Neither RegRipper and Registry Viewer show either WordWheelQuery or TypedPath. From this, we can infer either that medved did not use the search bar or type in a direct internet address. This can be seen in figures 1 and 2.

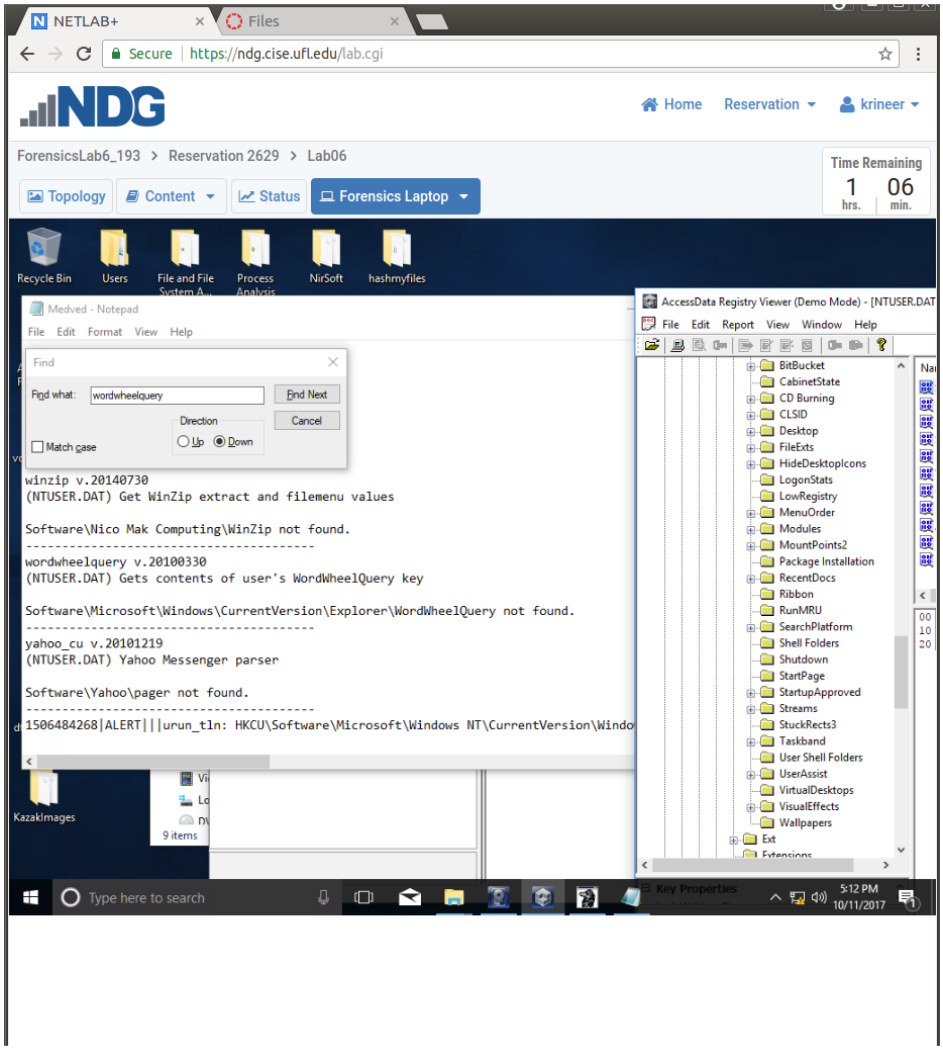

