1. Describe your reversing environment (OS name and version) and the version of Chrome.

Use Process Explorer (or another system monitor) to answer the following questions:

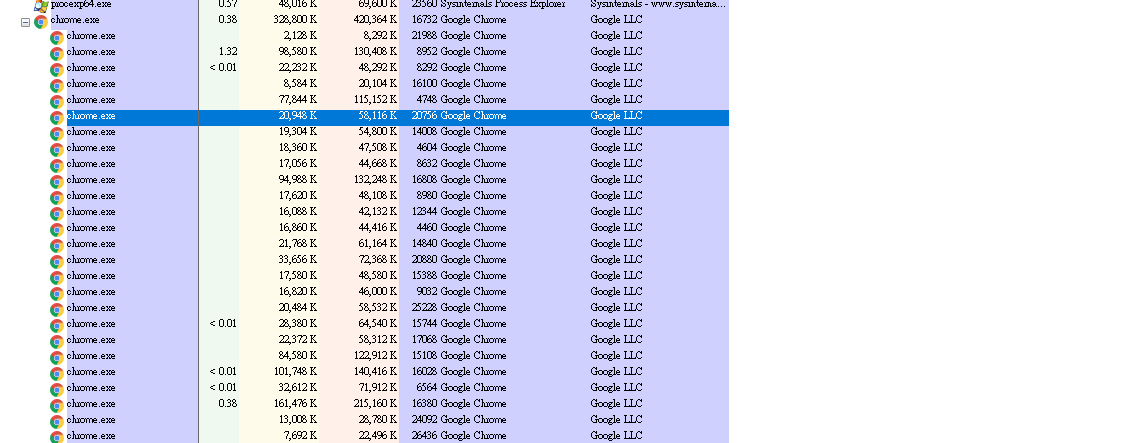
* OS: Windows 10 Home
* Chrome: 97.0.4692.99 (64bits)

2. Which system monitor tool did you use? Why?

* I used Process Explorer, because it provides more information than windows’ build in task manager.

3. How many Chrome windows and tabs are open? How many processes are grouped under the chrome.exe/chrome process tree?

I opened a chrome tab, and there are 24 processes under the process tree.



4. (Answer this question only if you're using Windows and Process Explorer) Minimize the Chrome browser, then use Process Explorer to bring the browser in focus. Bringing a process in focus means it's the active window on your GUI to accept keyboard/mouse input. List the steps you used to accomplish this task.

* Right click the process
* Select “bring to front “

5. Where is the Chrome executable file located on the system? List the steps you used to find this answer.

* Right click on the process
* Select properties
* Select Image tab
* The executable file will be located under the path label

“C:\Program Files (x86)\Google\Chrome\Application\chrome.exe”

6. List 3 format strings in the Chrome executable image. List the steps you used to accomplish this task.  This may require you to use the 'strings' executable from the command line for mac/linux.  A format string is a string used in C/C++ functions to format input or output, e.g. the first argument to a call to printf.

* Right click on the process
* Select Strings under properties
* Too few levels in Next()/ file exists/!This program cannot be run in DOS mode.$

7. Where is Chrome most likely writing its temporary data on the disk? List the steps you used to find this answer.

* Right click on the process
* Select properties
* Select Environment tab
* In the TEMP Variable
* C:\Users\kevin\AppData\Local\Temp