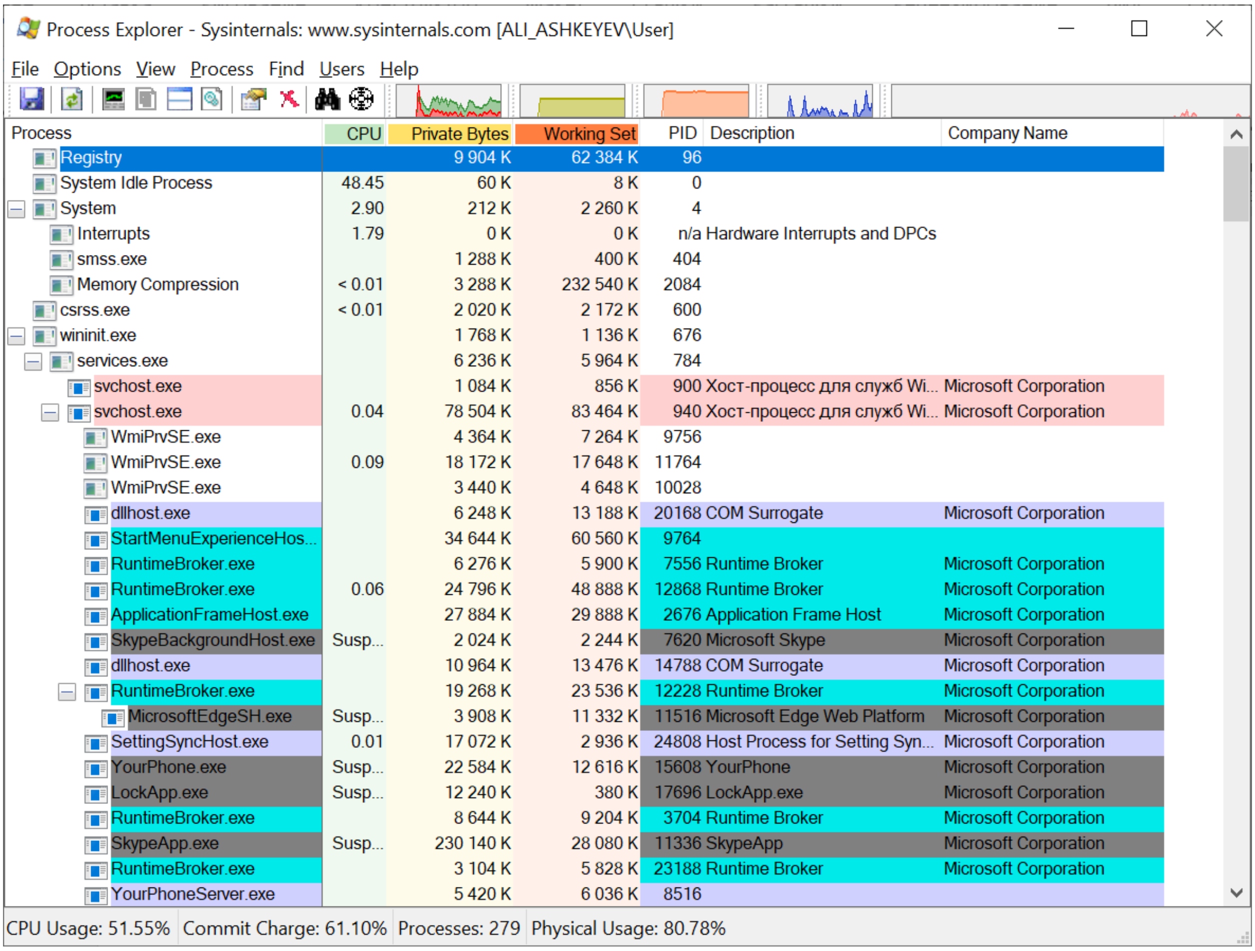
Ali Ashkeyev 18BD11079

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

Part1: Exploring Processes

Step2: Explore an active process

c. List of currently active processes

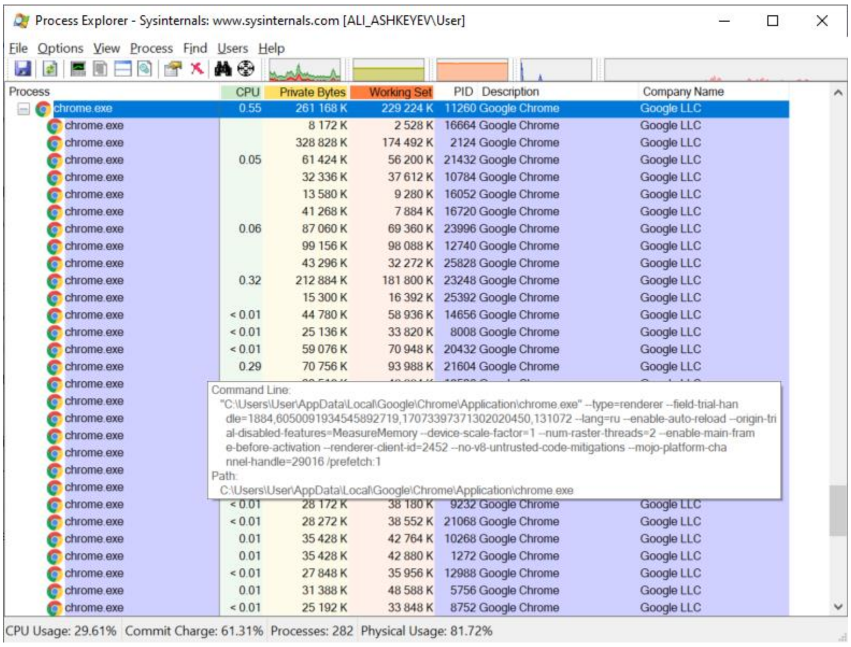


Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		9 904 K	62 384 K	96		
System Idle Process	48.45	60 K	8 K	0		
System	2.90	212 K	2 260 K	4		
Interrupts	1.79	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 288 K	400 K	404		
Memory Compression	< 0.01	3 288 K	232 540 K	2084		
csrss.exe	< 0.01	2 020 K	2 172 K	600		
wininit.exe		1 768 K	1 136 K	676		
services.exe		6 236 K	5 964 K	784		
svchost.exe		1 084 K	856 K	900	Хост-процесс для служб Wi...	Microsoft Corporation
svchost.exe	0.04	78 504 K	83 464 K	940	Хост-процесс для служб Wi...	Microsoft Corporation
WmiPrvSE.exe		4 364 K	7 264 K	9756		
WmiPrvSE.exe	0.09	18 172 K	17 648 K	11764		
WmiPrvSE.exe		3 440 K	4 648 K	10028		
dllhost.exe		6 248 K	13 188 K	20168	COM Surrogate	Microsoft Corporation
StartMenuExperienceHos...		34 644 K	60 560 K	9764		
RuntimeBroker.exe		6 276 K	5 900 K	7556	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	0.06	24 796 K	48 888 K	12868	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe		27 884 K	29 888 K	2676	Application Frame Host	Microsoft Corporation
SkypeBackgroundHost.exe	Susp...	2 024 K	2 244 K	7620	Microsoft Skype	Microsoft Corporation
dllhost.exe		10 964 K	13 476 K	14788	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		19 268 K	23 536 K	12228	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH.exe	Susp...	3 908 K	11 332 K	11516	Microsoft Edge Web Platform	Microsoft Corporation
SettingSyncHost.exe	0.01	17 072 K	2 936 K	24808	Host Process for Setting Syn...	Microsoft Corporation
YourPhone.exe	Susp...	22 584 K	12 616 K	15608	YourPhone	Microsoft Corporation
LockApp.exe	Susp...	12 240 K	380 K	17696	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		8 644 K	9 204 K	3704	Runtime Broker	Microsoft Corporation
SkypeApp.exe	Susp...	230 140 K	28 080 K	11336	SkypeApp	Microsoft Corporation
RuntimeBroker.exe		3 104 K	5 828 K	23188	Runtime Broker	Microsoft Corporation
YourPhoneServer.exe		5 420 K	6 036 K	8516		