Figure 1: Results from searching for WordWheelQuery

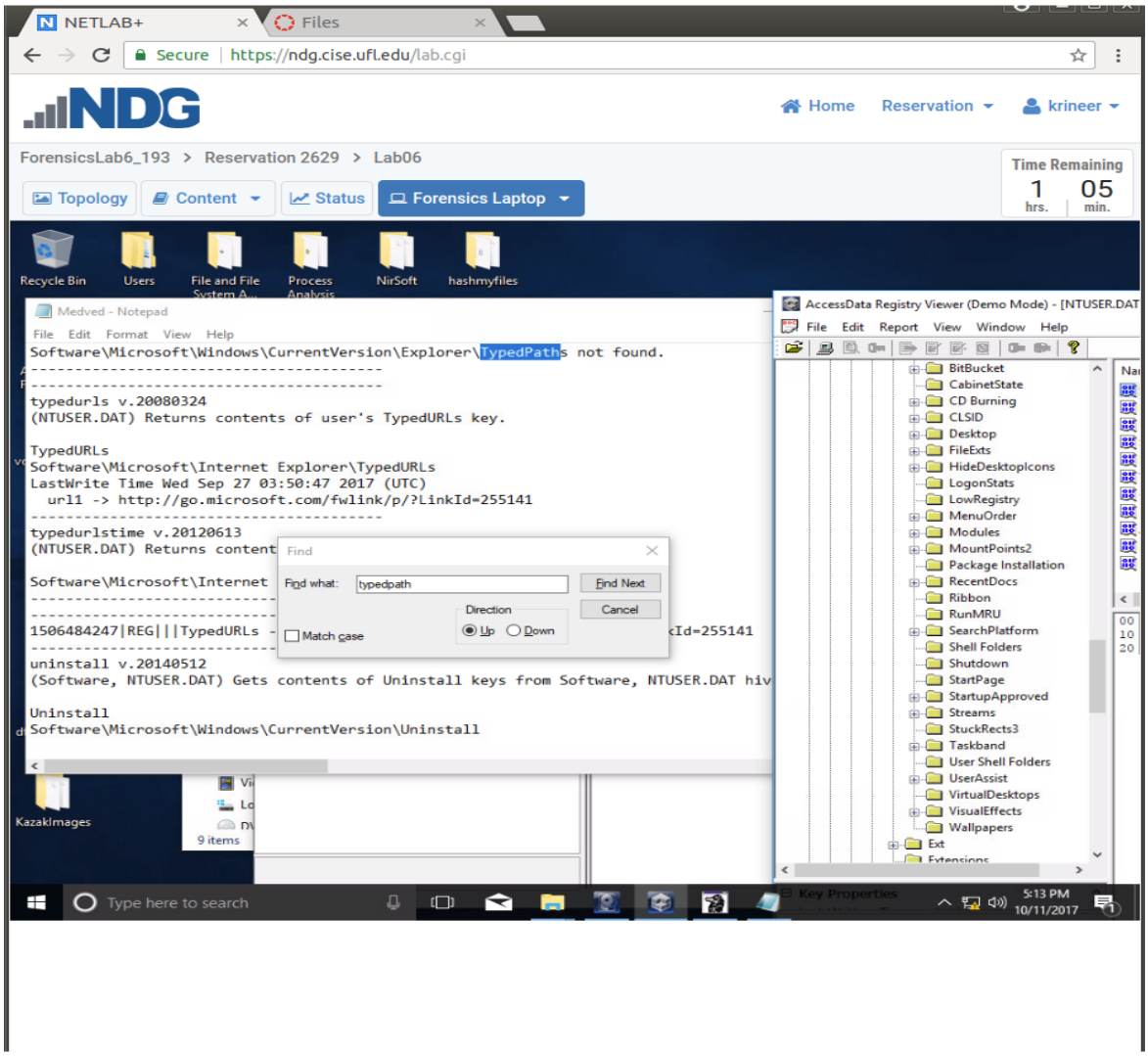

Figure 2: Results from searching for TypedPath

Opening Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs in registry viewer caused it to crash.

