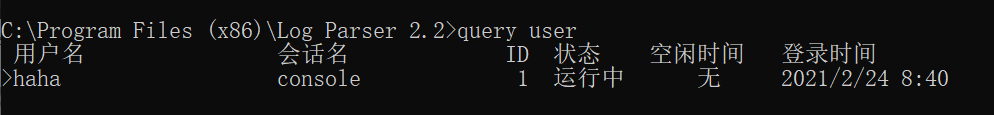
# 账号安全

query user 查看当前登录账户



logoff ID 注销用户id

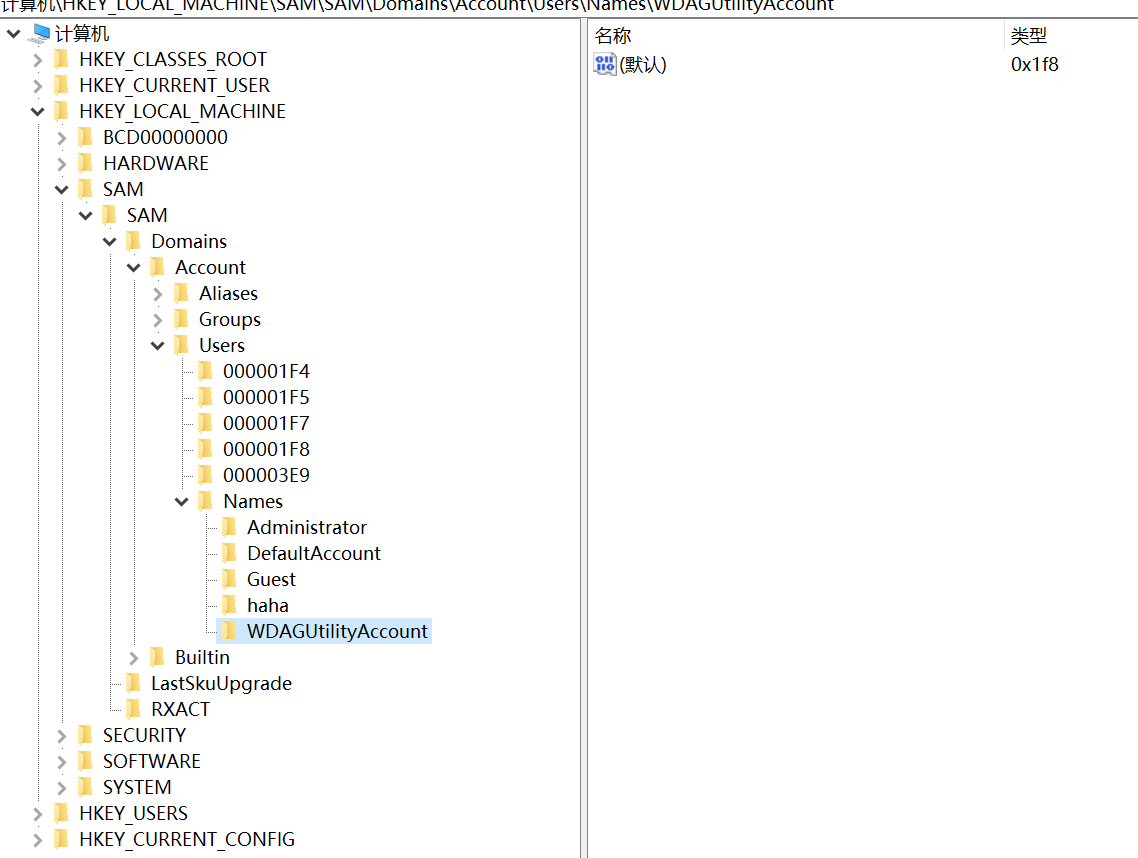
net user 查看用户

net user username 查看用户登录情况

lusrmgr.msc 打开本地用户组

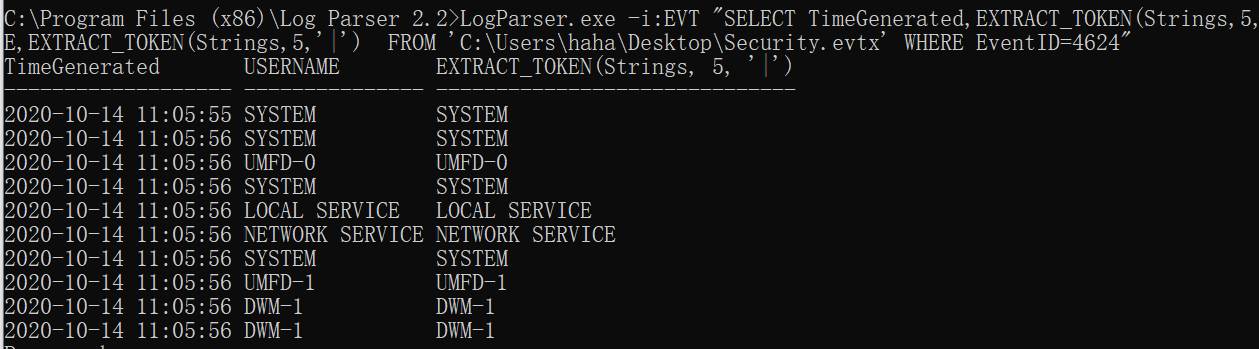


regedit注册表查看账户，确认系统是否存在隐藏账户



利用LogParser.exe查看event日志，查询用户登录情况

LogParser.exe -i:EVT "SELECT TimeGenerated,EXTRACT\_TOKEN(Strings,5,'|') AS USERNAME,EXTRACT\_TOKEN(Strings,5,'|') AS