CPU Usage: 51.55% Commit Charge: 61.10% Processes: 279 Physical Usage: 80.78%

d. Drag Window’s Process icon



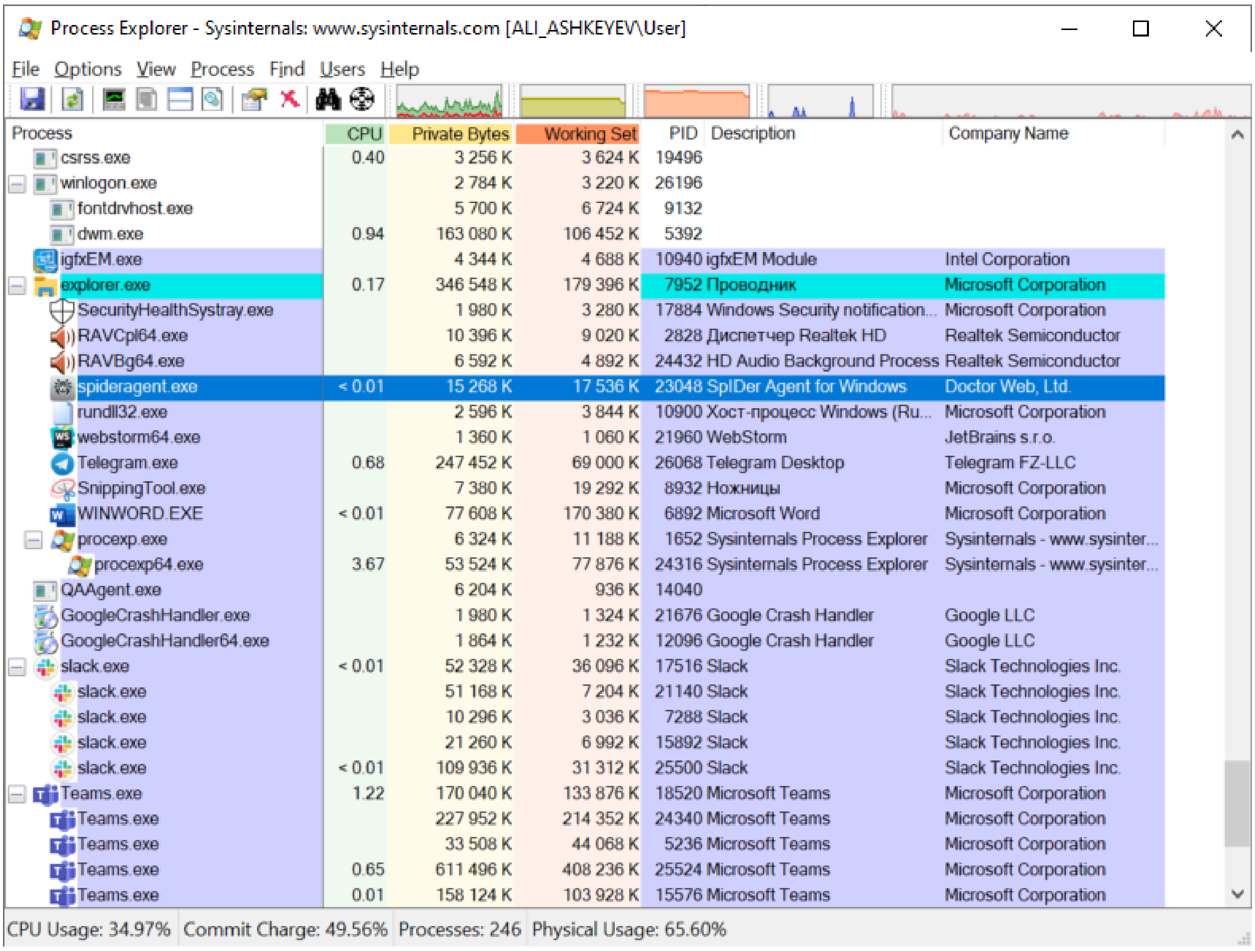
Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
chrome.exe	0.55	261 168 K	229 224 K	11260	Google Chrome	Google LLC
chrome.exe		8 172 K	2 528 K	16664	Google Chrome	Google LLC
chrome.exe		328 828 K	174 492 K	2124	Google Chrome	Google LLC
chrome.exe	0.05	61 424 K	56 200 K	21432	Google Chrome	Google LLC
chrome.exe		32 336 K	37 612 K	10784	Google Chrome	Google LLC
chrome.exe		13 580 K	9 280 K	16052	Google Chrome	Google LLC
chrome.exe		41 268 K	7 884 K	16720	Google Chrome	Google LLC
chrome.exe	0.06	87 060 K	69 360 K	23996	Google Chrome	Google LLC
chrome.exe		99 156 K	98 088 K	12740	Google Chrome	Google LLC
chrome.exe		43 296 K	32 272 K	25828	Google Chrome	Google LLC
chrome.exe	0.32	212 884 K	181 800 K	23248	Google Chrome	Google LLC
chrome.exe		15 300 K	16 392 K	25392	Google Chrome	Google LLC
chrome.exe	< 0.01	44 780 K	58 936 K	14656	Google Chrome	Google LLC
chrome.exe	< 0.01	25 136 K	33 820 K	8008	Google Chrome	Google LLC
chrome.exe	< 0.01	59 076 K	70 948 K	20432	Google Chrome	Google LLC
chrome.exe	0.29	70 756 K	93 988 K	21604	Google Chrome	Google LLC
chrome.exe						
chrome.exe						
chrome.exe						
chrome.exe						
chrome.exe						
chrome.exe						
chrome.exe						
chrome.exe	< 0.01	28 172 K	38 180 K	9232	Google Chrome	Google LLC
chrome.exe	< 0.01	28 272 K	38 552 K	21068	Google Chrome	Google LLC
chrome.exe	0.01	35 428 K	42 764 K	10268	Google Chrome	Google LLC
chrome.exe	0.01	35 428 K	42 880 K	1272	Google Chrome	Google LLC
chrome.exe	< 0.01	27 848 K	35 956 K	12988	Google Chrome	Google LLC
chrome.exe	0.01	31 388 K	48 588 K	5756	Google Chrome	Google LLC
chrome.exe	< 0.01	25 192 K	33 848 K	8752	Google Chrome	Google LLC

```
Command Line:
  "C:\Users\User\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-han
   dle=1884,6050091934545892719,17073397371302020450,131072 --lang=ru --enable-auto-reload --origin-tri
   al-disabled-features=MeasureMemory --device-scale-factor=1 --num-raster-threads=2 --enable-main-fram
   e-before-activation --renderer-client-id=2452 --no-v8-untrusted-code-mitigations --mojo-platform-cha
   nnel-handle=29016 /prefetch:1
Path:
  C:\Users\User\AppData\Local\Google\Chrome\Application\chrome.exe
```

CPU Usage: 29.61% Commit Charge: 61.31% Processes: 282 Physical Usage: 81.72%

e. Kill process



Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
csrss.exe	0.40	3 256 K	3 624 K	19496		
winlogon.exe		2 784 K	3 220 K	26196		
fontdrvhost.exe		5 700 K	6 724 K	9132		
dwm.exe	0.94	163 080 K	106 452 K	5392		
igfxEM.exe		4 344 K	4 688 K	10940	igfxEM Module	Intel Corporation
explorer.exe	0.17	346 548 K	179 396 K	7952	Проводник	Microsoft Corporation
SecurityHealthSystray.exe		1 980 K	3 280 K	17884	Windows Security notification...	Microsoft Corporation
RAVCpl64.exe		10 396 K	9 020 K	2828	Диспетчер Realtek HD	Realtek Semiconductor
RAVBg64.exe		6 592 K	4 892 K	24432	HD Audio Background Process	Realtek Semiconductor
spideragent.exe	< 0.01	15 268 K	17 536 K	23048	SpIDer Agent for Windows	Doctor Web, Ltd.
rundll32.exe		2 596 K	3 844 K	10900	Хост-процесс Windows (Ru...	Microsoft Corporation
webstorm64.exe		1 360 K	1 060 K	21960	WebStorm	JetBrains s.r.o.
Telegram.exe	0.68	247 452 K	69 000 K	26068	Telegram Desktop	Telegram FZ-LLC
SnippingTool.exe		7 380 K	19 292 K	8932	Ножницы	Microsoft Corporation
WINWORD.EXE	< 0.01	77 608 K	170 380 K	6892	Microsoft Word	Microsoft Corporation
procexp.exe		6 324 K	11 188 K	1652	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	3.67	53 524 K	77 876 K	24316	Sysinternals Process Explorer	Sysinternals - www.sysinter...
QAAgent.exe		6 204 K	936 K	14040		
GoogleCrashHandler.exe		1 980 K	1 324 K	21676	Google Crash Handler	Google LLC
GoogleCrashHandler64.exe		1 864 K	1 232 K	12096	Google Crash Handler	Google LLC
slack.exe	< 0.01	52 328 K	36 096 K	17516	Slack	Slack Technologies Inc.
slack.exe		51 168 K	7 204 K	21140	Slack	Slack Technologies Inc.
slack.exe		10 296 K	3 036 K	7288	Slack	Slack Technologies Inc.
slack.exe		21 260 K	6 992 K	15892	Slack	Slack Technologies Inc.
slack.exe	< 0.01	109 936 K	31 312 K	25500	Slack	Slack Technologies Inc.
Teams.exe	1.22	170 040 K	133 876 K	18520	Microsoft Teams	Microsoft Corporation
Teams.exe		227 952 K	214 352 K	24340	Microsoft Teams	Microsoft Corporation
Teams.exe		33 508 K	44 068 K	5236	Microsoft Teams	Microsoft Corporation
Teams.exe	0.65	611 496 K	408 236 K	25524	Microsoft Teams	Microsoft Corporation
Teams.exe	0.01	158 124 K	103 928 K	15576	Microsoft Teams	Microsoft Corporation

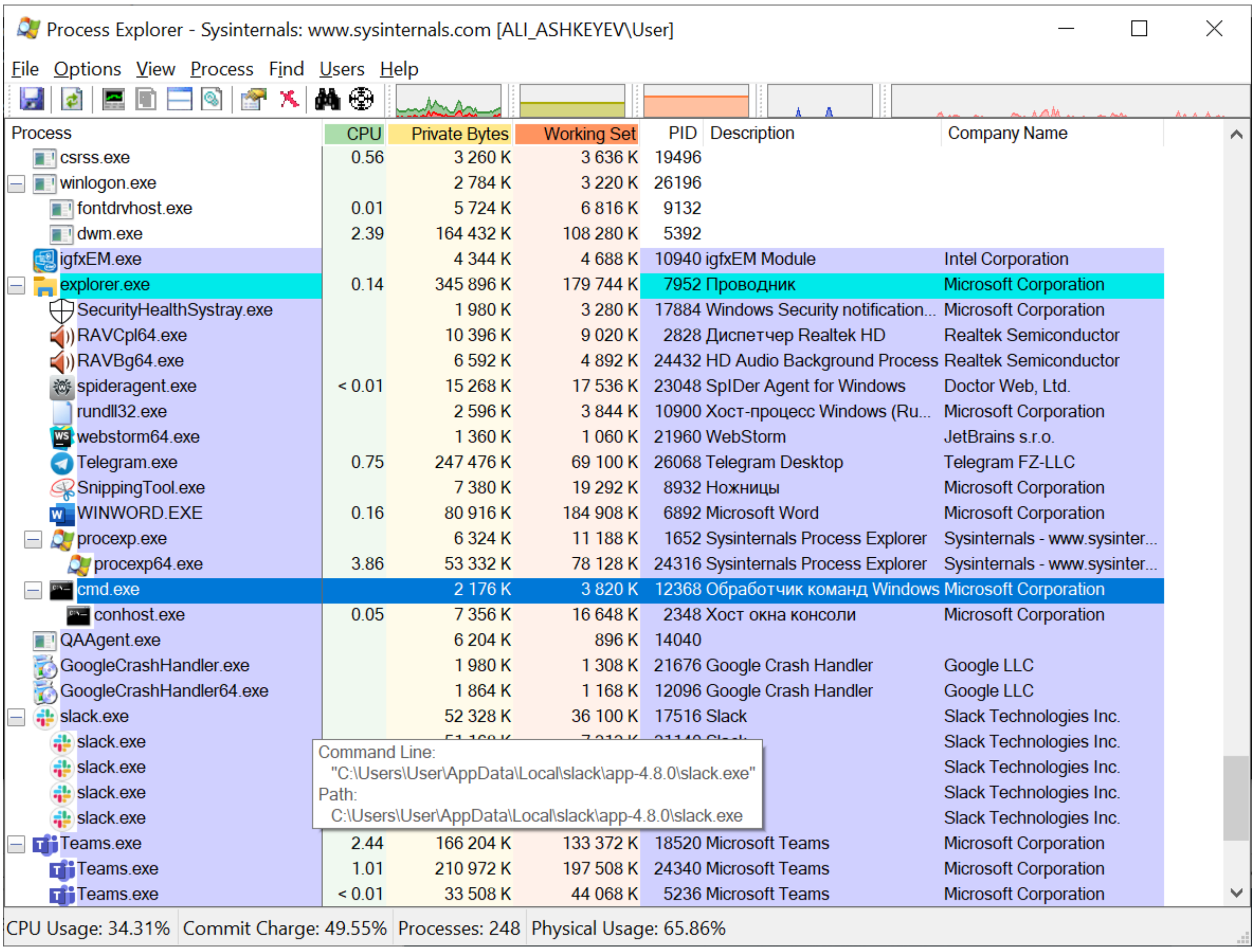
CPU Usage: 34.97% Commit Charge: 49.56% Processes: 246 Physical Usage: 65.60%

