Table of Contents

Win7SP1x64 after a fresh start (no RDP connections to the system)

```
D:\volatility-2.5>python vol.py --profile=Win7SP1x64 -f "D:\fresh-boot.raw" rdpkeys
Volatility Foundation Volatility Framework 2.5
ERROR   : volatility.debug    : Please specify a dump directory (--dump-dir)

D:\volatility-2.5>python vol.py --profile=Win7SP1x64 -f "D:\fresh-boot.raw" rdpkeys -D D:\dump
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
RC4    1340 L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
RC4     380 L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d
ERROR   : volatility.debug    : [!] Unable to find Machine Keys in Cache Manager

D:\volatility-2.5>
```

Verbose:

```
D:\volatility-2.5>python vol.py --profile=Win7SP1x64 -f "D:\fresh-boot.raw" rdpkeys -D D:\dump -v
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
INFO    : volatility.debug    : [*] Extracting LSA Secrets...
INFO    : volatility.debug    : [+] Done.
INFO    : volatility.debug    : [*] Extracting DPAPI Master Keys...
INFO    : volatility.debug    : [*] Found a Master Key: \Device\HarddiskVolume1\Windows\System32\Microsoft\Protect\S-1-5-20\37359665-d20d-4c78-b3f5-ab
f653e9519f
INFO    : volatility.debug    : [+] Extracted from Cache Manager: 37359665-d20d-4c78-b3f5-abf653e9519f
INFO    : volatility.debug    : [*] Found a Master Key: \Device\HarddiskVolume1\Windows\System32\Microsoft\Protect\S-1-5-18\User\f22e410f-f947-4e08-8f
2a-8f65df603f8d
INFO    : volatility.debug    : [+] Extracted from Cache Manager: f22e410f-f947-4e08-8f2a-8f65df603f8d
INFO    : volatility.debug    : [*] Found an RC4 key: L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
INFO    : volatility.debug    : [+] Successful DPAPI decryption
INFO    : volatility.debug    : [+] Converted to PEM
INFO    : volatility.debug    : [+] Written to file: D:\dump\L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75.pem
RC4    1340 L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
INFO    : volatility.debug    : [*] Found an RC4 key: L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d
INFO    : volatility.debug    : [+] Successful DPAPI decryption
INFO    : volatility.debug    : [+] Converted to PEM
INFO    : volatility.debug    : [+] Written to file: D:\dump\L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d.pem
RC4     380 L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d
INFO    : volatility.debug    : [*] Extracting Machine Keys to identify the private SSL key...
ERROR   : volatility.debug    : [!] Unable to find Machine Keys in Cache Manager

D:\volatility-2.5>
```

Win7SP1x64 after an RDP connection attempt to the system

```
D:\volatility-2.5>python vol.py --profile=Win7SP1x64 -f "D:\post-connection-attempt.raw" rdpkeys -D D:\dump
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
SSL    1340 f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478

D:\volatility-2.5>
```

Verbose:

```
D:\volatility-2.5>python vol.py --profile=Win7SP1x64 -f "D:\post-connection-attempt.raw" rdpkeys -D D:\dump -v
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
INFO    : volatility.debug    : [*] Extracting LSA Secrets...
INFO    : volatility.debug    : [+] Done.
INFO    : volatility.debug    : [*] Extracting DPAPI Master Keys...
INFO    : volatility.debug    : [*] Found a Master Key: \Device\HarddiskVolume1\Windows\System32\Microsoft\Protect\S-1-5-18\bdeda075-d6ce-4993-9236-c8
1f12a83998
INFO    : volatility.debug    : [+] Extracted from Cache Manager: bdeda075-d6ce-4993-9236-c81f12a83998
INFO    : volatility.debug    : [*] Found an RC4 key: L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
WARNING : volatility.debug    : [-] Failed DPAPI decryption, none of the recovered Master Keys matched.
INFO    : volatility.debug    : [*] Found an RC4 key: L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d
WARNING : volatility.debug    : [-] Failed DPAPI decryption, none of the recovered Master Keys matched.
INFO    : volatility.debug    : [*] Extracting Machine Keys to identify the private SSL key...
INFO    : volatility.debug    : [*] Found a SSL key: \Device\HarddiskVolume1\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f686aace6942fb7f7ceb231212ee
f4a4_8062fa51-cca7-47ae-8c5b-044d913de478
INFO    : volatility.debug    : [+] Extracted from Cache Manager: f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478
INFO    : volatility.debug    : [+] Successful DPAPI decryption
INFO    : volatility.debug    : [+] Converted to PEM
INFO    : volatility.debug    : [+] Written to file: D:\dump\f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478.pem
SSL    1340 f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478
D:\volatility-2.5>
```

