1.What is the most used Desktop Operating System right now?

Ans: Windows is the most used Operating System

2.What is the short form for HKEY\_LOCAL\_MACHINE?

Ans: HKLM

3.What is the path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM?

Ans: The majority of these hives are located in the C:\Windows\System32\Config directory and are:

DEFAULT (mounted on HKEY\_USERS\DEFAULT)

SAM (mounted on HKEY\_LOCAL\_MACHINE\SAM)

SECURITY (mounted on HKEY\_LOCAL\_MACHINE\Security)

SOFTWARE (mounted on HKEY\_LOCAL\_MACHINE\Software)

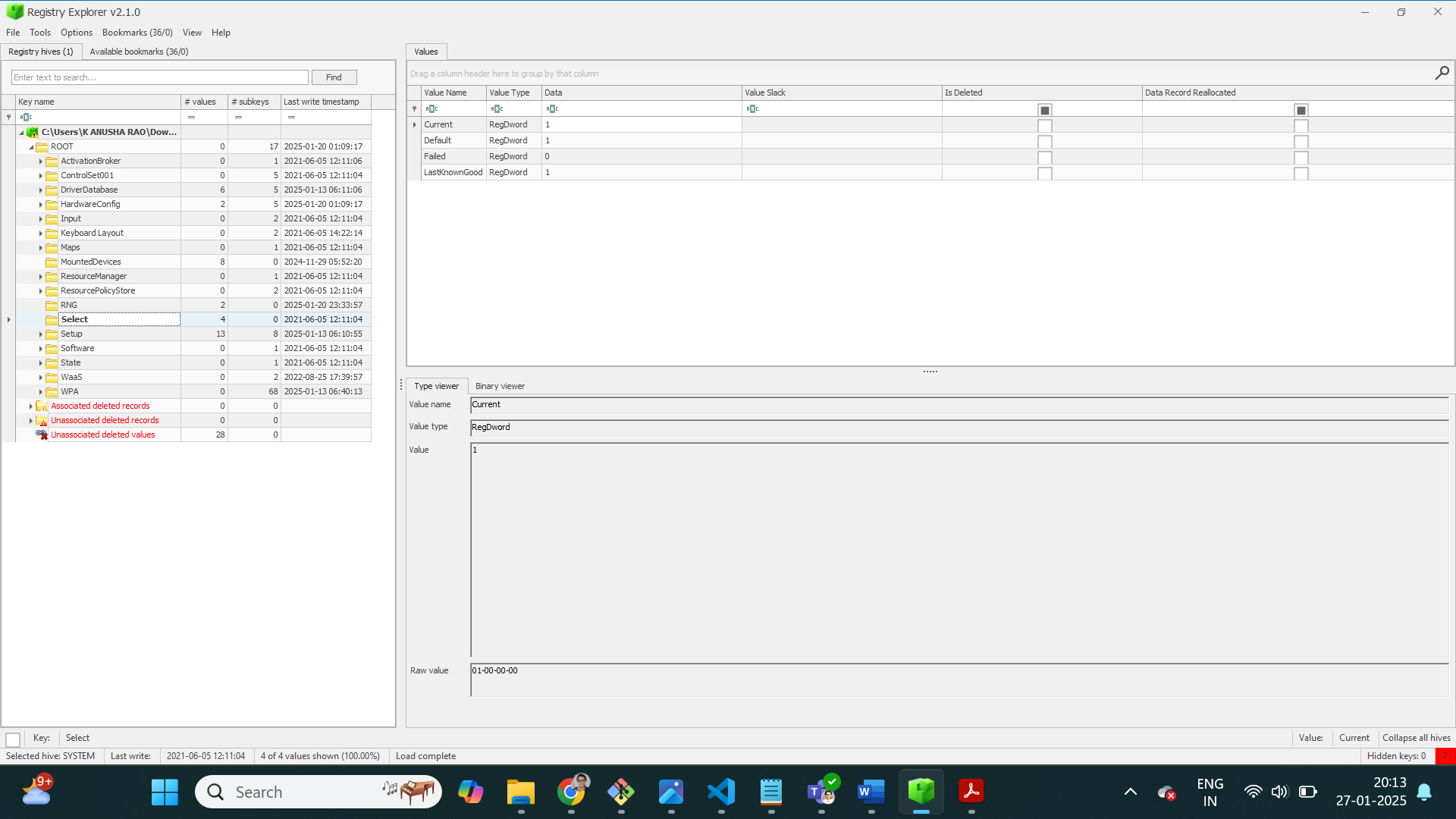
SYSTEM (mounted on HKEY\_LOCAL\_MACHINE\System)

4.What is the path for the AmCache hive?