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

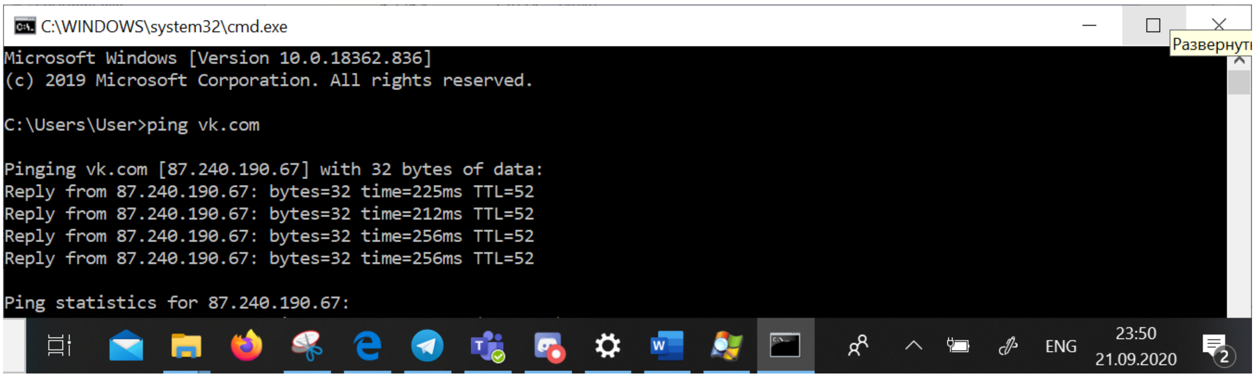


Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
csrss.exe	0.56	3 260 K	3 636 K	19496		
winlogon.exe		2 784 K	3 220 K	26196		
fontdrvhost.exe	0.01	5 724 K	6 816 K	9132		
dwm.exe	2.39	164 432 K	108 280 K	5392		
igfxEM.exe		4 344 K	4 688 K	10940	igfxEM Module	Intel Corporation
explorer.exe	0.14	345 896 K	179 744 K	7952	Проводник	Microsoft Corporation
SecurityHealthSystray.exe		1 980 K	3 280 K	17884	Windows Security notification...	Microsoft Corporation
RAVCpl64.exe		10 396 K	9 020 K	2828	Диспетчер Realtek HD	Realtek Semiconductor
RAVBg64.exe		6 592 K	4 892 K	24432	HD Audio Background Process	Realtek Semiconductor
spideragent.exe	< 0.01	15 268 K	17 536 K	23048	SpIDer Agent for Windows	Doctor Web, Ltd.
rundll32.exe		2 596 K	3 844 K	10900	Хост-процесс Windows (Ru...	Microsoft Corporation
webstorm64.exe		1 360 K	1 060 K	21960	WebStorm	JetBrains s.r.o.
Telegram.exe	0.75	247 476 K	69 100 K	26068	Telegram Desktop	Telegram FZ-LLC
SnippingTool.exe		7 380 K	19 292 K	8932	Ножницы	Microsoft Corporation
WINWORD.EXE	0.16	80 916 K	184 908 K	6892	Microsoft Word	Microsoft Corporation
procexp.exe		6 324 K	11 188 K	1652	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	3.86	53 332 K	78 128 K	24316	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		2 176 K	3 820 K	12368	Обработчик команд Windows	Microsoft Corporation
conhost.exe	0.05	7 356 K	16 648 K	2348	Хост окна консоли	Microsoft Corporation
QAAgent.exe		6 204 K	896 K	14040		
GoogleCrashHandler.exe		1 980 K	1 308 K	21676	Google Crash Handler	Google LLC
GoogleCrashHandler64.exe		1 864 K	1 168 K	12096	Google Crash Handler	Google LLC
slack.exe		52 328 K	36 100 K	17516	Slack	Slack Technologies Inc.
slack.exe		51 168 K	7 212 K	21140	Slack	Slack Technologies Inc.
slack.exe						Slack Technologies Inc.
slack.exe						Slack Technologies Inc.
slack.exe						Slack Technologies Inc.
Teams.exe	2.44	166 204 K	133 372 K	18520	Microsoft Teams	Microsoft Corporation
Teams.exe	1.01	210 972 K	197 508 K	24340	Microsoft Teams	Microsoft Corporation
Teams.exe	< 0.01	33 508 K	44 068 K	5236	Microsoft Teams	Microsoft Corporation

Command Line:
"C:\Users\User\AppData\Local\slack\app-4.8.0\slack.exe"
Path:
C:\Users\User\AppData\Local\slack\app-4.8.0\slack.exe

CPU Usage: 34.31% Commit Charge: 49.55% Processes: 248 Physical Usage: 65.86%



C:\WINDOWS\system32\cmd.exe

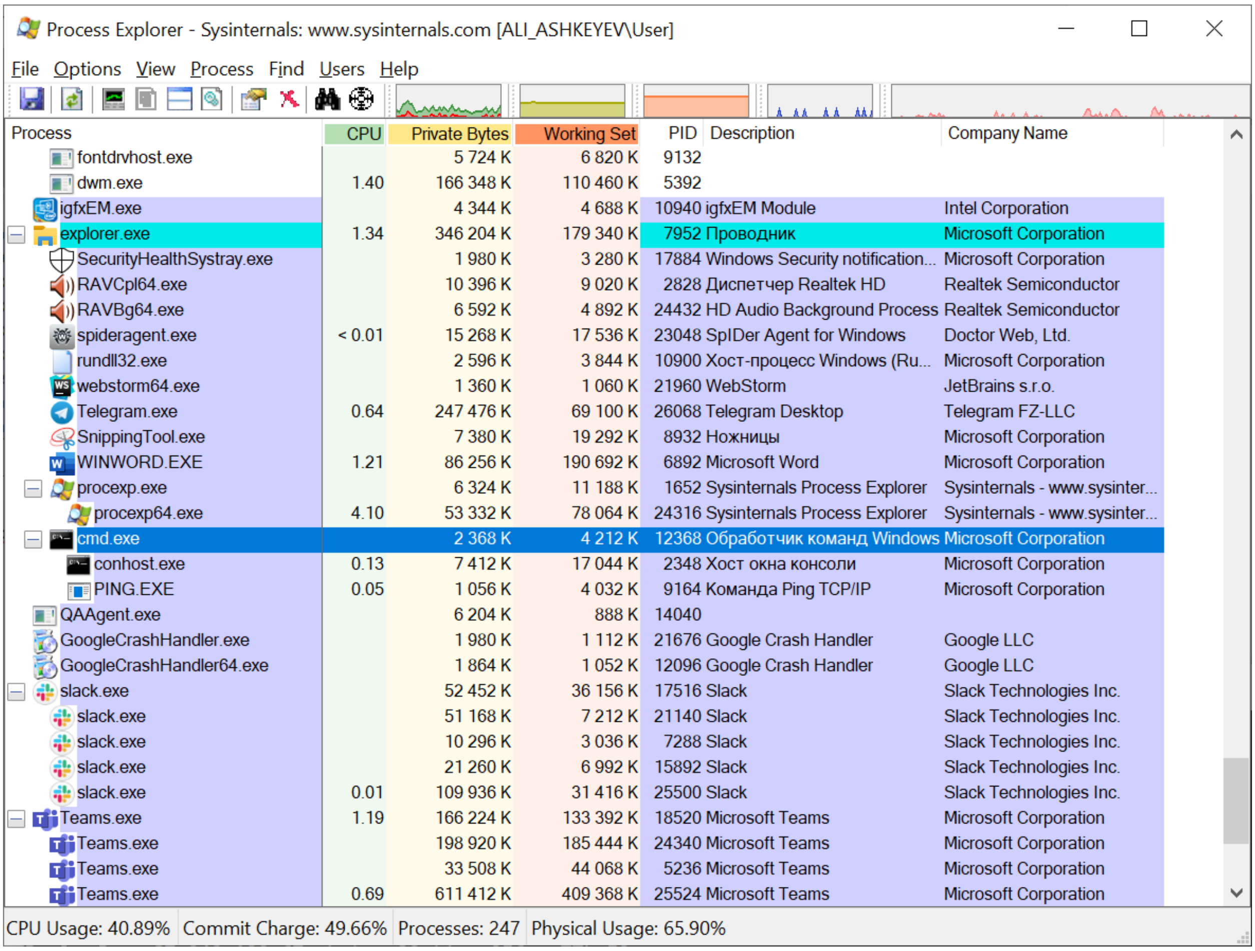
```
Microsoft Windows [Version 10.0.18362.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User>ping vk.com

Pinging vk.com [87.240.190.67] with 32 bytes of data:
Reply from 87.240.190.67: bytes=32 time=225ms TTL=52
Reply from 87.240.190.67: bytes=32 time=212ms TTL=52
Reply from 87.240.190.67: bytes=32 time=256ms TTL=52
Reply from 87.240.190.67: bytes=32 time=256ms TTL=52

Ping statistics for 87.240.190.67:
```

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?

