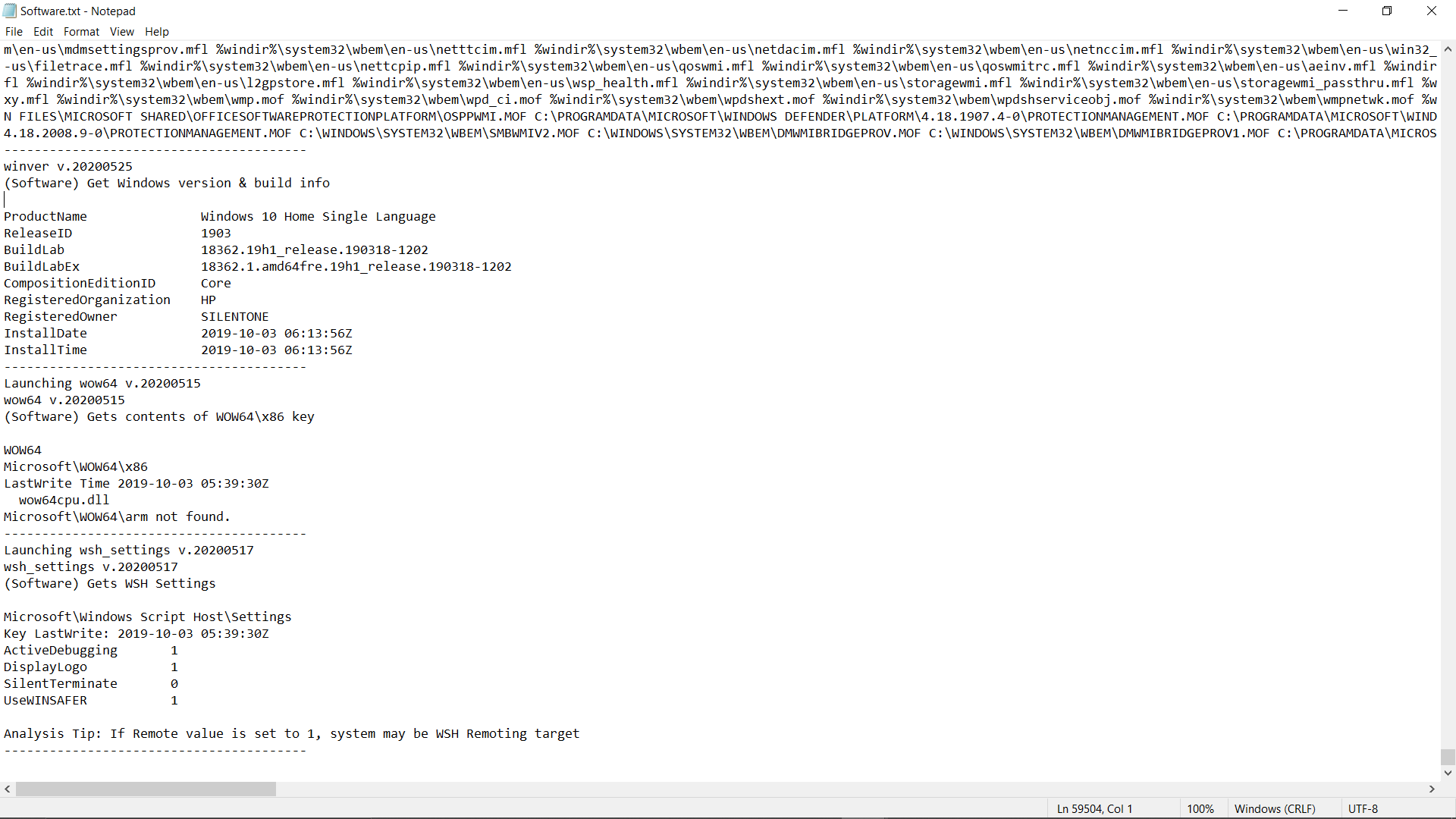


Fig 4.1: OS install date and time from Software hive file

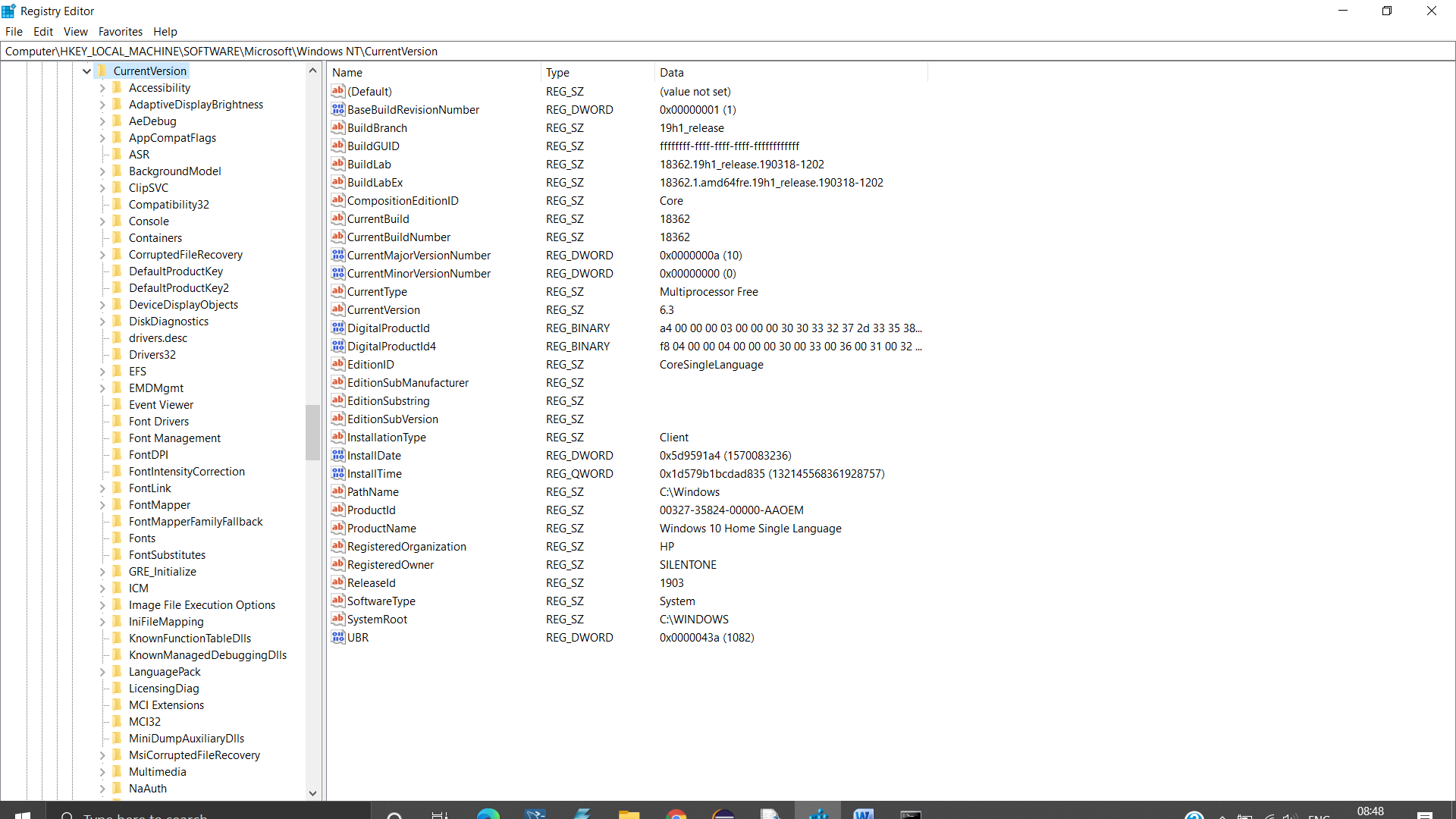


Fig 4.2: Install Date from Registry Editor

\*\*Just follow the link in Registry Editor and you will get your output\*\*

Install-Date (DWORD Value) : 0x5d9597a4 (1570083236)

Install-Time (QWORD Value): 0x1d579b1bcda835(132145568361928757)

DWORD (Double Words) value contains total number of seconds since January 1st, 1970. QWORD (Quad Words) value contains total number of seconds.

Using Dcode tool value comes out to be,

Installation Date comes to be: October 3rd, 2019.

Installation Time comes to be: 06:13:56.

