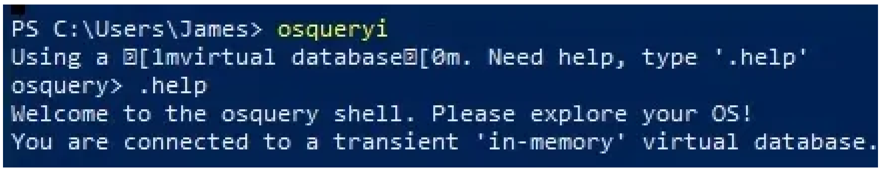
OSQuery

Task 3

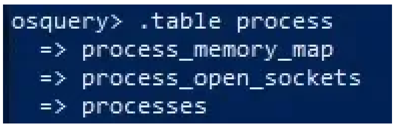
Question: How many tables are returned when we query “table process” in the interactive mode of Osquery?

Answer: 3

Explanation:



```
PS C:\Users\James> osqueryi
Using a ▯[1mvirtual database▯[0m. Need help, type '.help'
osquery> .help
Welcome to the osquery shell. Please explore your OS!
You are connected to a transient 'in-memory' virtual database.
```



```
osquery> .table process
  => process_memory_map
  => process_open_sockets
  => processes
```

Question: Looking at the schema of the processes table, which column displays the process id for the particular process?

Answer: pid

Question: Examine the .help command, how many output display modes are available for the .mode command?

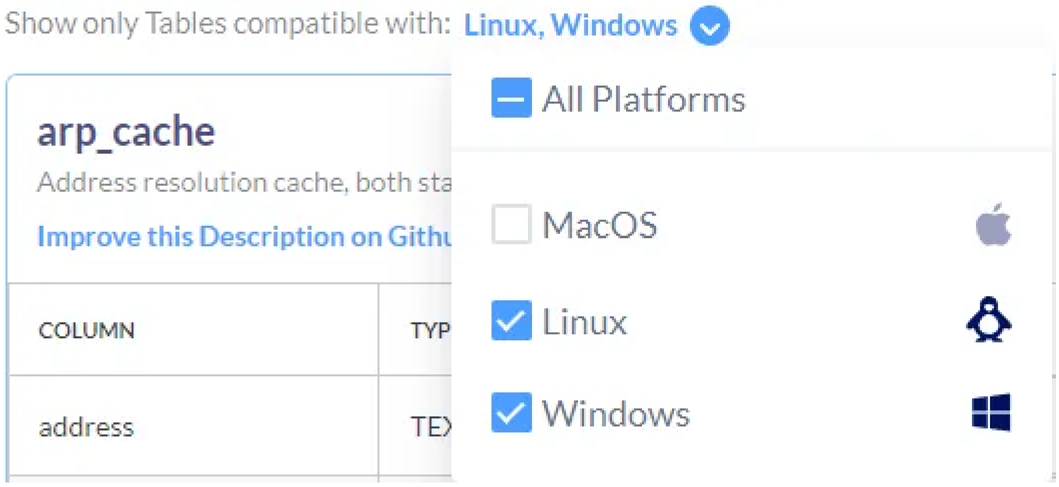
Answer: 5

Task 4

Question: In Osquery version 5.5.1, how many common tables are returned, when we select both Linux and Window Operating system?

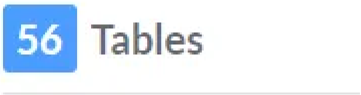
Answer: 56

Explanation: check the windows os



Show only Tables compatible with: Linux, Windows

▬ All Platforms
□ MacOS
☑ Linux
☑ Windows
arp_cache
Address resolution cache, both sta
Improve this Description on Githu
COLUMN
TYP
address
TE