SERVICE\_NAME,EXTRACT\_TOKEN(Strings,5,'|') AS Client\_IP FROM 'C:\Users\haha\Desktop\Security.evtx' WHERE EventID=4624"



LogParser.exe日志分析工具更多用法可参考：

https://wooyun.js.org/drops/windows%E5%AE%89%E5%85%A8%E6%97%A5%E5%BF%97%E5%88%86%E6%9E%90%E4%B9%8Blogparser%E7%AF%87.html

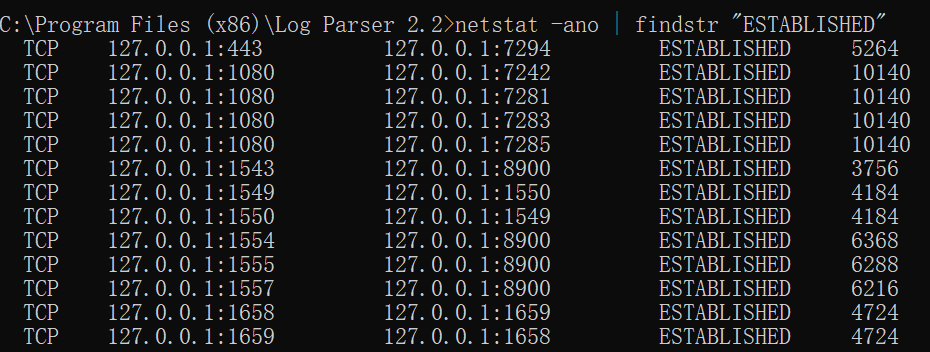
# 二、检查异常端口进程

查看目前连接：

netstat -ano

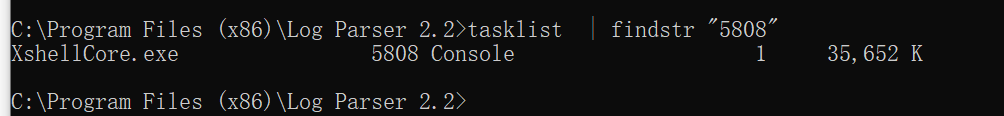
一般是查看已经成功建立的连接：

netstat -ano | findstr "ESTABLISHED"