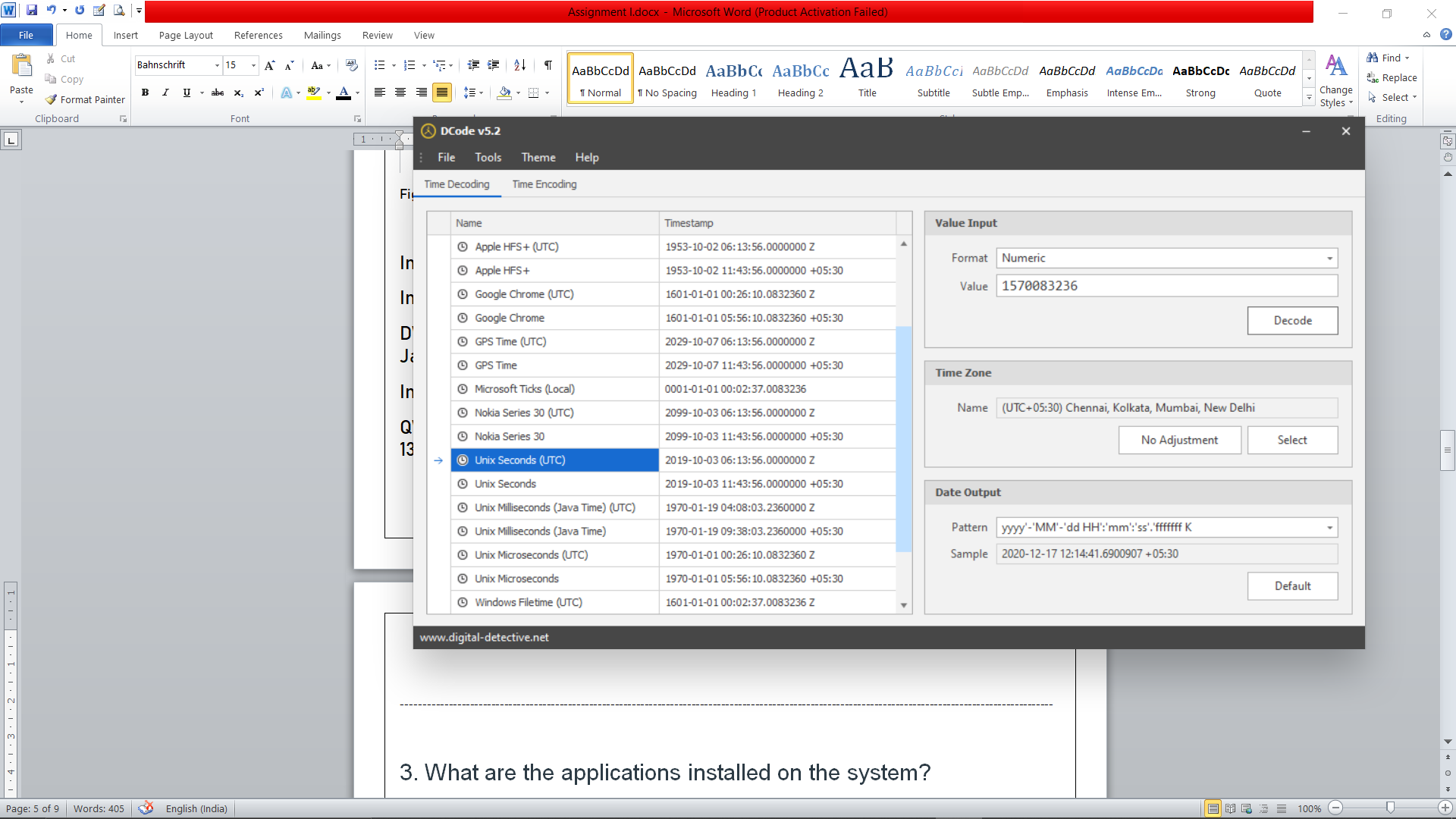


Fig 4.3: Dcode tool for Install-Date.

---------------------------------------------------------------------------------------------------------------------------------------------------------

Q.5 Is Remote Desktop service enabled? How do you know?

Remote Desktop service is enabled when the value of fDenyTSConnections is 0 otherwise if it is 1 then it is disabled. We can check this value in the system hive file.

Since its value is 1 in my PC this means that Remote Desktop Service is not enabled.

