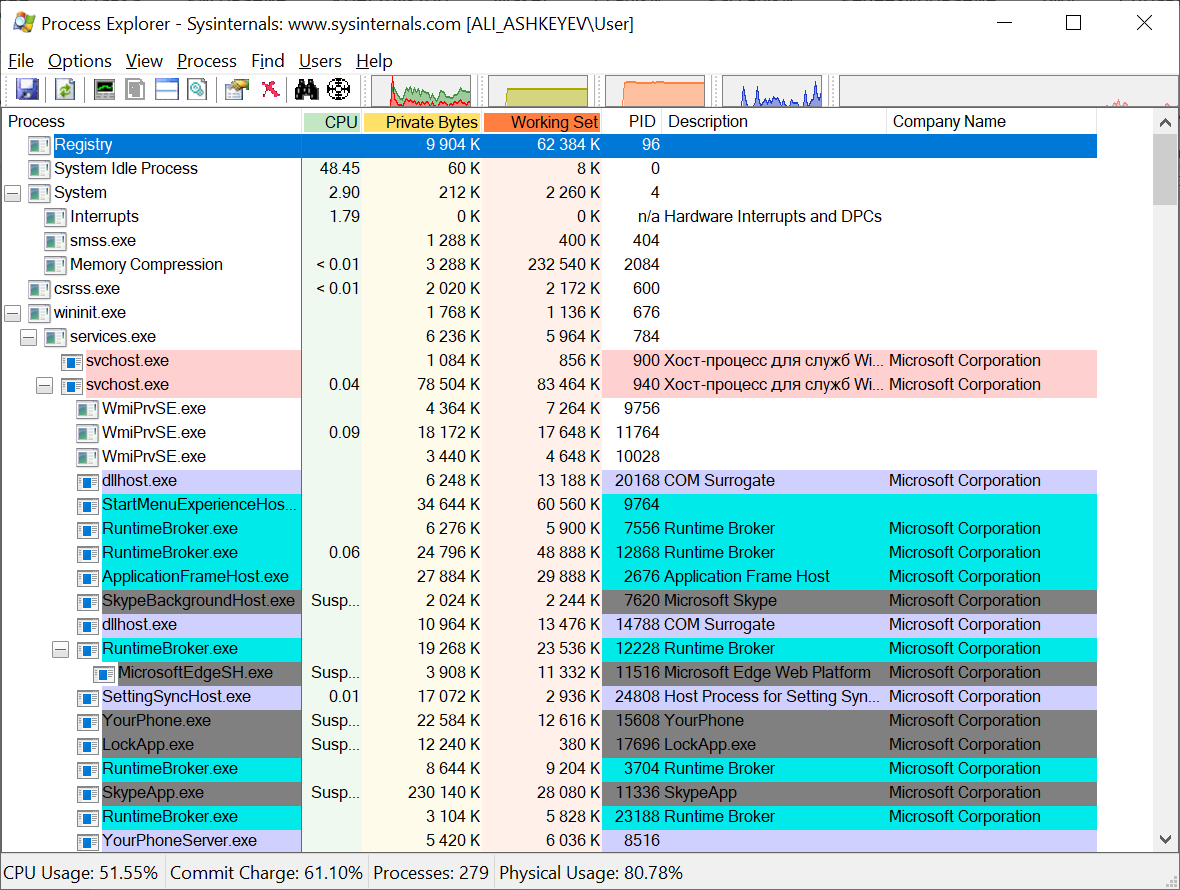
Ali Ashkeyev 18BD11079

Lab – Exploring Process, Threads, Handles, and Windows Registry

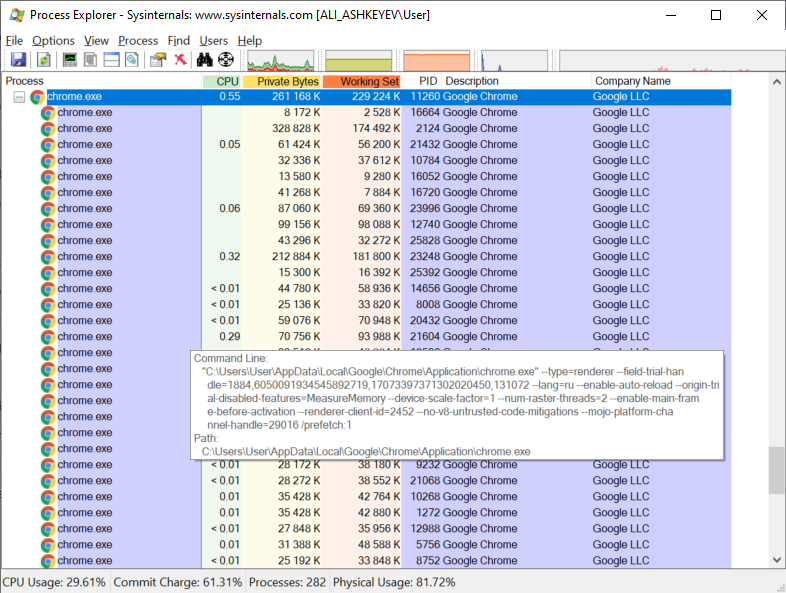
Part1: Exploring Processes

Step2: Explore an active process

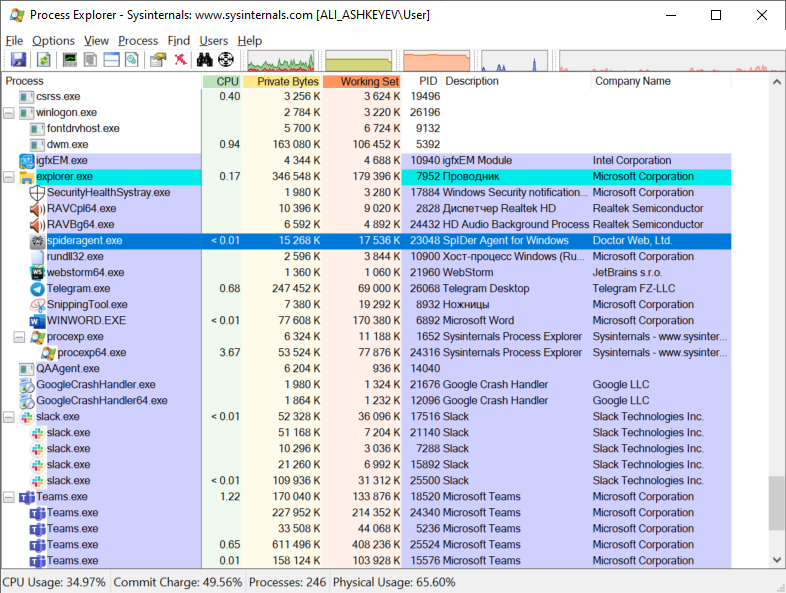
