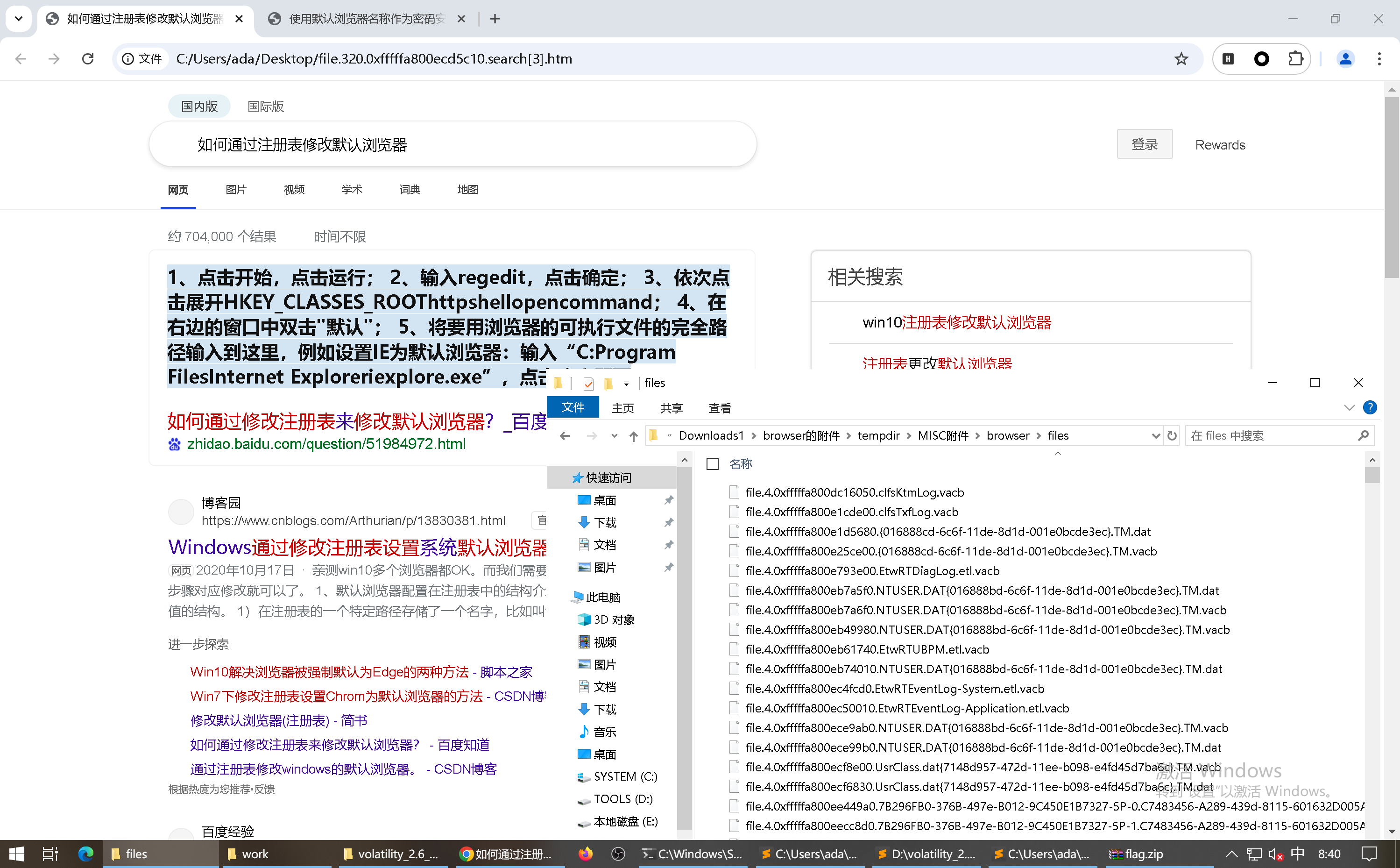
Browser

内存取证题，volatility 一步一步看，发现是win7sp1的，进程和浏览器历史记录没东西，然后提取全部的文件和注册表

volatility\_2.6\_win64\_standalone.exe -f browser.raw --profile Win7SP1x64 dumpfiles --dump-dir files > file.txt

volatility\_2.6\_win64\_standalone.exe -f browser.raw --profile Win7SP1x64 dumpregistry --dump-dir reg

翻看文件目录，发现有几个浏览器缓存的htm文件，打开后分别是“如何通过注册表修改默认浏览器”和“将默认浏览器作为密码安全么”，同时找到flag.zip。



volatility\_2.6\_win64\_standalone.exe -f browser.raw --profile Win7SP1x64 -o 0xfffff8a000609010 printkey -K "Classes\http\shell\open\command"

结果发现这个注册表路径下的值就是iexplorer，而且作为密码也不对，很坑的是，如果你仔细在网上搜寻，会发现有100条让你找上面这个路径，然后才有1条告诉你win7之后这个路径不好使了，要找

"Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice"

volatility\_2.6\_win64\_standalone.exe -f browser.raw --profile Win7SP1x64 -o 0xfffff8a001c33010 printkey -K "Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice"

REG\_SZ Progid : (S) Tor-Browser-V12.01.25

获得flag