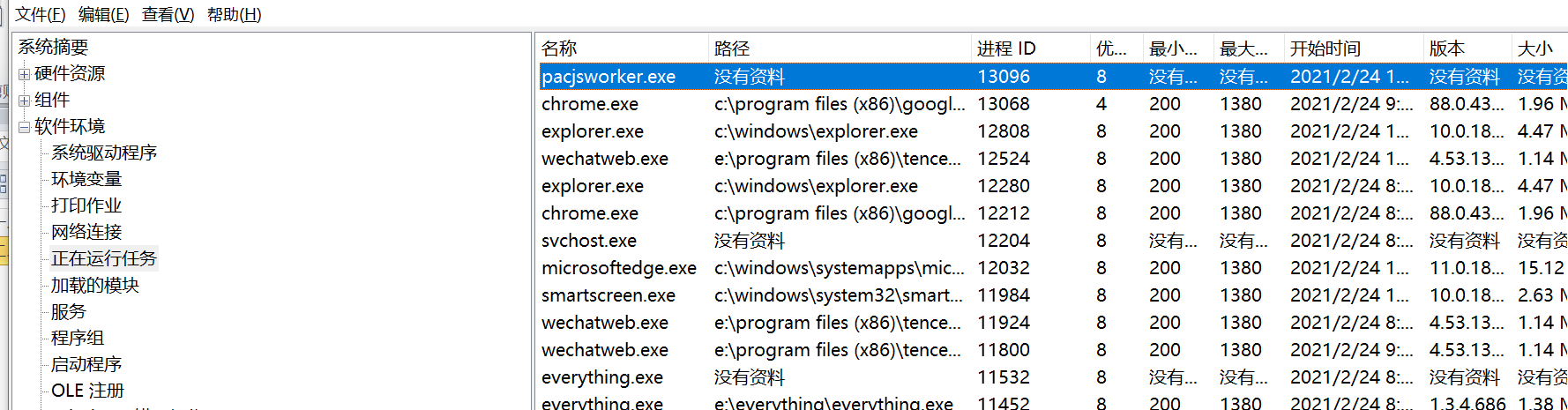


根据pid定位程序名称

tasklist | findstr "pid"

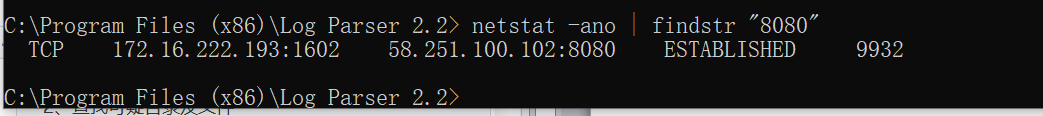


运行中输入msinfo32，可打开系统信息，在“正在运行任务”中可获取进程详细信息，包括进程的开始时间、版本、大小等信息。



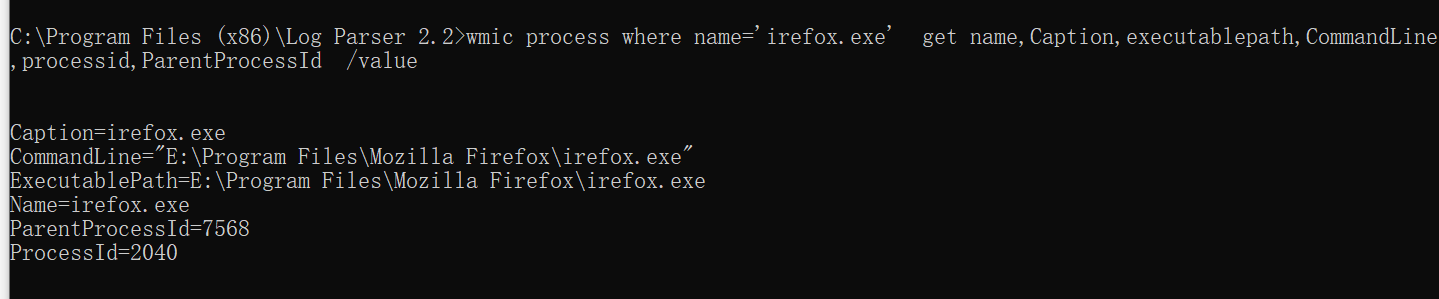
根据端口查看pid

netstat -ano | findstr "8080"

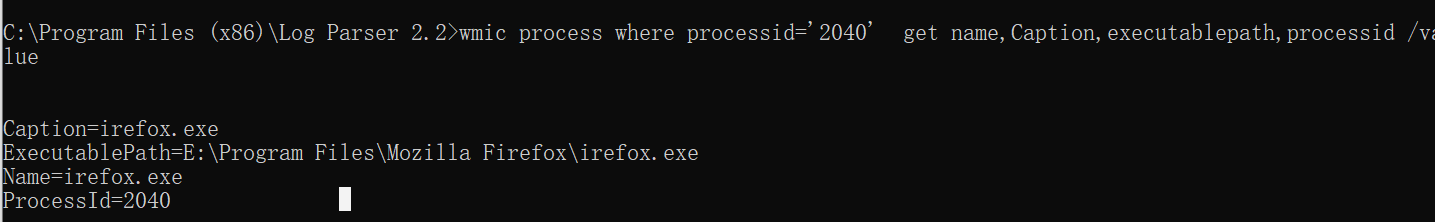


利用wmic查看进程执行时的命令

Wmic process where name='irefox.exe' get name,Caption,executablepath,CommandLine ,processid,ParentProcessId /value