56 Tables

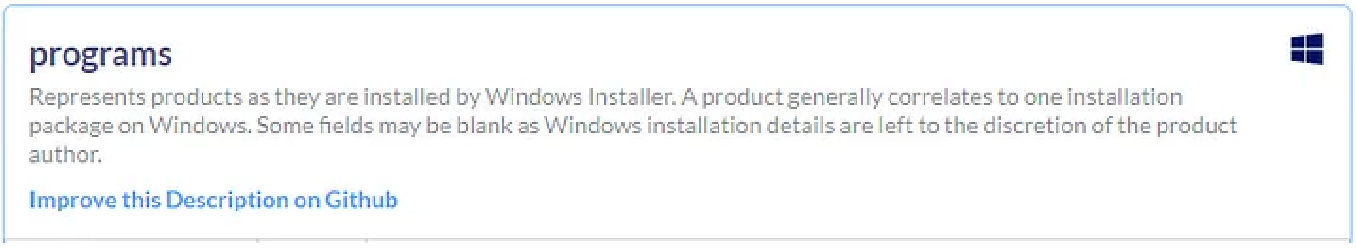
Question: In Osquery version 5.5.1, how many tables for MAC OS are available?

Answer: 180

Question: In the Windows Operating system, which table is used to display the installed programs?

Answer: Programs

Explanation:



programs

Represents products as they are installed by Windows Installer. A product generally correlates to one installation package on Windows. Some fields may be blank as Windows installation details are left to the discretion of the product author.

Improve this Description on Github

Question: In Windows Operating system, which column contains the registry value within the registry table?

Answer: Data

Task 5

Question: Using Osquery, how many programs are installed on this host?

Answer: 19

Explanation:

- enter this command: `SELECT count(*) FROM programs;`

Question: Using Osquery, what is the description for the user James?

Answer: Creative Artist

Explanation:

- enter the following command: `SELECT description from users WHERE username=’James’;`

Question: When we run the following search query, what is the full SID of the user with RID ‘1009’?

Answer: S-1-5-21-1966530601-3185510712-10604624-1009 (different for everyone)

Question: When we run the following search query, what is the Internet Explorer browser extension installed on this machine?

Answer: C:\Windows\System32\ieframe.dll

Question: After running the following query, what is the full name of the program returned?

Answer: Wireshark 3.6.8 64-bit

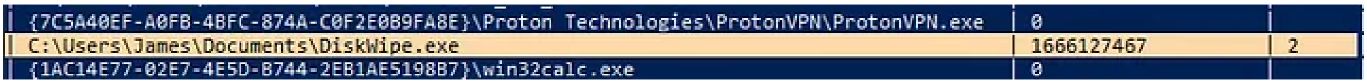
Question: Which table stores the evidence of process execution in Windows OS?

Answer: userassist

Question: One of the users seems to have executed a program to remove traces from the disk; what is the name of that program?

Answer: DiskWipe.exe

Explanation:

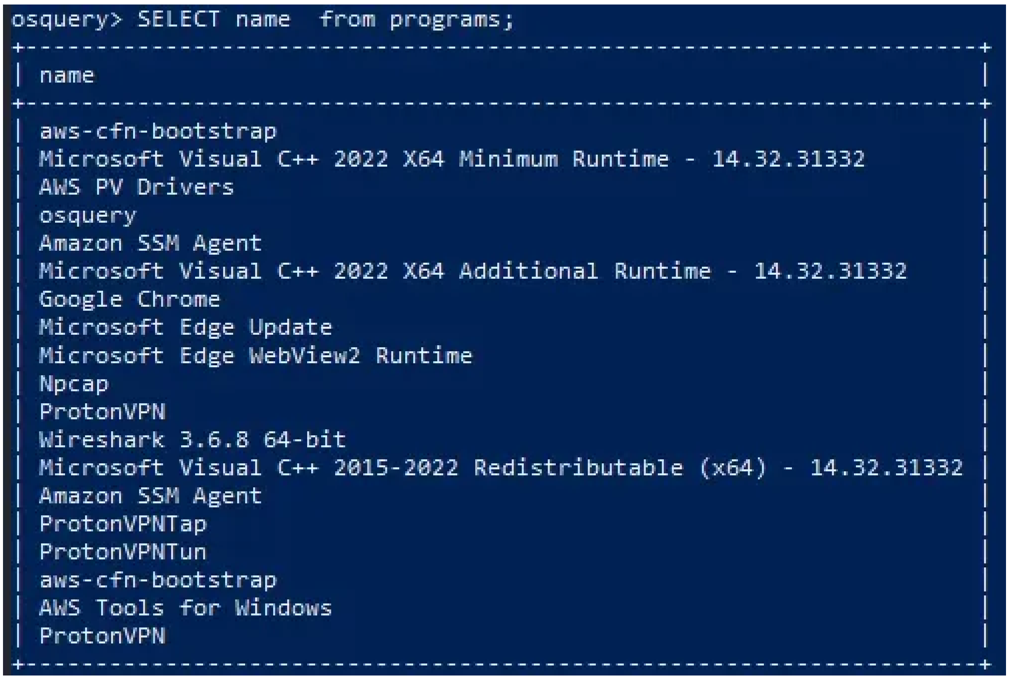


```
| {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Proton Technologies\ProtonVPN\ProtonVPN.exe | 0          |
| C:\Users\James\Documents\DiskWipe.exe                                             | 1666127467 | 2
| {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\win32calc.exe                              | 0          |
```

