

# Finding Secret RDP Registry Keys Using IDA Free



#### ANYONE CAN PERFORM SIMPLE REVERSE ENGINEERING TASKS

**IDA** is a state-of-the-art reverse engineering tool commonly used in the software industry to analyze closed-source binaries. While free or cheaper alternatives like <u>Ghidra</u> are gaining in popularity, they are no match for IDA's decompiler in terms of accuracy and maturity. Luckily for us, <u>IDA Free</u> now includes an <u>x64 decompiler</u>, which makes reversing possible *without assembly language skills.* 

The goal of this blog post is to show how anyone can perform simple reverse engineering tasks using nothing more than logical deduction and the right set of tools. Instead of focusing on the final result, the steps include detailed screenshots and comments to show the complete thought process.

#### Prerequisites

Download and install <u>IDA Free</u>. Please note that this specific edition of IDA is not suitable for commercial use, but since this guide is meant as an introduction, it shouldn't be an issue. While I have access to <u>IDA Pro</u> at work, all the screenshots were taken using IDA Free to avoid confusion.

A Windows machine with RDP enabled is recommended to follow all the steps, but it is possible to do some of the tasks from another platform if necessary. I have used a clean Windows Server 2019 virtual machine for this project.

### **Finding a Goal**

This may sound obvious, but rather than poke around random binaries, it is a good thing to start with a goal in mind. In this article, our goal will be to **identify secret registry keys affecting the RDP H.264 video encoder**.

How you choose the goal doesn't matter, but I picked this one because I am familiar with H.264 in RDP through my work in the <u>FreeRDP project</u>.

The Microsoft RDP server is handled by the **Remote Desktop Services** system service, which is called **TermService** and uses termsrv.dll as its entry point:



### **Getting Started**

Create a new directory called «Reversing» in «My Documents» and copy «termsrv.dll» from «C:\Windows\System32» into it. Launch IDA and click **New** in the **Quick Start** dialog:



Browse to the «Reversing» directory, select «termsrv.dll» and then click **Open**:

		- • ×	
File Edit Jump Sea	#ch View Options Windows Help   物 物 物 物 本 刻 函 @   途 虚 ぼ ま・ま 編 X   ▶ 回 □ 物 数 書 留 評 野		
	Drag a file here to disassemble it		
	9 Select file to disassemble	×	
	← → · · ↑ Is PC > Documents > Reversing	✓ ♂ Search Revening P	
	Organize  New folder	III 🕶 🔟 \\	
	Name     Date modified     Type     Size		
	Image: Could access         Name         Date modified         Type         Size           Image: Could access         Image: Could access         Image: Could access         2021-10-29 418 PM         Application extens.         1,028 KB		
	Name     Date modified     Type     Size		
Travo II	Cach acces     C		
() over	Cock Acces      Cock Acce		
Colput	Cach acces     C		
II Cuput	Cock Acces      Cock Acce		

In the **Load a new file** dialog, check «Load resources» and then click **OK**. This option is not mandatory, but resource segments can sometimes contain valuable information.

Code new file      Code new file      Code file:     C Users (Advecteds: 17 + 62.P'Documents (iverening lammar, ull as      Protective accounties for AdVect (PD) [pe64.dt]      Denote Type (Souther data to and)      V     Intel Object excess     AdVD Advect (NT)     AdVEct     Ad			×
Proteine rescalable for AMD24 (PS) (ps64.dll)           Brary (fe           Processor type (skalled ck to set)           V         Intel Stable procession           AMD Ablon (K7)         ablon           Intel Stable procession         ablon           Intel Stable procession         ablon           Intel Stable procession         ablon           Intel Stable procession         BD36p           Intel Stable real         p2           Intel Stable real         p3			
Brary Re  Proteins response for the set of t			
Processor type (Rudle-Gk to set)			
V         Mode Body processors           AMD Mode To To         within           AMD Kalows (XT)         within           Head Body processor         8028p           Intel Argentum 4         8028p           Intel Fortum 1         p2           Intel Fortum 1         p3			
V         Mode Body processors           AMD Mode To To         within           AMD Kalows (XT)         within           Head Body processor         8028p           Intel Argentum 4         8028p           Intel Fortum 1         p2           Intel Fortum 1         p3			
AMD Abbon (N7) athlen AAD (24 with 30 Noval (24 with 30 Noval) at 22 Intel 1028 protected Intel 1028 protected Intel 1028 real Intel 1028 real			
AMD 65-2 web 3DNowl k2 Inel 0206 real 00206 Inel 0206 real 00206 Inel 0206 real 00206 Inel 0206 real 00206 Inel 0206 reat 00206 Inel 0206 Inel 0206			
Intel 8028/real         8028/r           Intel 8028/protected         8038/p           Intel 8038/protected         8038/r           Intel 8038/protected         8048/p           Intel 8048/protected         8048/r           Intel 8048/protected         8048/p           Intel 8048/protected         8048/r           Intel 8048/real         8048/r           Intel 8048/real         8048/r           Intel 8048/real         8048/r           Intel 8048/r         8048/r			
Intel 8038 protected         8038 protected           Intel 8038 real         8038 r           Intel 8048 protected         8048 protected           Intel 8048 protected         8048 r           Intel 8048 real         8			
Intel 8036 real 8036 r Intel 8036 protected 8046 p Intel 8046 real 8046 r Intel 8046 r Intel 8046 r Intel 8046 r Intel 8040 n Intel 804			
Intel 80467 real         80467           Intel 8086         8086           Intel Pertium 4         p4           Intel Pertium II         p2           Intel Pertium II         p3			
Intel 8086         8086           Intel Pentium II         p4           Intel Pentium II         p2           Intel Pentium II         p3			
Intel Pentium 4         p4           Intel Pentium II         p2           Intel Pentium II         p3			
Intel Pentium III p3			
Intel Pentium Pro (P6) with MMX 80686p			
Intel Pentium protected with MMX 80586p			
Intel Pentium real with MMX 80586r			
MetaPC (disassemble all opcodes) metapc			
Loading segment		Kernel options 1 Kernel options 2 Kernel optio	009.3
Enabler		Nerriel options 2 Kernel options 2	
Loading offset 0x00000000000000000000000000000000000	or enabled	Processor options	
Options			
Loading options     Create s	Jegments	Load resources	
Fill segment gaps     Create F     Load as code segment     Create i	FLAT group imports segment	Rename DLL entries     Manual load	

Confirm that you want to load the matching debug symbols by clicking **Yes** when prompted:



Once the main IDA interface appears, wait for the **Output** window at the bottom to say «the initial autoanalysis has been finished». This can take a few minutes and varies a lot depending on the size of the binaries.

Characterization of Constitution of High Documents for the state from the Constitution of High Documents for the State from the Constitution of the Constitution of the Constitution of the Constitution of the Constitution of the Constitution of the Constitution of th	ine Hig and at at a t → a is the first state of	
🚺 Auctions 🗖 🔿	e 😨 IDA Ver-A 💶 🐼 Hex Ver-1 🔹 🕭 Structures 📮 🗓 Bruns 📑 📆 Imports 📑 😥 Baparts 🖬	
To deter a difference of the second s		
	100.00% (+400,-200) (204,412) 0001/WED 000000010010000DIMBACIFIFMATUM (Fyminismalase with Res Ylev-1)	
Di Dvápul	o ø x	
The desceptization instruct prior 1.7. Protect order to field/Display for the prior of the descep- tion of the desception of the desception of the desception (requestion provide desception) of the desception (requestion provide desception) of the desception (requestion) of the desception of the desception (requestion) of the desception of the desception of the desception (requestion) of the desception of the desception of the desception (requestion) of the desception of the desception of the desception (requestion) of the desception of t	runtike ged odd	
nc		

That's it! You are now ready to begin investigating the contents of «termsrv.dll». Refer to this procedure to create IDA projects for new binaries in the future.