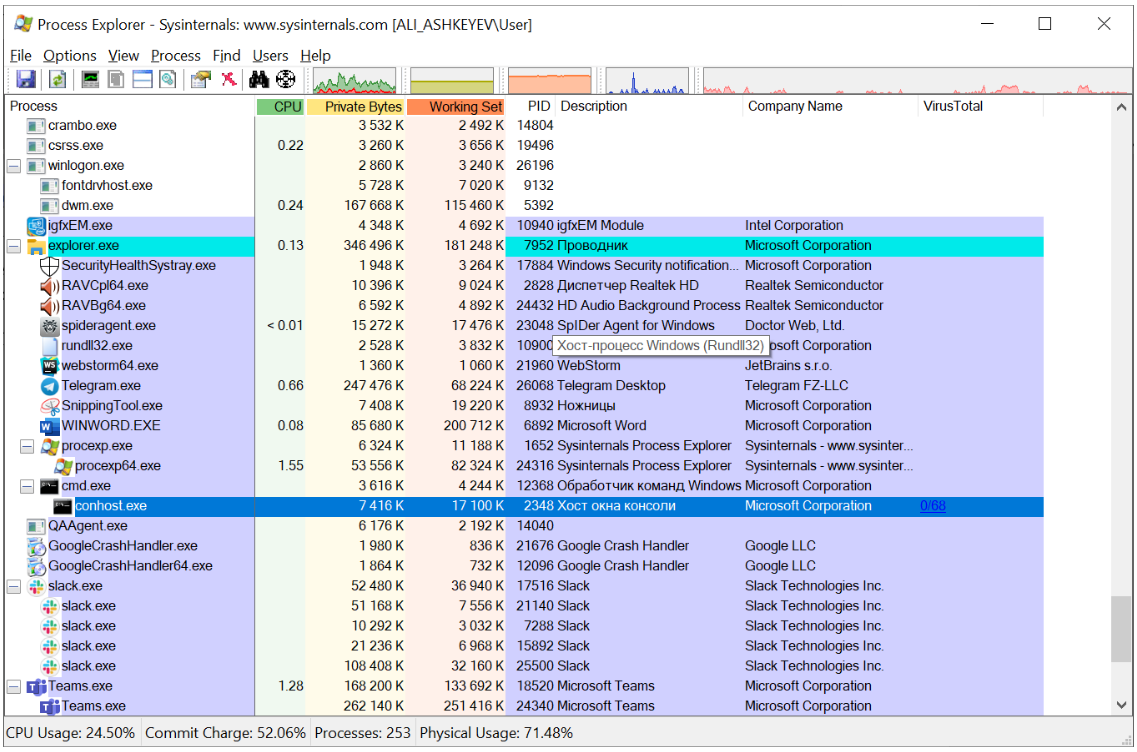

Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
fontdrvhost.exe		5 724 K	6 820 K	9132		
dwm.exe	1.40	166 348 K	110 460 K	5392		
igfxEM.exe		4 344 K	4 688 K	10940	igfxEM Module	Intel Corporation
explorer.exe	1.34	346 204 K	179 340 K	7952	Проводник	Microsoft Corporation
SecurityHealthSystray.exe		1 980 K	3 280 K	17884	Windows Security notification...	Microsoft Corporation
RAVCpl64.exe		10 396 K	9 020 K	2828	Диспетчер Realtek HD	Realtek Semiconductor
RAVBg64.exe		6 592 K	4 892 K	24432	HD Audio Background Process	Realtek Semiconductor
spideragent.exe	< 0.01	15 268 K	17 536 K	23048	SpIDer Agent for Windows	Doctor Web, Ltd.
rundll32.exe		2 596 K	3 844 K	10900	Хост-процесс Windows (Ru...	Microsoft Corporation
webstorm64.exe		1 360 K	1 060 K	21960	WebStorm	JetBrains s.r.o.
Telegram.exe	0.64	247 476 K	69 100 K	26068	Telegram Desktop	Telegram FZ-LLC
SnippingTool.exe		7 380 K	19 292 K	8932	Ножницы	Microsoft Corporation
WINWORD.EXE	1.21	86 256 K	190 692 K	6892	Microsoft Word	Microsoft Corporation
procexp.exe		6 324 K	11 188 K	1652	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	4.10	53 332 K	78 064 K	24316	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		2 368 K	4 212 K	12368	Обработчик команд Windows	Microsoft Corporation
conhost.exe	0.13	7 412 K	17 044 K	2348	Хост окна консоли	Microsoft Corporation
PING.EXE	0.05	1 056 K	4 032 K	9164	Команда Ping TCP/IP	Microsoft Corporation
QAAgent.exe		6 204 K	888 K	14040		
GoogleCrashHandler.exe		1 980 K	1 112 K	21676	Google Crash Handler	Google LLC
GoogleCrashHandler64.exe		1 864 K	1 052 K	12096	Google Crash Handler	Google LLC
slack.exe		52 452 K	36 156 K	17516	Slack	Slack Technologies Inc.
slack.exe		51 168 K	7 212 K	21140	Slack	Slack Technologies Inc.
slack.exe		10 296 K	3 036 K	7288	Slack	Slack Technologies Inc.
slack.exe		21 260 K	6 992 K	15892	Slack	Slack Technologies Inc.
slack.exe	0.01	109 936 K	31 416 K	25500	Slack	Slack Technologies Inc.
Teams.exe	1.19	166 224 K	133 392 K	18520	Microsoft Teams	Microsoft Corporation
Teams.exe		198 920 K	185 444 K	24340	Microsoft Teams	Microsoft Corporation
Teams.exe		33 508 K	44 068 K	5236	Microsoft Teams	Microsoft Corporation
Teams.exe	0.69	611 412 K	409 368 K	25524	Microsoft Teams	Microsoft Corporation

CPU Usage: 40.89% Commit Charge: 49.66% Processes: 247 Physical Usage: 65.90%

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.