c. List of currently active processes



d. Drag Window’s Process icon



e. Kill process

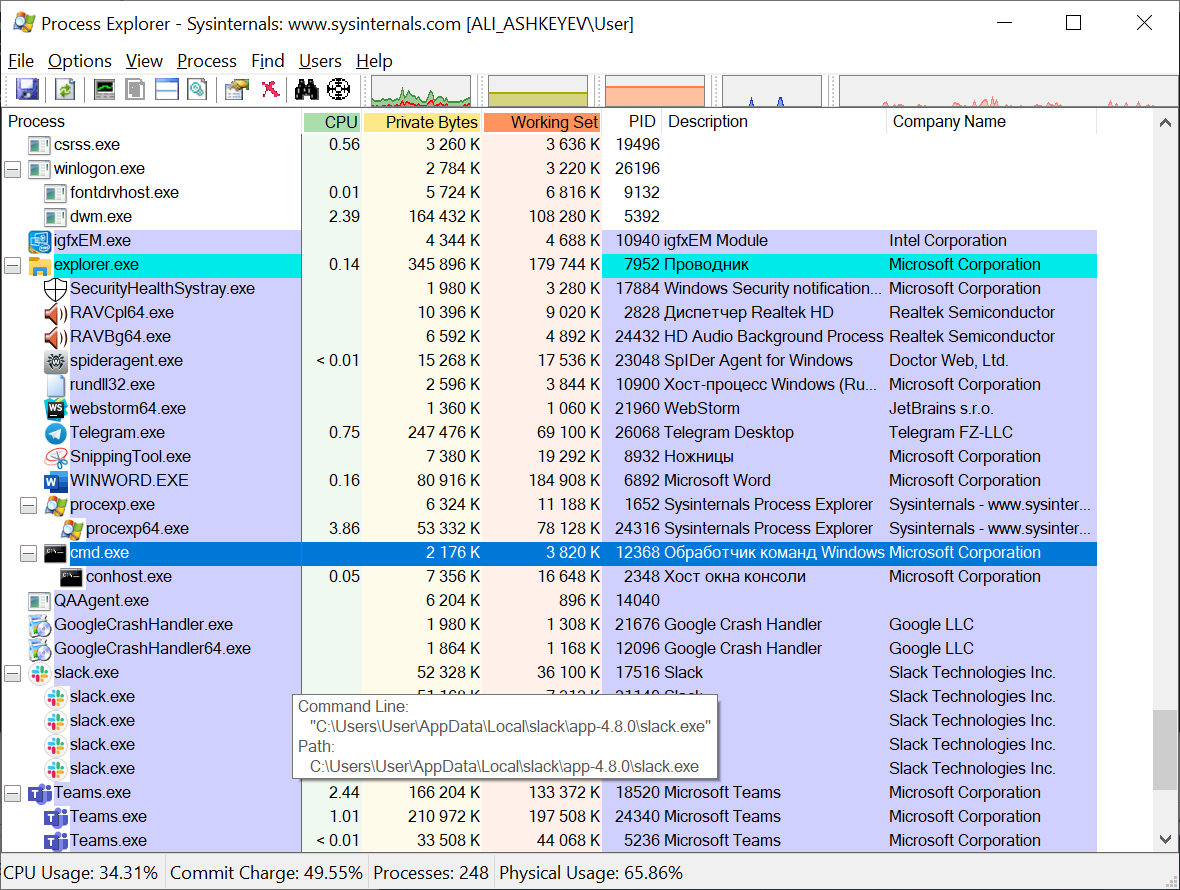


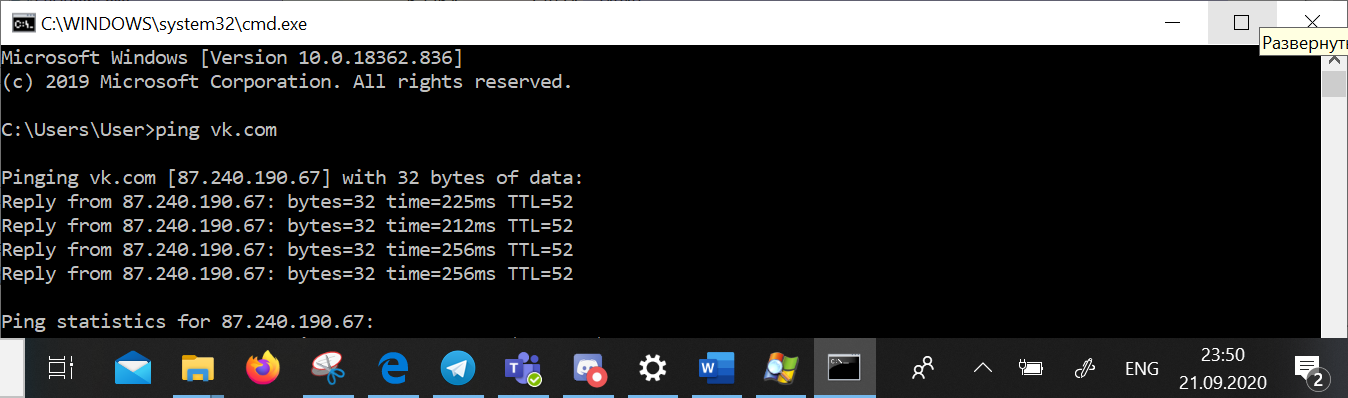
What happened to the web browser window when the process is killed?