Win7SP1x64 after an RDP logon to the system

```
D:\volatility-2.5>python vol.py --profile=Win7SP1x64 -f "D:\post-logon.raw" rdpkeys -D D:\dump
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
RC4    1340 L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
RC4     380 L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d
SSL    1340 f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478

D:\volatility-2.5>
```

Verbose and PVK:

```
D:\volatility-2.5>python vol.py --profile=Win7SP1x64 -f "D:\post-logon.raw" rdpkeys -D D:\dump --pvk -v
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
INFO    : volatility.debug    : [*] Extracting LSA Secrets...
INFO    : volatility.debug    : [+] Done.
INFO    : volatility.debug    : [*] Extracting DPAPI Master Keys...
INFO    : volatility.debug    : [*] Found a Master Key: \Device\HarddiskVolume1\Windows\System32\Microsoft\Protect\S-1-5-18\bdeda075-d6ce-4993-9236-c8
1f12a83998
INFO    : volatility.debug    : [+] Extracted from Cache Manager: bdeda075-d6ce-4993-9236-c81f12a83998
INFO    : volatility.debug    : [*] Found a Master Key: \Device\HarddiskVolume1\Windows\System32\Microsoft\Protect\S-1-5-20\37359665-d20d-4c78-b3f5-ab
f653e9519f
INFO    : volatility.debug    : [+] Extracted from Cache Manager: 37359665-d20d-4c78-b3f5-abf653e9519f
INFO    : volatility.debug    : [*] Found a Master Key: \Device\HarddiskVolume1\Windows\System32\Microsoft\Protect\S-1-5-18\User\f22e410f-f947-4e08-8f
2a-8f65df603f8d
INFO    : volatility.debug    : [+] Extracted from Cache Manager: f22e410f-f947-4e08-8f2a-8f65df603f8d
INFO    : volatility.debug    : [*] Found an RC4 key: L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
INFO    : volatility.debug    : [+] Successful DPAPI decryption
INFO    : volatility.debug    : [+] Written to file: D:\dump\L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75.pvk
INFO    : volatility.debug    : [+] Converted to PEM
INFO    : volatility.debug    : [+] Written to file: D:\dump\L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75.pem
RC4    1340 L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
INFO    : volatility.debug    : [*] Found an RC4 key: L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d
INFO    : volatility.debug    : [+] Successful DPAPI decryption
INFO    : volatility.debug    : [+] Written to file: D:\dump\L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d.pvk
INFO    : volatility.debug    : [+] Converted to PEM
INFO    : volatility.debug    : [+] Written to file: D:\dump\L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d.pem
RC4     380 L$HYDRAENCKEY_52d1ad03-4565-44f3-8bfd-bbb0591f4b9d
INFO    : volatility.debug    : [*] Extracting Machine Keys to identify the private SSL key...
INFO    : volatility.debug    : [*] Found a SSL key: \Device\HarddiskVolume1\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f686aace6942fb7f7ceb231212ee
f4a4_8062fa51-cca7-47ae-8c5b-044d913de478
INFO    : volatility.debug    : [+] Extracted from Cache Manager: f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478
```

```
INFO    : volatility.debug    : [+] Successful DPAPI decryption
INFO    : volatility.debug    : [+] Written to file: D:\dump\f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478.pvk
INFO    : volatility.debug    : [+] Converted to PEM
INFO    : volatility.debug    : [+] Written to file: D:\dump\f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478.pem
SSL    1340 f686aace6942fb7f7ceb231212eef4a4_8062fa51-cca7-47ae-8c5b-044d913de478

D:\volatility-2.5>
```

WinXPSP3x86 after enabling RDP on the host (no connections to the system)