### **No Strings Attached**

**Strings** is the most useful view in IDA, but it is unfortunately not present in the default configuration. On the **View** menu, navigate to **Open subviews** then select **Strings**:



The new **Strings** view will be added, and show textual strings found anywhere inside the binary. Right-click anywhere inside the view to open the contextual menu, then select **Setup...**:



Check **Unicode C-style (16 bits)** to enable Unicode UTF-16 literals that are frequently used on Windows. The minimal string length can be changed if desired (5 is the default). Click **OK** to apply the changes:



The **Strings** view now shows a lot more strings than before. It took me years before I realized that IDA didn't look for UTF-16 strings by default, and it would have saved me a lot of time!



Press **Alt+T**, then type «H264» and press **Enter** to search for that specific substring in all of the strings in termsrv. dll. The **Output** window at the bottom should say «String H264 not found».

#### What's Your Name?

So «H264» as a string is not present in termsrv.dll, but maybe it can be found in function names or symbols? On the **View** menu, navigate to **Open subviews** then select **Names**:



The **Names** view functions in the same way as the **Strings** view. Press **Alt+T**, then type «H264» and press **Enter** to search for the keyword in all symbol names. Unfortunately, we still have no results for «H264», indicating that termsrv.dll may not be the right place to look.

Is this the end of the road? Not at all! Reversing is a lot like fishing, where it can take time to catch one fish but it's exciting when it finally happens. Let's try a different type of bait: <u>Process Explorer</u> from the <u>Sysinternals Suite</u>. Download and launch the tool on the RDP server, then look for a process called «svchost.exe» with the «rdpclip. exe» and «rdpinput.exe» subprocesses:

2 Process Explorer - Sysinternals: www	sysinternals.com IIT-HE	P\Administrate	arl (Administrate	c)			- 🗆 X
File Options View Process Find	-			· ·			
		1	i		1 1		<filter by="" name=""></filter>
Process	CPI	Private Byter	Muddae Ca	PID Description	A Commentation	Command Line	sinter by numes
RuntmeBroker.exe	CFI	1.828		5544 Puntime Broker	Company Name Monsoft Composition	C:\Windows\System32\RuntimeBroker.exe -Embedding	
RuntimeBroker.exe		10,392	C 22,100 K	5640 Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe -Embedding	
a: dihost.exe	< 0.0	1 5,268		5816 COM Surrogate	Microsoft Corporation	C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:(973D20D7-562D-44B9-B	70B-5A0F49CCDF3F)
RuntimeBroker.exe     smartscreen.exe		2,476		5336 Runtime Broker 3116 Windows Defender SmartScreen	Microsoft Corporation Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe -Embedding C:\Windows\System32\smartscreen.exe -Embedding	
WmiPrvSE.exe		2,396	K 8,588 K	7036 WMI Provider Host	Microsoft Corporation	C:\Windows\system32\wbem\wmiprvse.exe	
at background Task Host	0.7			6024 Background Task Host 1016 Host Process for Windows Services	Microsoft Corporation Microsoft Corporation	*C:\Windows\øystem32\backgroundTaskHost.exe* -Servert -e*CortanaUI AppXy7w C:\Windows\system32\sychost.exe +k RPCSS-o	o4pe2dr3ke93kfe509b1d0arkfb2x
sychost exe	0.3			468 Host Process for Windows Senices	Monsell Composition	C1Wodows\system32\sychostleve & DoomLaus I SM	
= svchost.exe	0.3	3 218,700	< 129,440 K		Microsoft Corporation	C:\Windows\System32\svchost.exe -k.temsvcs -s.TemService	
rdpcip.exe	< 0.0	1 3,496		4608 RDP Clipboard Monitor 3100 RDP Session Input Handler	Microsoft Corporation Microsoft Corporation	rdpclip "C:\Windows\System32'rdpinput.EXE"	
sychost exe		2,124	2.688 K	1132 Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbServic	8
<ul> <li>svchost.exe</li> </ul>	< 0.0			1144 Host Process for Windows Services 1152 Host Process for Windows Services	Microsoft Corporation Microsoft Corporation	C:\Windows\system32\sychost.exe & LocalService & W32Time C:\Windows\system32\sychost.exe & LocalServiceNetworkRestricted or & TimeBroke	
svchost.exe		1,900		1152 Host Process for Windows Services 1160 Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe +k LocalServiceNetworkRestricted -p -s TimeBroke C:\Windows\System32\svchost.exe +k LocalServiceNetworkRestricted -o -s Imhosts	rove
svchost.exe	<						>
Name	Description	Co	mpany Name	Path			^
profapi dli	User Profile Basic API	Me	rosoft Corporation				
propsys.dl dobase.dl	Microsoft Property Syste Rdp OneCore Base Ser	n Ma	rosoft Corporation	C:\Windows\System32\propsys.dll C:\Windows\System32\rdpbase.dll			
dpcorets dl	TS RDPCore DLL	Mic	rosoft Corporation	C:\Windows\System32'vdpcorets.dll			
dpcorets dil mui donano di	TS RDPCore DLL	Ma	rosoft Corporation	C:\Windows\System32\en-US\vdpcor C:\Windows\System32\vdpnano.dll	rets di mui		
doserverbase dl	Rdp Server OneCore Ba			C:\Windows\System32\vdpserverbase	e.dl		
regapi di molient di	Registry Configuration A Resource Manager Clier		rosoft Corporation rosoft Corporation	C:\Windows\System32\regapi.dl C:\Windows\System32\rmclient.dl			
port4.dl	Remote Procedure Call	Runtime Mic	rosoft Corporation	C:\Windows\System32\rpcrt4.dll			
saenh.dll RTWorkQ.dll	Microsoft Enhanced Cry Reatime WorkQueue D		rosoft Corporation rosoft Corporation				
sanci di	Security Accounts Man	ger Client Mic	rosoft Corporation	C:\Windows\System32\samcli.dll			
schannel.dll SDClient.dl	TLS / SSL Security Pro Session Directory Client		rosoft Corporation				
sechost.dll	Host for SCM/SDDL/LS	A Lookup Mic	rosoft Corporation	C:\Windows\System32\sechost.dll			
setupapi.dl SHCore.dl	Windows Setup API SHCORE		rosoft Corporation rosoft Corporation				
shell32.dl	Windows Shell Common		rosoft Corporation	C:\Windows\System32\shell32.dll			
shiwapi.dli SortDefault.nls	Shell Light-weight Utility	Library Mic	rosoft Corporation	C:\Windows\System32\shlwapi.dll C:\Windows\Globalization\Sorting\So	ut Dafault als		
spici.dl	Security Support Provid		rosoft Corporation	C:\Windows\System32\sepicli.dll			
StateRepository.Core.dll sychost.exe	StateRepository Core Host Process for Windo		rosoft Corporation		ory.Core.dll		
svchost exe svchost exe mui	Host Process for Windo	vs Services Mic	rosoft Corporation	C:\Windows\System32\en-US\svcho	ist.exe.mui		
	Fusion 2.5		rosoft Corporation	C:\Windows\System32\sxs.dl C:\Windows\System32\temsrv.dl			
and di				C:\Windows\System32\temsrv.dl C:\Windows\System32\en-US\temsr	v.dl.mui		
	Remote Desktop Sessio Remote Desktop Sessio	n Host Ser Mic					
emsrv.dl temsrv.dl facep.dl	Remote Desktop Sessio Microsoft® Remote Des	ktop Servi Mic	rosoft Corporation	C:\Windows\System32\tlscsp.dll			
aa di temaru di mui temaru di mui fisep di TSplog di	Remote Desktop Sessio Microsoft® Remote Des Web Service Securty P	itop Servi Mic ackage Mic	rosoft Corporation rosoft Corporation	C:\Windows\System32\tiscsp.dll C:\Windows\System32\TSpkg.dll	ore.dl		
emsrv.dl temsrv.dl facep.dl	Remote Desktop Sessio Microsoft® Remote Des	top Servi Mic ackage Mic Mic brary Mic	rosoft Corporation rosoft Corporation rosoft Corporation rosoft Corporation	C:\Windows\System32\tiscap.dll C:\Windows\System32\TSpkg.dll C:\Windows\System32\twinapi.appco C:\Windows\System32\uctbase.dll	are.dl		

