macOS RDP Forensics

Jonathan Holtmann
ITP 445 - Macintosh, OSX, & iOS Forensics
University of Southern California
Los Angeles, CA, USA

CONTENTS

Abstract—**This document provides a forensic examination of the Microsoft Remote Desktop application for macOS.**

Index Terms—**rdp, forensics, macOS, remote desktop**

I. Remote Desktop Protocol

The Microsoft Remote Desktop Protocol (RDP) is used for communication between a terminal server and a terminal client [1]. The protocol only runs over TCP/IP. The protocol is used to remotely access systems running the Microsoft Windows operating system. For a more detailed and complete overview of the protocol, please refer to Microsoft's documentation [2].

II. macOS RDP Client Application

The Windows operating system ships with the built-in RDP client *mstsc.exe*. This client creates various artifacts that can be analyzed to make determinations as to when connections were initiated, as well as certain information relating to user actions while remoted into a system. While no native RDP client exists on macOS, Microsoft has developed one and made it available on the Mac App Store [3]. This client implemented the RDP protocol and can be used as a terminal client to remotely access Windows systems. Analyzing data stored on the system by this client can help in making determinations relating to a suspect's use of the application to access remote Windows systems. This macOS RDP application will be further referred to as "Microsoft Remote Desktop" or "application", not to be confused with *mstsc.exe*.

III. Available Forensic Artifacts

As a Mac App Store applications, the Microsoft Remote Desktop application is forced to run in the App Sandbox [4]. Therefore, it's configuration files and data stores can be found at the path `/Users/{Username}/Library/Containers/com.microsoft.rdc.macos`. Note that this folder will be referred to as `{base}` throughout the rest of this document.

Three major sources of artifacts are located within this folder:

1) `{base}/Data/Library/ApplicationSupport/com.microsoft.rdc.macos/com.microsoft.rdc.application-data.sqlite`
2) `{base}/Data/Library/ApplicationSupport/MicrosoftRemoteDesktop/`
3) `{base}/Data/Library/Preferences/com.microsoft.rc.macos.plist`

Throughout the rest of this document the above sources will be referred to as source1 through source3, or by their folder name. The remaining items in this section will outline various artifacts available within the above folders.

A. 1 — *com.microsoft.rdc.application-data.sqlite*

This artifact is an SQLite [5] database used to store various objects used by the application, including saved connections, gateways, and credentials. The following is an overview of the information contained within each table. As this table has a large number of columns, the detailed descriptions of all columns are available in the appendix.

1) Z_METADATA, Z_MODELCACHE, Z_PRIMARYKEY: These tables contain data relating to the SQLite database format and were not analyzed in detail by the author.

2) ZBOOKMARKENTITY: When a user adds a remote connection to the application, a corresponding entry is created in this table. The table will also contain a record of the most recently used "Quick Connect" connection initiated by the application. Note that when a new quick connection is attempted (regardless of whether or not it successfully establishes a connection), the QuickConnect row is updated and the previous data is lost.

3) ZBOOKMARKFOLDERENTITY: This table defines the bookmark folders a user can create in the application using the "Add Group" option.

TABLE I
ZBOOKMARKFOLDERENTITY - Columns

Property	Description
ZID	Unique ID (GUID) of this folder.
ZTITLE	The folder name displayed in the application.

4) ZBOOKMARKORDERENTITY: This table defines the layout of bookmarks and bookmark folders on the main application window.

TABLE II
ZBOOKMARKORDERENTITY - Columns

Property	Description
ZROOT	Binary PLIST detailing which folder each bookmark is contained in, as well as their order. The order of the folders themselves can also be determined. Note that this PLIST uses the ZID values of both bookmarks and folders instead of the SQLite Z_PK identifiers.

5) ZCONNECTIONTIMEENTITY: The author was not able to determine what purpose this table serves. None of the tests performed led to data being added to this table.

6) ZCREDENTIALENTITY: This table defines credentials stored by the user. These credentials can be used to bypass the default credential prompt that appears when a connection is attempted. A credential must have a username but must not necessarily have a password.

A credential with the ZNILPASSWORD property set to 0 will have a corresponding entry in the login keychain. The keychain is a secure credential storage service built in to macOS [6].

TABLE III
ZCREDENTIALENTITY - COLUMNS

Property	Description
ZNILPASSWORD	1 if no password is defined for this credential, 0 if a password is defined.
ZFRIENDLYNAME	The display name of the user. If not set, ZUSERNAME is used.
ZID	Unique ID (GUID) of this credential.
ZUSERNAME	Username associated with this credential

TABLE IV
ZCREDENTIALENTITY - KEYCHAIN ENTRY

Property	Description
Property	Column Property / Value
Name	ZUSERNAME
Kind	application password
Where	com.microsoft.rdc.macos
Modified	Date/Time at which the credential was created, a password was added to an existing credential, or the password for an existing credential was modified.
Expires	–

7) ZGATEWAYENTITY: This table tracks gateways configured by the user in the application's preferences window. Each entry stores the gateway's IP address as well as a friendly name and Z_PK of the associated ZCREDENTIAL, if one is configured.

