

# 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	zh View Options Windows Help 雪雪雪雪雪雪云 ● 金融波力・水磁× ● ■ ■ ・ 电合 固計的		
	Drag a file here to disassemble it		
	9 Select file to disassemble	×	
	← → → ↑ 📙 > This PC > Documents > Reversing	✓ δ Search Revening P	
	Organize • New folder		
	Diganize * New folder  * Quick access Compared to the second seco		
	Cogunia - New folder     Nome     Date modified     Type     Size     Date modified     Type     Size     Date modified     Type     Size     Date modified     Type     Size		
	Cepera × New failer  Name  Date modified  Type Stat  Control of the second sec		
Travo II	Cepera * New failer  Nerre  Nerre  Date modified  Type Stat  Comparison  Type Stat  Date modified  Type Stat  Date modifie		
() over	Oppers         Neuror         Date modified         Type         Sate           Image: Source of the source of th		
Colput	Cepera Non-fallow Name Carlos State Carlos S		
II Cuput	Copyers * New failer     Norm     Date modified Type Size     Date modified     Date modified Type Size     Date modified     Date modified Type Size     Date modified	■ • ■ ● ■ ● ×	

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.

👷 Load a new file				×
Load file C: \Users\Administrator.IT+HELP\Documents\Reversing\tr	ermsrv.dl as			
Portable executable for AMD64 (PE) [pe64.dll]				
Binary file				
Processor type (double-click to set)				_
MID Athlon (K7)	athion			
AMD K6-2 with 3DNow!	k62			
Intel 80286 protected	80286p			
Intel 90286 real	80286r 90286n			- 117
Intel 80386 protected	80386r			
Intel 80486 protected	80486p			- 10
Intel 80486 real	80486r			- 11
Intel 8086	8086			
Intel Pentium II	p2			
Intel Pentium III	p3			
Intel Pentium Pro (P6) with MMX	80686p			
Intel Pentium real with MMX	80586p			
MetaPC (disassemble all opcodes)	metapc			
Loading segment	0x0000000000000000	nalysis	Kernel options 1 Kernel options 2 Kernel options 3	
	6	_ Enabled		_
Loading offset	0x0000000000000000000000000000000000000	Indicator enabled	Processor options	
Options				
Loading options	×	Create segments	Load resources	
<ul> <li>Fill segment gaps</li> </ul>		Create FLAT group	Rename DLL entries	
I NOT AND AND ADDRESS OF ADDRESS OF ADDRESS ADDRES	P	) create input a argument		

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.

Chi tanua di Cata Amaria dal 1417 Supersita da ta di cata da c ta di cata da c	ovýhenod – O X n Do obla za stala – O X na do stala za stala – O X na do stala za stala – Stala za stala za stala – Stala za stala – Stala za	
📝 Functions 🛛 🖉 🛪	😨 EA Vier-A 🖪 🕅 Hex Vier-1 🗌 🕼 Stockares 🗌 🗓 Eruns 🗌 📆 Expans 🔹 🚼 Expans	
Table to the second sec	International line     International line       International line     International line <td></td>	
	100.004 (~405,-20) (254,422) 00017750 00000010010800: _DIBALBCETSTARTON (Fyendenised with New Yiew-1)	
Di Odavi		
<ul> <li>the constraints before it is.</li> <li>Please tasks the MCHO plaqs are not proven that the MCHO plaqs are not provide the model of the MCHO plane. The MCHO plane because the MCHO plane plane plane plane because the MCHO plane plane plane plane plane plane plane plane plane plane plane plane plane plane plane plane plane plane.</li> </ul>	non and and a second se	
The set of		

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:

<b>* •</b> • • • • • • • • • • • • • • • • •								
Process Explorer - Sysinternals: www.s	sysinternais.com (11-i	HELPGAdmin	istrator) (Ac	aministrator				~
File Options View Process Find I	DLL Users Help							
🔜 🗃 🔳 🖻 🧮 🖓 🗙	<b>A</b> 💮			mar 1	1 A . A			<filter by="" name=""></filter>
					he Alexand I have and I he was a			in the synamic
Process	(	CPU Private	Bytes W	Vorking Set	PID Description	Company Name	Command Line	
RuntmeBroker.exe		1	1,828 K	3,148 K	5544 Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe -Embedding	
HuntimeBroker.exe		10	),392 K	22,100 K	5540 Runtime Broker	Microsoft Corporation	C:\Windowa\System32\RuntimeBroker.exe -Embedding	
a) dihost.exe	<	0.01	5,268 K	7,120 K	5816 COM Surrogate	Microsoft Corporation	C:\WINDUWS\SYSTEM32\DLLHUST.EXE /PROCESSID:(973D20D7-562D-44	B3-B70B-SA0F43CCDF3F}
I HuntmeBroker.exe			C,475 K	8,668 K	2006 Huntime Broker	Microsoft Corporation	C: Windows System 32 Houtenetroxer exer-Embedding	
di WmiPn/SE ava			2 396 K	8 588 W	2036 WMI Provider Host	Monoration Monoration	C-Windows wystem 32 when screen exe - Chibedong	
and background Task Host		0.76	2,536 K	12 992 K	6024 Background Task Host	Monart Corporation	C: Windows/system/2/hank.on/indTaskHost evel "Security of Cataon III Ann	Xv7xh4nc2dr3kc93kfc509h1d0x44h2v
sychost exe		0.38	5 544 K	8 160 K	1016 Host Process for Windows Services	Microsoft Comprision	C:\Windows\system32\sychott exe & BPCSS o	in the second of the second
suchast eve		0.01	784 K	5 152 K	468 Host Process for Windows Services	Memore Comparation	C\Windows\system32\system32\system42	
E T avchost exe		0.38 218	3,700 K	129,440 K	1072 Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\avchost.exe.k.temsvcs.is.TemService	
- tdpclip.exe	<	0.01 3	3,496 K	10,676 K	4608 RDP Clipboard Monitor	Microsoft Corporation	rdpclip	
rdpinput.exe		1	1,596 K	4,924 K	3100 RDP Session Input Handler	Microsoft Corporation	"C:\Windows\System32\rdpinput.EXE"	
svchost.exe		- 2	2.124 K	2.688 K	1132 Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe -k:LocalSystemNetworkRestricted -p -s Ncb:	Service
svchost.exe	<	0.01 1	1,924 K	4,292 K	1144 Host Process for Windows Services	Microsoft Corporation	C:\Windows\system32\svchost.exe +k LocalService -s W32Time	
svchost.exe	<	0.01 1	1,900 K	4,576 K	1152 Host Process for Windows Services	Microsoft Corporation	C:\Windows\system32\svchost.exe +k LocalServiceNetworkRestricted -p -s Time	BrokerSvc
svchost.exe			1.840 K	3.144 K	1160 Host Process for Windows Services	Microsoft Corporation	C:\Windows\Svstem32\svchost.exe + LocalServiceNetworkRestricted -o -s Imho	ete
I N SVGDOSLEXE								
Name	Description		Company	y Name	Path			
profapi.dll	User Profile Basic AP	PI	Mcrosoft	Corporation	C-\Wedows\Sustem22\perfact dl			
propeys.dl	Manager Property Co.				C. THE BOTH STREETS A PROPERTY			
	recrosort property Sy	ystem	Microsoft	Corporation	C:\Windows\System32\propsys.dll			
dpbase.dl	Rdp OneCore Base 3	ystem Services	Microsoft Microsoft	Corporation Corporation	C:\Windows\System32\propsys.dll C:\Windows\System32\rdpbase.dll			-
dpbase.dl dpcorets.dl	Rdp OneCore Base 3 TS RDPCore DLL	ystem Services	Mcrosoft Mcrosoft Mcrosoft	Corporation Corporation Corporation	C:\Windows\System32\propsys.dl C:\Windows\System32\vdpbase.dl C:\Windows\System32\vdpbase.dl C:\Windows\System32\vdpcorets.dl			-
dpbase dl dpcorets dl dpcorets dl mui dpcored dl	Rdp OneCore Base 3 TS RDPCore DLL TS RDPCore DLL	ystem Services	Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation	C:Windows/System32/propsys.dl C:Windows/System32/vropsys.dl C:Windows/System32/vdpcorets.dl C:Windows/System32/vdpcorets.dl C:Windows/System32/vdpcorets.dl	ets dil mui		-
dpbase.dl dpcorets.dl.mui dpcano.dl dpsano.dl dpsanvebase.dl	Rdp OneCore Base 3 TS RDPCore DLL TS RDPCore DLL Rdp Server OneCore	ystem Services a Base Service	Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation	C: Windows System 32 upopp all C: Windows System 32 upopps all C: Windows System 32 upopers all C: Windows System 32 upopers all C: Windows System 32 upopers all C: Windows System 32 upoperovehaae	eta di mui		
dpbase dl dpcorets dl dpcorets dl mui dpnano dl dpasnverbase dl respei dl	Report Property Sy Rep OneCore Base 3 TS RDPCore DLL TS RDPCore DLL Rep Server OneCore Registry Configuration	ystem Services a Base Service in APIs	Microsoft Microsoft Microsoft Microsoft s Microsoft Microsoft	Corporation Corporation Corporation Corporation	C. Windows System 32, propaga all C. Windows System 32 vdpbare. dl C. Windows System 32 vdpbare.	ets all mui		-
dpbase dl dpcorets dl dpcorets dl mui dprano dl dpasevethase dl regari dl molent dl	Rdp OneCore Base 3 TS RDPCore DLL TS RDPCore DLL Rdp Server OneCore Registry Configuration Resource Manager O	ystem Services a Base Service in APIa Client	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation	C. Windows System 22 yroppys off C. Windows System 22 yroppys off C. Windows System 22 yroppys off C. Windows System 22 en US vebcore C. Windows System 22 en US vebcore C. Windows System 22 wroppy of C. Windows System 22 wroppy of C. Windows System 22 wroppid fil C. Windows System 22 wroppid fil C. Windows System 22 wroppid fil C. Windows System 22 wroppid fil	ets di mui di		-
dobase di docoreta di docoreta di mui doponeno di doperverbase di regapi di molent di port4 di 	Rep OneCore Base 3 TS RDPCore DLL TS RDPCore DLL Rdo Server OneCore Registry Configuration Resource Manager C Remote Procedure C	ystem Services a Base Service in APIs Dient Cal Runtime	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C: Windows System 32 propps all C: Windows System 32 https://www. C: Windows System 32 https://www.dialac. C: Windows System 32 https://www.sistem.s	ets all mui		-
dobase dl docenta dl docenta dl mui docence dl docence dl docence da docence dl docence dl port 4 dl avenh dl avenh dl	Red Oncore Base 3 TS RDPCore DLL TS RDPCore DLL Rdo Server OneCore Registry Configuratio Resource Manager C Remote Procedure C Morosoft Enhanced	ystem Services a Base Service in APIs Client Call Runtime Cyptographic.	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C. Windows System 32 (props) all C. Windows System 32 (props) all C. Windows System 32 vipcorets all C. Windows System 32 vipcorets all C. Windows System 32 vipcorets all C. Windows System 32 vipcorets C. Windows System 32 vipcoret all C. Windows System 32 vipcort all C. Windows System 32 vipcot 4 all System 32 vipcot 4 a	ets all mui , all		