Windows system services all run within «service host» (svchost) processes, which makes it harder to tell them apart. The Process Explorer **Command Line** column is quite helpful, otherwise the Get-CimInstance PowerShell cmdlet can be used to find the process id for a given service name:

Get-CimIns	stance -Class	s Win32_Se	rvice -Fi	ilter "M	Name LIKE	'TermService'"
ProcessId	Name	StartMode	State	Status	ExitCode	
1072	TermService	Manual	Running	ОК	0	

What matters is that we can see a list of DLLs loaded in the RDP server alongside termsrv.dll. Let's expand our search area to include a few DLLs that begin with «rdp» and copy them into our «Reversing» project directory:



While it is possible to have multiple IDA instances open at the same time, I would not recommend it, as it is easy to get lost. On the **File** menu, select **Close**. In the **Save database** dialog, select **Pack database** (**Store**) and then click **OK**:



We now have new files to look at, which I have decided to investigate in the following order:

- rdpserverbase.dll
- rdpbase.dll
- rdpcorets.dll
- rdpcore.dll
- rdpnano.dll

For each of those files, I repeat the entire process:

- Create new IDA project
- Search for «H264» string

The string «H264» is found a few times in rdpserverbase.dll and rdpbase.dll, but it's nothing significant. We finally hit the jackpot when searching for «H264» in rdpcorets.dll:



Not only do we see a lot of references to «H264», but some strings clearly hint at registry keys. We decide to focus on rdpcorets.dll and close all other IDA projects.

#### **Searching for Functions**

Now that we've found the strings, we can start searching for the functions that use them. Double-click on the string that appears to be a registry key path named «H264Encoding»:

#### Software\Policies\Microsoft\Windows NT\Terminal Services\H264Encoding

The corresponding symbol is automatically selected and shown in the **IDA View-A** tab. A lot of times, strings do not have a proper name in the binary, so IDA generates a name for them. In this case, our string is called «aSoftwarePolici\_0». Right-click on the symbol name, then select **Jump to xref to operand...**:



A list of functions using this specific string symbol appears. «SetH264EncodingParametersFromRegistry» looks like a good choice, so double-click on it:

DA - releasests di C. Wasse's demonstrates (T-HEP) Deservents / Rever	X 0 -	
File Edit Jurne Search View Debusser Options Windows		
	金 オ チ・オ mi × ト ■ □ Load Wedsene debugger ト 年 第 第	
	1 D 5, A, A, 5, 18, V b, D D reasonable, A K 10, 1, 1,	
Library function 🗮 Regular function 🗮 Detruction 🗮 Data 📕 Library	lored 🛑 External symbol 📕 Lumine function	
Theotom D # x	TA Werk C Mexicani C A Structure C D Drune C A Structure C	
	Lodata:0000001001501573 text "VT-1614", "Salvda record M Schöd 24a.reb".0	
Function name	* rdsta 000000100150C56 a dlaga 5 rdsta 000000100150C56 a draga 6 rdsta 00000100150C56 a draga 6 rdsta 000000000000000000000000000000000000	
2 _dynemic_initializer_for_Kdp.VFatOoba/Depets_s_initiance_ 7 _dynemic_initializer_for_Module_	Lindata:elementalisticial actingi da "GMVAG", 0 ; BATA 350F: GMVAG1:GMVAG1	
7 J. dynamic, initializer, for_Module_ 7 J7L_dynamic, initializer, for_J2BaseModule_	.rdata:000000100155CC0 : const NCNWR N507twarePolici 0	
7 ATL_dwaris_initiation_fileModule_	rdata:000000100150000 #SoftwarePolici_d: ; DATA XXEF: _monymous_namespaceCreateCompressorOutpubAcc4010	
7 ATL dynamic initializer for AtComModule	rdsraueeeeensiaalisticce j Actomyrstori (distattige/cold)+3310 rdsraueeeeensiaalisticce text "UT-10.6", "Softwarry/Valicies/Uterminal Ser"	
7 dynamic initializer for _g cflype_	rdata exemptions text "UTF-16LF", 'vicesVH264Fecoding',0	
7 wil details, dynamic initializer for a hender ind initializer for	<ul> <li>Index::000000010050504</li> <li>Align::00000010050504</li> <li>Andex::000000010050504</li> <li>Andex::000000010050504</li> <li>Andex::000000010050504</li> <li>Andex::000000010050504</li> <li>Andex::000000010050504</li> <li>Andex::00000001050504</li> <li>Andex::000000001050504</li> <li>Andex::00000000010504</li> <li>Andex::0000000000000504</li> <li>Andex::000000000000504</li> <li>Andex::00000000000504</li> <li>Andex::00000000000504</li> <li>Andex::00000000000504</li> <li>Andex::000000000000504</li> <li>Andex::00000000000000000000000000000000000</li></ul>	
7 wil details dynamic initializer for a header int initializer for	. rata interesting and a sense precording () (and a sense precording () () () () () () () () () () () () ()	
7 wil_details_dynamic_initialize_for_g_beader_init_Wilmitialize		
7 wil_detaikdynamic_initializer_for_g_procent.ocalData_	rdes:recompositions.com tubue disablescond i pata XEP anonymic seecond Creationercsscruturulace#10e	
vil_detaikdynamic_initializer_for_g_threadFailureCallbacks_	- rdsta recommendations and the stabler conduction in the stabler of block in	
🗾 _enonymeus_nemespicedynemic_initializer_form_timeSta.	<ul> <li>relation 20000001201127235</li> <li>alies 5</li> </ul>	
Thiothycatalc/indProc(HMAD1uit,unsignedint)4int	/rdss:recompositionstops ; comes tubble also adjusth : D4TA 3KEP; enormedia = tubble ComercisionOv/Arc+1451e	
T McGenControlCalbackV2		
CUMBDPhysicoc0Menager/NotifySettingsChangel_WRDS_SETTI 77 ATL: CC:emModule: CC:emModule: void	rdsts:00000010015015055 text "UTF-18LE", 'RecordFath',0	
ATL:CCemMedule:CComMedule:ComMedule:Com     ATL:CAtWoMedule:CAtWoMedule:edd	Adata (000000010015014) adata (000000010015004) data (00000000000000000000000000000000000	
7 ATL: CARCombindues CarCombindues (car	rdata:eeeeeeiikhiSSDC1 alias #	
7 ATL: CAtBaseModule: CAtBaseModule/visit	Indata:000000001015000 akee444/LCompressor*,0	
ATL: CComCriticaSection: inth/oid	· data model i data model i data data data data data data data da	
7 RDPStackTraceLogging:RDPStackTraceLogging,Register(void)	- ndstatements - ndstatements	
7 WppintUm	rate: cool preston hy Address	
7 RdpXPlatSlobalObjects:RdpXPlatSlobalObjects(void)		
ATL: CCemModule::http://tl:_ATL_DERMAP_ENTRY30 */HINSTAP		
WPP_INIT_CONTROL_AFRAV	<ul> <li>Instance (# is a Creationyaland and Interlay and Interlay</li></ul>	
1 McGeréventRegister		
CRdpinputChannelPluginFactory: initializationance(void)	-rdstarter and the o GBroughnooder.CasteToerform(void)=1115 ite at, aSoftwarePolic(2, SoftwarePolic(2, Softw	
CUMPDPListenerinet:EnableTectMode(ulong)	crists:1000 g2 (b) = CBanaplacoder.CenetTendtombode-1115 (e) as als alstheamPrice(a), Statuaret/Valcies/Microsoft/Windows "     crists:1000 g2 (b) = O. CBroader.CenetDeploidy-10 (e) as als alstheamPrice(a), Statuaret/Valcies/Microsoft/Windows "	
CUMRDPListenerRasel FinalRidease(void)	rdata (600	
CROPP coledSemple:RemoveAlBuffers(void) CRessStringT-subsct=cinitialas(void)	rdate:000	
CBaudStringTrusherts_initialize(void)     CFermatDataPackers.initialize(void)	- data 1000 - data 1000 incluit 7	
Compatibility access installey cody	- rdata (899	
C COMPANY CONTRACTOR OF COMPANY CONTRACTOR OF CONTRACTOR O	rdata:000 OK Canoal Search Hep e *)+23310	
Line Lat 2029	Oligate 0000001018ECC01 .edstataBeftwarePublic 0 (Eventualized with New Yorv-1)	
Diaput	0 # ×	
10001CEAD: propagate_stkargs: function is already types	A	
100101040: propagate stkargs: function is already typed 1000C7250: propagate_stkargs: function is already typed		
100072520: propagate stkargs: function is already typed		
1000C76AB: propagate stkargs: function is already typed Function argument information has been propagated		
The initial autoanalysis has been finished.	•	
DC .		
AU: idle Down Disk: 19658		