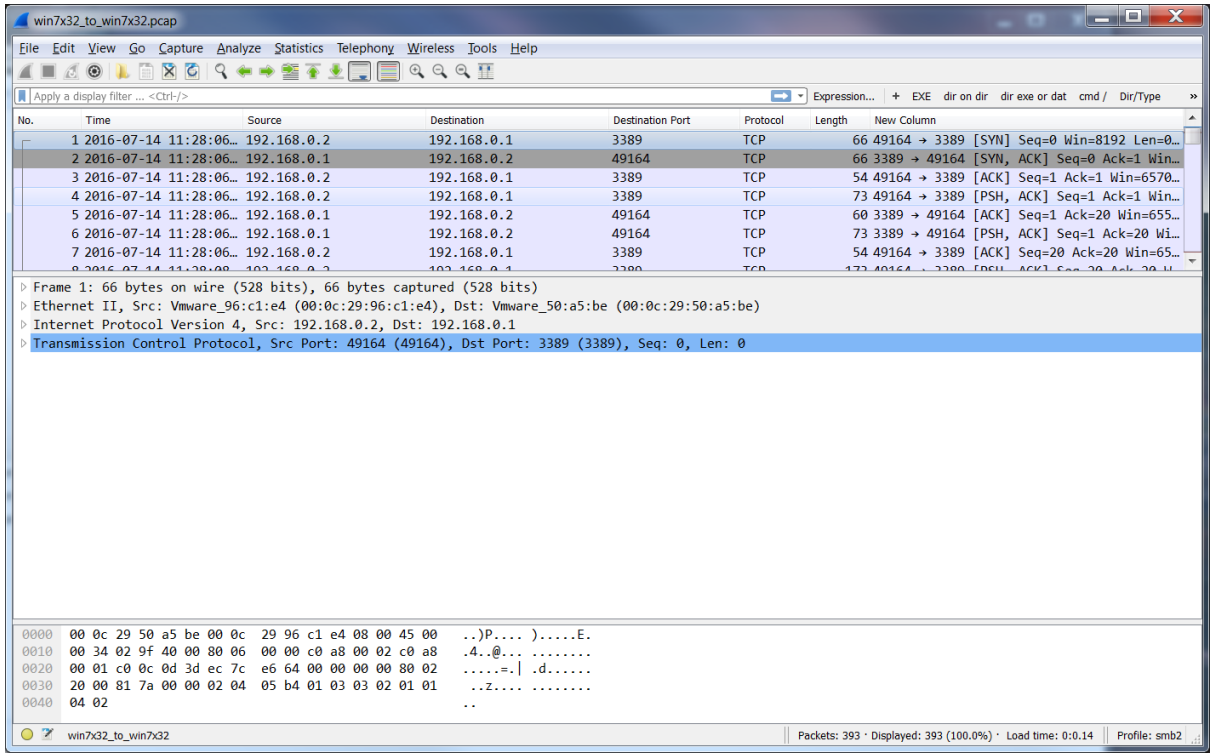
```
D:\volatility-2.5>python vol.py --profile=WinXPSP3x86 -f "D:\winxp.raw" rdpkeys -D D:\dump
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
RC4     380 L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75

D:\volatility-2.5>
```

Verbose:

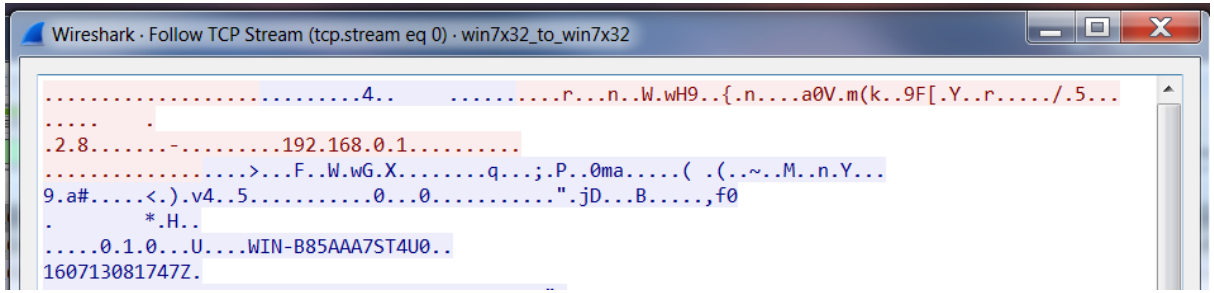
```
D:\volatility-2.5>python vol.py --profile=WinXPSP3x86 -f "D:\winxp.raw" rdpkeys -D D:\dump -v
Volatility Foundation Volatility Framework 2.5
Type Length Name
---- ------ ----
INFO    : volatility.debug    : [*] Extracting LSA Secrets...
INFO    : volatility.debug    : [+] Done.
INFO    : volatility.debug    : [+] Found an RC4 key: L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
INFO    : volatility.debug    : [+] Converted to PEM
INFO    : volatility.debug    : [+] Written to file: D:\dump\L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75.pem
RC4     380 L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75

D:\volatility-2.5>
```