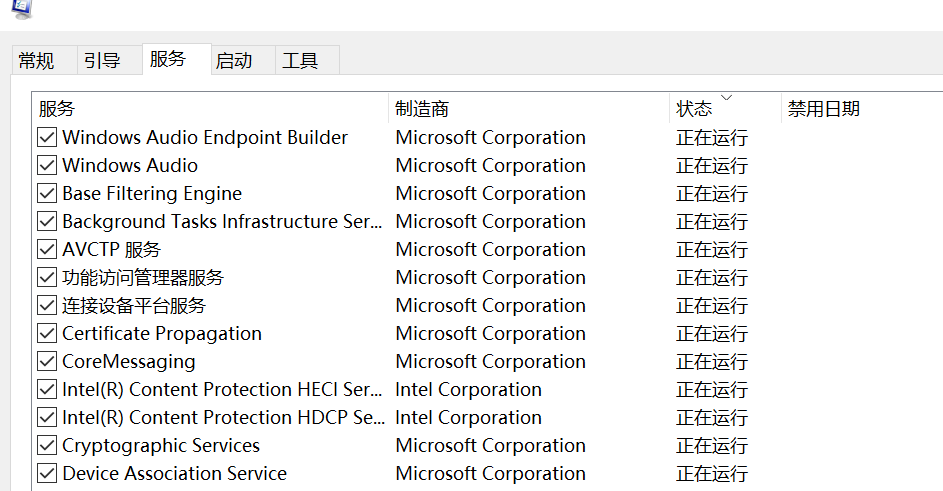


Wmic process where processid='2040' get name,Caption,executablepath,CommandLine ,processid,ParentProcessId /value