The IDA view now presents the disassembled «SetH264EncodingParametersFromRegistry» function, with commented assembly instructions:



While some advanced reverse engineers like this kind of view, it is quite difficult to read, especially without knowledge of assembly language. Press F5 to decompile the function into readable pseudocode. When IDA prompts for confirmation, click **Yes** to proceed:

<b>9</b>	lease confirm	×
•	The decompilation functionality is provided by a decompiler plug This plugin is not part of IDA. It is a separate product. The demo decompiler has limited functionality, namely: 1. Only x64 code is supported 2. Some advanced features are turned off 3. Batch decompilation is disabled 3. It is cloud based	jin.
	Naturally, the commercial version comes without these limitation It supports more processors than the demo version. Do you want to continue? Don't display this message again	IS.
	Yes No	

The decompiled function is now shown in all of its glory. Please bear in mind that since a lot of information is lost at compile time, IDA can only reconstruct automatically certain things, and make an educated guess at the rest. This particular example is surprisingly well decompiled, but most functions will have a lot of inaccuracies in them.

di la la 101

Decompiling a function is exciting, but did we find the right one? «EnableQPSingleStep» and «VideoDetectorRectDisplayMode» are clearly registry keys, but they have names that don't mean much except to someone well versed in H.264 codec internals. You can right-click on a function name or string constant in the pseudocode to find more cross-references to them. Let's try it on the «RegOpenKeyExW» function and see where we land:



As expected, «RegOpenKeyExW» is used in a lot of other places that deal with registry keys, most of which are unrelated to H.264. However, we can spot a few of the functions from the previous list of cross-references on the «H264Encoding» string, so let's move on to the «CreateOutputAvc» function:



Now that's what I'm talking about! We can see the following registry key names that hint at H.264 recording capabilities in the RDP server:

- RecordPath
- EnableRecord264
- EnableRecordYUV

DA - rdpconts.dll CIUsers/Administrator.IT-HELP/Documents/Reve	
File Edit Arrop Search View Debugger Options Window	
	i II マーイ ai X ト 日 日 Ia ant Windows Schupper → 知 注 「
1	
📄 Library function 📕 Regular function 📕 Instruction 📰 Data 📕 Lines	
Z functions D # X	🗓 (SA Non-A 🔹 🔯 Preválován-A 💶 🐼 Hox Nen-1 🔅 🕅 Structures 🔹 🛄 Structures 🔹 📆 Structures 🔹 📆 Structures
Function same	1 Datputke: "_fastcall CreateOutputke(int al, int a)
7 _dynamic_initializer_for_RdpXPlatGlobalObjects_s_instance_	3 int64 viz // rbx
7 dynamic initializer forModule	4 FLG TAGE // rax
ATL_dynamic_initializer_for_AdBaseModule_	3 BRARD dowing // [resetted] [resetted] and reset
All_dynamic_initializer_forAdWinModule	2 BYTE Datalali // [convisit] [cho-cith] BYTEF
ATL_dynamic_initializer_forAdComModule_	8 HEV Nov: // [mp-444] [rig-544] [rig-54] [rig-54]
Z _dynamic_initializer_for_g_cfType_ 7 wl_details_dynamic_initialzer_for_g_header_init_initialzeRec	10 int64 v121 // rap(54b) rtp:/4Cb
7 vi_bitai_pranic_intiator_to_g_biador_int_intiatoriat 7 vi_detaic_dynamic_intiator_to_g_biador_int_intiatoriat	11 [ 000; v43; // [rus-de] [ris-de] ] 2
7 wil_detaits_dynamic_initializer_for_q_header_init_Wilhitialize	12 WTC V123811 // [cspt60] [cfg-94] 0782 13 0860 V15 // [cspt74] [cfg-144]
wil_details_dynamic_initializer_for_g_processLocalData_	14
7 wil_deteits_dynamic_initializer_for_g_threadFailureCalibacks_	1 3 (vi = eldel) 16 (vice = eldel)
_enonymous_nerrespacedynemic_initializer_form_timeSta.	17 wennet 0(v11, 0, 0x220x104);
CTNet#yontaticWndPrecHMND_1uint,unsigned_int64_int0 7 McGenControlCaliback12	LI IT (Imported/Set) 1 Here Victor Account
McGenControlCaliback//2     CUMEDPProtocolManager:NotifySettingrChangel_WRDS_SETTI	20 L'Software/Volicies/Viirosoft/Windows NT/Terminal Services/W264Encoding",
ATL:CComMedule:CCemMedule:CcemMedule:oid	21 9, 0, 00000, 22 9, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
7 ATU: CARNiebBodule: CARNiebBodule(void)	23 Bridge )
T ATL: C48ComModule: C48ComModule(void)	24 ( 25 clots = 4;
ATL::C4tBaseModule:C4tBaseModule(void)	
ATL:CComCriticalSection:Init(void)	27 (DOMORD(st.) = (_DOMO ')Ovin (= 0; Dat chlata = 4)
7 PDPStackTraceLogging:#DPStackTraceLogging_Register(void)	
7 WppinitUm 7 Rdx/PlatGloba/Directs:Rdx/PlatGloba/Directs/void)	■ a) (this a) + (
7 Reporter and a sector of the sector of	32 if [ NewDerryshieted(New, L'Enable264.cg", 0064, &Type, Date, &chiete) 48 Type == 4 )
7 WPP_INT_CONTROL_ARRAY	22 v12 = "( De080 "Korta  = 0
7 McGenEventRegister	8.54 (coleta = 530) = 51 (ff (barrenning ((obe, C'Accordent), 6464, Elyes, vié, Acténts)    Type 1= 1 )
CRdpinputChannelPluginFactory:InitializeInstance(void)	
CUM#DPListenerinet:EnableTextMode(slong)	9 27 VLS = 92 94 VLS = 9464
CLWHEPL interefase: FinalRelease(void) CEEPPooledSample: RemoveAlBuffers(void)	22 y13 = 0:
CEDevelopareparation of Calestation (Calestation Calestation)	40 }
Const Data Review Installand with	42 6
CUMEDPLizenerRaser/sTerminated/void)	■ 43 5 × 50 × 51 × 51 × 51 × 51 × 51 × 51 ×
6 3	As RegCloseKey(Nev));
Line 1 of 3639	40
🛕 Graph overview 🗆 🖉 🗙	8-47 + mg_L64g ■49 i #f (105   H 1/42 ₩ 1/45 )
·····	42 return 9664:
	9.9 (v) = (FLE **)perator neu(Moduld3)) 51 (H (v) )
	52 return Output/wcirOutput/wcirG, si, s2, (struct RecordSettings ")vil, g Ids);
	33 ethern (Output/we *)-4)
3	
3	COUNTERA CREATE-PROVIDENT IS (LIDUITALA)
AD: idle Down Disk: 10468	