dobase off docorets off mul docorets off mul docorets off mul docorrects and sequent off molent off molent off molent off more off more off molent off more off molent off molen	Red One core Base 3 TS RDPCore DLL TS RDPCore DLL TS RDPCore DLL Red Server OneCore Registry Configuration Resource Manager C Remote Procedure C Microsoft Enhanced Restlime Work/Queue	ystem Services In APIs Client Call Runtime Cryptographic. e DLL Innaner Client	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C. Windows System 32 ppropagati C. Windows System 32 propagati C. Windows System 32 propagati C. Windows System 32 professional C. Windows System 32 pro	ts di mui di		-
dobese di docente di docente di mui docente di mui docente data docente di soport di maneria di maneria di FTVockó di tanceli di	Red One Core Base 3 TS RDPCore DLL TS RDPCore DLL TS RDPCore DLL Red Server One Core Registry Configuration Resource Manager C Microsoft Enhanced Reatime WorkQueur Security Accounts M 15 / SSL Security 1	stem Services In APIs Clent Call Runtime Cryptographic. e DLL Ianager Clent - Provider	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C: Windows System 32: plopsing at C: Windows System 32: plopsing at C: Windows System 32: plopsing at C: Windows System 32: en-105 report C: Windows System 32: plopsing at C: Windows System 32: planeth at	ets oli mui di		-
dobese di docente di mui docente di mui docente data docente desarra di docente data modert di sente di scharre di Scollert di	Red OneCore Base 3 TS RDPCore DLL TS RDPCore DLL Red Server OneCore Registry Configuration Resource Manager C Remote Procedure C Microsoft Enhanced Restlame WorkQueue security Accounts M TLS / SSL Security 1 Session Directory Ch	stem Services In APIs Client Jall Runtime Cryptographic. e DLL Ianager Client . Provider ent Connectio.	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C: Windows System: 32: perspan at C: Windows System: 32: perspan at C: Windows System: 32: per-105 vectors C: Windows System: 32: per-105 vectors C: Windows System: 32: perspan at C: Windows System: 32: perspan at System: 32: per	ets all mui di		
dobeen di docenta di docenta di mui docenta di mui docenta di molent di porti di stato di RTIVek di stato di SSCient di docenta di	Red OneCore Base 5 TS RDPCore DLL TS RDPCore DLL TS RDPCore DLL Red Server OneCore Registly Configuration Resource Manager C Microsoft Enhanced Restime WorkQueue Security Accounts M TLS / SSL Security I Session Directory CM	stem Services in APIs Client Call Runtime Cryptographic. e DLL Ianager Client . Provider ent Connectio. JLSA Lookup .	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C. Whichew System 32 propsy all C. Whichew System 32 robusts C. Whichew System 32 robusts C. Window System 32 robusts C. Window System 32 robusts C. Window System 32 ropsy all C. Window System 32 ropsy all C. Window System 32 ropsy all C. Window System 32 rough 43 C. Window System 32 rough 41 C. Window	eto all mui di		-
bipbase al disconte al discon	Red OneGree Base 3 TS RDPCore DLL TS RDPCore DLL Red Server OneGree Registry Configuration Resource Manager C Remote Procedure C Morosoft Enhanced Reatime WorkQueur Security Accounts M TLS / SL Security A Security Accounts Morosoft Enhanced Reatine WorkQueur Security Accounts Morosoft Security A	stem Services in APIs Client Jall Runtime Cryptographic, e DLL Ianager Client . Provider ent Connectio, /LSA Lookup .	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C. Window System 32 porcys all C. Window System 32 robust a	ets oll mui di		-
biochean al doconte al mui doconte al mui doconte al mui doconte al motor al motor al motor al motor al motor al motor al school al SCOare al exclosed SCOare al exclosed SCOare al SCOare al S	Red OneGore Base 3 TS RDPCore DLL TS RDPCore DLL Redo Server OneCore Resource Manager C Resource Manager C Remote Procedure C Moroadt Enhanced Reatime WorkClacus Security Accounts M TLS / SSL Security I Session Directory Clu Session Directory Clu SetONSE DE Seturity I Windows Setup API SHCORE	stem Services In APIs Clent Call Runtime Coptographic. e DLL Ianager Clent . Provider ent Connectio. /LSA Lookup .	Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C. Whiteway System 32 percept all C. Whiteway System 32 relations and C. Whiteway System 32 relations and System 32 relations and C. Whiteway System 32 relations and System 32 relations and C. Whiteway System 32 relations and System 32 relations and C. Whiteway System 32 relations and System 32 relations and C. Whiteway System 32 relations and System 32 relations and System 32 relations and System 32 relations and System 32 relations and C. Whiteway System 32 relations and System 32 relations	eto di mui di		-
biologies al docorte al docorte docorte al docorte al d	Nacional Frippity 2) Ralo CincCore Base 3 TS RDPCore DLL TS RDPCore DLL Ralo Server OncCore Restativ Corriguetto Restative WorkDaeus Security Accounts MonoCount Security Accounts MonoCount Monocounts MonoCount MonoCount Security Accounts MonoCount Monocounts Accounts MonoCount Monocounts Accounts MonoCounts MonoCount Accounts MonoCounts MonoCounts MonoCounts Accounts MonoCounts Mono	stem Services In APIs Clent Call Runtime Cryptographic, e DLL Ianager Clent . Provider ent Connectio, /LSA Lookup .	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corpor	C. Windows System 32 process 2 C. Windows System 32 https://www.system.32 C. Windows System.32 https://www.system.32 Kindows System.32 https://wwww.system.32 Kindows System.32 https:/	to di mui di		-
bickees al control al mail control and an control and control and	Red officers Frage State Red officers Base S 1'S RDPCom DLL Red Server OneCore Resource Nanager C Resource Nanager C Remote Procedure C Morosht Erhancod Restime WorkQueue Session Directory Cli Host for SCM/SDDL Windows Stetp API SHCORE Windows Shel Core Shel Light-weight Ub	ystem Ease Services in APIs Client Client Call Rurtime Crystographic. e DLL Isnager Client . Provider ent Connectio. /LSR Lookup. mon DII lity Library	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation	C. Whiteway System 32 percept all C. Whiteway System 32 relationships C. Whiteway System 32 relationsh	ets all mui di		-
hkkese di kootta di Kootta di Kootta di Kootta di Markana Kootta di Kootta d	Woodst Froppfy 2) Rio Chicken Essel 5 15 RDPCare DLL 15 RDPCare DLL Rio Server OneCore Respace Nanager C Resource Nanager C Resource Nanager C Macoutt Enhanced Resource Nanager C Macoutt Enhanced Resource Nanager C Macoutt Enhanced Nanager C Macoutt Enhanced Nanager C Macoutt State C Security State S Security State S	ystem Rase Services In APIs Clent Call Ruture Cryptographic. D DL Isnager Clent. Provider ent Connectio. /LSA Lookup. mon DII lity Library vider Interface.	Nicrosoft Microsoft	Corporation Corpor	C:Wickow System 22 properts of C:Wickow System 22 properts of	to al mu al		-