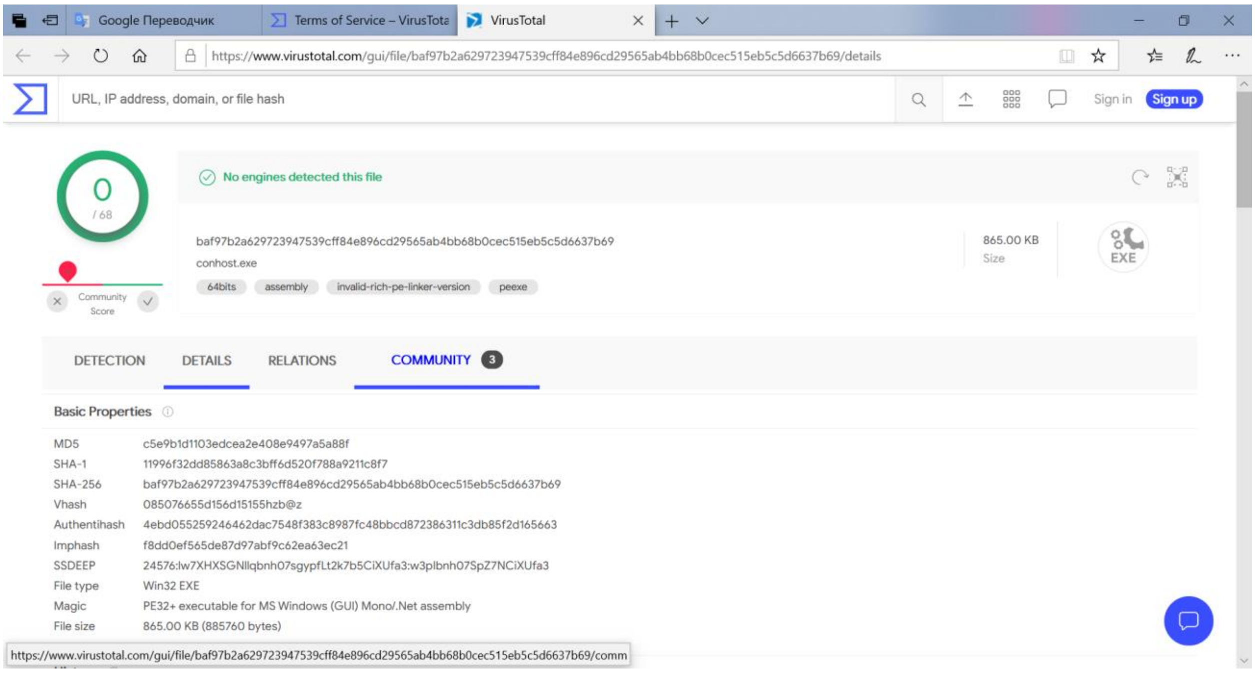
e. Check Virtual Total


Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
crambo.exe		3 532 K	2 492 K	14804			
csrss.exe	0.22	3 260 K	3 656 K	19496			
winlogon.exe		2 860 K	3 240 K	26196			
fontdrvhost.exe		5 728 K	7 020 K	9132			
dwm.exe	0.24	167 668 K	115 460 K	5392			
igfxEM.exe		4 348 K	4 692 K	10940	igfxEM Module	Intel Corporation	
explorer.exe	0.13	346 496 K	181 248 K	7952	Проводник	Microsoft Corporation	
SecurityHealthSystray.exe		1 948 K	3 264 K	17884	Windows Security notification...	Microsoft Corporation	
RAVCpl64.exe		10 396 K	9 024 K	2828	Диспетчер Realtek HD	Realtek Semiconductor	
RAVBg64.exe		6 592 K	4 892 K	24432	HD Audio Background Process	Realtek Semiconductor	
spideragent.exe	< 0.01	15 272 K	17 476 K	23048	SpIDer Agent for Windows	Doctor Web, Ltd.	
rundll32.exe		2 528 K	3 832 K	10900	Хост-процесс Windows (Rundll32)	osoft Corporation	
webstorm64.exe		1 360 K	1 060 K	21960	WebStorm	JetBrains s.r.o.	
Telegram.exe	0.66	247 476 K	68 224 K	26068	Telegram Desktop	Telegram FZ-LLC	
SnippingTool.exe		7 408 K	19 220 K	8932	Ножницы	Microsoft Corporation	
WINWORD.EXE	0.08	85 680 K	200 712 K	6892	Microsoft Word	Microsoft Corporation	
procexp.exe		6 324 K	11 188 K	1652	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	1.55	53 556 K	82 324 K	24316	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		3 616 K	4 244 K	12368	Обработчик команд Windows	Microsoft Corporation	
conhost.exe		7 416 K	17 100 K	2348	Хост окна консоли	Microsoft Corporation	0/68
QAAgent.exe		6 176 K	2 192 K	14040			
GoogleCrashHandler.exe		1 980 K	836 K	21676	Google Crash Handler	Google LLC	
GoogleCrashHandler64.exe		1 864 K	732 K	12096	Google Crash Handler	Google LLC	
slack.exe		52 480 K	36 940 K	17516	Slack	Slack Technologies Inc.	
slack.exe		51 168 K	7 556 K	21140	Slack	Slack Technologies Inc.	
slack.exe		10 292 K	3 032 K	7288	Slack	Slack Technologies Inc.	
slack.exe		21 236 K	6 968 K	15892	Slack	Slack Technologies Inc.	
slack.exe		108 408 K	32 160 K	25500	Slack	Slack Technologies Inc.	
Teams.exe	1.28	168 200 K	133 692 K	18520	Microsoft Teams	Microsoft Corporation	
Teams.exe		262 140 K	251 416 K	24340	Microsoft Teams	Microsoft Corporation	

CPU Usage: 24.50% Commit Charge: 52.06% Processes: 253 Physical Usage: 71.48%

f. Link redirection to virustotal website with description of file


Google Переводчик
Terms of Service – VirusTota
VirusTotal
https://www.virustotal.com/gui/file/baf97b2a629723947539cff84e896cd29565ab4bb68b0cec515eb5c5d6637b69/details
URL, IP address, domain, or file hash
Sign in
Sign up
0
/ 68
Community Score
865.00 KB
Size
EXE
DETECTION
DETAILS
RELATIONS
COMMUNITY 3

No engines detected this file

baf97b2a629723947539cff84e896cd29565ab4bb68b0cec515eb5c5d6637b69
conhost.exe
64bits assembly invalid-rich-pe-linker-version peexe

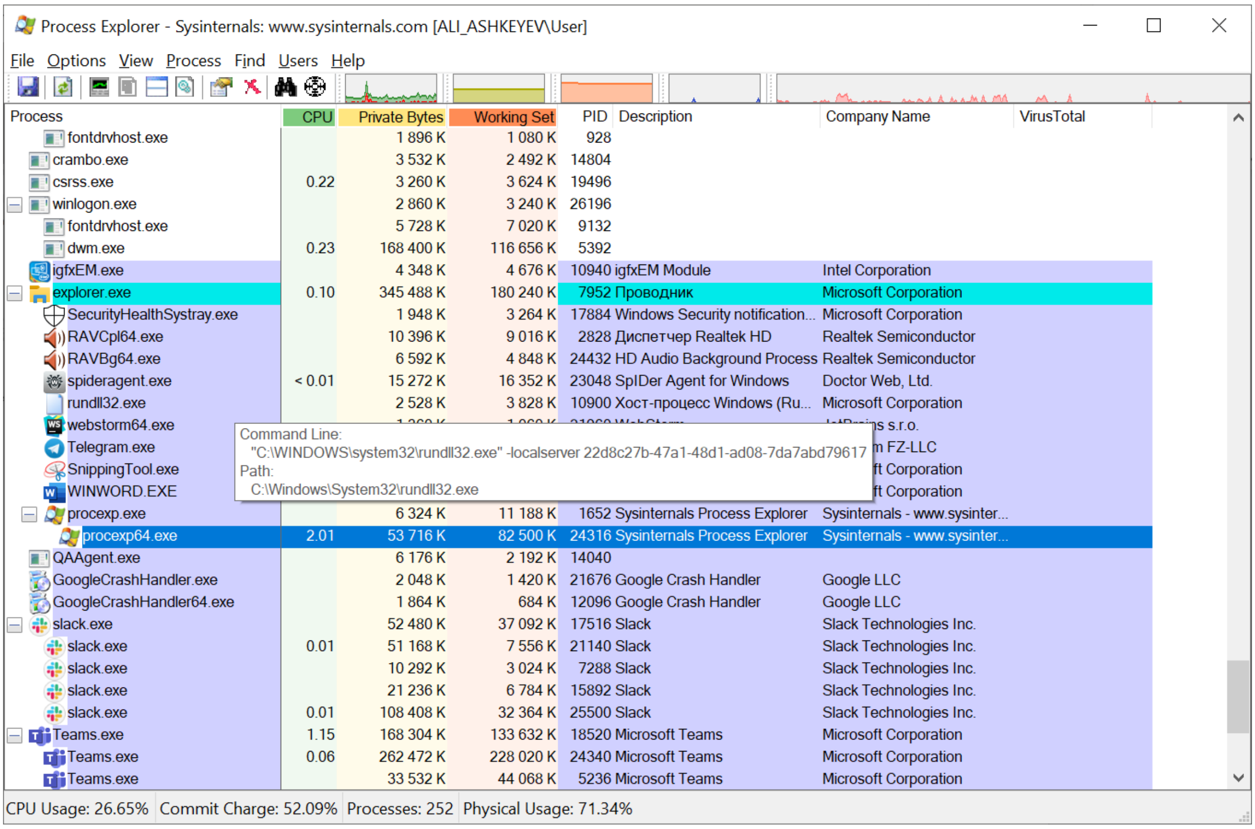
Basic Properties

MD5	c5e9b1d1103edcea2e408e9497a5a88f
SHA-1	11996f32dd85863a8c3bff6d520f788a9211c8f7
SHA-256	baf97b2a629723947539cff84e896cd29565ab4bb68b0cec515eb5c5d6637b69
Vhash	085076655d156d15155hzb@z
Authentihash	4ebd055259246462dac7548f383c8987fc48bbcd872386311c3db85f2d165663
Imphash	f8dd0ef565de87d97abf9c62ea63ec21
SSDEEP	24576:lw7XHXSGNllqbnh07sgypfLt2k7b5CiXUfa3:w3plbnh07SpZ7NCiXUfa3
File type	Win32 EXE
Magic	PE32+ executable for MS Windows (GUI) Mono/.Net assembly
File size	865.00 KB (885760 bytes)

https://www.virustotal.com/gui/file/baf97b2a629723947539cff84e896cd29565ab4bb68b0cec515eb5c5d6637b69/comm

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.


Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
fontdrvhost.exe		1 896 K	1 080 K	928			
crambo.exe		3 532 K	2 492 K	14804			
csrss.exe	0.22	3 260 K	3 624 K	19496			
winlogon.exe		2 860 K	3 240 K	26196			
fontdrvhost.exe		5 728 K	7 020 K	9132			
dwm.exe	0.23	168 400 K	116 656 K	5392			
igfxEM.exe		4 348 K	4 676 K	10940	igfxEM Module	Intel Corporation	
explorer.exe	0.10	345 488 K	180 240 K	7952	Проводник	Microsoft Corporation	
SecurityHealthSystray.exe		1 948 K	3 264 K	17884	Windows Security notification...	Microsoft Corporation	
RAVCpl64.exe		10 396 K	9 016 K	2828	Диспетчер Realtek HD	Realtek Semiconductor	
RAVBg64.exe		6 592 K	4 848 K	24432	HD Audio Background Process	Realtek Semiconductor	
spideragent.exe	< 0.01	15 272 K	16 352 K	23048	SpIDer Agent for Windows	Doctor Web, Ltd.	
rundll32.exe		2 528 K	3 828 K	10900	Хост-процесс Windows (Ru...	Microsoft Corporation	
webstorm64.exe						s s.r.o.	
Telegram.exe						m FZ-LLC	
SnippingTool.exe						ft Corporation	
WINWORD.EXE						ft Corporation	
procexp.exe		6 324 K	11 188 K	1652	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	2.01	53 716 K	82 500 K	24316	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
QAAgent.exe		6 176 K	2 192 K	14040			
GoogleCrashHandler.exe		2 048 K	1 420 K	21676	Google Crash Handler	Google LLC	
GoogleCrashHandler64.exe		1 864 K	684 K	12096	Google Crash Handler	Google LLC	
slack.exe		52 480 K	37 092 K	17516	Slack	Slack Technologies Inc.	
slack.exe	0.01	51 168 K	7 556 K	21140	Slack	Slack Technologies Inc.	
slack.exe		10 292 K	3 024 K	7288	Slack	Slack Technologies Inc.	
slack.exe		21 236 K	6 784 K	15892	Slack	Slack Technologies Inc.	
slack.exe	0.01	108 408 K	32 364 K	25500	Slack	Slack Technologies Inc.	
Teams.exe	1.15	168 304 K	133 632 K	18520	Microsoft Teams	Microsoft Corporation	
Teams.exe	0.06	262 472 K	228 020 K	24340	Microsoft Teams	Microsoft Corporation	
Teams.exe		33 532 K	44 068 K	5236	Microsoft Teams	Microsoft Corporation	