Question: Create a search query to identify the VPN installed on this host. What is name of the software?

Answer: ProtonVPN

Explanation:

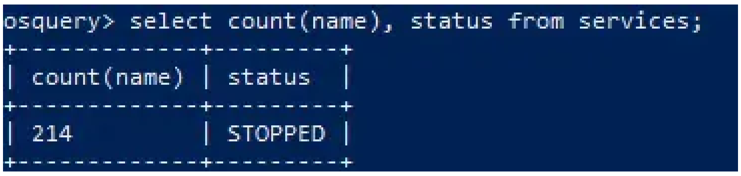


```
osquery> SELECT name  from programs;
+-----------------------------------------------------------------+
| name                                                            |
+-----------------------------------------------------------------+
| aws-cfn-bootstrap                                               |
| Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332     |
| AWS PV Drivers                                                  |
| osquery                                                         |
| Amazon SSM Agent                                                |
| Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332  |
| Google Chrome                                                   |
| Microsoft Edge Update                                           |
| Microsoft Edge WebView2 Runtime                                 |
| Npcap                                                           |
| ProtonVPN                                                       |
| Wireshark 3.6.8 64-bit                                          |
| Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31332 |
| Amazon SSM Agent                                                |
| ProtonVPNTap                                                    |
| ProtonVPNTun                                                    |
| aws-cfn-bootstrap                                               |
| AWS Tools for Windows                                           |
| ProtonVPN                                                       |
+-----------------------------------------------------------------+
```

Question: How many services are running on this host?

Answer: 214

Explanation:

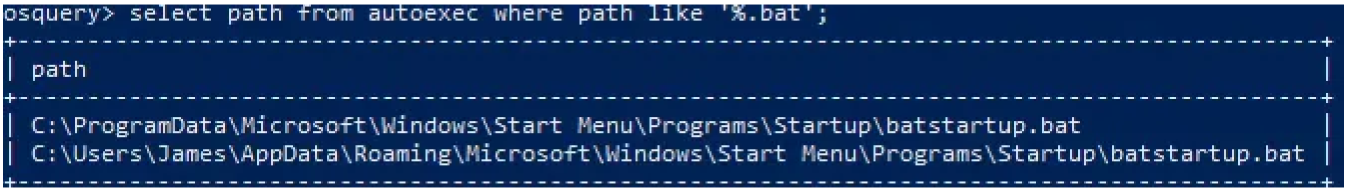


```
osquery> select count(name), status from services;
+-------------+---------+
| count(name) | status  |
+-------------+---------+
| 214         | STOPPED |
+-------------+---------+
```

Question: A table autoexec contains the list of executables that are automatically executed on the target machine. There seems to be a batch file that runs automatically. What is the name of that batch file (with the extension .bat)?

Answer: batstartup.bat

Explanation:



```
osquery> select path from autoexec where path like '%.bat';
+------------------------------------------------------------------------------------------+
| path                                                                                     |
+------------------------------------------------------------------------------------------+
| C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\batstartup.bat              |
| C:\Users\James\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\batstartup.bat |
+------------------------------------------------------------------------------------------+
```

Question: What is the full path of the batch file found in the above question? (Last in the List)

Answer: C:\Users\James\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\batstartup.bat

The tasks, questions or answers not mentioned here means there were no answers needed.