Advance all document all multi document all documents all docu	Halo Ghecken Freperty 39 Rajo Checken Elses 1 TS RDPCare DLL TS RDPCare DLL TS RDPCare DLL Resource Nanager C Resource Nanager	ystem Page Services Page Services Page Services Page Service Page S	Nerosoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	C: Whole Spenz Departs and C: Whole Spenz Depart	ts di mu di 104eut nis 105eut nis		-
hickes al hickes al downsheed higher has a higher has	Woodski Frippety 2) Rab Chicken Ease 5 TS RDPCare DLL TS RDPCare DLL Rab Senser OneCore Registry Configuratio Resource Nanager C Morand Enhancel Morand Enhancel Reatime WorkCareus Security Accounts M Nord Care Security Accounts M Security Accounts M Hoat for SCM/SDDL Windows Shell Care Michael Security Support Pro Statel Repository Care Statel Repository Care Mark Statel Repository Care Statel Repository Care Stat	ystem a Base Services a Rase Services or APIs Clerk 2014 Rutime Crystographic. a DLL Contection Powider ent Connectio. /LSA Lookup. mon DII lity Library wider Interface a down Servicer	Nerosoft Microsoft	Corporation Corporation	C:Wickow System 22 properts of C:Wickow System 22 protocols C:Wickow System 22 protocol C:Wickow Sy	ets dl mui dl tDefeuit nis ry Core dl		-
abclass al document al document al document al document al document do	Hab Chicken Freeholds TS RDPCare DLL TS RDPCare DLL Rab Stream Chicken Base Headstream Chicken Base Restret Configuration Resource Manager Restret WorkCureus Restret WorkCureus Restret WorkCureus Restret WorkCureus Restret WorkCureus Restret WorkCureus Restret WorkCureus Restret Restre	vstem Resee Services Page Services an APIs Chert Chert Chyptographic. a DLL Chyptographic. a DLL Chyptographic. b DLL Chyptographic. a DLL Singer Clert. Provider ent Connectio. /LSA Lookup. mon DII ity Library wider Interface ent mows Services molows Services	Microsoft Microsoft	Corporation Corpor	C:Window Spenz Zapasa at C:Window Spenz Zapasa	its di mu di tCoffeut nis yy Core di 4.ee mui		-
Ackess at Accord at and Accord at and Accord at an Accord at a Accord at a Ac	Heat office and the second sec	ystem Services n APIs Clent all Runtime Crystographic. e DLL Israger Clent. Provider ent Connectio. /LSA Lookup mon DII lity Library wider Interface e ndows Servicer	Microsoft Microsoft	Corporation Corpor	C. Who was the present of the second	ets all mui all Defeuit nia ry Care all 6. ese mui		-
hkkese at hkkese at	Hab Chicken Fropper System TS RDPCare DLL TS RDPCare DLL Rab Stream Chicken Ball Resetty Configuration Resetty Configuration Resetting WorkCurrent Restime WorkCurrent Statel Reports State Hoat Procees for Wir Statel Reports Of Con- Statel Reports Of Con- Statel Reports Of Con- Hoat Procees for Wir Fusion 2.5 Remote Desides Data	ystem Services n APIs Clent AI Rurtime Crystographic, e DLL Isnager Clent - Provider ent Connector /LSA Lookup. - mon DII sity Library vvider Interface e ndows Servicer assion Host, Servicer	Microsoft Microsoft	Corporation Composition Corporation Corpor	C. Whole Spenz Departs of C. Whole Spenz Departs of C. Whole Spenz Departs of C. Whole Spenz Departs of Computing C. Whole Spenz Departs of Computing Computing Computing Computing Computing Computin	da di mu da 1Defeut ris y Core di dese mu		-
bokes al boots	Head Proceed Processors Processor	ystem Services Plase Services in APIs Clerk all Rurtime Crystographic. Povider ent Connectio. /LSA Lookup . mon DII ally Library wider Interface e ndows Servicet asson Hoto Servicet asson Hoto Servicet	Microsoft Microsoft	Corporation Corpor	C. Whole Spenz Departs and C. Whole Spenz Departs and Departs C. Whole Spenz Departs C.	ts di mui di 1Defeuit ris γ, Core di ti ese mui riti mui		-
hkkees at hkkees at hyperson	The second registry Second Sec	ystem Services Pase Services In APIs Cert Jel Ruttine Crystographic. e DLL Ionaper Clert : Provider ert Connectio. 7LSA Lookup man DII Illy Library vider Interface e hodows Servicer dows Servicer Desktop Servic.	Microsoft Microsoft	Corporation Composition Corporation Corpor	C. Whole Spenz Departs and C. Whole Spenz Departs and C. Whole Spenz Departs and C. Whole Spenz Departs and Spenz Departs C. Whole Spenz De	ts di mui di tDefeut nia ry Core di Leve mui		-
bickees at bickorth at an bickorth at an bickorth at an bickorth at a bickorth at a bickorth at a bickorth at bickorth at bick	The source of th	ystem Services In APIs Dent 21 Runtime Crystographic, et all Runtime Crystographic, et all Runtime Crystographic, et all Runtime Crystographic et all Runtime Crystographic et all Provider et Connectio, /LSA Lockup. mon DII sitty Library wider Interface endows Services notws Services sation Host Ser Desitop Services sation Host Ser Desitop Services host Services sation Host Ser Desitop Services host Services sation Host Ser Desitop Services host Services sation Host Ser Desitop Services	Microsoft Microsoft	Corporation Composition Corporation Corpor	C: Whole Spenz Departs and C: Whole Spenz Depart	to di mui di tDefaut ris y, Core di di en mi ridi mu		-
hickees at bickees at bickees at biggeld at biggeld at biggeld at biggeld at biggeld at biggeld at bickees at bickee	- active model 3: - active model 3: - active model 3: 	ystem Ease Services Pase Services Pase Services Cert 218 Runtime Cryptographic Powder ent Connectio. ULSA Lookup - ULSA Lookup - Moves Servicer Servicer Servicer Servicer Servicer Desktop Servicer Desktop Servicer	Microsoft Microsoft	Corporation Composition Corporation Corpor	C. Who down Speers 20 program of C. Who down Speers 20 progr	ts di mui di tDefeut ris y Core di di mu di mu re di		-
hkkese at hkkese at	encoder secondo 3y and a secondo 3y a	ystem Services e Base Services on APIs Cent Call Ruttine Crystorgaphic Ranger Clert. Provider ent Connectio. /LSA Lookup. mon DII lifty Ubrary wider Interface e son Host Ser Desistors Service ndows Service ndows Service ndows Service rodows Servi	Microsoft Microsoft	Corporation Corpor	C: Whole Spenz Departs of C: Whole Spenz Dep	to di mui di Dofesă ris y Core di di ese mui est mui mui		-
bokes al bokes al box al bo	entropy model by entropy model by Star (Section 2014) and Star (Section 2014) and Restarce Manager Restarce	vstem Rese Services in APIs Cert all Runtime Crystographic. e DUL Granger Clert I. Rowider en Connetion its Libraty mon DII its Libraty wider Interface e ndows Services sation Hoat Ser sation Hoat Ser sation Hoat Ser sation Hoat Ser sation Hoat Ser Services Desktop Servit IV Package le Libraty en Interna Hoat Services Desktop Servit IV Package le Libraty en Interna Hoat Services Desktop Servit IV Package	Microsoft Microsoft	Corporation Corpor	C. Whole Speer 2 periods of the second secon	to di mu di tDefaut ris y Core di di nu tinu		-