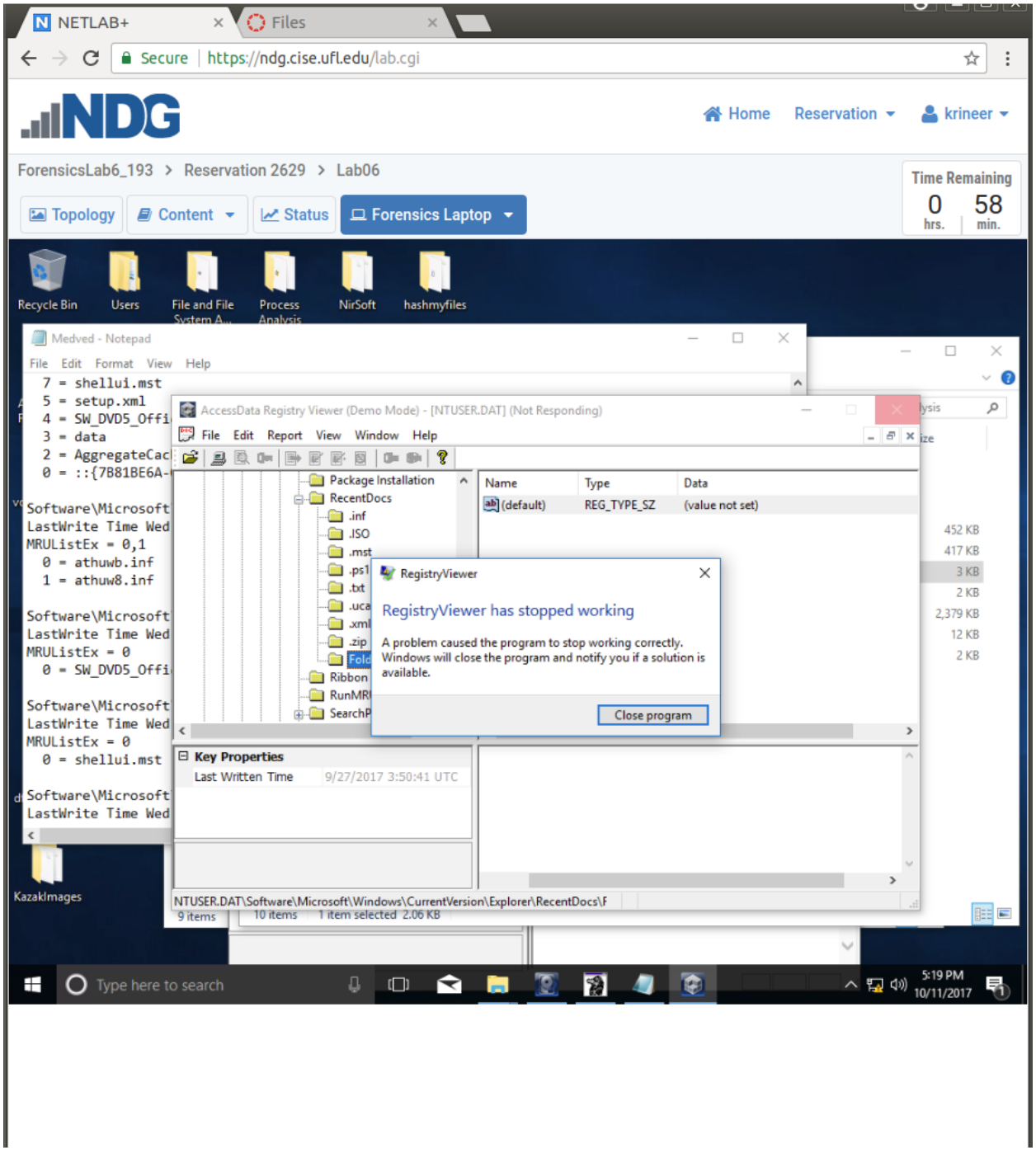

Figure 3: Registry Viewer crashes upon inspection of Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Using RegRipper, Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Reveals the contents of the directory. However, the dates attributed to the files are all the same. This most likely corrupted the directory, which explains the Registry Viewer crash. My educated guess is that these files were changed by a faulty anti-forensics program, causing the directory corruption.