It colored red and after it is closed with all tree.

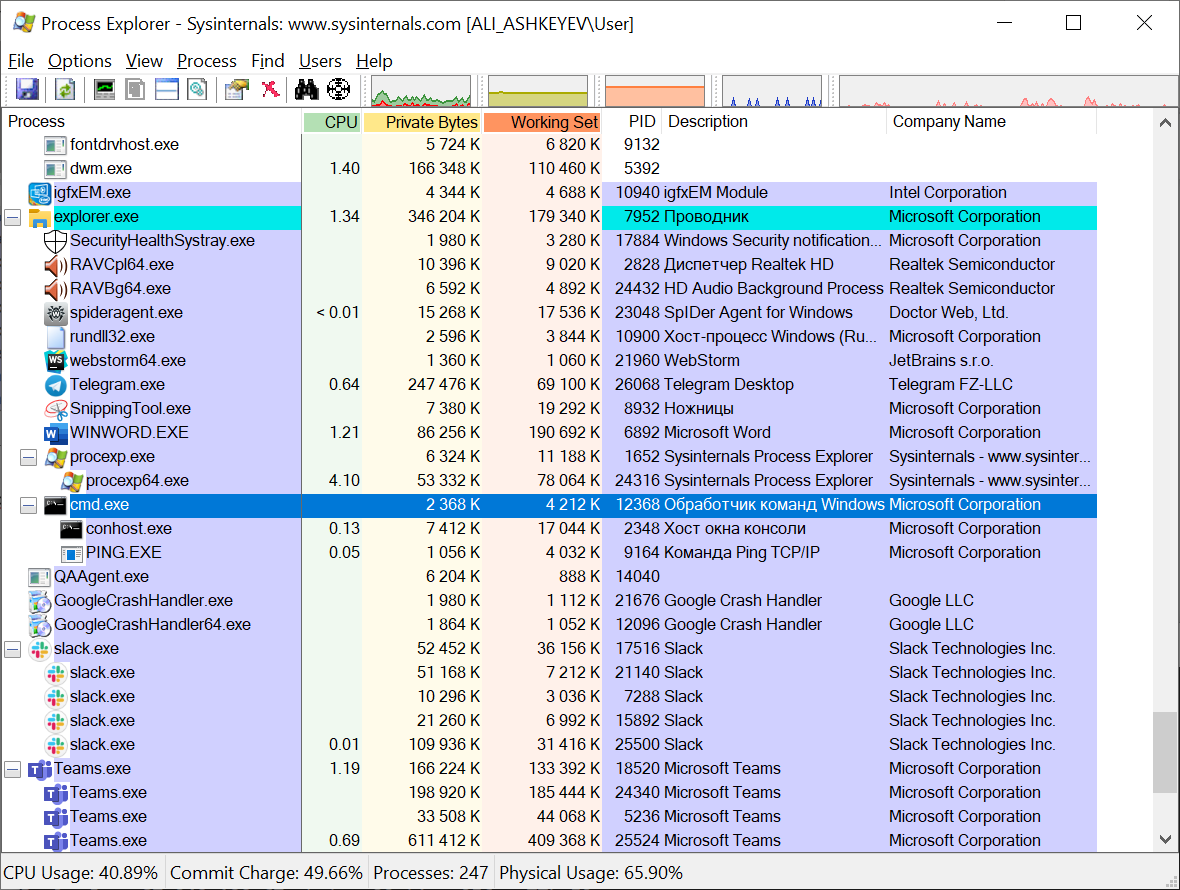
Step 3: Start another process

c. Drag Window’s Process icon to cmd



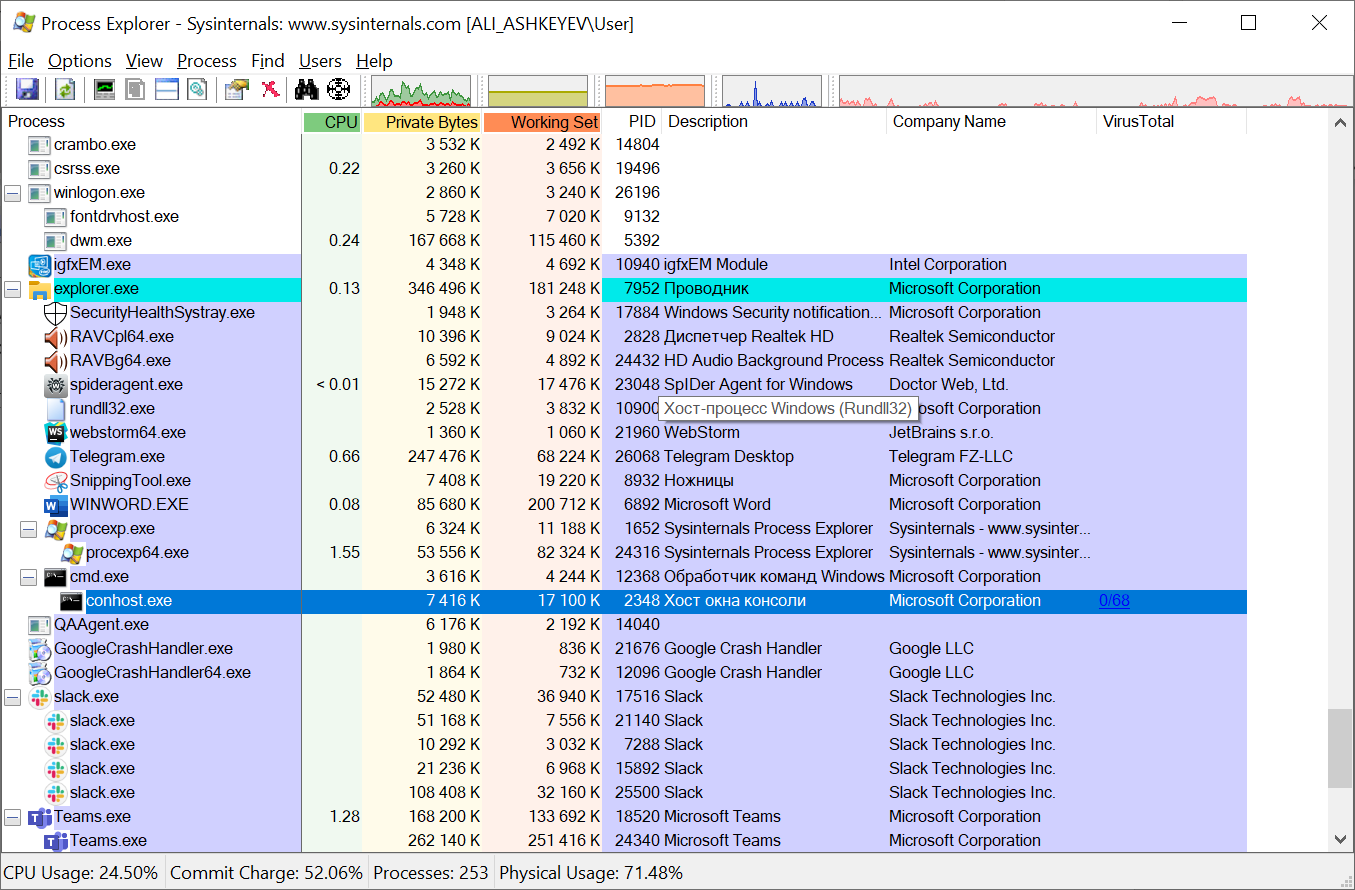


d. Navigate to the Command Prompt window. Start a ping at the prompt and