Hunting

Dựa vào đề bài ta dùng công cụ volatility3 để lấy thông tin dll. Trước hết dùng lệnh option dlllist tuy nhiên các đường dẫn và tên của dll tương đối hợp lệ và hầu hết nằm ở system32 nên đây không có dấu hiệu bất thường.

Ta dùng option ldrmodules để liệt kê các unlinked dll.

vol -f <dump file> ldrmodules

3244 notepad++.exe	0x7fef2310000	TRUE	TRUE	TRUE	\Program Files\Notepad++\plugins\NppConverter\NppConverter.dll
3244 notepad++.exe	0x7fef7710000	TRUE	TRUE	TRUE	\Windows\System32\d3d10_1.dll
3244 notepad++.exe	0x7fef7100000	TRUE	TRUE	TRUE	\Windows\System32\dxgi.dll
3244 notepad++.exe	0x7fef6470000	FALSE	FALSE	FALSE	\test\BLUECTF.dll
3244 notepad++.exe	0x7fef7650000	TRUE	TRUE	TRUE	\Windows\System32\d3d10_1core.dll
3244 notepad++.exe	0x7fef79c0000	TRUE	TRUE	TRUE	\Windows\System32\IconCodecService.dll

Tên và vị trí của dll này bất thường vì vậy ta nộp virtual address là 7feff6470000.