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_Ser	rvice -Fi	ilter "I	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:

The endocrastic diff C illinguity index and the IC is	- 0 X	
the contrast of the state of th		
M ++++ 昭和昭 +	i El S. A. + A. M. Y.   ▶ 🔲 🗆 From August approba. → J. 🛐 (D. L. L.	
Library function Regular function Data Library	Sored Datamal symbol 📕 Lumina function	
Zhum D. C. C.	The Name of the Na	
Function name A	rdata:00000000000000000000000000000000000	
	reata:0000000100150008 adwfapt da "OMFApt";0 ; DATA XXEF: OMFAp1:cOMFAp1(vold)+?to	
🗾 _dynamic_initializer_forModule	- refer:00000010015CCP = dig 20 refer:00000010015CCP = reset blue refer:00000010015CCP = reset blue refer:00000015CCP = reset blue refer:00000015CCP = reset blue refer:00000015CCP = reset blue refer:000000015CCP = reset blue refer:00000015CCP = reset blue refer:00000015CCP = reset blue refer:00000015CCP = reset blue refer:000000015CCP = refer:0000000000000000000000000000000000	
IIdynamic_ividalcer_forAtBaseModule_	rdata:800000130150CC SoftwareFolic: 4: : DATA XEF: evonymous remespace CreateCompressorOutputArcidIte	
1 AT	rdata:000000100156CC0 j AxcCompressor::GetSettIngs(vold)+0010	
All_dynamic_initializer_for_ARCenModule_	<ul> <li></li></ul>	
7 January Maada Jor_g_d type_	Crists: 000000012015004C alim 120	
Z webse planet material participation	, rdata (00000130115ED50 ) const WOWA abablerecording	
2 w one of the second s	- data: decenced.doi:SDISS afmablerecordrg: : : : : : : : : : : : : : : : : : :	
2 of data is detailed a second collaboration of the sec	-data:00000010015078 ; cont HCNR afmablerecorded	
7 wil details desarris initialize for a threadfahard-alliaris	relata:000000100150070 atrablereconded: j DATA X02F1ononymdnamespaceCreateCorpressorOutputArceF310	
7 anonymess namesases dynamic initializer for m timebla	reats:000000010015017070 tax 107-16LC, thatsecorecepter,0	
CINet#vatetx/indProcHVMD Setturniened int54. int	-data:00000001001505001 ; cont WOWR aBecordpath	
7 McGer/CattolCalbackV2	relata:000000100150350 aleccendpath: ; DATA X007: _enorymosi_na_posceCreateCorpressOrDutbuck14310	
CUMPDPProtocolMenager=NotifySettingsChange(_WRDS_SETT)	Creates international Control	
Alt::CCemModule:CCemModule:Void	· /data:000000010015015034 align 100	
ATL: CAtWinMedule: CAtWinMedule(void)	- rdsts:0000001201250150 #Ave428Compress db 'Are428Compressor',0 ; DATA XXEF: CRD74ve428CmcodeFigurestsEnstance+LCCTo	
	- rate: 000000010150CL #Artf44/LOBERTEROT'.0	
ATL: CAtBaseModule: CAtBaseModule(void)		
ATL: CComCritica/Section.init/void)	- U X	
RDPStackTraceLogging:RDPStackTraceLogging.Register(void)	data see Direction Typ Address	
V WppintUm	relata 1000 🔤 Up o _anonymour_namespace_CrusteCompessorCutpetAcc+81 Max_adx_s5athwareFold();? "SothwareFold();?"SothwareFold();"SothwareF	
2 napx/letOlobalObjects://dp/0/letOlobalObjects/void)	i refata z 100 🕱 Up o AvcCompresser. GetSettingsbridg-13 🛛 in alçı alçıtlıyane Polici (2, "Sativane) (Policie()) Microsoff () (iindows "	
7 WER INT CONTROL ADRW	🔹 🖂 😰 🕼 🖉 🕼 🕹 👘 🕹 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘	
7 Michael and South and South	- refacta zono 🖂 Up o Satti Olden coding Paramétron Registry z A 👘 👘 sty, a Software Wolk in: White coding Paramétron Registry z A 👘 ) + 35 to	
CErkinger Changel	ChitraphrooderCnateTunderms(vold)+10     Ina str, #SoftwarePolicle,"SoftwarePolicle, "SoftwarePolicle, "SoftwarePolicle," SoftwarePolicle, "SoftwarePolicle, "SoftwarePolicle, "SoftwarePolicle," SoftwarePolicle, "SoftwarePolicle, "SoftwarePol	
CUMEDFListenerinet.EnableTestMode(ulong)	Trates 2000     Multi Up     Offersplacoder/CestsTandoms(vold)=113     Isa sk; als/twareFold; 0; "Sthware/Policie/Utilindows"	
CUMPOPListenerRase FinalRelease(void)	<ul> <li>rdata:000 III Up o Utroden:Uncidegived)=15</li> <li>Ize sts, abothwardfolog, "Setward/Policies/Microsoft/Windows"</li> </ul>	
CRDPPooledSemple:RemoveAlBuffes(void)	narainee narainee	
CBaseStringTrushert=cinitialize(void)	• //4x2+000	
CFermatDatePacker: Initialize(void)	<ul> <li>rdata:000 Use4af7</li> </ul>	
CUMPOPListenerBase: hTerminated(veid) v	rdstarded org_slong_slong_blong_blong_blong_blong_blong_blong	
< >	Carlos Anno Anno Anno Anno Anno Anno Anno An	
Line 1 of 3639	011878C9 000000110188CC0: .ndsta:shuftwarefulloi_0 (Nywohroniaed with New Yiew-1) v	
Dataset .	D.4 ×	
18001CEAD: propagate_stkargs: function is already type 190101040; propagate_stkargs; function is already type	^	
1800C7250: propagate_stkargs: function is already type		
1000054600: propagate_stkargs: function is already type		
1000r2520: propagate_stkargs: function is already type 1000C2588: propagate stkargs: function is already type		
Function argument information has been propagated		
The initial autoanalysis has been finished.	×	
DC .		
The data Deep Deep 19678		