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

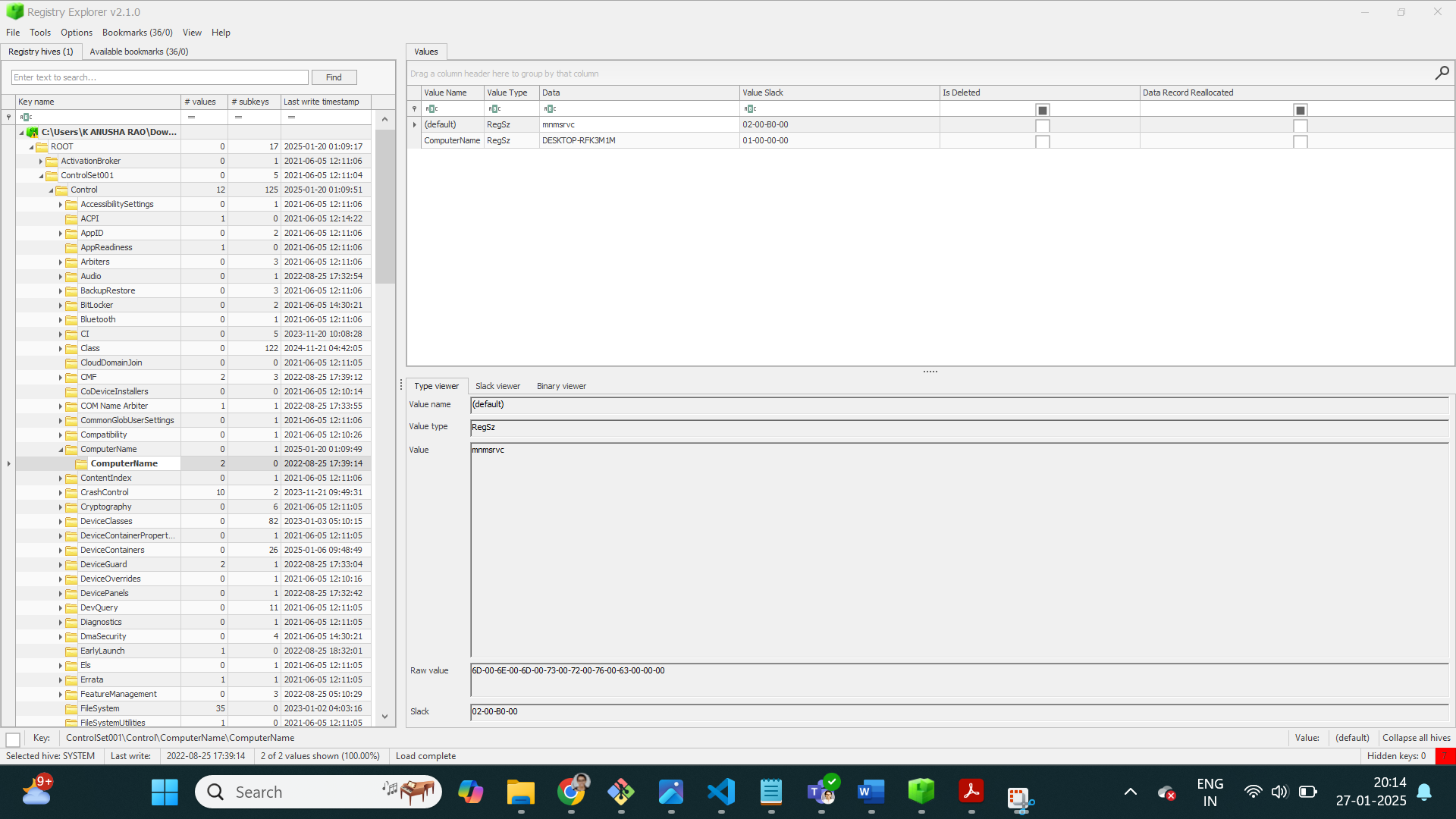
5.What is the Current Build Number of the Target machine whose data is being investigated?