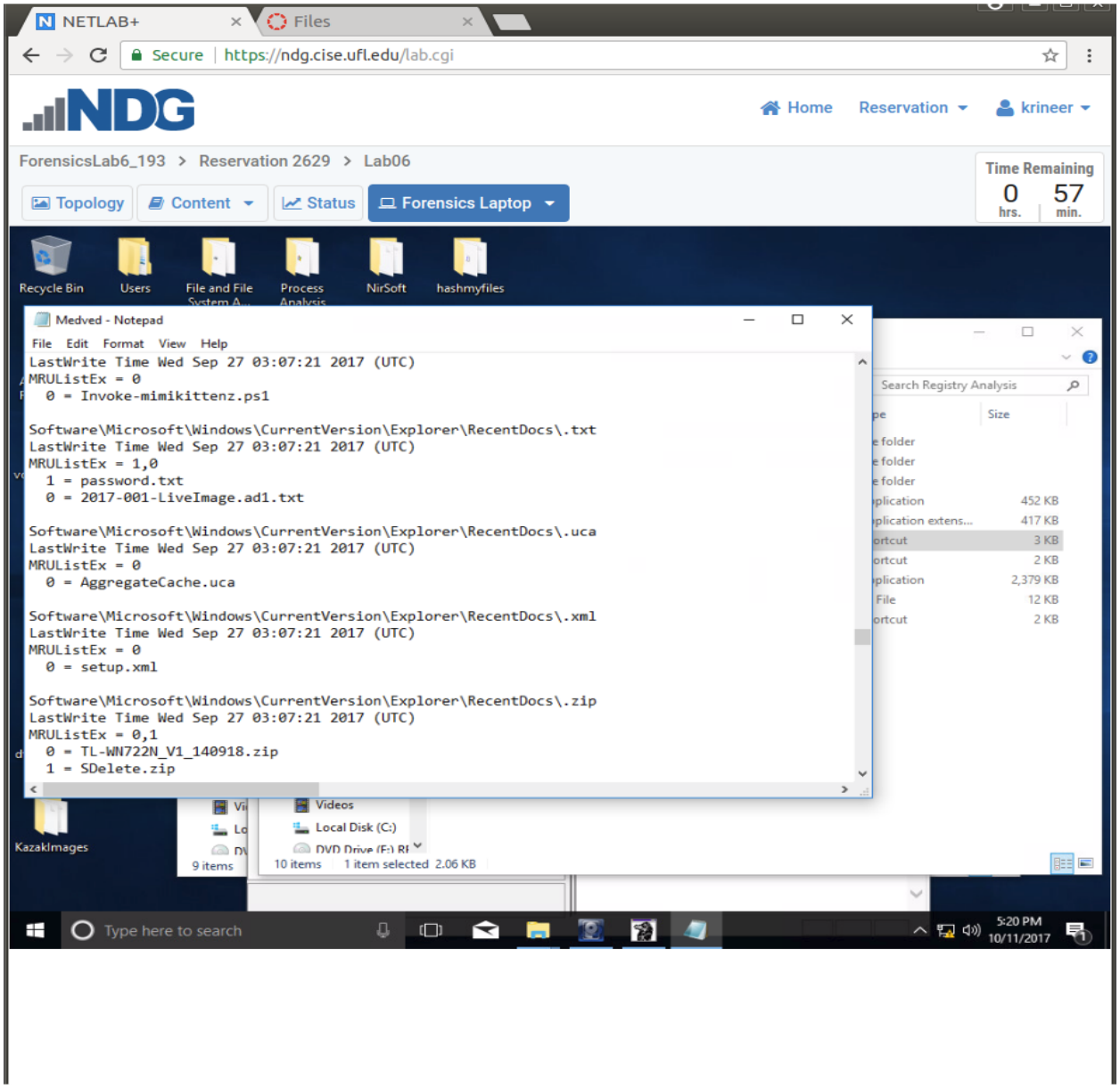

Figure 4: RegRipper showing the contents of Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs as well as the erroneous timestamps associated with the files inside

Inside the Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist filepath, we can find that FTK Imager has been run on the Kazak system. It seems to have been run twice.

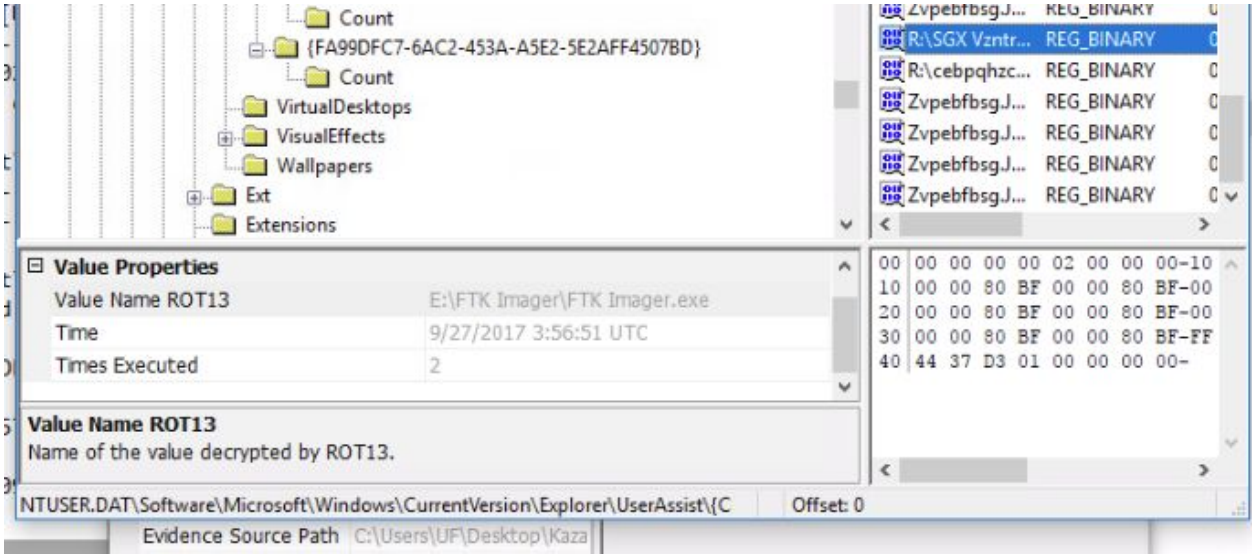

Figure 5: Evidence that Medved has run FTK Imager on his system