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>R</b> •	lease confirm	×
2	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	gin.
	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	ns.
	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.

E if by Det Det Det Det

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

👰 IDA - rdpcorets.dll C./Users/Administrator.IT-HELP/Documents//Reven	ing/rdpcontull – $\sigma$ ×
File Edit Jump Search View Debugger Options Windows	Help
😸 🖬 🔶 🔸 🐁 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓	A A A A A A A A A A A A A A A A A A A
1	
Library function 🗧 Regular function 📕 Instruction 🔢 Data 📕 Lines	and External syntox Lumin function
Z Destres D. 6 X	🕼 Tablen A 🛛 🕼 Pendesalt A 🔲 🖉 Hereina I 🕼 Structure D 🕼 From D 🖓 Structure D 🖗 From D
	1 Detective * fastcall Created/start/vec(int al. int al)
A second la factular des Data Martine Miller - La second	20
Assessing including for Markets	3
7 AT dynamic initializer for AlBoueldouble	5 DADRO CADADA // [rsp:Soh] [rhp:Doh] DVIEP
ATL_dynamic_initializer_for_AdWinModule_	6 00000 Type; // (nor+3h) (trip-Ch) 0/07 2 0775 0000 Type; // (nor+3h) (trip-Ch) 0/07 2 0775 00000 Type; // (nor+3h) (trip-Ch) 0/07 2 0/07
ATL_dynamic_initializer_forAllComModule	8 MCY Moy; // (rsy-4/h) [cbp-0h] 0%Z
dynamic_initializer_for_g_cfType_	9 char vi1[4]1 // (rop-60) [P09-60] [P09F 10 intervent of the second se
📶 wi_detals_dynamic_initialour_for_g_baader_init_initialooRes	11 001 v13; // [ray-fact] [ray-fact]
7) we_ontake_ontakes_for_g_beadw_init_initalizeRec	12 BYTE VIA[530], // [cspeck] [chp-54b] BYTE
7 will details departie initiative for a sourcestoralized	14 Proceeding of the second se
7 wil details dwarmic initiation for a threadfailureCalibacks	15 vi= 0164;
7 eronymous nemespace_dynemic initializer for_m timeSta	1 mov = 4104) 1 move = 0(41,0,0,0x2204)4)
CTNet#ystaticWindPrec(HWND'uint,unsigned_int64_int6	1a 1f ( Regterritytal)
McGenControlCallback//2	19 MRY_LOCAL_MACHINE, 19 INSTRUME_ID1101101101000000000000000000000000000
CUM#EPPretacolManager:Not#ySettingsChange[_WRD5_SETTI	21 0,
T ATC/CCOMMODUM (CCMMODUM(VOID)	22 0x0050, 23 0x0015, 15
AD + Catt Card Andrew Catt Card Andrew Catt	24 (
7 ATL-CA4BaseModule:CA4BaseModule(void)	23 closets = 4; 35 of Charter and Chart
ATL::ComCritica/Section:Init(void)	27 LOBORD(12) = *[_0000 *]0eta [= 6]
7 RDPStackTraceLogging:RDPStackTraceLogging_Register(void)	2 21 charts = 4) 22 listen and the second s
7 WppinitUm	27 LT ( Independent Control (Control (Contro) (Control (Contro) (Contro) (Contro)
Rdp/PlatEloba/Objects:Rdp/PlatEloba/Objects(void)     Rdp/PlatEloba/Objects:Rdp/PlatEloba/Objects(void)	31 douts = 4
<ul> <li>WERE BAT CONTROL ARENC</li> </ul>	as ( ) memory comparison ( may ) a comparison ( may ) accord as ( process a ) as ( process
7 McCenfuntResister	e 54 cb0ete = 520;
CRdpirpstChannelPluginFactory:InitializeInstance(void)	37 [ Henrichten (1997), Checkenster, eine, Kippe, vol., Konstal [] type (+ 1.)
CUM#DPListenerinet:EnableTextMode(slong)	• 77 v15 = 0;
CLMRDPListenerBase:FinaRelease(void)	55 v12 = 9064
CECFPooledSample:RemoveAlBuffero(void)	
7 Casesburg ( category contacts contacted with a contact of the co	41 else 42 I
CINERS internet and and a set of the set of the set	43 v15 - closts
¢ >	44 } #5 Berloadharthanh
Line 1 of 3639	as mg.usery(my)
A Cashamatan	47 ing dag
	9 50 v <sub>2</sub> = (FILE **)operator new(0x80x164);
	31 if (v5) of return duration (duration)(v5, a), a), (trust incondictions "bill, a fail)
	33 return (Output/we ")-4;
9	
ē.	
<u> </u>	OCODEKIA CEWEGONGUINE (INCODEKIA)
AUI 1010 DOWN LIFE: 10658	