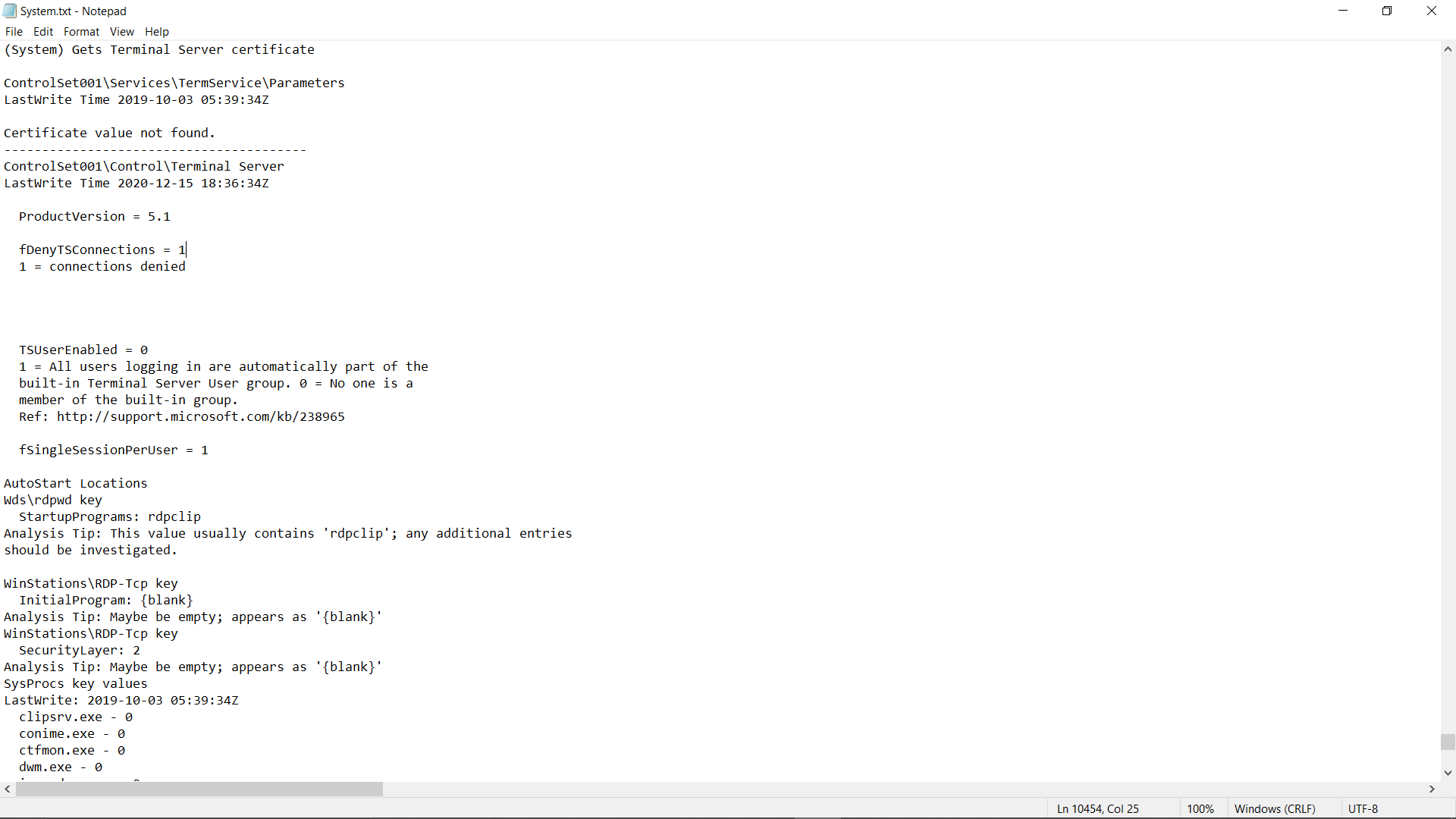


Fig 5.1: Remote Desktop access from System hive file

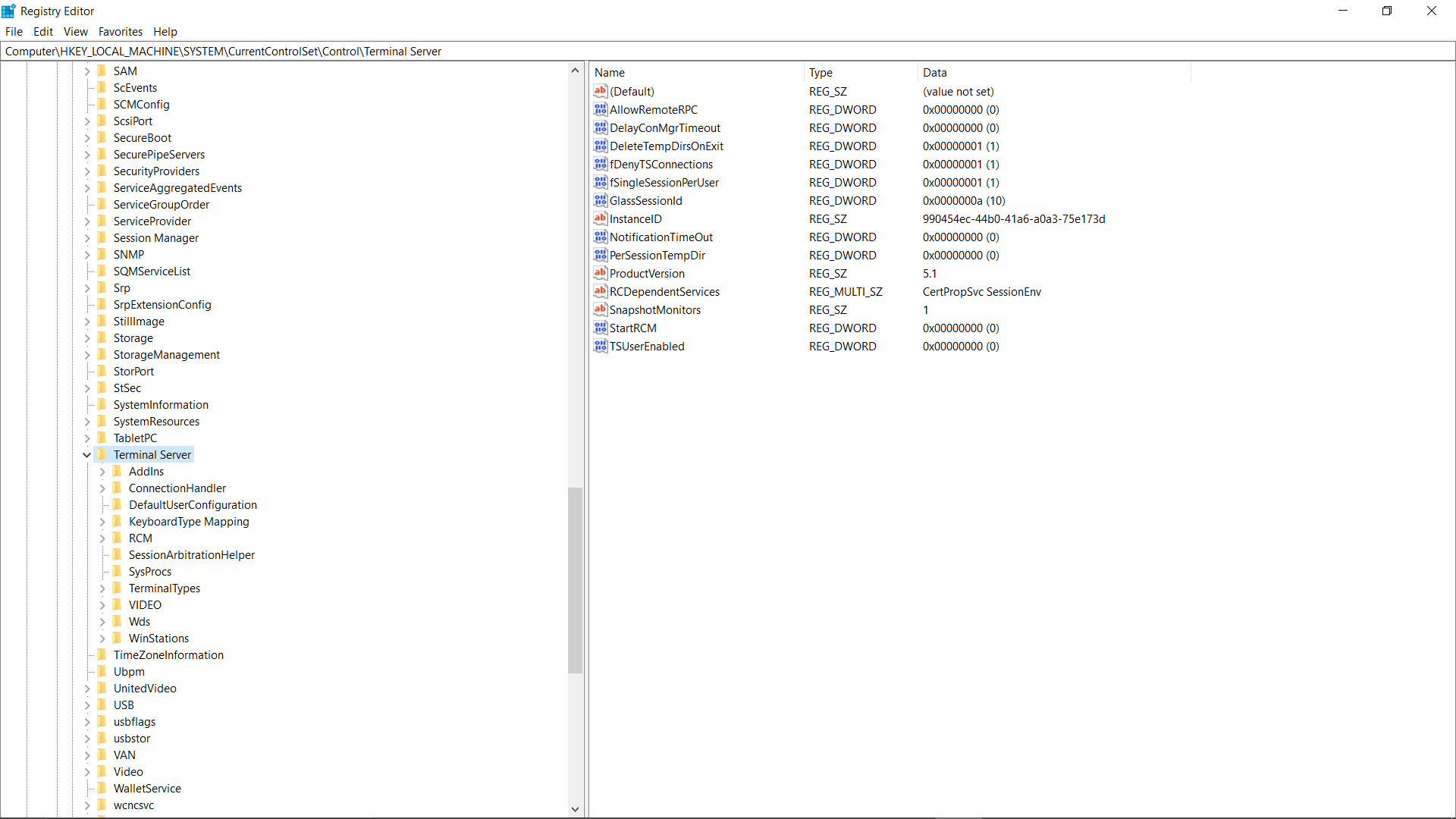


Fig 5.2: Remote Desktop access from Registry Editor

\*\*Just follow the link in Registry Editor and you will get your output\*\*

---------------------------------------------------------------------------------------------------------------------------------------------------------

Q.6 What is the IP address of the system?