Let's try the «CreateCompressorOutputAvc» function to see if we can find more. It looks similar to the previous function, but with a few different registry keys:

- RecordPath
- EnableRecordRGB
- EnableRecordRdp264

😰 IDA - répcorets-dil.i64 (répcorets-dil) C/Users/Administrator.IT-HE		ns/Revening/adjocents.dl.id4 —	σ×
File Edit Jump Search View Debugger Options Windo			
😸 🖬 🖛 🖛 🐴 🆓 🆓 🖉 🖉	清武	🗠 📌 📽 📾 🗙 🕨 🖬 🖬 Local Windows debugger 💌 🕸 🛃 🚰	
1			
Library function 📕 Regular function 📕 Instruction 📃 Data 🗮 Un	explored	External symbol 🧧 Lumina function	
7 Functions D & X		IDA New A 🖸 🔯 Panulocode-A 🔯 🖉 Hex Verva1 😨 🕅 Structures 🔅 🔃 Drums 🔍 📆 Strupts 💭 Strupts 💭 Exports 💭	
Punctico name	· 1	<pre>LLE **fastcall anonymous_namespace_rifreateCompressorOutputAnc(int al, int a2)</pre>	
CProsyStream:-CProsyStream(void)		inté vá // réx	
CProxyStreamManager:-CProxyStreamManager(void)	4	Int vis // etil	
CProxyStream: scalar deleting destructor (uint)	2	FILE "V\$() // rax Deb00 chemistry // rrax=001 trib-r0h1 trib-	
CProxyStreamManagen/vector deleting destructor(uint)		DMDR Type: // [rsp-3db] [rbs-60] [PBF	
CProxyStreamManager:AddStreamToRegister(CProxyStream*)/o CProxyStream:CopyTo()Stream*_ULARGE_INTEGER_ULARGE_P		aver busia(4), // [res-whi] [res-chi] water water // [res-whi] [res-chi] water	
CProxyStream:CopyTo)Stream *_ODANCE_INTEDER_ODANCE_P		char v12[12]; // [rsp+50h] [rbp-00h] 8V807	
CProyStreamManager:CreateInstance(StreamDateAcquire *,CP	11	1st v1; // (reprise) (reprise)	
CProxyStreamManager:CreateStream(ulong.long.int,IStream * *)	13	BYTE V15[528]: // [rap-6Ch] [rbp-94h] BYRE	
CProxyStream:FilReceiveBuffer(uchar *,ulong.int)	14	sume viš; // (ripiz746) (ripiz1266)	
CProxyStreamManager: FreeRegisterEntry(STREAM_ENTRY ')     CProx/StreamManager:Initialize/vpid)	0 16	v4 = 8164;	
CProxyStreamManager:initialize(void)	17	http:= 0164; vi= 0;	
ChronyStreamManager: OnStreamDataReceivedTona.uchar *.ule	0 19	memort_0(v12, 0, 0x228ui64);	
CPron/Stream/Read/void ".ulong.ulong ")	• 28 21	if ( Ingeperteption) NEW DOL PARTNER.	
CProxyStreamManager: RemoveUnusedStreamsFromRegister(vo	22	L"Software(Vallicias)/Vicrosoft/Windows NT/\Terminal Services/VA204Encoding",	
CProxyStream:Seek(_LARGE_INTEGER_ulong_ULARGE_INTEGER	22 23 24 25 26	e, exosita,	
CProxyStream:SendFileContentsRequest(ulong.ulong)     CProxyStream:SeniceReadFromCechelvoid ".ulong.ulong ")	25	alicej )	
ChronyStream:ServiceAcadmonLache(void ',ulong,ulong ')	26	( doeta = 4)	
7 CProx/StreamManagen/Terminate/void)	0.28	<pre>if ( !trgperyvalueto@key, L*twoleRecord#68*, 0164, &amp;type, Osto, &amp;chOsto) 48 type == 4 )</pre>	
WPP_SF_Ddl	29 9 38	{	
CProxyDataObject:CProxyDataObject(CProxyDataObjectManage	• 31	v13 = v5	
CProxyDataObjectManager:CProxyDataObjectManager/Format     CProxyDataObject:-CProxyDataObject/void)	32 • 33	} closta = 41	
CProsyDataObject: - CProsyDataObject(void)	• 34	<pre>if ( HaggeryWaluetim(HKey, L"EnableSecondRdp264", 0164, 8Type, Data, &amp;chOata) 84 Type == 4 )</pre>	
CProv/DataObject: scalar deleting destructor (uint)	35	{ v14 = 7( Du0RD ")Dots (= 0)	
CProxyDataObjectManager: vector deleting destructor (uint)	0.37	v5  = v34g	
CProsyDataObjectManager:AcquireUniqueId(along *)	38	} chota = 520;	
DynAmay <int,ulong>=AddAt(ulong,int 8)</int,ulong>		if ( RegDuryValueIni(NKey, L'RecordPath", 0164, BType, v15, BcbDuta)    Type != 1 )	
CProxyDetaObject:CopyStgMedium(tagSTGMEDIUM const *,tag     CProxyDetaObjectManager CreateDataObjectSint)	• 41 42	vice • 0; else	
CProvyDataObjecti/KanageriCreateDataObjecti/H) CProvyDataObjecti/CreateInstance(CProvyDataObjectManager),	• 43	v16 = cbBeta:	
( )	• 44 45	RegClassRey(Hisy):	
Line 3617 of 3639	46	++'anonymous namespace'::g_ompIdx;	
A Graph overview	47	if (1/6) [1/8]) to 1 internet (1/8)	
	. 42	v6 = (FILT **)operator new(0x50u164);	
i		<pre>if ('0')</pre>	
	• 52	return (122 **)/45	
9	• 53		
8		-	
뢴		0015EAl_anonymous_mamespace_::CreateCompressorDurputAvo:10 (1000197A1)	
AU: idle Down Disk: 8108			