Decrypting RDP session with Wireshark 2.0 on Windows

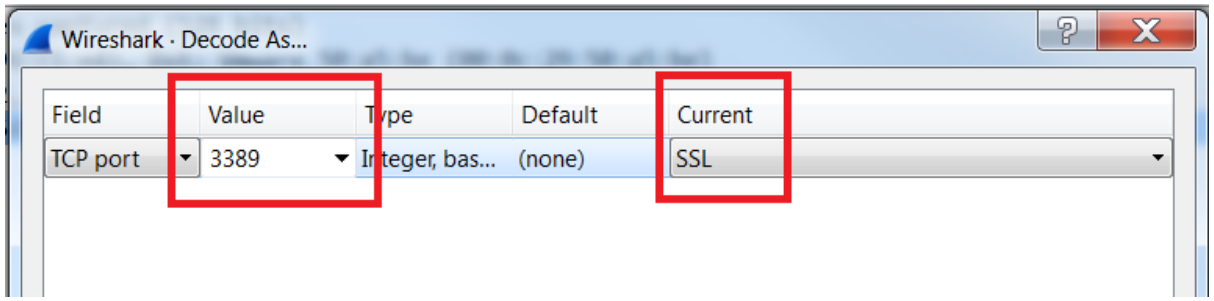
1. Open the PCAP.



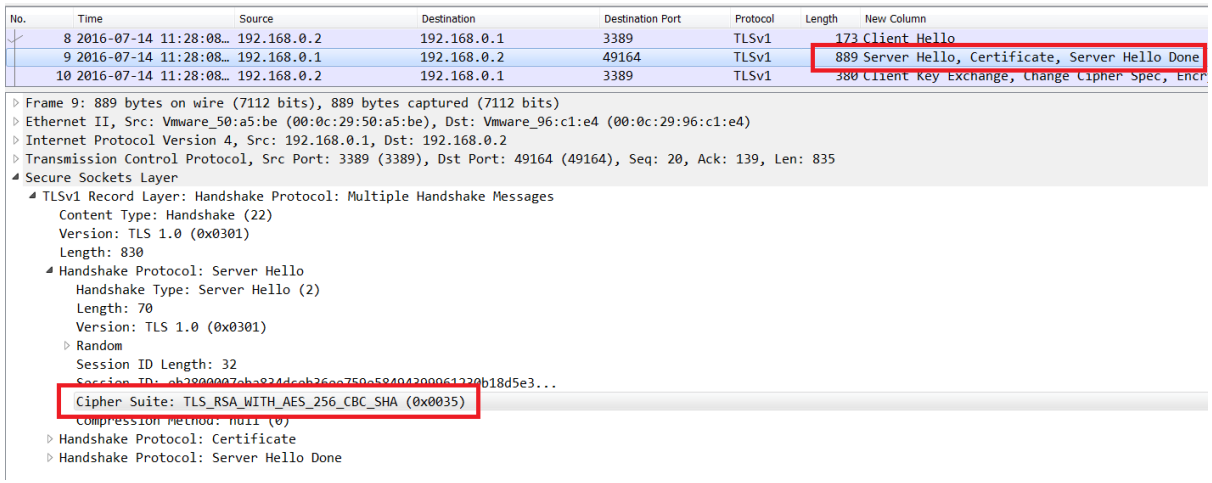
2. Follow the stream of your RDP session: right click on a packet within the RDP session, and select “Follow -> TCP Stream”.