1.Which ControlSet contains the last known good configuration?



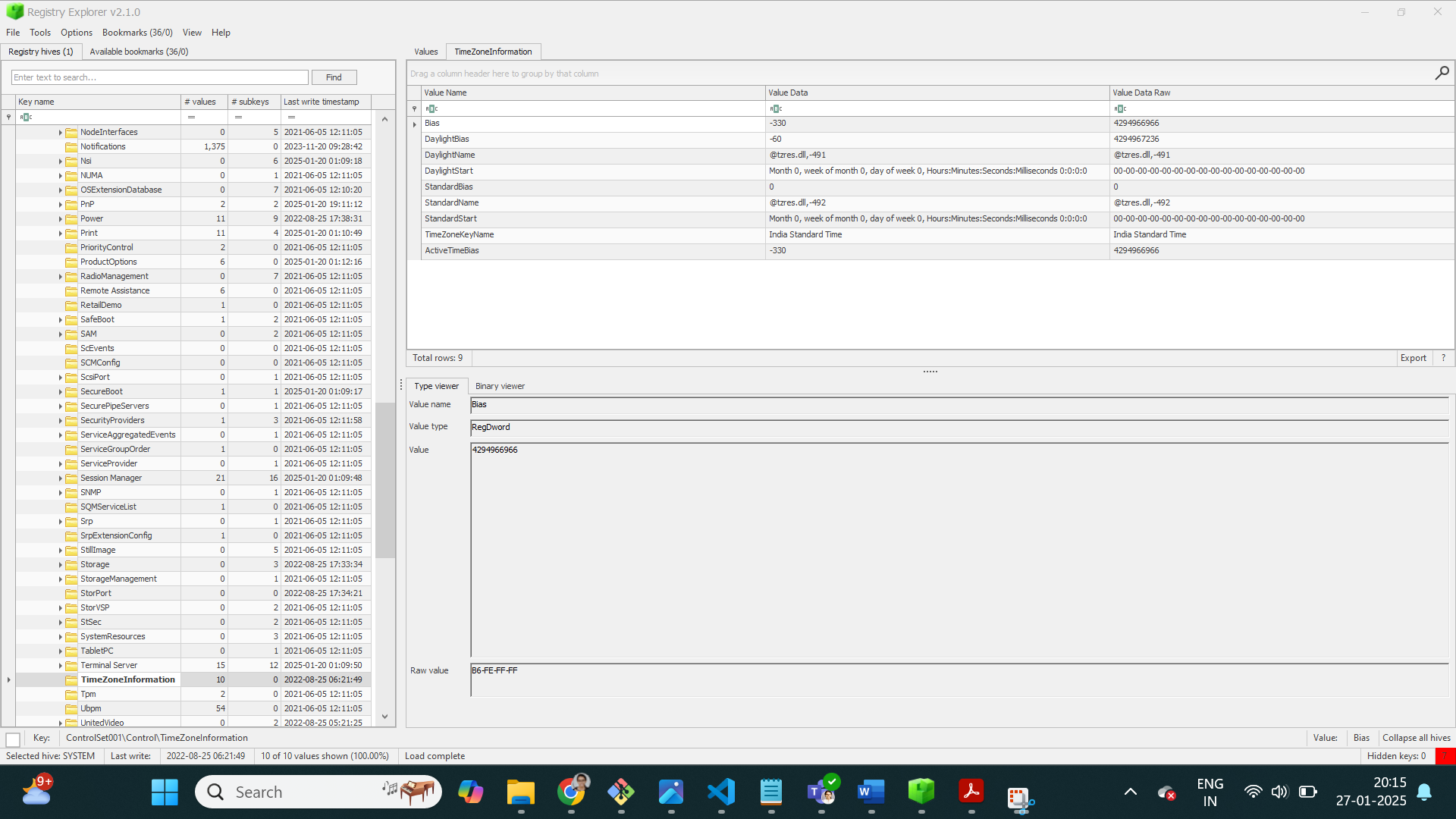
2.What is the Computer Name of the computer?