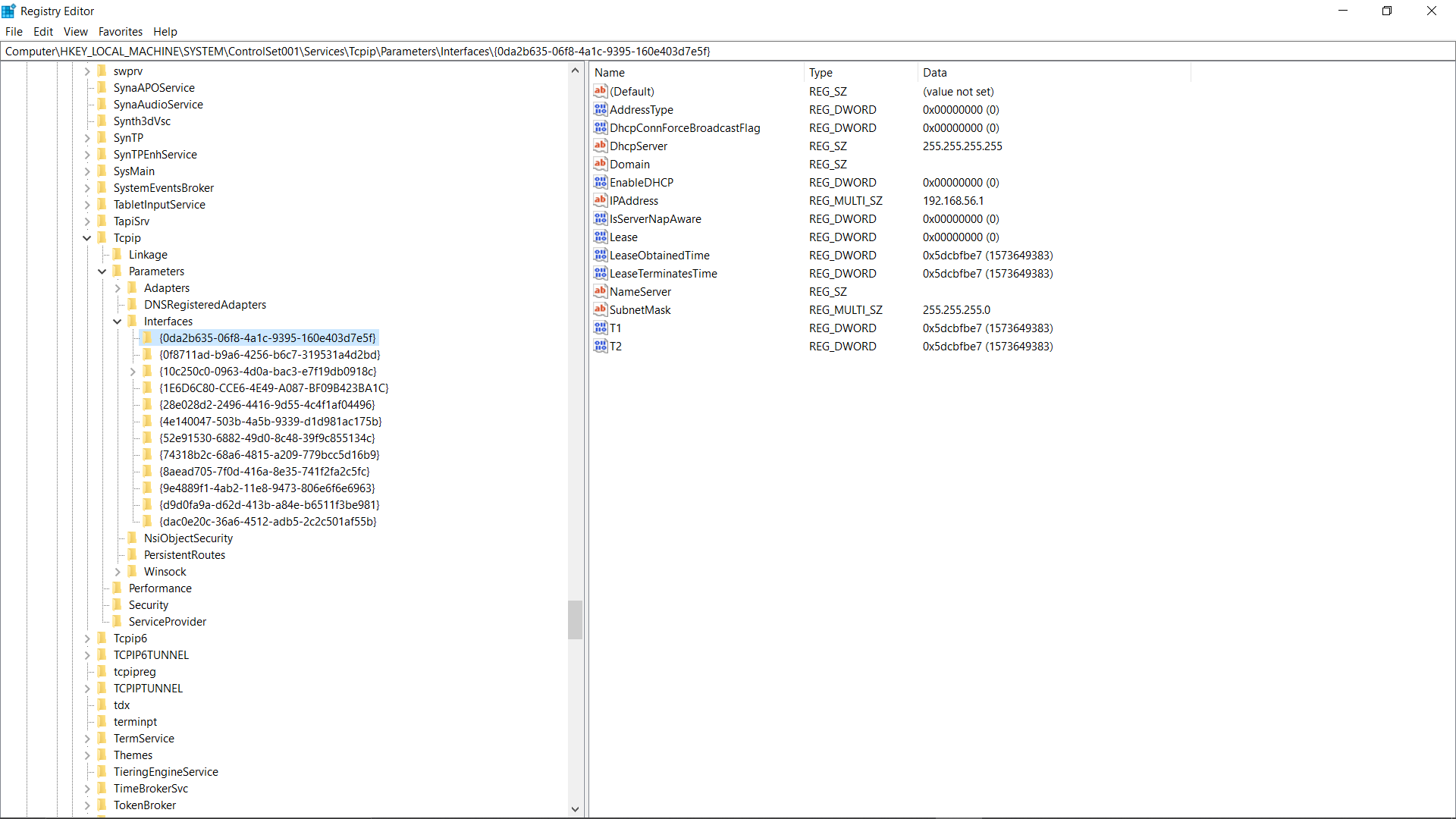


Fig 6.1: IP Address of System using Registry Editor

\*\*Just follow the link in Registry Editor and you will get your output\*\*

---------------------------------------------------------------------------------------------------------------------------------------------------------

Q.7 When was the system last shutdown?