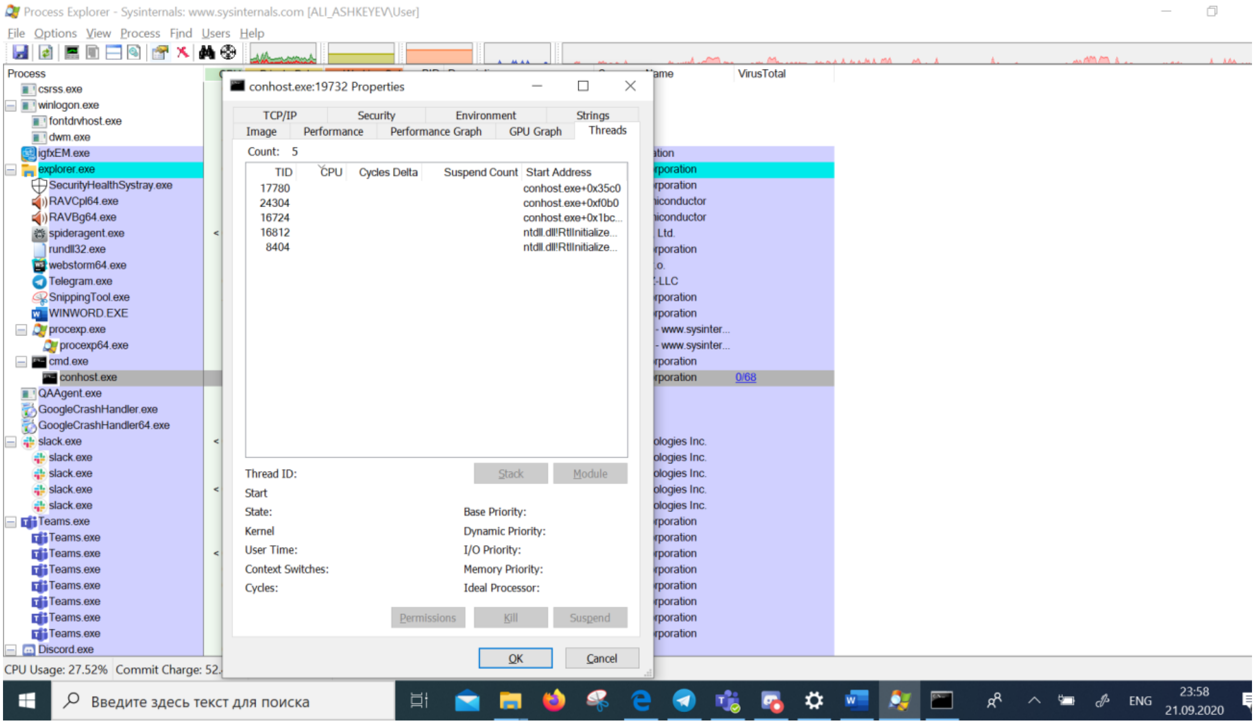
```
Command Line:
  "C:\WINDOWS\system32\rundll32.exe" -localserver 22d8c27b-47a1-48d1-ad08-7da7abd79617
Path:
  C:\Windows\System32\rundll32.exe
```

CPU Usage: 26.65% Commit Charge: 52.09% Processes: 252 Physical Usage: 71.34%

Part2 Exploring Threads and Handles

Step 1: Explore threads

b. conhost.exe properties.



Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]

conhost.exe:19732 Properties

Count: 5

TID	CPU	Cycles Delta	Suspend Count	Start Address
17780				conhost.exe+0x35c0
24304				conhost.exe+0xf0b0
16724				conhost.exe+0x1bc...
16812				ntdll.dll!RtlInitialize...
8404				ntdll.dll!RtlInitialize...

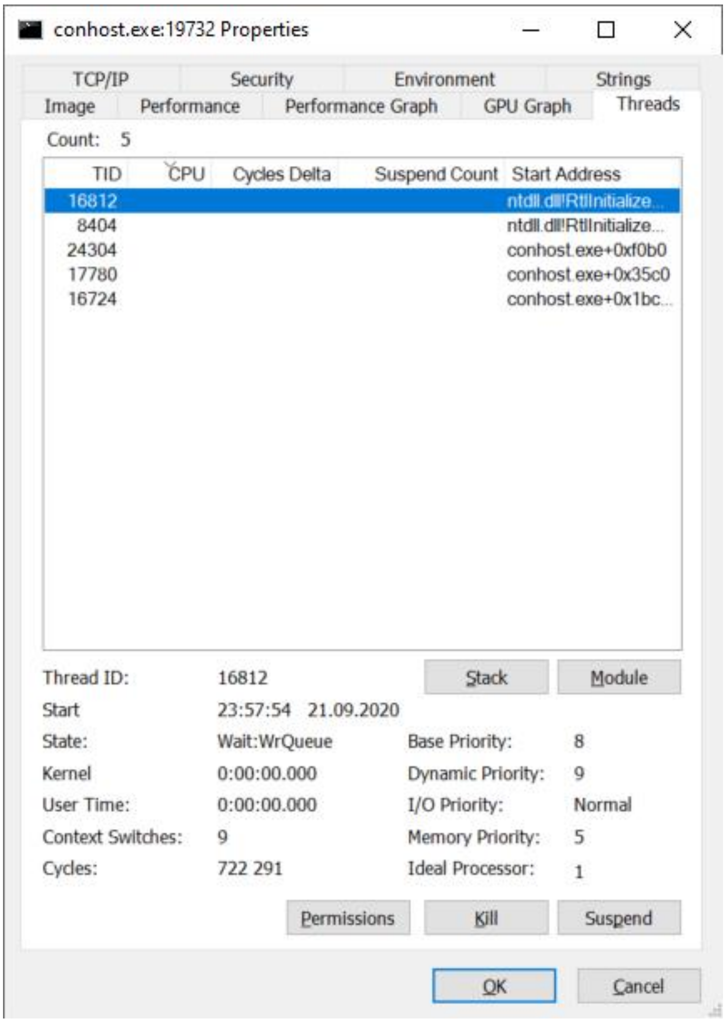
Thread ID:
Start
State:
Kernel
User Time:
Context Switches:
Cycles:

Base Priority:
Dynamic Priority:
I/O Priority:
Memory Priority:
Ideal Processor:

CPU Usage: 27.52% Commit Charge: 52.

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



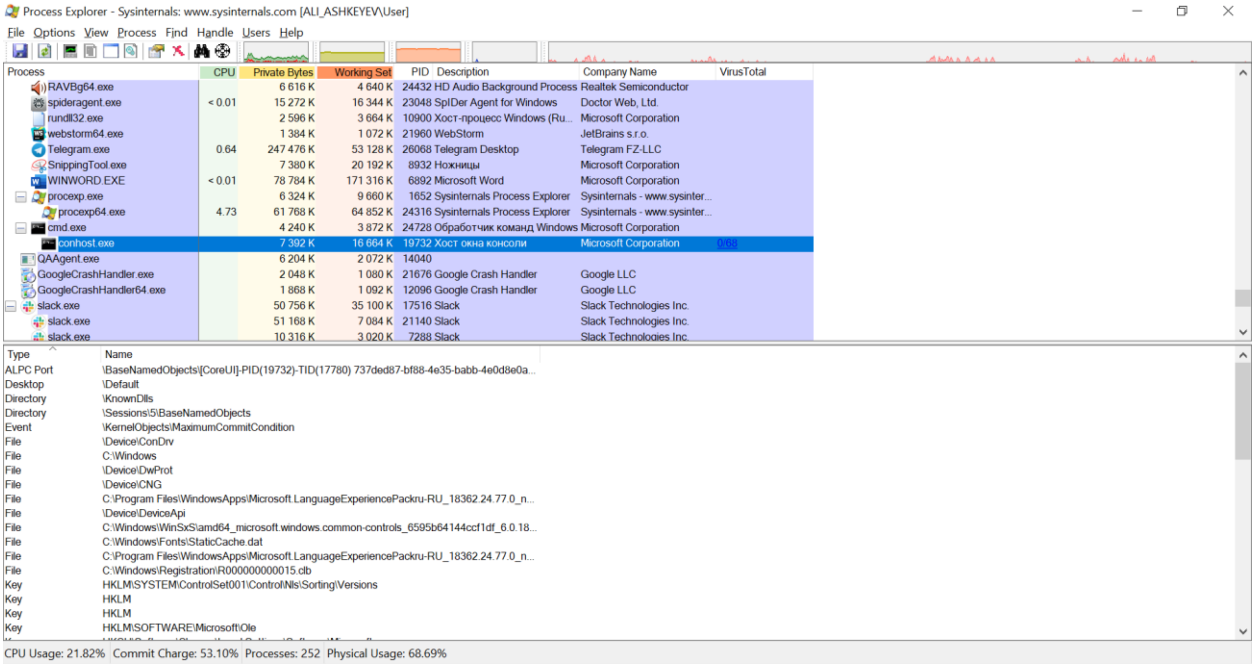
Count: 5

TID	CPU	Cycles Delta	Suspend Count	Start Address
16812				ntdll.dll!RtlInitialize...
8404				ntdll.dll!RtlInitialize...
24304				conhost.exe+0xf0b0
17780				conhost.exe+0x35c0
16724				conhost.exe+0x1bc...

Thread ID:	16812		
Start	23:57:54 21.09.2020		
State:	Wait:WrQueue	Base Priority:	8
Kernel	0:00:00.000	Dynamic Priority:	9
User Time:	0:00:00.000	I/O Priority:	Normal
Context Switches:	9	Memory Priority:	5
Cycles:	722 291	Ideal Processor:	1

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


Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]
File Options View Process Find Handle Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
RAVBg64.exe		6 616 K	4 640 K	24432	HD Audio Background Process	Realtek Semiconductor	
spideragent.exe	< 0.01	15 272 K	16 344 K	23048	SpIDer Agent for Windows	Doctor Web, Ltd.	
rundll32.exe		2 596 K	3 664 K	10900	Хост-процесс Windows (Ru...	Microsoft Corporation	
webstorm64.exe		1 384 K	1 072 K	21960	WebStorm	JetBrains s.r.o.	
Telegram.exe	0.64	247 476 K	53 128 K	26068	Telegram Desktop	Telegram FZ-LLC	
SnippingTool.exe		7 380 K	20 192 K	8932	Ножницы	Microsoft Corporation	
WINWORD.EXE	< 0.01	78 784 K	171 316 K	6892	Microsoft Word	Microsoft Corporation	
procexp.exe		6 324 K	9 660 K	1652	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	4.73	61 768 K	64 852 K	24316	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		4 240 K	3 872 K	24728	Обработчик команд Windows	Microsoft Corporation	
conhost.exe		7 392 K	16 664 K	19732	Хост окна консоли	Microsoft Corporation	0/68
QAAgent.exe		6 204 K	2 072 K	14040			
GoogleCrashHandler.exe		2 048 K	1 080 K	21676	Google Crash Handler	Google LLC	
GoogleCrashHandler64.exe		1 868 K	1 092 K	12096	Google Crash Handler	Google LLC	
slack.exe		50 756 K	35 100 K	17516	Slack	Slack Technologies Inc.	
slack.exe		51 168 K	7 084 K	21140	Slack	Slack Technologies Inc.	
slack.exe		10 316 K	3 020 K	7288	Slack	Slack Technologies Inc.	