DESKTOP-RFK3M1M



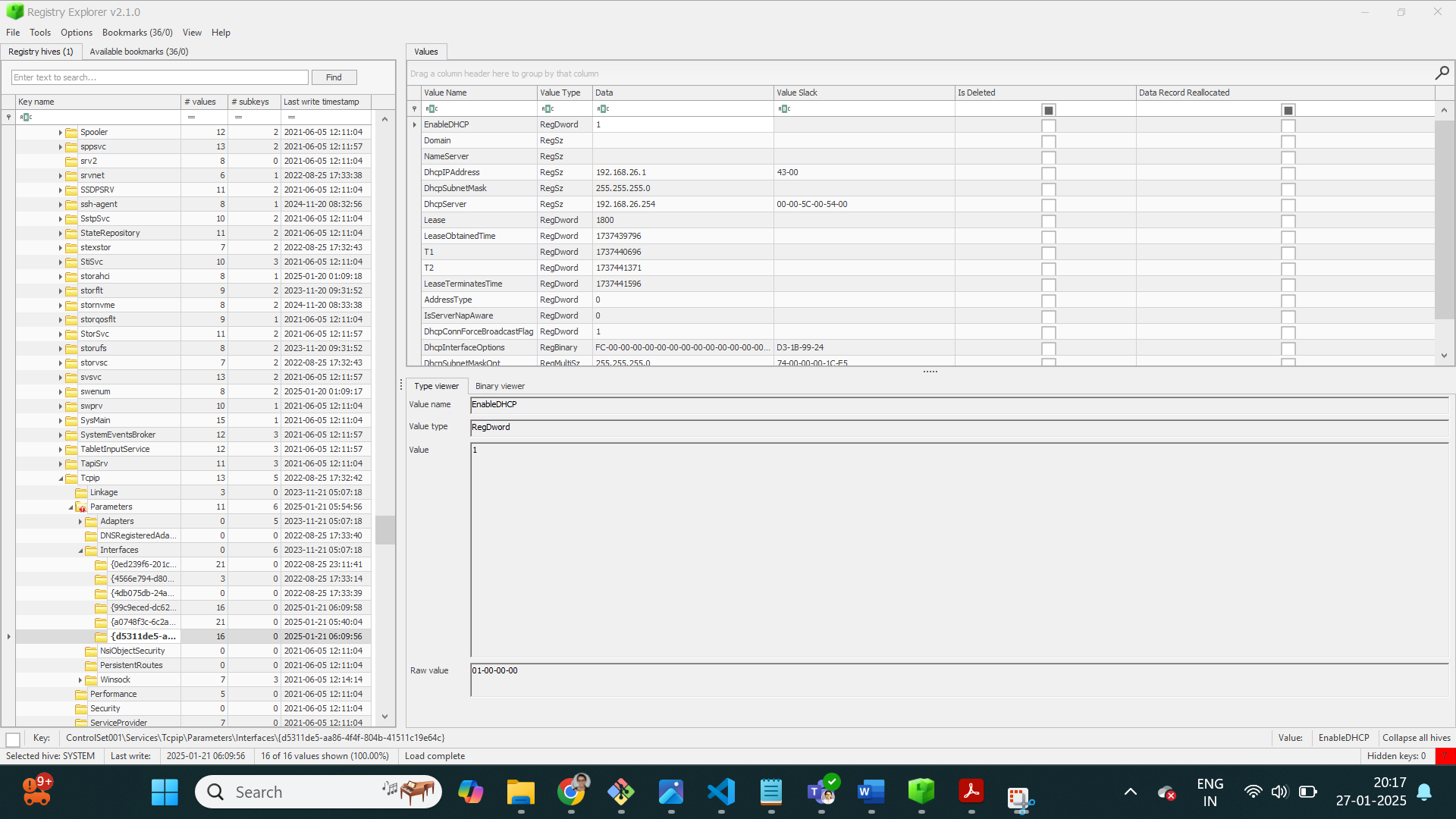
3.What is the value of the TimeZoneKeyName?