# 三、启动项检查

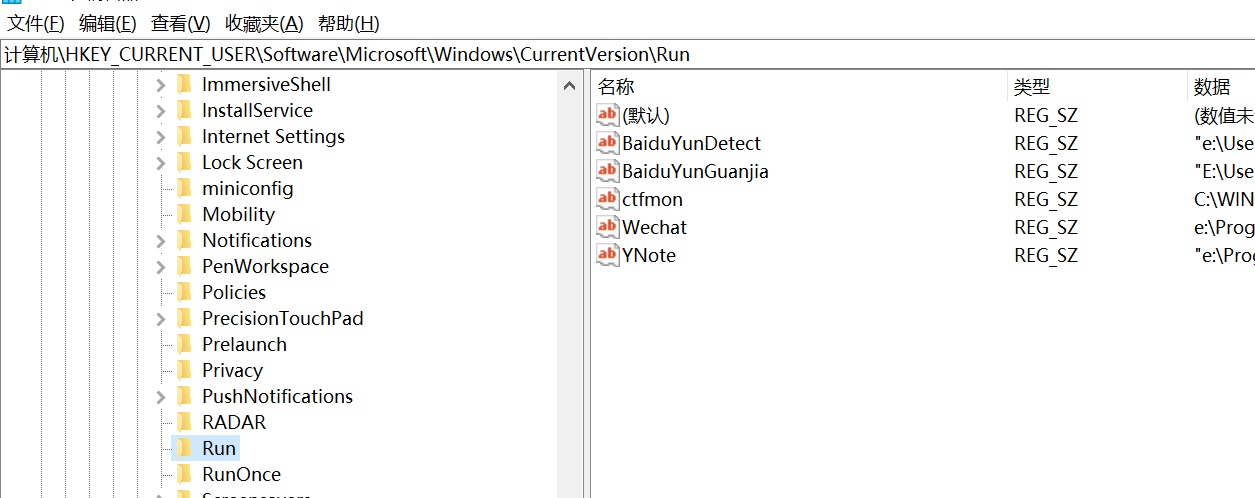
msconfig查看系统启动项



查看注册表是否有异常启动项

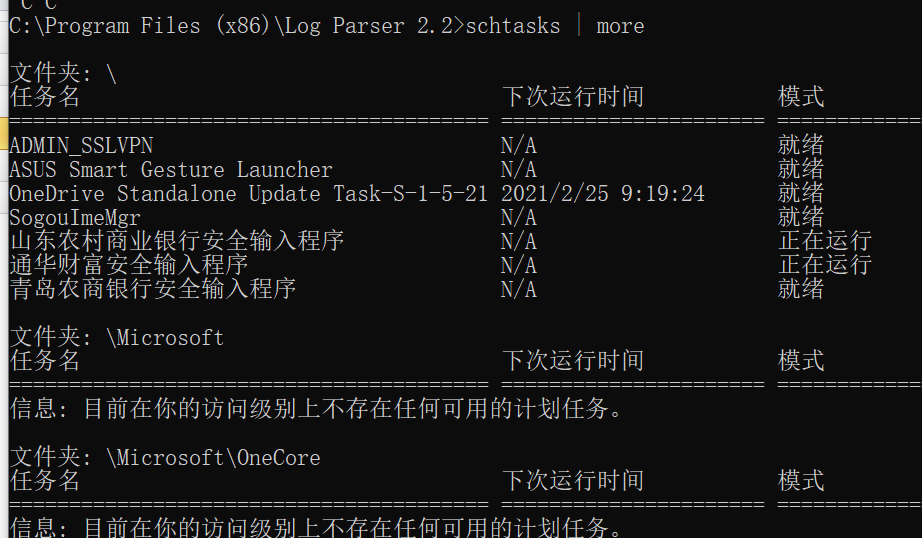
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