Type	Name
ALPC Port	\BaseNamedObjects\[CoreUI]-PID(19732)-TID(17780) 737ded87-bf88-4e35-babb-4e0d8e0a...
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\5\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	\Device\DwProt
File	\Device\CNG
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackru-RU_18362.24.77.0_n...
File	\Device\DeviceApi
File	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18...
File	C:\Windows\Fonts\StaticCache.dat
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackru-RU_18362.24.77.0_n...
File	C:\Windows\Registration\R000000000015.clb
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole

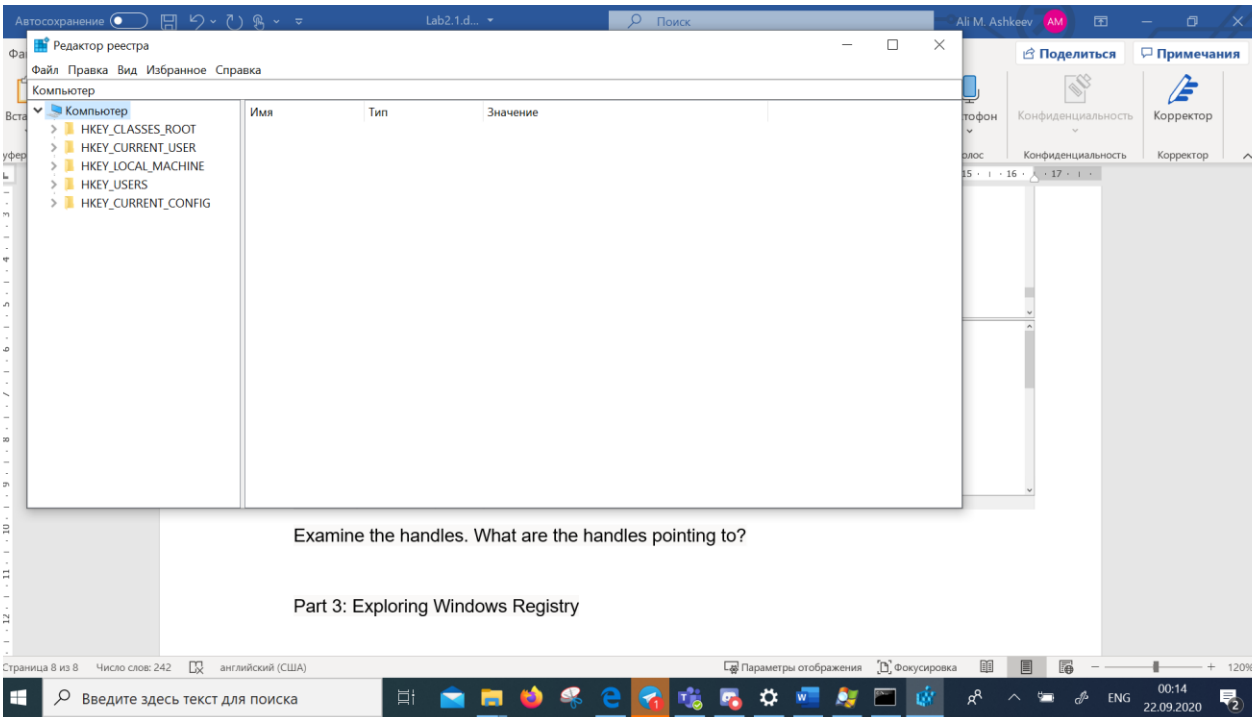
CPU Usage: 21.82% Commit Charge: 53.10% Processes: 252 Physical Usage: 68.69%

Examine the handles. What are the handles pointing to?

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

Part 3: Exploring Windows Registry

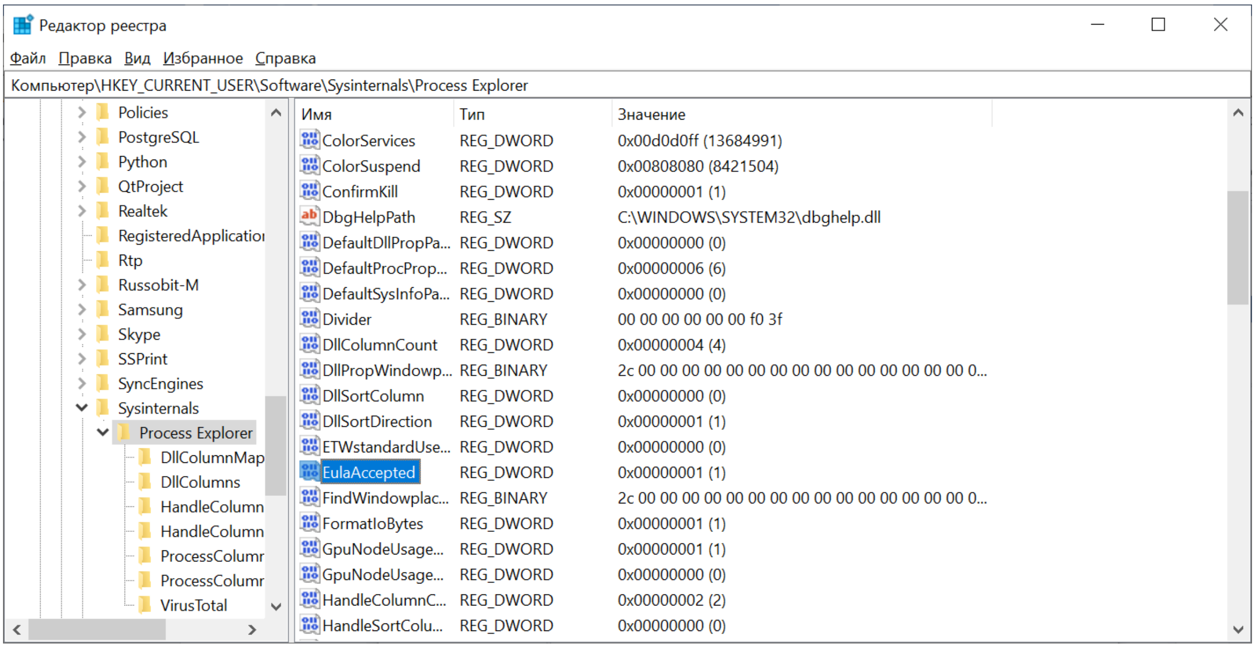
a. Regedit window



Examine the handles. What are the handles pointing to?

Part 3: Exploring Windows Registry

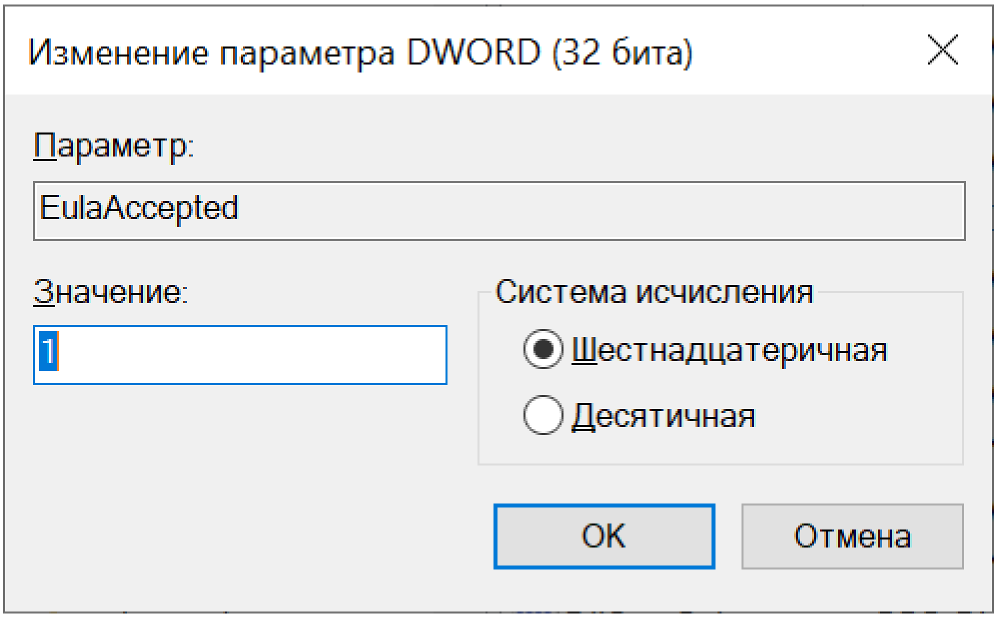
b. EulaAccepted key


Редактор реестра

Компьютер\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer

Имя	Тип	Значение
ColorServices	REG_DWORD	0x00d0d0ff (13684991)
ColorSuspend	REG_DWORD	0x00808080 (8421504)
ConfirmKill	REG_DWORD	0x00000001 (1)
DbgHelpPath	REG_SZ	C:\WINDOWS\SYSTEM32\dbghelp.dll
DefaultDllPropPa...	REG_DWORD	0x00000000 (0)
DefaultProcProp...	REG_DWORD	0x00000006 (6)
DefaultSysInfoPa...	REG_DWORD	0x00000000 (0)
Divider	REG_BINARY	00 00 00 00 00 00 f0 3f
DllColumnCount	REG_DWORD	0x00000004 (4)
DllPropWindowp...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
DllSortColumn	REG_DWORD	0x00000000 (0)
DllSortDirection	REG_DWORD	0x00000001 (1)
ETWstandardUse...	REG_DWORD	0x00000000 (0)
EulaAccepted	REG_DWORD	0x00000001 (1)
FindWindowplac...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
FormatIoBytes	REG_DWORD	0x00000001 (1)
GpuNodeUsage...	REG_DWORD	0x00000001 (1)
GpuNodeUsage...	REG_DWORD	0x00000000 (0)
HandleColumnC...	REG_DWORD	0x00000002 (2)
HandleSortColu...	REG_DWORD	0x00000000 (0)

c. Value data of EulaAccepted


Изменение параметра DWORD (32 бита)