observe the changes under the cmd.exe process. What happened during the ping process?

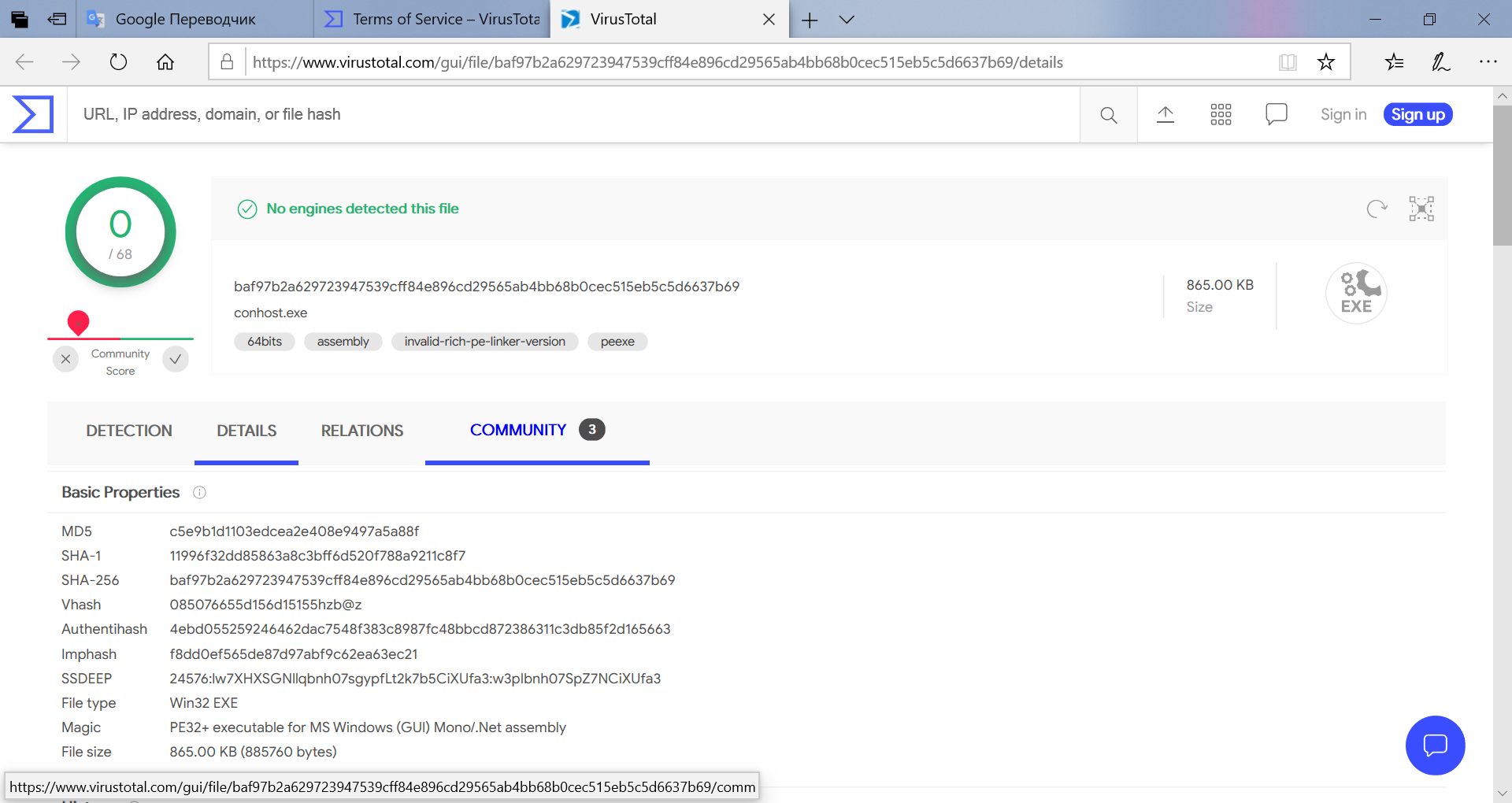


Cmd.exe opened ping.exe as a child program. After finishing sending queries to server ping.exe closed as child in Process Explorer, but remained as a window.