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.dll.864 (répcorets.dll) C/Wsers'vAdministrator.IT-F	ELP\Decun	ns/Revening/adjocents/AU/A	0 X
File Edit Jump Search View Debugger Options Win	lovis Hel		
📶 🔂 🗰 🕶 🕶 🐴 🖓 🖓 🖓 🔬 🖾 🚇	14.03	💱 📲 🛪 🕼 🔀 🕨 💷 💷 Local Windows debugger 💌 🐮 🛃 👔 🚰 🎬	
1			
Library function Regular function Instruction Data	hexplaned	External symbol _ Lumina function	
7 briders	к 🖪	IDA New-A 🔹 🕼 Pesudocule-A 📮 🔄 Hex Ven-1 🗉 🕼 Stuckares 🖉 Erums 🖉 Sin Security 🖾 Sincer b 🕼 Erums	
Europico parte	^ 1	ILE **_fastcall anonymous_nomespace_iiCreateCompressorOutputAvc(int at, int at)	
Chronofitaami- (Drosofitaamionid)	2	for the sets of the sets	
CProx/StreamManager:CProx/StreamManager(void)	4	int v5/// edi	
CProxyStream: scalar deleting destructor (uint)	5	FILE "#v61 // rax	
CProxyStreamManagen/vector deleting destructor(uint)	2	WWWW WWWWW // Copyright Co	
CProxyStreamManager:AddStreamToRegister(CProxyStream Us	8	avre twin(a); // (rep-tin) (rep-tin) aver	
CProxyStream:CopyTo/Stream *_ULARGE_INTEGER_ULARGE_E		MXY Mayy // [rsp-dbh] [rbp-Ch] IVRF	
CProxyStream:CreateInstance(CProxyStreamManager*,ulong.)c	11	int visi // (rspsto) (rsp-Ad)	
CProxyStreamManager:CreateInstance(StreamDataAcquire *,Cl 27, CProxyStreamManager:CreateInstance(StreamDataAcquire *,Cl 2	12	BODL VAS; // (reg-ddb) [rbp-db) And	
ChronyOreamManager/CreateStream(utong.long.int/Oream **	13	BYTE VS[SAD] // (FSP-VS) (FSP-VS) (FSP-VS) BWDP VSE: / (FSP-VSH) (FSP-VSH)	
CProx/StreamManager: FreeRegisterEntry/STREAM ENTRY ')	15		
CProxyStreamManager:Initialize(void)	10	ve = storij http://elifeti	
CProxyStream:NonDelegatingQueryInterface(_GUD const &;vo)	• 15	$v_{2}^{2} = 0$	
CProxyStreamManager:OnStreamDataReceived/long.uchar *,uk	• 19	mmmark ()(11, 0, 0x22buis4);	
CProsyStream:Read(void ", ulong, ulong ")	21	HIT LOAL MARKINE,	
CProxyStreamManager:RemoveUnusedStreamsFromRegister/vo	22	L"Software\/Policies\/Microsoft\/Windows NT/\Terminal Services\/M264Encoding",	
CProxyStream:Seek_LARGE_INTEGER_ulong_ULARGE_INTEGER	25	9,00150,	
Consystement senderate contenting using using	25	8/00y) )	
CProsyStream:StatitegSTATSTG *.ulong)	• 27	dopeta = 41	
CProxyStreamManaget:Terminate(void)	• 28	if ( http://wiluston@ikey, L"tnableRecord#68", 0164, &type, Data, &choata && type == 4 )	
WPP_SF_Dol	29	1 1007TF(-5) = 70 0000 "Notes I= 0:	
CProxyDataObject:CProxyDataObject(CProxyDataObjectManag	• 31	v3 • v3	
CProsyDataObjectManager:CProsyDataObjectManager/Format	32	}	
CProsyDataObject:-CProsyDataObject(void)	• 34	<pre>if ( lisgery/alueba(hkey, L*EnableRecordRdp264", 0164, 8Type, Outa, &amp;ctOuta) 8&amp; Type == 4 )</pre>	
ChronyDetaObjectivenageri-ChronyDetaObjectManager(void)     ChronyDetaObjectVicealar delation destructor(viet)	35	f and the second se	
CProx/DataDbiectManager:/vector deleting destructor/uant)	• 37	val = -(_verses_trate = *) v5  = v54;	
CProxyDataObjectManager:AcquireUniqueId(along *)	38		
DynAmay <int, ulong="">=AddAt(ulong, int 8)</int,>	- 39 - 40	cometa = 520; 17 ( Second Marchaland Marchale, L'BecondPath", 0164, Alves, v15, Actional    Tves != 1 )	
CProsyDataObject::CopyStgMedium(tagSTGMEDIUM const *,tag	• 41	v16 = 0;	
CProxyDataOkjectManageriCreateDataObject(int)	42	else videar	
CProxyDataObject:CreateInstance(CProxyDataObjectManager*	¥ 0 44	RefLorence(New):	
	45		
Line Jo17 of Jose	46	++ ascrymcus namespace ::g_cmpics; if (1vis)   vis)	
A Graph overview	× 45	return Bids;	
· · · · · · · · · · · · · · · · · · ·	• 49 • 50	<pre>wv = (rist = _jobstator upsi(atsoutse); if (vd)</pre>	
	• 51	return OutputAvec:OutputAvec(v0, sl, s2, (struct RecordSettings *)v12, 'anonymous namespace'::g_cmpIdx);	
<b></b>	52	return (FLE **)+6	
三			
8			
8		001EBA1_shorymous_samespace_::CreateCompressorDutputEvo:10 (10001979A1)	
AU: idle Down Disk: 5108			