Indian Standard Time



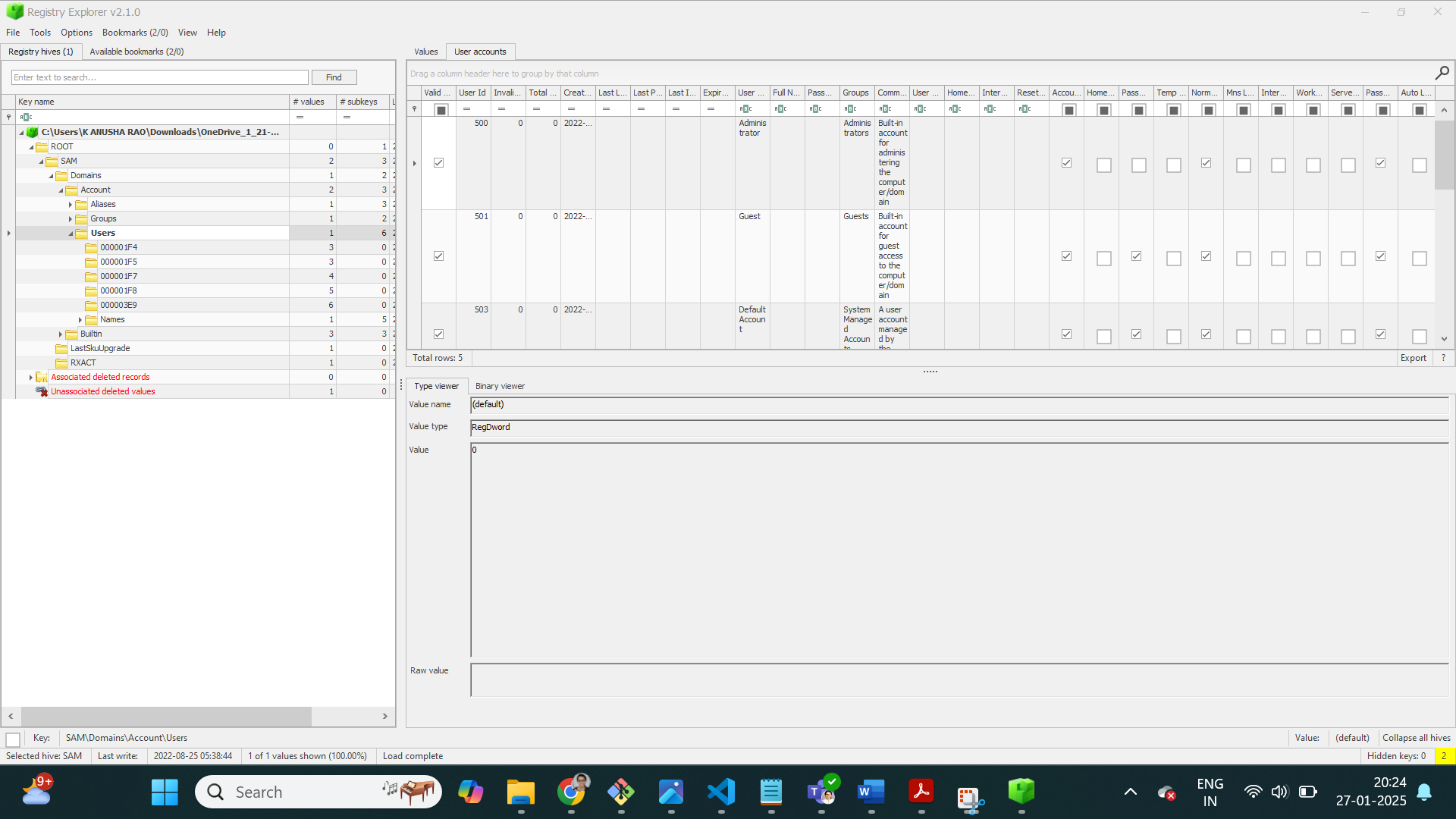
4.What is the DHCP IP address

192.168.26.1



5.What is the RID of the Guest User account?