e. Check Virtual Total

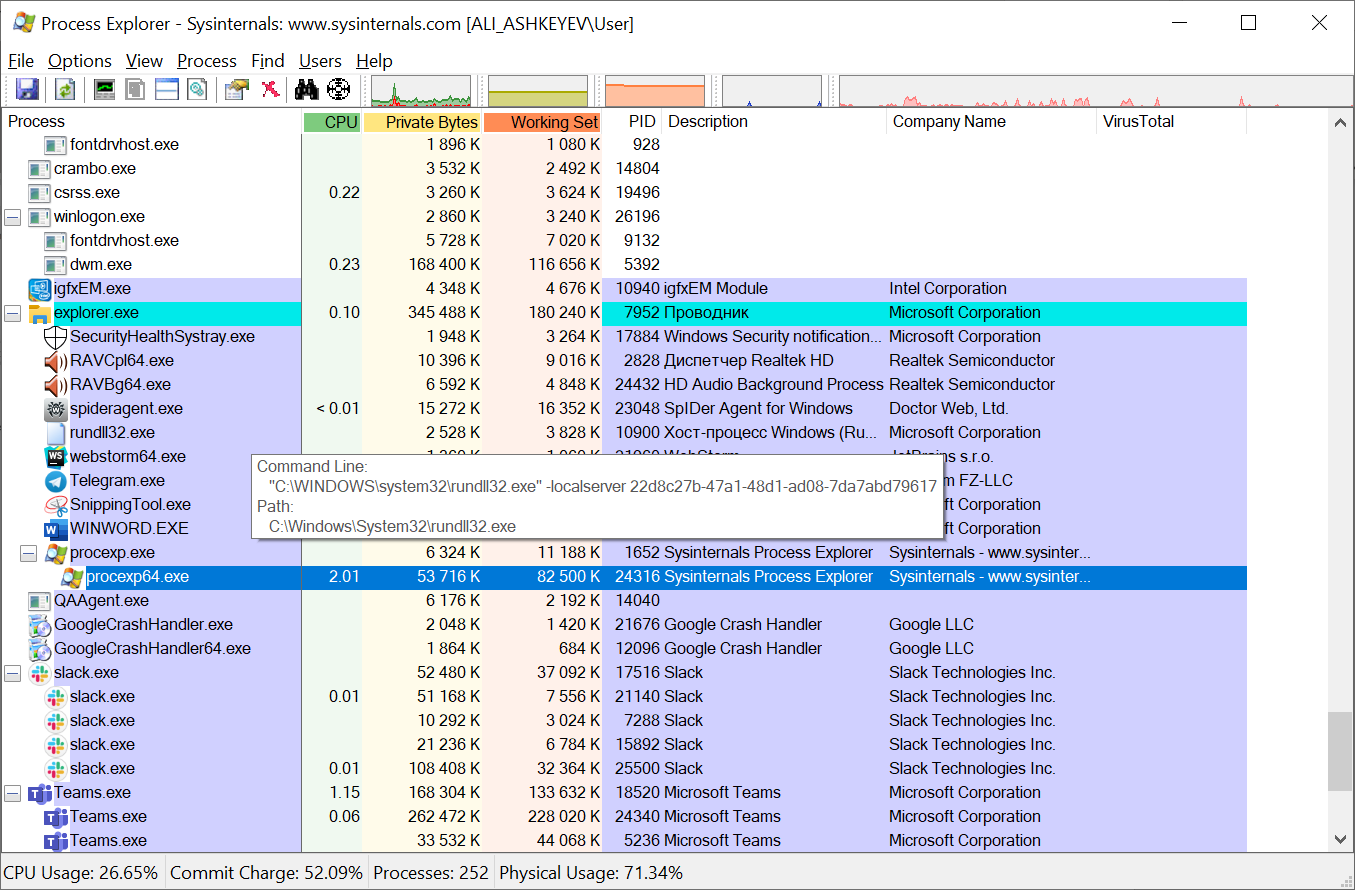


f. Link redirection to virustotal website with description of file



g. Right-click the cmd.exe process and select Kill Process. What happened to the child process conhost.exe?

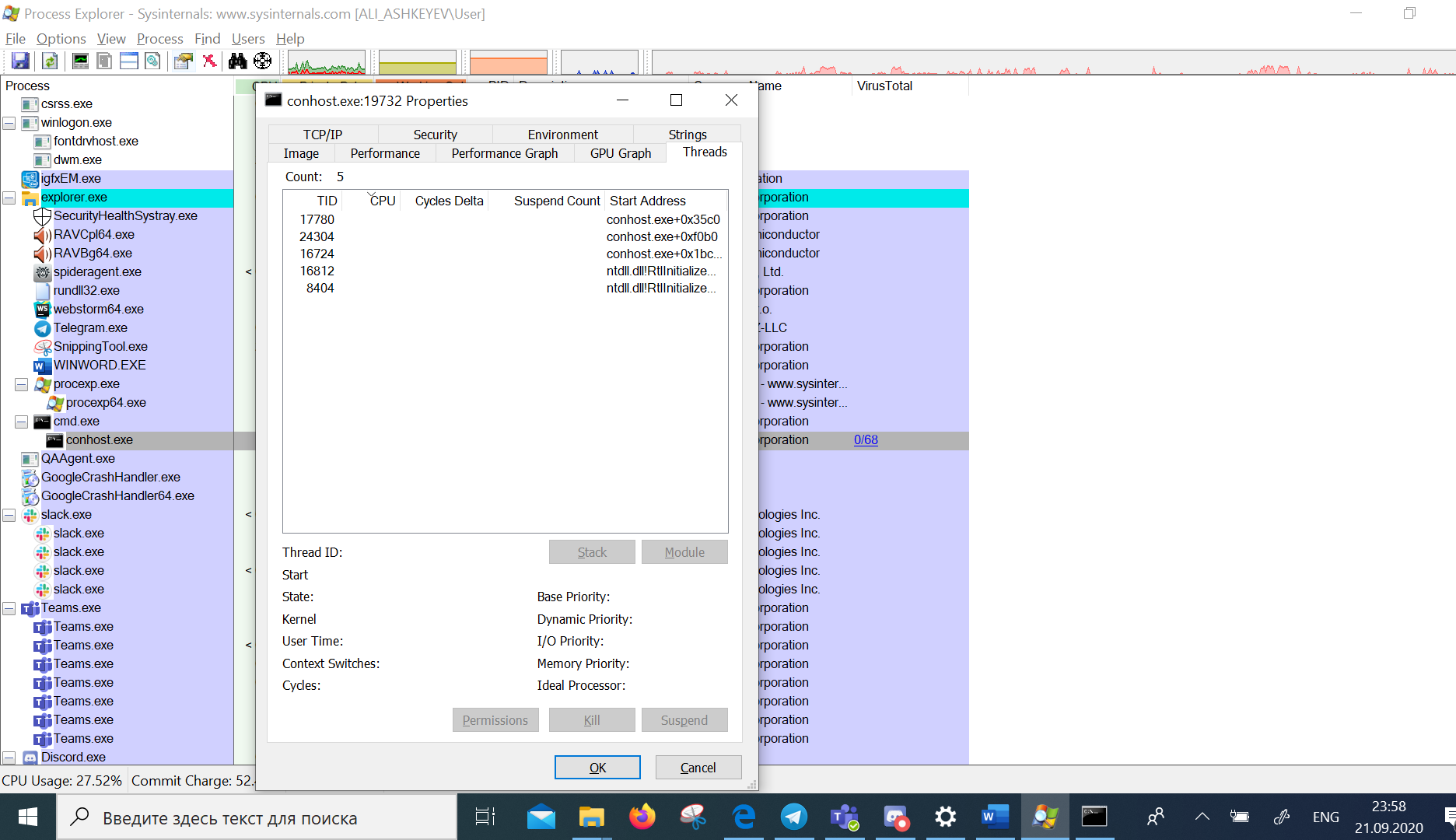
With cmd.exe it was killed conhost.exe too.