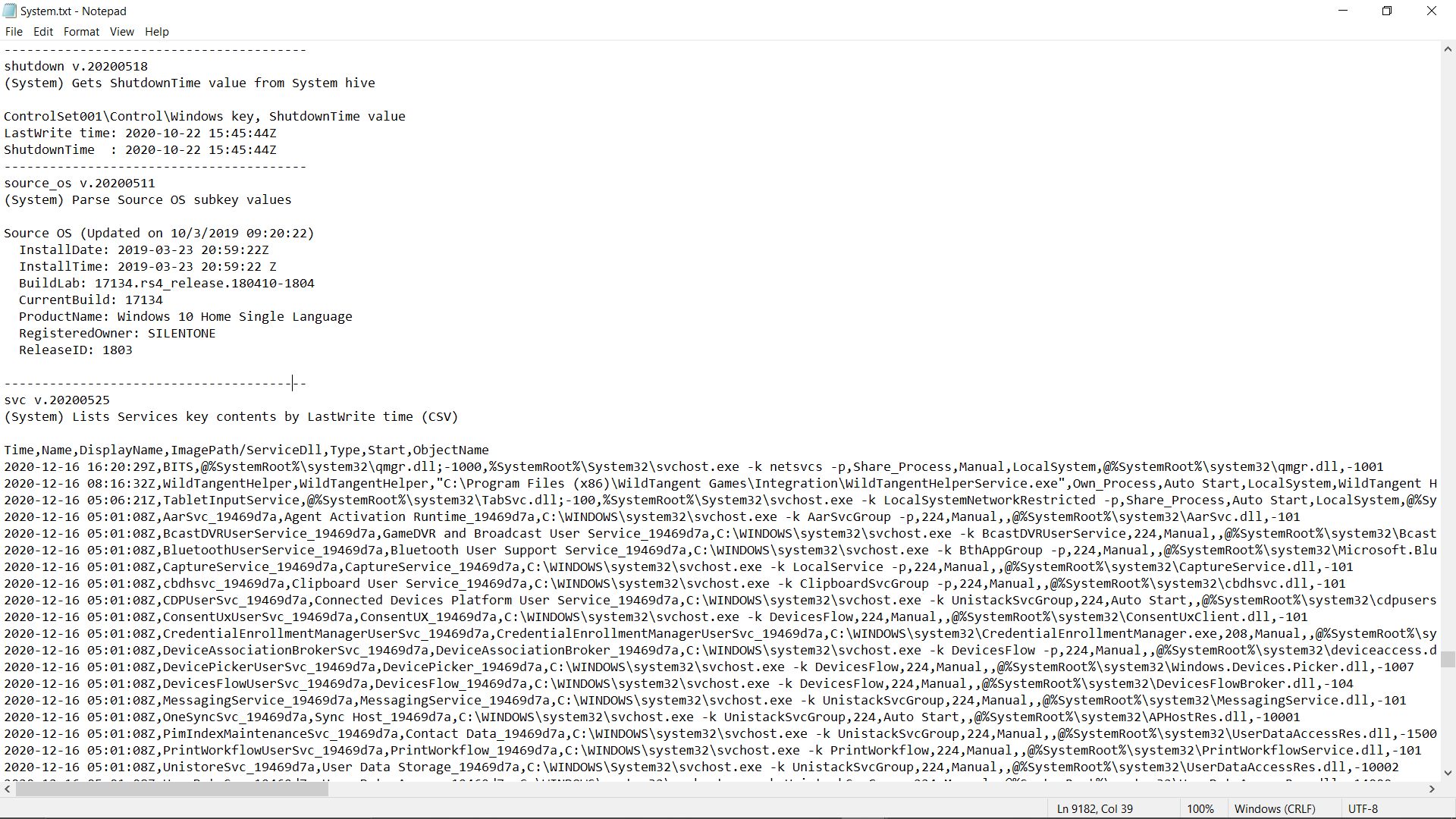


Fig 7.1: Shut Down Time using System hive

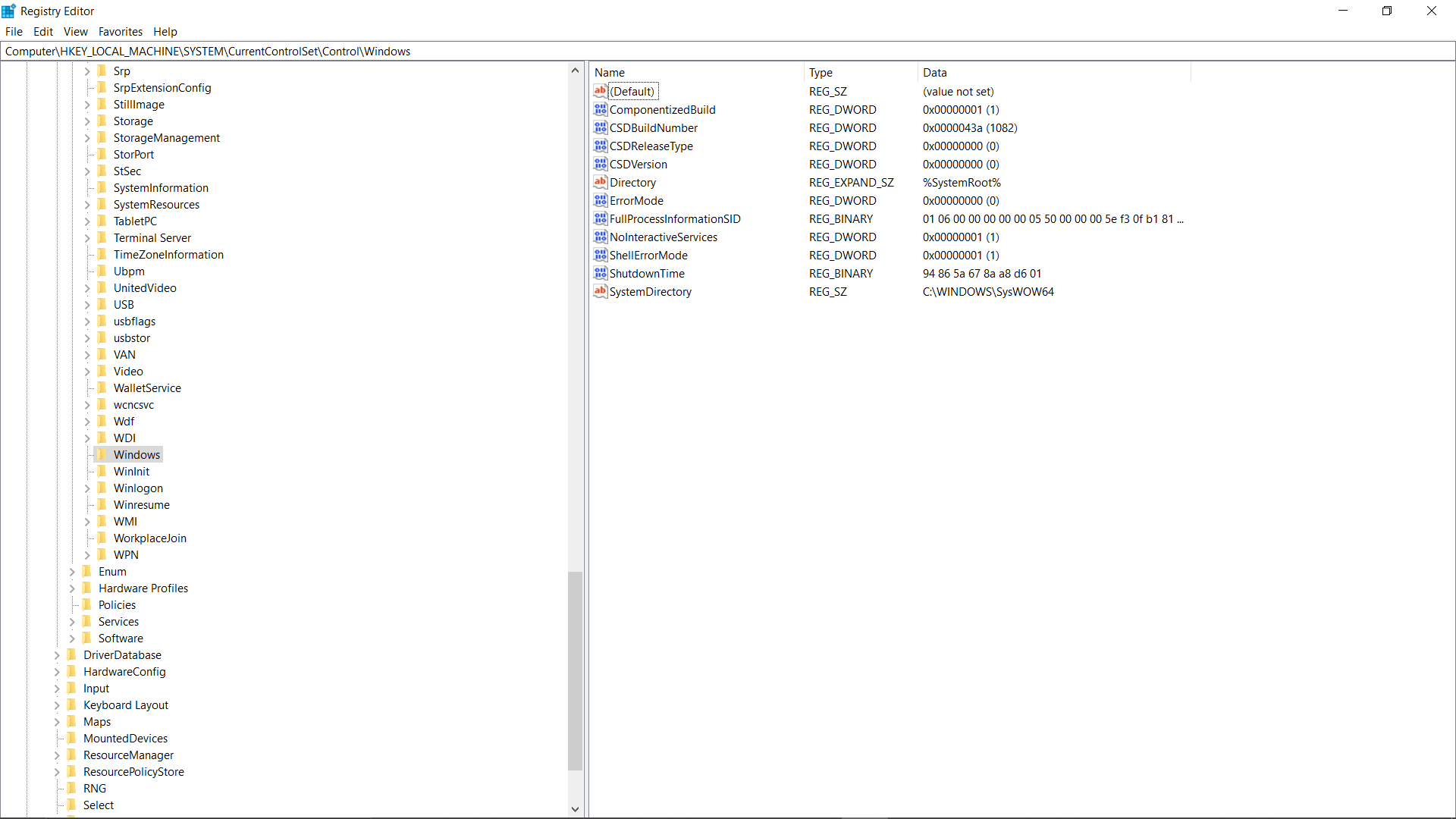


Fig 7.2: Shut Down Time using Registry Hive

\*\*Just follow the link in Registry Editor and you will get your output\*\*

Value: 94 86 5a 67 8a a8 d6 01

Using Dcode Tool, the value comes out to be 2020-10-22 15:45:45:44.69Z.