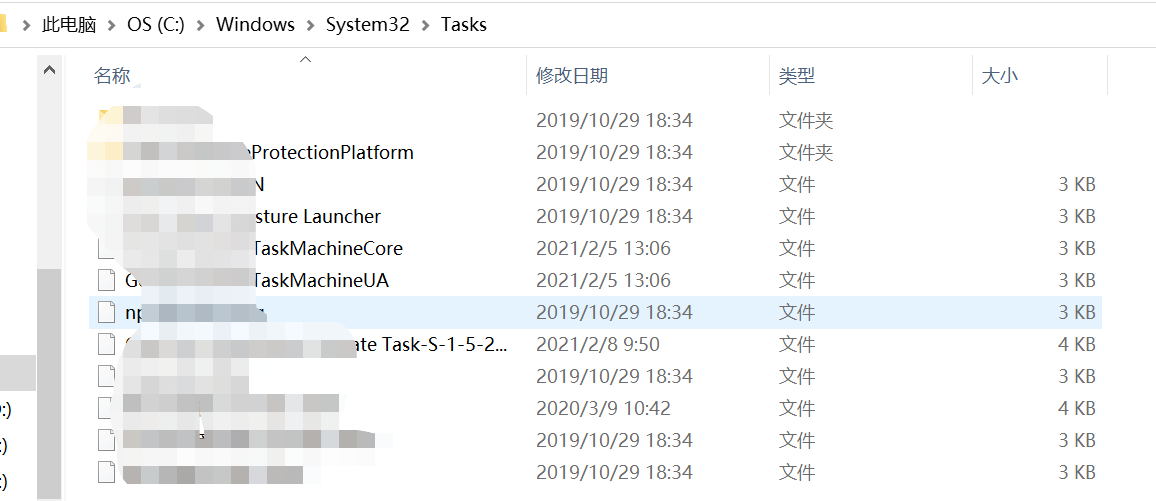


# 四、查看系统定时任务

Cmd下运行schtasks（win7系统利用at），查看定时任务



C:\Windows\System32\Tasks 查看任务清单



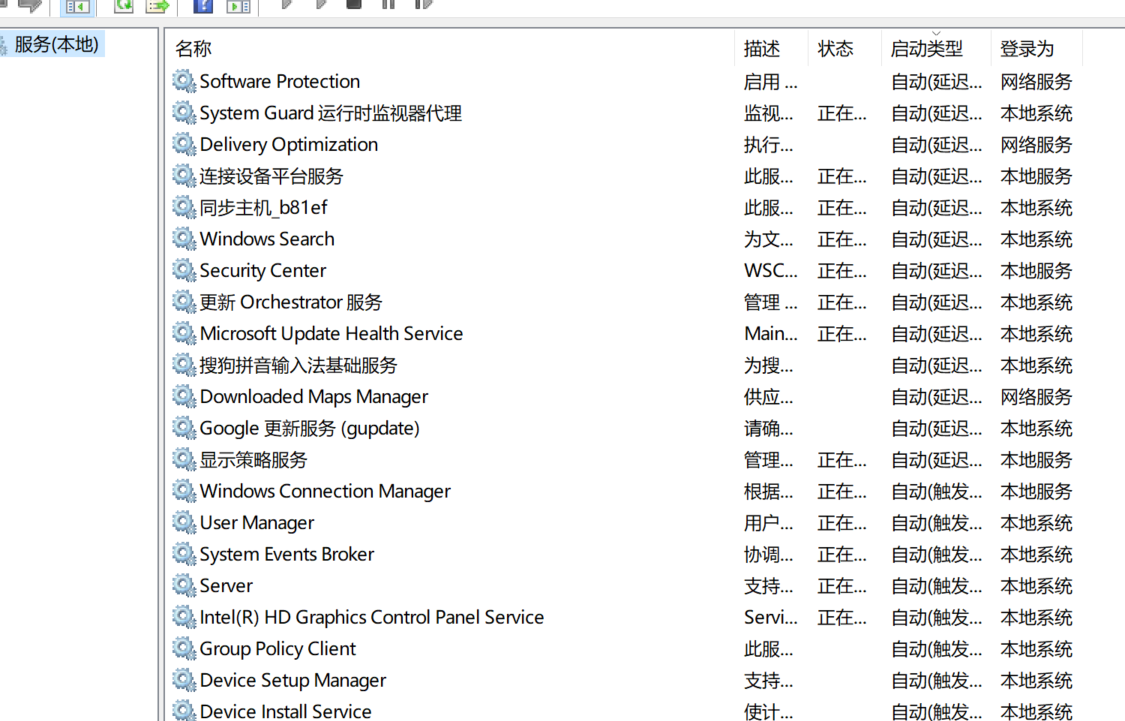
删除任务计划

建议删除任务计划时以管理员登录

SchTasks /Delete /TN 任务计划名称

# 五、查看系统服务

Services.msc



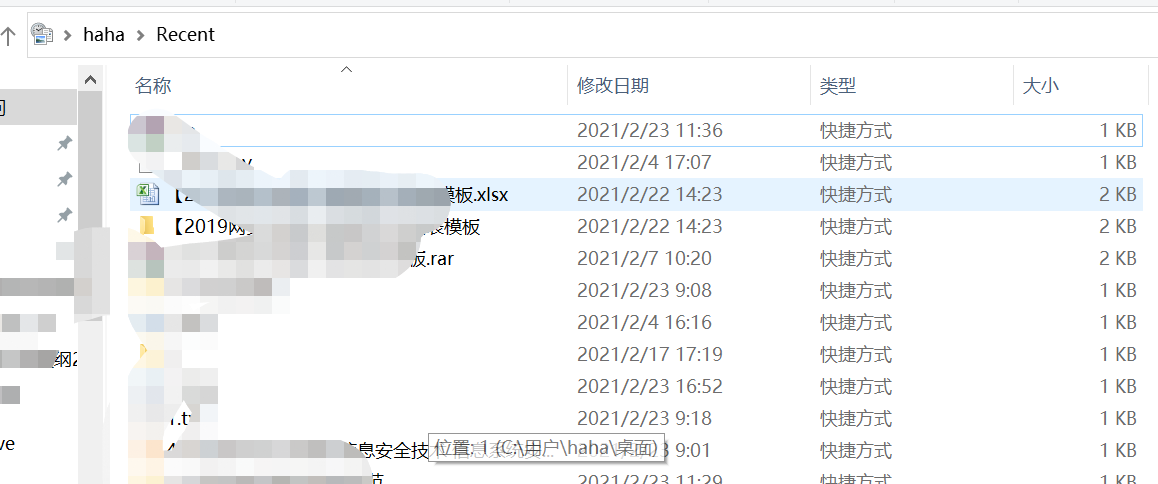
删除服务可从任务管理器中手动删除，也可使用命令：

sc stop [服务名称]停止服务后，

sc delete [服务名称]删除服务

# 六、文件查看

查看最近打开的文件，运行窗口中输入“%UserProfile%\Recent”



查看C:\Documents and Settings，C:\Users下是否存在可疑用户或文件