Part2 Exploring Threads and Handles

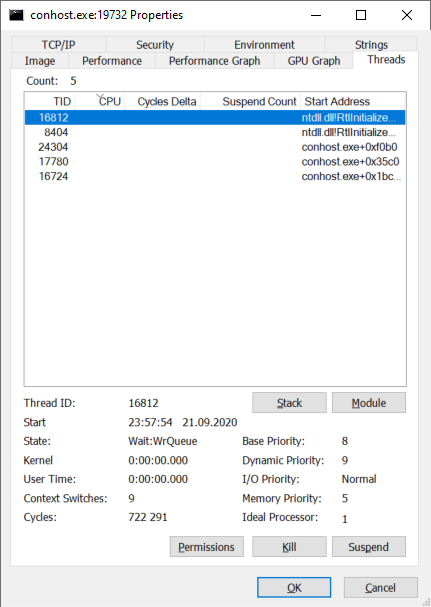
Step 1: Explore threads

b. conhost.exe properties.



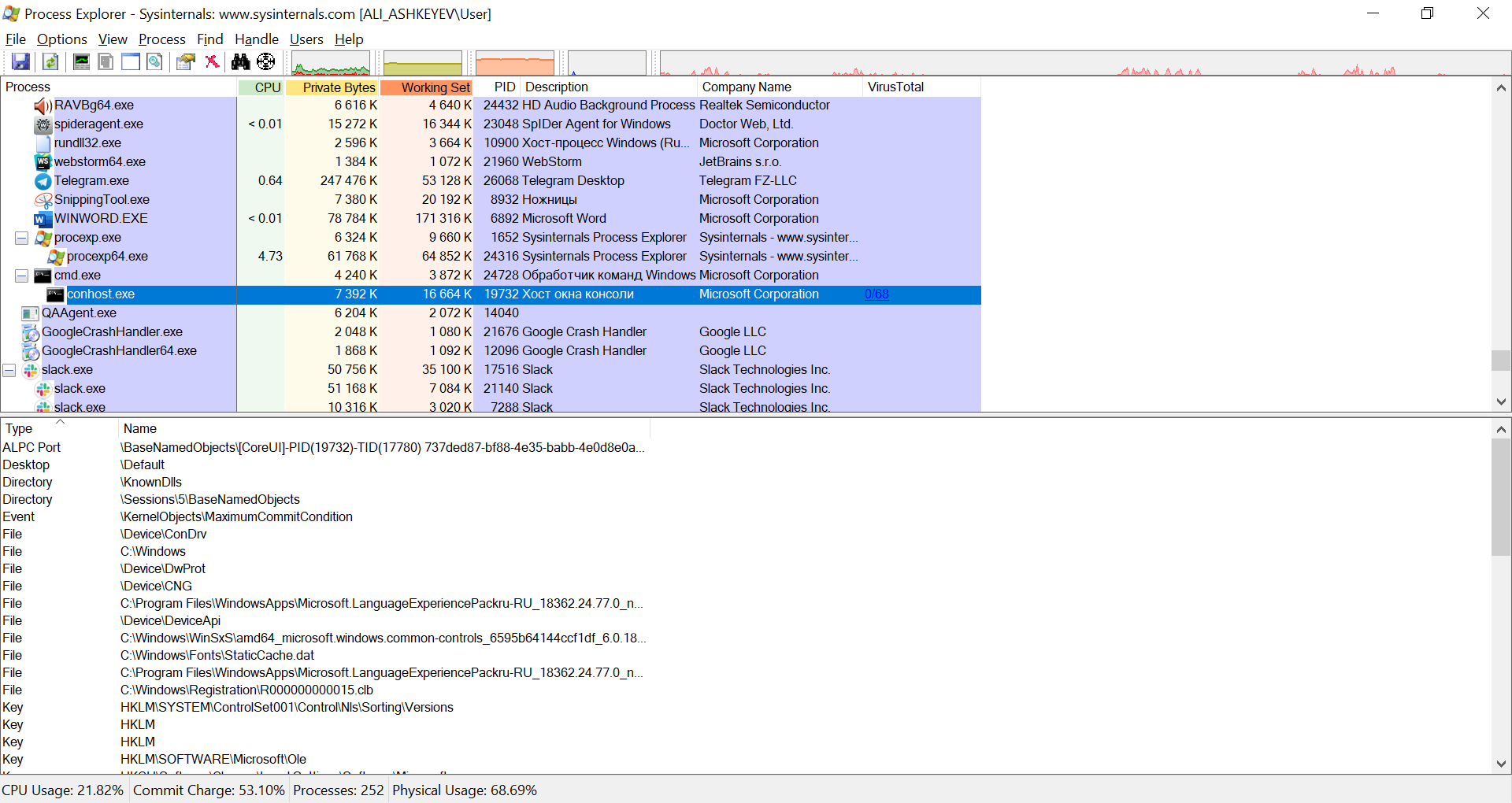
c. Examine the details of the thread. What type of information is available in the Properties window?