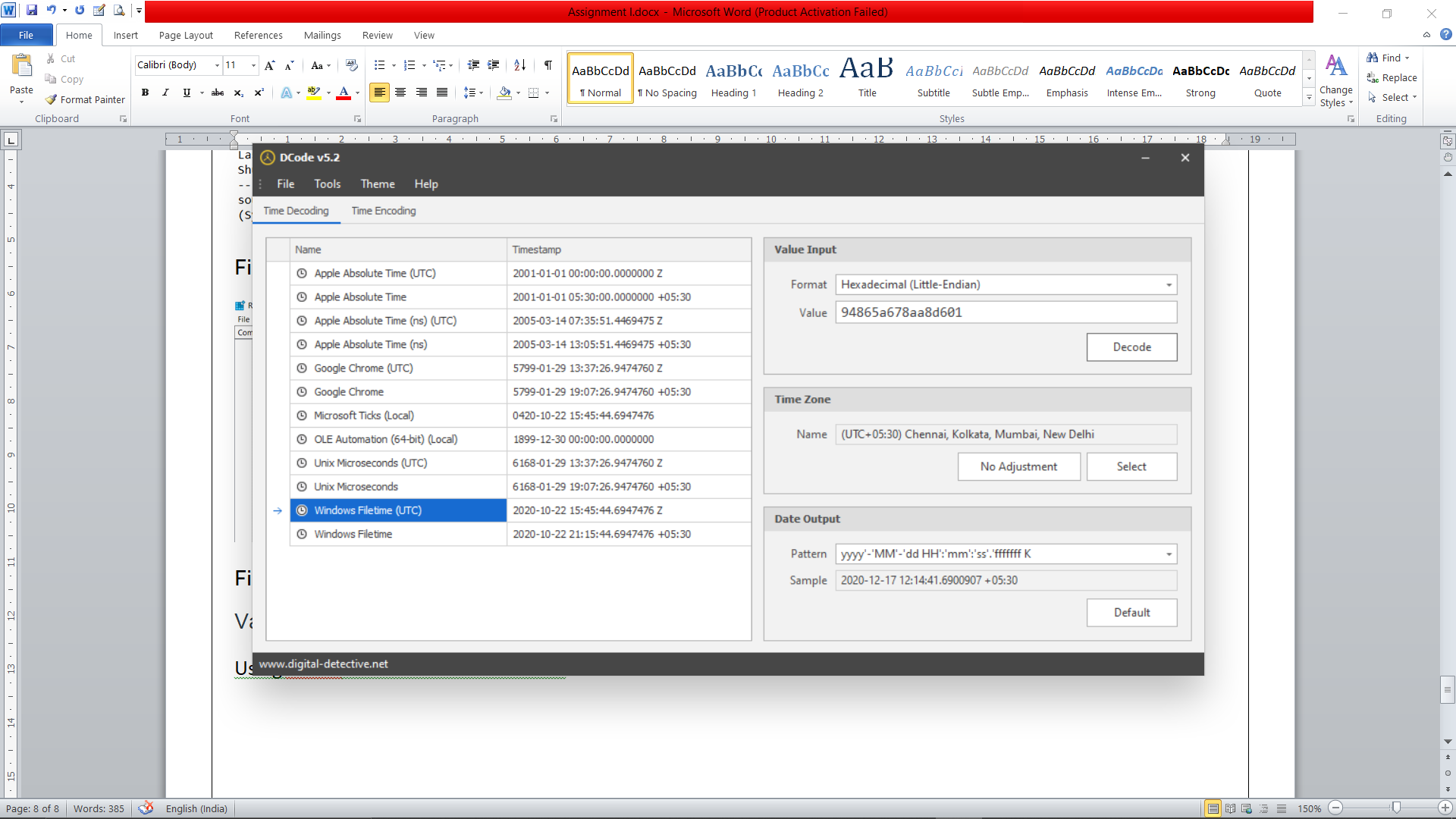


Fig 7.3: Dcode Tool for conversion of hexadecimal value.

---------------------------------------------------------------------------------------------------------------------------------------------------------