We are definitely onto something here, but we still haven't seen a function that makes use of the values from the registry keys. Class constructions or initialization functions are usually great spots, so let's try «OutputAvc::OutputAvc»:



The decompiled output from this OutputAvc constructor is more complex and contains more inaccuracies, but we can still see that it creates files with a specific name formatting. We could continue this for hours, so let's stop and see if we can act on the information we already have.

### **Collecting Information**

Once you get started with IDA, one issue most people face is finding a lot more information than they can process. You should see your primary goal as the «main quest» of the game, and everything else as «side quests». If you start taking too many tangents, you will lose track of your initial goal.

The best way to collect information is to use your favorite text editor to paste all sorts of clues as you find them. Do not try to organize them too much it's not worth it. You often learn the true value of individual pieces of information once they have been linked to something else.

Let's go back to our functions of interest for the RDP H.264 registry keys, and make a proper list. We have the names, but not the types, so let's look at the API documentation for <u>RegQueryValueExW</u>.

The lpType output parameter contains the type as defined in <u>Registry Value Types</u>, but unfortunately we do not have the numerical values for each. This is a frequent problem that can be fixed by using a copy of the <u>Windows</u> <u>SDK</u> headers. In this case, only two types are used **REG\_SZ** (1) and **REG\_DWORD** (4).

The only string type (REG\_SZ) is «RecordPath» all other registry keys are numbers (REG\_DWORD) with a value of 1 or 0. Please note that since «RecordPath» is a «REG\_SZ» type and not a «REG\_EXPAND\_SZ» type, it cannot contain environment variables like «%SystemRoot%». We end up with the following list of registry keys with comments:

#### HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\H264Encoding

- RecordPath: full path to an output directory for recording
- Enable264Log: enables H.264 logging, must be set to 1
- EnableRecordYUV: enables raw YUV capture dump (very large!)
- EnableRecordRGB: enables raw RGB capture dump (very large!)
- EnableRecord264: enables raw H.264 bitstream dump
- EnableRecordRdp264: enables raw RDP H.264 stream dump

#### **Testing It Out**

Now that we have collected valuable information, let's try using the registry keys to confirm that they actually work. Open the registry editor (regedit.exe), then create the «H264Encoding» registry key. Create the «C:\Windows\ Temp\RdpRecording» directory, then set the «RecordPath» key value accordingly. Create and set all of the other registry key values to 1 to enable all types of recording.



RDP H.264 registry keys are only going to be used if H.264 is used for the RDP connection, so let's tweak the RDP server configuration. Open the group policy editor (gpedit.msc) then browse to the following section under **Computer Configuration**:

#### Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment

Enable the following policies:

- Prioritize H.264/AVC 444 graphics mode for remote desktop connections
- Configure H.264/AVC hardware encoding for remote desktop connections

Enable and set the **Limit maximum color depth** policy to **32 bit** as it can affect codec negotiation as well.



Reboot the RDP server to apply the changes, then connect with RDP, do a few things to create image updates, and then sign out. Reconnect with RDP and then open the «C:\Windows\Temp\RdpRecording» directory to see if it worked:

Image: Solution         Image: Sol	I I RdpRecording				- 🗆 × ~ 0
→ Dark acces       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       ₩ Rev CVF       № 0.8         → Dendesder       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       № 0.8         → Dendesder       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       № 0.8         → Dendesder       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       № 0.8         → Porture W       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       № 0.8         → The PC       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       № 0.8         → The PC       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       1.022.80         → The PC       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       1.022.80         → The PC       → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       1.022.80         → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       1.022.80       □mary coverd, 1,920-0002,44p up to 2021-11-0.2039         → Imary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       1.53,500.80       □mary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       1.53,500.80       □mary coverd, 1,920-0002,44p up to 2021-11-0.2039       № 000 Fie       1.53,500.80       □mary coverd, 1,920-0002,44p up		Temp > RdpRecording			
Description         *         Imf_greeod_11982-0000_App.or/c         2011-13-20.359         MR DC File         0.83           Description         Imf_greeod_11982-0000_App.0f         2011-13-20.359         MR DC File         0.83           Description         Imf_greeod_11982-0000_App.0f         2011-13-20.359         MR To File         0.83           Description         Imf_greeod_11982-0000_App.0f         2011-13-20.359         MR To EDecoment         0.83           Imf_greeod_12902-0000_App.0f         2011-13-20.359         MR To EDecoment         1.83           Imf_greeod_12902-0000_App.0f         2011-13-20.359 <td< th=""><th>Name</th><th>Date modified</th><th>Type</th><th>Size</th><th></th></td<>	Name	Date modified	Type	Size	
■ Density         m/g.vcccl, 1(282:000)/2,4p.up         2021-11-39.250         M0 File         0.80           ■ Density         m/g.vcccl, 1(282:000)/2,4p.up         2021-11-39.250         M0 File         0.80           ■ Density         m/g.vcccl, 1(282:000)/2,4p.up         2021-11-39.250         M0 File         0.80           ■ Polycover         m/g.vcccl, 1(282:000)/2,4p.up         2021-11-39.250         M0 VIF 16         0.80           ■ Polycover         m/g.vcccl, 1(282:000)/2,4p.up         2021-11-39.50         MN VIF 16         0.80           ■ Polycover         m/g.vcccl, 1(282:000)/2,4p.up         2021-11-39.50         MN VIF 16         1.575.000           ■ Polycover         2021-11-39.50         AVM NO File         1.575.000         1.575.000           ■ m/g.vcccl, 1(292:000)/2,4p.up         2021-11-39.50         AVM To Elocurret         3.18           ■ m/g.vccccl, 1(292:000)/2,4p.up	de recent 1 1020-1020 24e	7021.11.30 3-26 PM	RAVC File	0 KB	
▶ Decimets         *         in #y.wcodd, 1,1920.0108,24p.24         2021-11-39.25 PM         204 File         0.0           ▶ Decimets         *         in #y.wcodd, 1,1920.0108,24p.24         2021-11-39.25 PM         Tob Decimets         0.0           ▶ Decimets         *         in #y.wcodd, 1,1920.0108,24p.24         2021-11-39.25 PM         Tob Decimets         0.0           ▶ This PC         *         in #y.wcodd, 1,1920.0108,24p.24         2021-11-39.25 PM         Tob Decimets         0.0           ▶ This PC         *         in #y.wcodd, 1,1920.0108,24p.24         2021-11-39.25 PM         Ruft File         1.02 File           ■         in #y.wcodd, 1,1920.0108,24p.24         2021-11-39.25 PM         Ruft File         1.02 EI         1.00 File           ■         in #y.wcodd, 1,1920.0108,24p.24p.22         2021-11-39.25 PM         Ruft File         1.02 EI         1.00 File           ■         in #y.wcodd, 1,200.0108,24p.24p.22         2021-11-39.25 PM         Ruft File         1.02 EI         1.00 File         1.00	Uesktop // Dirdn record 1 1920v1080 24n				
Potenset         //         indy_second_1,1920:0108,24p         2021-11-20.25.04M         VUF Fie         0.03           Photose         //         indy_second_2,1920:0108,24p         2021-11-20.25.04M         VUF Fie         0.03           Photose         //         indy_second_2,1920:0108,24p         2021-11-20.25.04M         VUF Fie         0.03           Photose         //         indy_second_2,1920:0108,24p         2021-11-20.95.04M         ROUT Fie         1.027.010           Photose         //         indy_second_2,1920:0108,24p         2021-11-20.95.04M         ROUT Fie         1.027.010           Indy_second_2,1920:0108,24p         2021-11-20.95.04M         ROUT Fie         1.027.010         1.029.010           Indy_second_2,1920:0108,24p         2021-11-20.95.04M         ROUT Fie         1.027.010         1.027.010           Indy_second_2,1920:0108,24p         2021-11-20.95.04M         ROUT Fie         1.027.010         1.027.010           Indy_second_2,1920:0108,24p         2021-11-20.20.04M         ROUT Fie         1.027.010         1.017.011           Indy_second_2,1920:0108,24p         2021-11-20.20.04M         ROUT Fie         1.027.010         1.017.011           Indy_second_2,1920:0108,24p         2021-11-20.20.04M         ROUT Fie         1.126.040         1.017.010					
P Network         // mp. proceed. 1, 1282-0038 (3, 4pg, yww. 2012) - 11-12-38.58 MM         PVVV File         0.83           The PC         // mp. proceed. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-38.58 MM         PVV File         0.81           Methods         // mp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-38.58 MM         PVV File         0.021 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-38.58 MM         PVV File         0.021 HS         1000 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-38.59 MM         PVV File         10.21 HS         1000 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-38.59 MM         PVV File         10.21 HS         10.21 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-28.59 MM         PVV File         10.21 HS         10.21 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-28.59 MM         PVV File         10.21 HS         10.21 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-28.59 MM         PVF File         10.14 HS         10.14 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-28.59 MM         PVF File         10.14 HS         10.14 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-28.59 MM         PVF File         12.14 HS         10.14 HS           Imp. proced. 2, 1282-0038 (3, 4pg, yww. 2012) - 11-12-28.59 MM <td< td=""><td></td><td></td><td></td><td></td><td></td></td<>					
This PC         infg.recol.2, 1920:0003,24p.row         2021-11-39.95.0A.M         RUC Tile         1,027.01           IF Marcol.         infg.recol.2, 1920:0003,24p.row         2021-11-39.95.0A.M         RUG Tile         1,027.01           IF Marcol.         infg.recol.2, 1920:0003,24p.row         2021-11-39.95.0A.M         RUG Tile         1,027.01           IF Marcol.         infg.recol.2, 1920:0003,24p.row         2021-11-39.95.0A.M         Tole Document         3.18           Infg.recol.2, 1920:0003,24p.row         2021-11-39.26.0FM         RUG Tile         12.00.18           Infg.recol.2, 1920:0003,24p.row         2021-11-39.26.0FM         RUG Tile         12.76.48           Infg.recol.2, 1920:0003,24p.row					
	D 1 1000 1000 01		RAVC File	1,027 KB	
Infly_record_2_N250.0008_App.         2021-11-30 95.00.40         YT et Document         31.83           Infly_record_2_N250.0008_App.ncb         2021-11-30 26.95 MA         YT FFE         595.07 KB           Infly_record_2_N250.0008_App.ncb         2021-11-30 26.95 MA         RAUC File         210.813           Infly_record_2_N250.0008_App.ncb         2021-11-30 26.95 MA         RAUC File         210.813           Infly_record_2_N250.0008_App.ncb         2021-11-30 26.95 MA         RAUC File         210.83           Infly_record_2_N250.0008_App.ncb         2021-11-30 26.95 MA         208 File         210.83           Infly_record_2_N250.0008_App.ncb         2021-11-30 26.95 MA         VEF File         51.04 KB           Infly_record_2_N250.0008_App.ncb         2021-11-30 26.95 MA         RAUC File         11.70 46.05           Infly_record_2_N250.0008_App.204         2021-1-30 26.95 MA         RAUC File         11.70 46.05           Infly_record_2_N250.0008_App.204         2021-1-30 26.95 MA         RAUC File         11.70 46.05	rdp_record_2_1920x1080_24p	.rgb 2021-11-30 9:50 AM	RGB File	1,579,500 KB	
Indipreced 2, 14920-0803 (Apply)         2021-11-10-2019 M         V/V File         99,070-88           Indipreced 3, 14920-0803 (Apply)         2021-11-10-2019 M         RUC File         12,00-88           Indipreced 3, 14920-0803 (Apply)         2021-11-10-2019 M         RUC File         12,00-88           Indipreced 3, 14920-0803 (Apply)         2021-11-10-2019 M         126 File         120 R           Indipreced 3, 14920-0803 (Apply)         2021-11-10-2019 M         126 File         120 R           Indipreced 3, 14920-0803 (Apply)         2021-11-10-2019 M         VFF File         14.08           Indipreced 4, 14920-0803 (Apply)         2021-11-10-2019 M         VFF File         13,176 K8           Indipreced 4, 14920-0803 (Apply)         2021-11-10-2019 M         VFF File         13,176 K8           Indipreced 4, 14920-0803 (Apply)         2021-11-10-2019 M         VFF File         13,776 K8           Indipreced 4, 14920-0803 (Apply)         2021-11-10-2019 M         KPC File         13,706 K8           Indipreced 4, 14920-0803 (Apply)         2021-11-10-2019 M         KPC File         13,706 K8           Indipreced 4, 14920-0803 (Apply)         2021-11-10-2019 M         KPC File         13,706 K8           Indipreced 4, 14920-0803 (Apply)         2021-11-10-2019 M         KPC File         13,706 K8	Network rdp_record_2_1920x1088_24p	.264 2021-11-30 9:50 AM	264 File	1,022 KB	
Infly_record_3_PB00.008_24p.up.         2001-11-30-205 PM         RNUC File         210 KB           Infly_record_3_PB00.008_24p.         2011-11-30-205 PM         RDE File         153 S00 KB           Infly_record_3_PB00.008_24p.         2011-11-30-205 PM         264 File         210 KB           Infly_record_3_PB00.008_24p.         2011-11-30-205 PM         264 File         210 KB           Infly_record_3_PB00.008_24p.         2011-11-30-205 PM         146 File         143 B           Infly_record_3_PB00.008_24p.         2011-11-30-205 PM         VVI File         54 Hol KB           Infly_record_3_PB00.008_24p.         2011-11-30-206 PM         VVI File         54 Hol KB           Infly_record_4_PB00.008_24p.         2011-11-30-206 PM         PMC File         11,204 KB           Infly_record_4_PB00.008_24p.	rdp_record_2_1920x1088_24p	2021-11-30 9:50 AM	Text Document	33 KB	
Imp_record_1,1920-0008_2Aproph         2021-11-10-22.05 PM         PAD File         153,800-88           Imp_record_1,1920-0008_2Aproph         2261-11-10-22.05 PM         2261-11-10-22.05 PM         2561-10-22.05 PM           Imp_record_1,1920-0008_2Aproph         2261-11-10-22.05 PM         Text Document         4.88           Imp_record_1,1920-0008_2Aproph         2261-11-10-22.05 PM         VTF VE         55,146.88           Imp_record_1,1920-0008_2Aproph         2221-11-10-20.05 PM         VTF VE         55,146.88           Imp_record_1,1920-0008_2Aproph         2221-11-10-20.05 PM         VTF VE         51,146.88           Imp_record_1,1920-0008_2Aproph         2221-11-10-20.05 PM         ROF File         12,776.80	rdp_record_2_1920x1088_24p	.yuv 2021-11-30 9:50 AM	YUV File	596,700 KB	
Infly_record_3_PR020408_24p_204         2021-11-102.205 PM         246 File         210 KB           Infly_record_3_PR020408_24p_204         2021-11-102.205 PM         Text Discument         443           Infly_record_3_PR020408_24p_2040         2021-11-102.205 PM         VVF File         55,104.83           Infly_record_3_PR020408_24p_2040         2021-11-102.005 PM         VVF File         12,124.83           Infly_record_4_PR020408_24p_2042         2201-11-102.005 PM         RMC File         11,276.83           Infly_record_4_PR020408_24p_2042         2201-11-102.005 PM         RMC File         11,276.83           Infly_record_4_PR020408_24p_2042         2201-11-102.005 PM         RME File         11,276.83           Infly_record_4_PR020408_24p_2042         2201-11-102.005 PM         RME File         11,276.83           Infly_record_4_PR020408_24p_2042         2201-1-102.005 PM         RME File         11,276.83					
Imfgreeced, 3, 1920-0008, App.         2021-11-10-20.09 MM         Yate Document         4.80           Imfgreeced, 4, 1920-0008, App.nev         2021-11-10-20.09 MM         VVD File         55, 14-16           Imfgreeced, 4, 1920-0008, App.nev         2021-11-10-20.09 MM         NUPC File         17, 276-86           Imfgreeced, 4, 1920-0008, App.nev         2021-11-10-20.09 MM         RAPC File         12, 777-100           Imfgreeced, 4, 1920-0008, App.24         2021-11-10-20.09 MM         RAPE File         12, 777-100           Imfgreeced, 4, 1920-0008, App.24         2021-11-10-20.09 MM         RAPE File         12, 777-100           Imfgreeced, 4, 1920-0008, App.24         2021-11-10-20.09 MM         RAPE File         12, 777-100					
Influenced, 2, 1920:0008, 24pp.uvc         2021-11-30 2.05 PM         YUV File         55,140 KB           Influenced, 1, 5920:0008, 24pp.uvc         2021-11-30 2.05 PM         RAUC File         11,2745 KB           Influenced, 1, 5920:0008, 24pp.uvc         2021-11-30 2.05 PM         RAUC File         11,2745 KB           Influenced, 1, 1920:0008, 24pp.uvc         2021-11-30 2.05 PM         RAUE File         11,2775 KB           Influenced, 1, 1920:0008, 24pp.04         2021-11-30 2.05 PM         RAUE File         11,2795 KB           Influenced, 1, 1920:0008, 24pp.04         2021-11-30 2.05 PM         Tebe Decoment         282 KB					
Imfgreexed, 4; 1920:108(2), 4panet         2201-11-10: 20.0 PM         PAUC File         11, 276: 80           Imfgreexed, 4; 1920:108(2), 4pa: 204         2201-11-10: 20.0 PM         R06 File         12,077: 100           Imfgreexed, 4; 1920:108(2), 4pa: 204         2201-11-10: 20.0 PM         10.6 File         12,770: 80           Imfgreexed, 4; 1920:108(2), 4pa: 204         2201-11-10: 20.0 PM         10.6 File         12,770: 80           Imfgreexed, 4; 1920:108(2), 4pa: 204         2201-11-10: 20.0 PM         Teb Executer         22.8 R0					
rdp_recod_4_1920.01080_24p.rdp         22011-11-30 20.6 PM         R06 File         12,077,100					
rdp_record_4_1922b1088_24p_284         2022-111-30 36.06 PM         264 File         13,709 KB           mdp_record_4_1922b1088_24p         2022-111-30 36.06 PM         Text Document         262 KB					
Text Document 262 KB					
☐ rep_recordinductioss_equiptiv doct-11-ou solo invin 1107 Hile 4,562,401 KS					
	rdp_record_4_1920x1088_24p	1.yuv 2021-11-30 3:06 PM	YUV File	4,562,460 KB	