There is written Thread ID, CPU, Cycles Delta, suspend Count and start address information of each thread. If click for one of them there is visible more information in details



Also there are several tabs as TCP/IP, security, environment, strings, image, performance, performance graph, GPU graph and threads in properties window.

Step 2: Explore handles

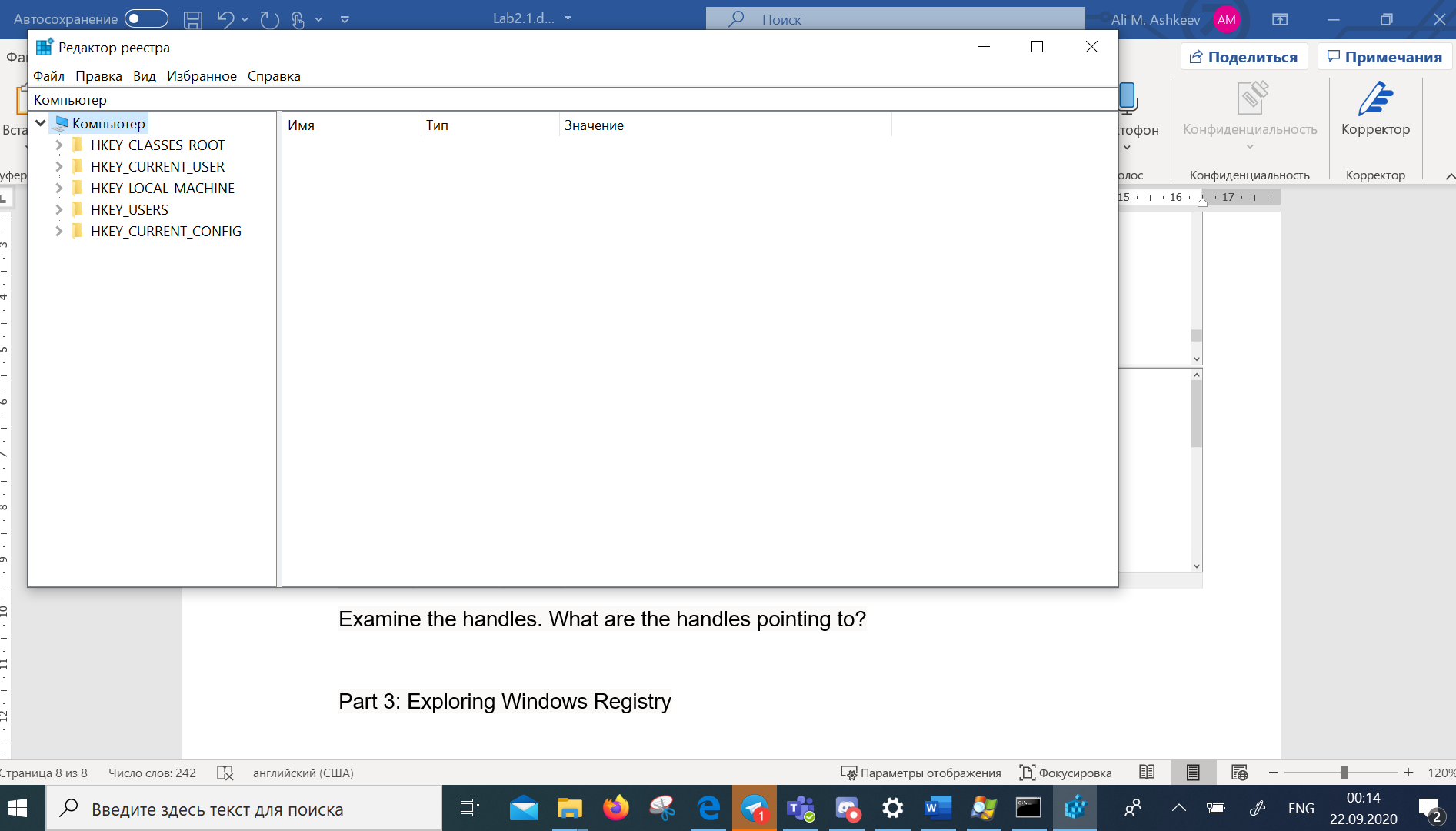


Examine the handles. What are the handles pointing to?