Параметр: EulaAccepted

Значение: 1

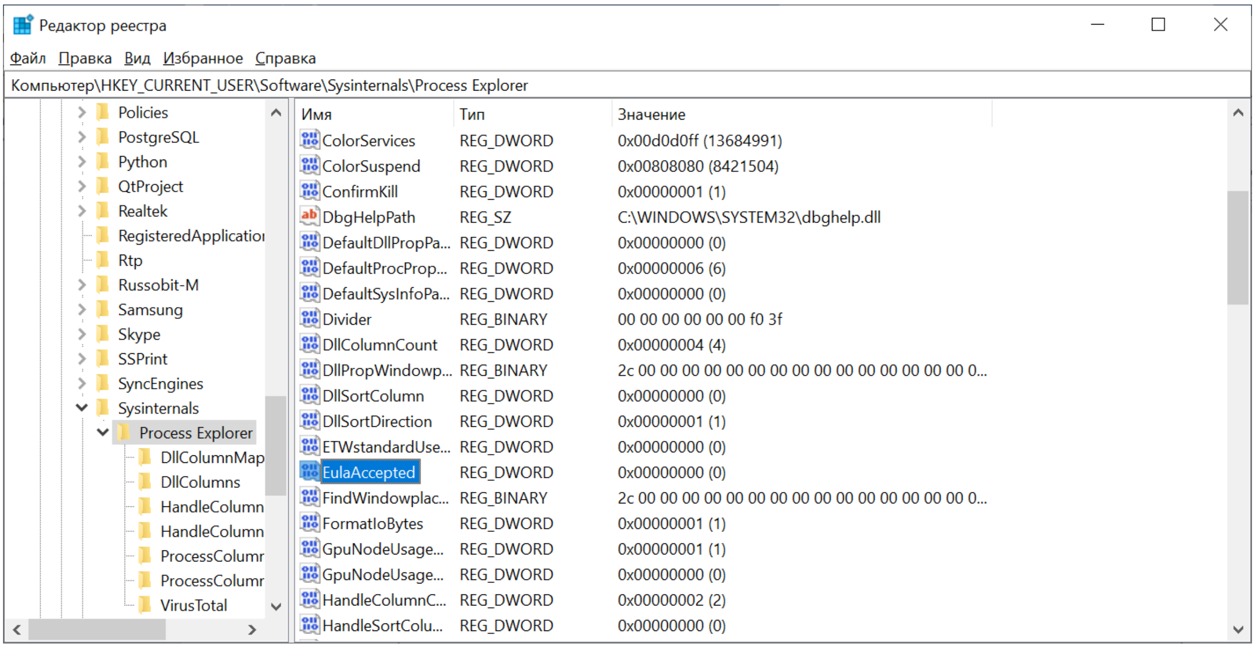
Система исчисления

● Шестнадцатеричная

○ Десятичная

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

Value for registry key is 0x00000000(0)



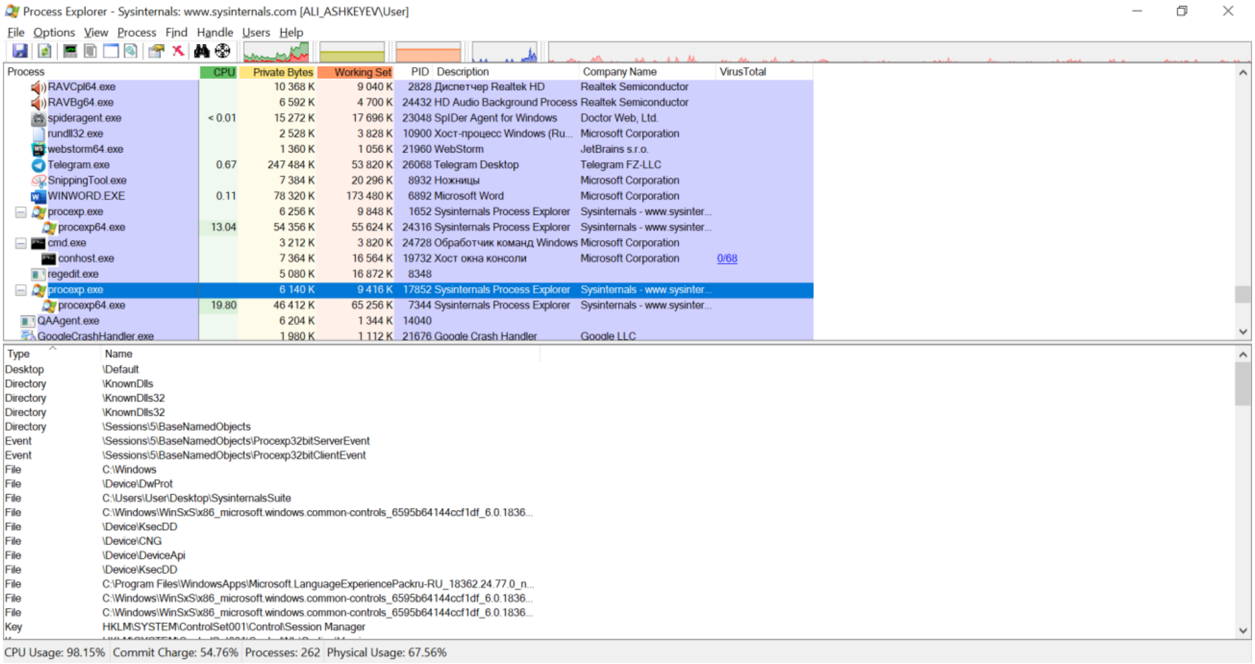
Компьютер\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer

Policies
PostgreSQL
Python
QtProject
Realtek
RegisteredApplicatioı
Rtp
Russobit-M
Samsung
Skype
SSPrint
SyncEngines
Sysinternals
Process Explorer
DllColumnMap
DllColumns
HandleColumn
HandleColumn
ProcessColumr
ProcessColumr
VirusTotal

Имя	Тип	Значение
ColorServices	REG_DWORD	0x00d0d0ff (13684991)
ColorSuspend	REG_DWORD	0x00808080 (8421504)
ConfirmKill	REG_DWORD	0x00000001 (1)
DbgHelpPath	REG_SZ	C:\WINDOWS\SYSTEM32\dbghelp.dll
DefaultDllPropPa...	REG_DWORD	0x00000000 (0)
DefaultProcProp...	REG_DWORD	0x00000006 (6)
DefaultSysInfoPa...	REG_DWORD	0x00000000 (0)
Divider	REG_BINARY	00 00 00 00 00 00 f0 3f
DllColumnCount	REG_DWORD	0x00000004 (4)
DllPropWindowp...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
DllSortColumn	REG_DWORD	0x00000000 (0)
DllSortDirection	REG_DWORD	0x00000001 (1)
ETWstandardUse...	REG_DWORD	0x00000000 (0)
EulaAccepted	REG_DWORD	0x00000000 (0)
FindWindowplac...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
FormatIoBytes	REG_DWORD	0x00000001 (1)
GpuNodeUsage...	REG_DWORD	0x00000001 (1)
GpuNodeUsage...	REG_DWORD	0x00000000 (0)
HandleColumnC...	REG_DWORD	0x00000002 (2)
HandleSortColu...	REG_DWORD	0x00000000 (0)

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

It was opened another precexp.exe with precexp64.exe


Process Explorer - Sysinternals: www.sysinternals.com [ALI_ASHKEYEV\User]
File Options View Process Find Handle Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
RAVCpl64.exe		10 368 K	9 040 K	2828	Диспетчер Realtek HD	Realtek Semiconductor	
RAVBg64.exe		6 592 K	4 700 K	24432	HD Audio Background Process	Realtek Semiconductor	
spideragent.exe	< 0.01	15 272 K	17 696 K	23048	SpIDer Agent for Windows	Doctor Web, Ltd.	
rundll32.exe		2 528 K	3 828 K	10900	Хост-процесс Windows (Ru...	Microsoft Corporation	
webstorm64.exe		1 360 K	1 056 K	21960	WebStorm	JetBrains s.r.o.	
Telegram.exe	0.67	247 484 K	53 820 K	26068	Telegram Desktop	Telegram FZ-LLC	
SnippingTool.exe		7 384 K	20 296 K	8932	Ножницы	Microsoft Corporation	
WINWORD.EXE	0.11	78 320 K	173 480 K	6892	Microsoft Word	Microsoft Corporation	
procexp.exe		6 256 K	9 848 K	1652	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	13.04	54 356 K	55 624 K	24316	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		3 212 K	3 820 K	24728	Обработчик команд Windows	Microsoft Corporation	
conhost.exe		7 364 K	16 564 K	19732	Хост окна консоли	Microsoft Corporation	0/68
regedit.exe		5 080 K	16 872 K	8348			
procexp.exe		6 140 K	9 416 K	17852	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	19.80	46 412 K	65 256 K	7344	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
QAAgent.exe		6 204 K	1 344 K	14040			
GoogleCrashHandler.exe		1 980 K	1 112 K	21676	Google Crash Handler	Google LLC	

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\KnownDlls32
Directory	\KnownDlls32
Directory	\Sessions\5\BaseNamedObjects
Event	\Sessions\5\BaseNamedObjects\Procexp32bitServerEvent
Event	\Sessions\5\BaseNamedObjects\Procexp32bitClientEvent
File	C:\Windows
File	\Device\DwProt
File	C:\Users\User\Desktop\SysinternalsSuite
File	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.1836...
File	\Device\KsecDD
File	\Device\CNG
File	\Device\DeviceApi
File	\Device\KsecDD
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackru-RU_18362.24.77.0_n...
File	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.1836...
File	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.1836...
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager

CPU Usage: 98.15% Commit Charge: 54.76% Processes: 262 Physical Usage: 67.56%