Empty files are usually the ones currently used by the RDP server; they are flushed to the disk only when the session is terminated, which is why a full sign out is required. Since these are raw data dumps used for internal debugging, they require a bit of transformation.

The uncompressed YUV pixels can be played directly using <u>VLC</u> and the right command-line options:



Alternatively, the raw H.264 bitstream can be embedded into an .mp4 video file using ffmpeg:



The actual file names and parameters will vary, so adjust them accordingly. Here is what it should look like when it works:

 7										
					_					
-										
- I I - I Aplance					- 0 X					
	a PC + System (C) + Windows + Semp				v 6 SeathRa. #					
Calif. Access	C Nerve	Data modified 2021-11-29 10:14 PM	Spe	504						
E Duittop /	10 Hp. mind, 1, 1925-1988, 24p	2021-11-20-10-14 PM	294 File Text Document	31.42					1051.5	
Desetlash /	C represent U. 1920/188, 24p per		Ville File	025,442.428						
E Patron /	<ul> <li>nip_mont_2_10254188_24p284</li> <li>nip_mont_2_10254188_24p</li> </ul>	2021-11-29 10:14 PM 2021-11-29 10:14 PM	204 File Test Document	101.425				and the second		
Co hak	C rtg., word, J., 1929-1988, 24p.par	2025-11-20-10-14 PM	V(N File	45,90148		and the second s		ALCONTRACTOR ALCONTRACTOR		
a famous	<ul> <li>Hp., econd., 3, 1920-1988, 34p.264</li> <li>Hp., econd., 3, 1920-1988, 34p.264</li> </ul>	2021-11-29 10:14 PM 2021-11-29 10:14 PM	204 File Text Document	148					a statistical second	
and the second	internet. (1, 1925-1988, Mp. part internet.), 1925-1988, Mp. part		Yull File	148				The second s	(Alternational)	
							Course and the second			
								CONTRACTOR STOCK		
1 mm						and the second sec				
	Ø Administratur ProverS						0	- D X		
	PS Cristininestrept	deflectrding)				elght 1000 - rawdd-throne 1				
									an della	
								•		
P 🔳 🏟 🗽								10 4a mo -	D MARK	

Just like most «secret» registry keys, they weren't hidden, but they weren't meant to be used or relied upon. There is also no guarantee that they will be supported in the future.

## **Closing Thoughts**

Without access to the source code, one can still gain insight into closed-source binaries used on millions of devices. There is a certain adrenaline rush associated with finding ways to achieve useful things that are not normally supported. While advanced reverse engineering takes a lot more work, one has to start somewhere. If you are a beginner in reverse engineering, did you find this blog post useful? If so, what would you like to learn next?