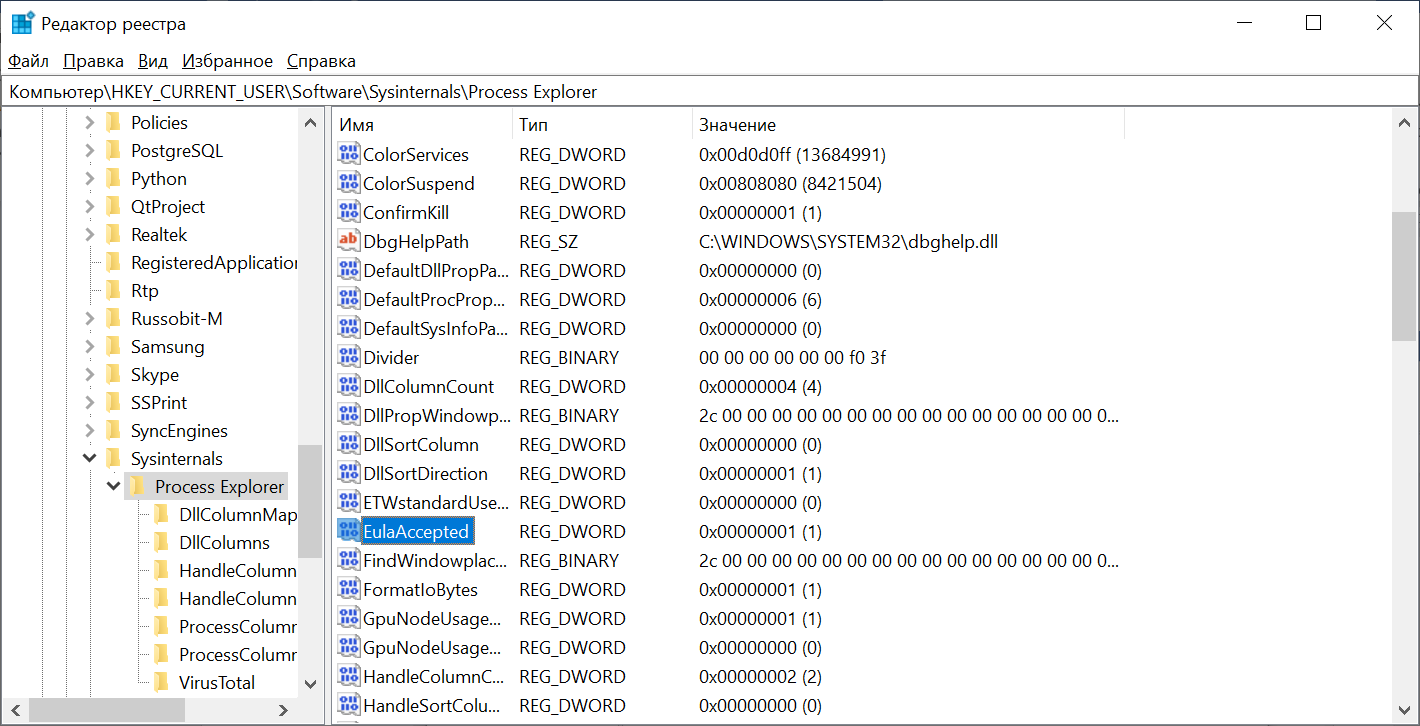
The handles are pointing to files, registry keys, and threads.

Part 3: Exploring Windows Registry

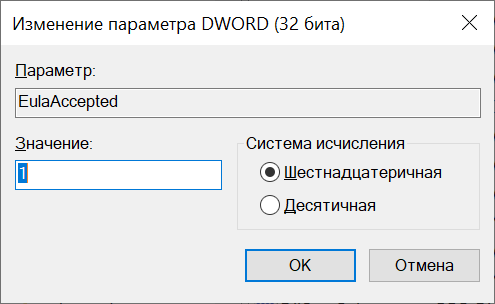
1. Regedit window



1. EulaAccepted key

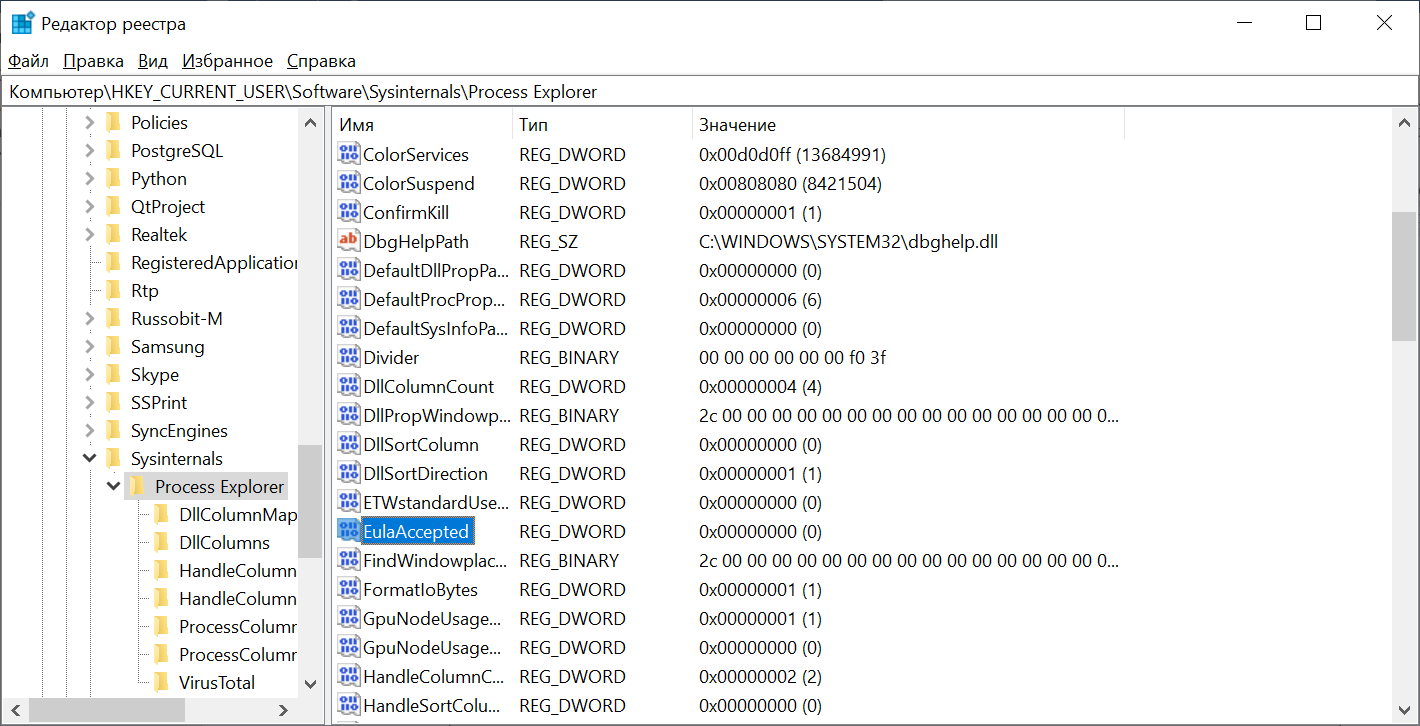


1. Value data of EulaAccepted



1. What is value for this registry key in the Data column?

Value for registry key is 0x00000000(0)



1. When you open the Process Explorer, what did you see?

It was opened another precexp.exe with precexp64.exe