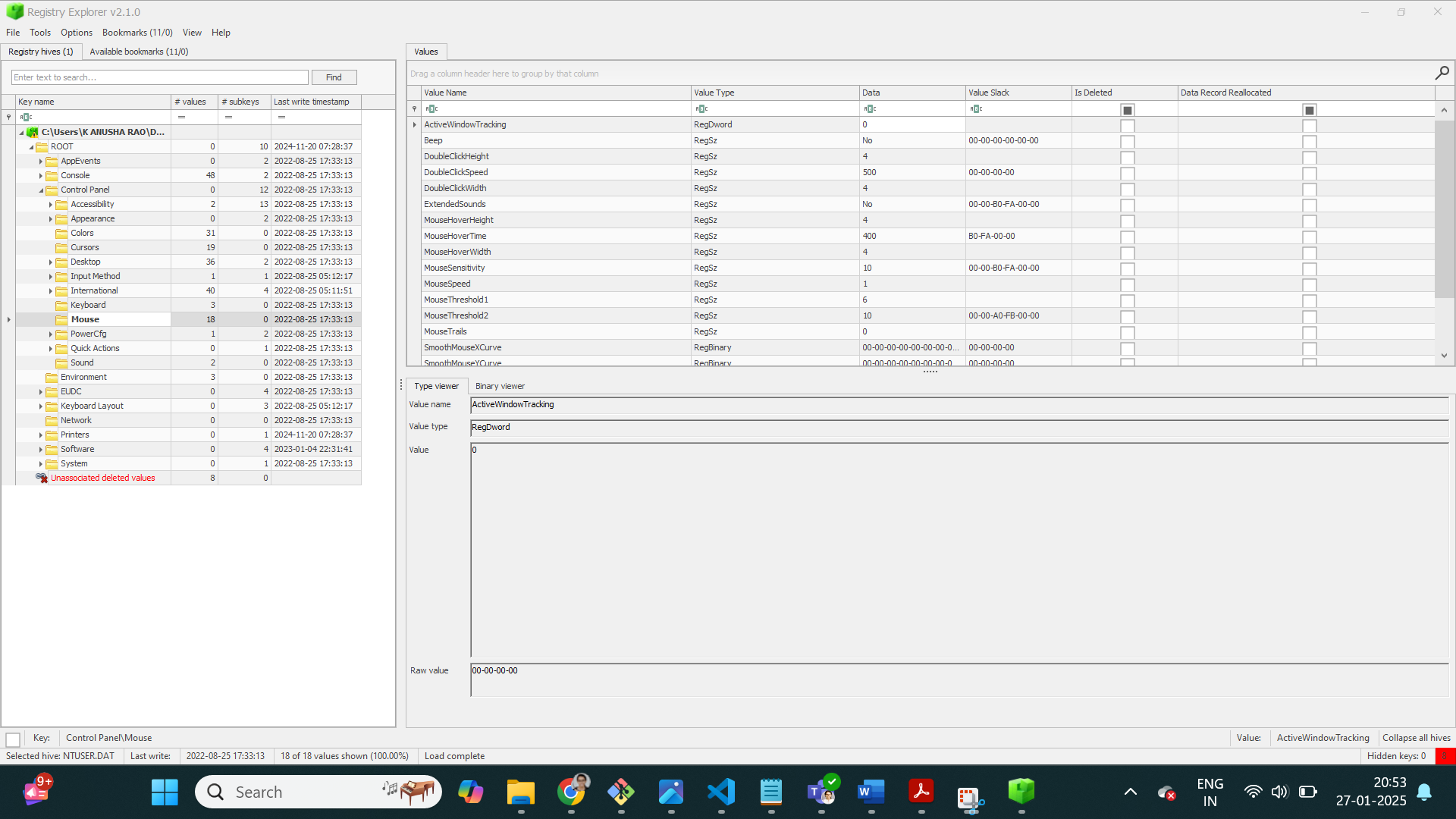
501



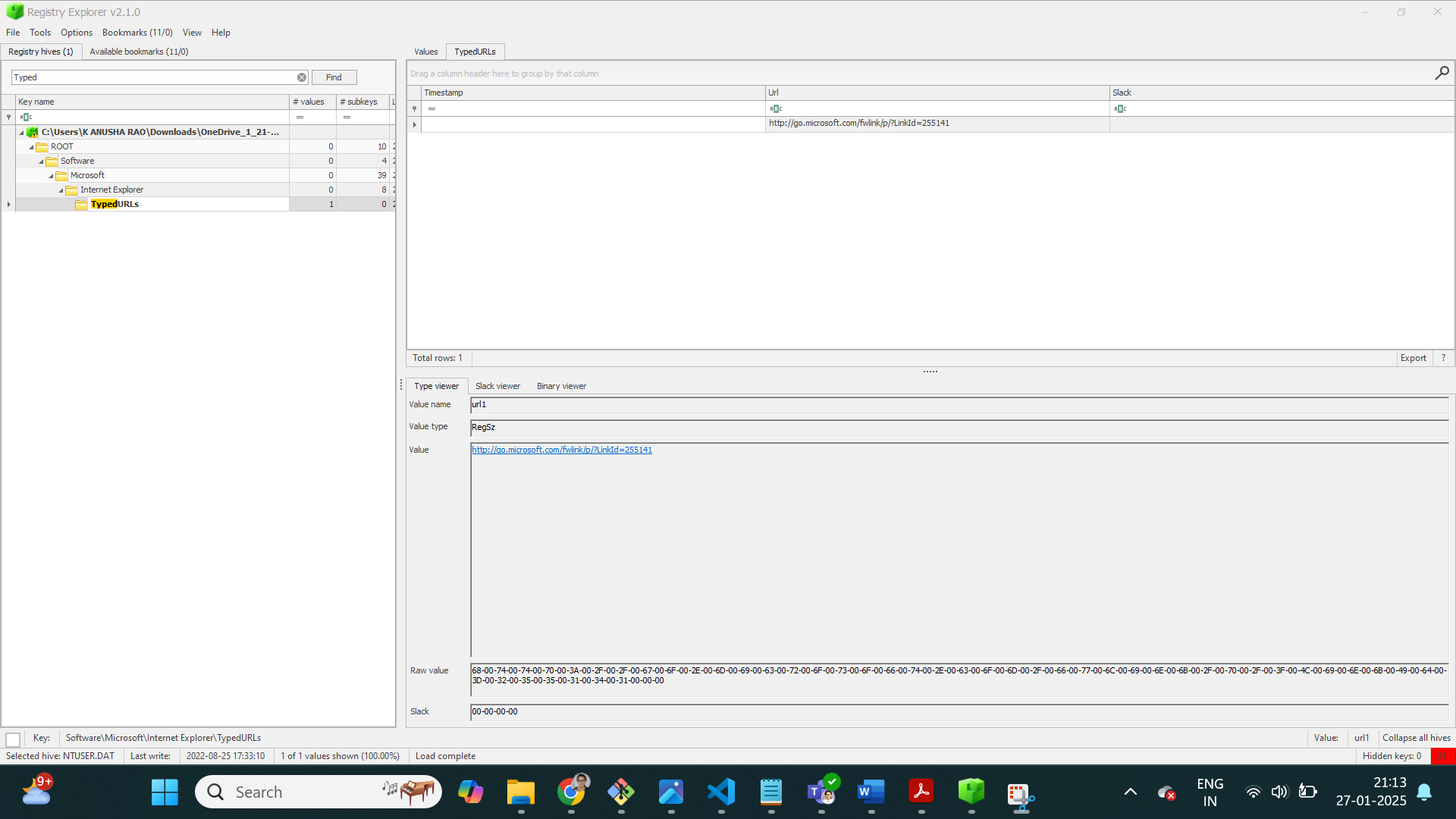
6.Given the registry file of a system that was compromised, answer the following:

I.What’s the mouse double-click speed?

500



II.What’s the most recent typed path accessed as recorded in the registry?



III.What’s the new value added to the registry by the malware in order to establish persistence over the system?

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