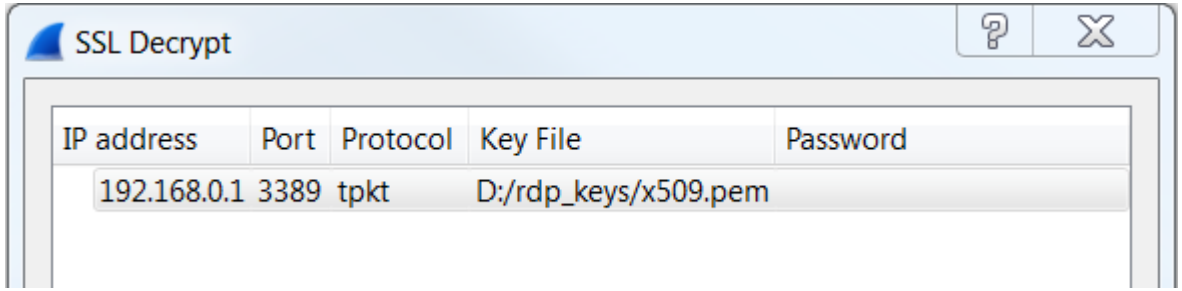
3. Close the TCP stream's window, click on a packet destined to the server ("destination port" is 3389, in this example), right click and select "Decode As…", change the value of the port to 3389 and the protocol to SSL.



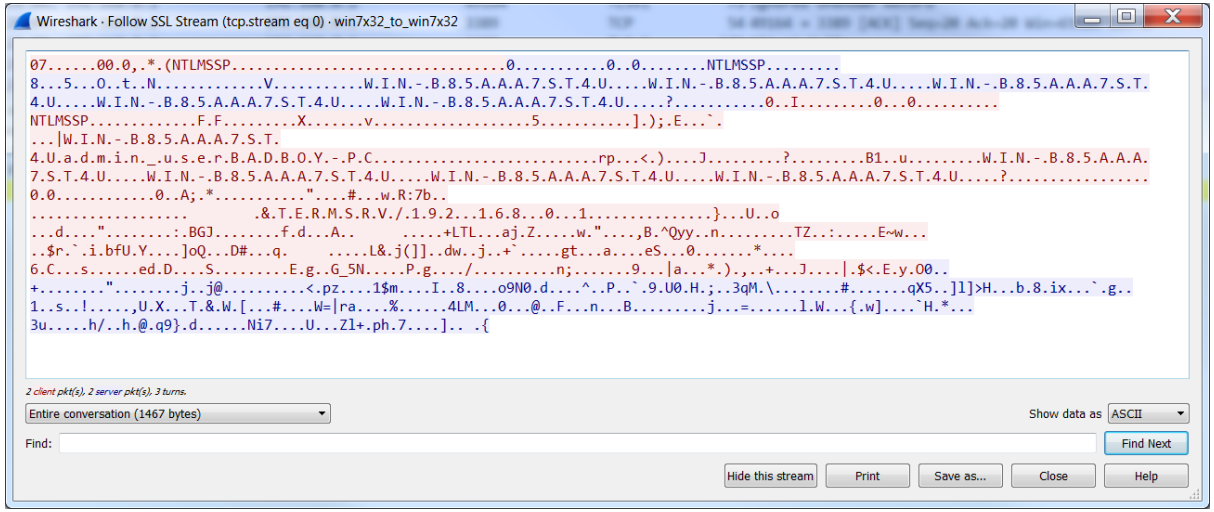
4. Select a packet that in the Protocol field says "TLSv1", right click it and choose "Protocol Preferences -> RSA keys list…".
5. Check that the RDP session you're looking at didn't use Diffie Hellman (DH) key exchange. That's because you can't decode sessions with DH key exchange.



6. Add a key with the following properties: RDP server's IP, the RDP server's port, "tpkt" (case-sensitive) and file path to the PEM file. You can leave the Password field empty.



7. Once you confirmed the key details, right click on any of the packets with the protocol field as "TLSv1" and select "Follow -> SSL Stream" and you should get decrypted RDP session.



8. That’s it, it worked. Now you’re confident you can replay the session.