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:

📙 i 🛃 📕 🛛 i RdpRe	cording	- 🗆 ×					
File Home Sha	are View				~ 0		
← → × ↑ 📕 >	This PC > System (C:) > Windows > Temp :	ν δ Search Rd ρ					
	Name ^	Date modified	Туре	Size			
🖈 Quick access	rdp record 1 1920x1080 24p.ravc	2021-11-30 3:26 PM	RAVC File	0 KB			
Desktop	* rdp record 1 1920x1080 24p.rdb	2021-11-30 3:26 PM	RGB File	0 KB			
Downloads	* dp record 1 1920x1088 24p.264	2021-11-30 3:26 PM	264 File	0 KB			
Documents	# rdp_record_1_1920x1088_24p	2021-11-30 3:26 PM	Text Document	0 KB			
Pictures	# rdp_record_1_1920x1088_24p.yuv	2021-11-30 3:26 PM	YUV File	0 KB			
This DC	rdp_record_2_1920x1080_24p.ravc	2021-11-30 9:50 AM	RAVC File	1,027 KB			
ins PC	rdp_record_2_1920x1080_24p.rgb	2021-11-30 9:50 AM	RGB File	1,579,500 KB			
i Network	rdp_record_2_1920x1088_24p.264	2021-11-30 9:50 AM	264 File	1,022 KB			
	rdp_record_2_1920x1088_24p	2021-11-30 9:50 AM	Text Document	33 KB			
	rdp_record_2_1920x1088_24p.yuv	2021-11-30 9:50 AM	YUV File	596,700 KB			
	rdp_record_3_1920x1080_24p.ravc	2021-11-30 2:06 PM	RAVC File	210 KB			
	rdp_record_3_1920x1080_24p.rgb	2021-11-30 2:06 PM	RGB File	153,900 KB			
	rdp_record_3_1920x1088_24p.264	2021-11-30 2:06 PM	264 File	210 KB			
	iii rdp_record_3_1920x1088_24p	2021-11-30 2:06 PM	Text Document	4 KB			
	dp_record_3_1920x1088_24p.yuv	2021-11-30 2:06 PM	YUV File	58,140 KB			
	rdp_record_4_1920x1080_24p.ravc	2021-11-30 3:06 PM	RAVC File	13,746 KB			
	rdp_record_4_1920x1080_24p.rgb	2021-11-30 3:06 PM	RGB File	12,077,100			
	<pre>iii rdp_record_4_1920x1088_24p.264</pre>	2021-11-30 3:06 PM	264 File	13,709 KB			
	rdp_record_4_1920x1088_24p	2021-11-30 3:06 PM	Text Document	262 KB			
	rdp_record_4_1920x1088_24p.yuv	2021-11-30 3:06 PM	YUV File	4,562,460 KB			
20 items					Too and		

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:

Taryok En									
📕 1 🛛 🍒 e   Salphanaire	•				- 0 ×				
0	C > System (C) > Windows > Samp	- Adplacarding			v & SeathRL P				
# Gast acres	Carbonard & Manager Tay and	Data modified	Type .	Son					
Dealtrap /	1 Highwood, C. McGellin, Phys. Rev B Highwood, J. (1929) 1981, 24p	2021-11-20 10:14 PM	Test Document	31.42					
Dooman /	3 Http:/wcard.1.1925/1088.24p.per	2525-11-29 10-54 PM	Ville File	525,440,428	10				
K Polyman /	[] rdp.mond.2,7625/188,34p	2025-11-29 10:14 PM	Test Document	2.42					
C That PC	dipurcent,2,1625-1888,24p.per	2025 11-20 10:14 PM	VON Film	47,90148					
and the second	10 stip, woord, 3, 1025-1088, 24p.254	2025-11-28 10:54 PM	Test Document	140					and the second second
	internet, 3, 7025-1088, 34p part	2025-11-2010/14-14	Vill File	148				STREET, STREET	and the second
								A STATE OF A	and the second second
								References and	
2 Apres								Contraction of the local distance	
	Administration ProverS	NET (KA)	inci realize	model for 28 to	ASS ALPO 1828 PROSE MUS	Million and Colores 10	o A Arabit monet 1 1838-185	- 0 X	A CHARTER OF
	PS Cristinino (Temp)	Adollecordings							and the second second
									200 C 200 C 200
									and the second second
									24 A.

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?