8) ZGLOBALSETTINGSENTITY: This table stores various global settings for the application. Many of these settings are configurable in the "General" tab of the application preferences pane.

TABLE V
ZGLOBALSETTINGSENTITY - COLUMNS

Property	Value
ZENABLETHUMBNAIL	User defined via checkbox "Show PC thumbnails". Set to 1 if enabled, 0 otherwise. See the "Connection Thumbnails" section (III-A14) for additional details on thumbnail images.
ZENABLEWORKSPACE	Set to 1 during all tests performed by the author.
ZISDEVSETTINGSACTIVE	Set to 0 during all tests performed by the author.
ZNOTIFYUNSUPPORTEDKEYBOARDS	Set to 1 during all tests performed by the author.
ZSENDDIAGNOSTICS	Used defined via checkbox "Help improve Remote Desktop"
ZUSECOMMANDKEYFORCLIPBOARD	User defined via checkbox "Use Mac shortcuts for copy, cut, paste and select all, undo, and find". 1 if the command key should be used with these shortcuts, 0 if control key should be used instead.
ZUSENEWHEADERLAYOUT	This property cannot be directly configured via the GUI and is always set to 0. Manually setting the property to 1 and restarting the application had no affect.
ZZOOMTHUMBNAILONHOVER	This property cannot be directly configured via the GUI and is always set to 1. Manually setting the property to 0 and restarting the application had no affect.

9) ZLICENSEENTITY: The author was not able to determine what purpose this table serves. None of the tests performed led to data being added to this table.

10) ZREMOTERESOURCEENTITY: The author was not able to determine what purpose this table serves. None of the tests performed led to data being added to this table.

11) ZRESOLUTIONENTITY: This table tracks the resolution options displayed in the application menu when adding a new remote connection.

12) ZTRUSTENTITY: The author was not able to determine what purpose this table serves. None of the tests performed led to data being added to this table.

13) ZWORKSPACEENTITY: The author was not able to determine what purpose this table serves. None of the tests performed led to data being added to this table. This is due to the fact that the author did not have access to a Remote Desktop Workspace, nor the ability to create one for testing purposes.

14) Connection Thumbnails:

B. 2 — Microsoft Remote Desktop/

Two files of interest exist within this folder, both related to the application's crash reporting telemetry system. They are created even if the user opts out of telemetry services at the time of first application launch.

1) {source2}/FirstStartTime.dat: This file begins with the signature "C3 0A 00 00", followed by a GUID and a plaintext ISO 8601 [7] date in UTC. This date represents the first time the application was launched by the user on the system.

TABLE VI
FirstStartTime.dat - PROPERTIES

Offset	Length	Property
0	4	Header
4	36	GUID
40	24	ISO 8601 Date

2) {source2}/offlinestorageHigh.dat: This file stores application crash reports and telemetry data. The data is periodically transmitted via a POST request to "https://in.appcenter.ms/logs?Api-Version=1.0.0" when telemetry services are enabled [8] [9]. The file contains encoded parameters that are sent to the API. Each entry begins with the hex values "C1 0A 00 00 03 00 00 00" and ends with the hex values "D0 18 02 00". A list of all parameters identified by the author can be found here. Many of these properties are defined in the Microsoft documentation.

Properties of interest include, but are not strictly limited to the following.

Note that while a variety of other properties exist in the file, the author was not able to determine the purpose for all of them. The author confirmed that those properties with

TABLE VII
offlineStorageHigh.dat - PROPERTIES OF INTEREST

Property	Description
AppInfo.Version	Version of the application.
ClientSettings.FirstRunExperienceLaunchedVersion	Version of application when first launched
DeviceInfo.Model	The model name of the Apple computer (e.g. MacBookPro11,4).
DeviceInfo.OsVersion	The Operating System version (e.g. 10.15.6).
EventInfo.Name	
EventInfo.Time	ISO 8601 date/time the event took place.
kMSAnalyticsIsEnabledKey	
pastDevidesKey	NSKeyedArchiver encoded binary data containing list of device history.
SessionIdHistory	NSKeyedArchiver encoded binary data containing list of sessions. Each entry includes a session ID and a timestamp.
Session.FirstLaunchTime	First time the application was launched.
TelemetryPreviousSendDiagnostics	Whether or not application should send diagnostic data to Microsoft.
UserIdHistory	NSKeyedArchiver encoded binary data containing TODO.
UserInfo.TimeZone	System time zone.

clear names contain the data that their names would indicate. However, the author was not able to determine the purpose of the following properties: *S_e, S_j, S_k, S_p, S_t, S_v, r_count, r_inv, n_r_count, n_r_inv, n_r_inv*.

C. 3 — *com.microsoft.rdc.macos.plist*

This file is a binary PLIST that defines operating parameters for the application. Properties of interest include, but are not strictly limited to the following.

TABLE VIII
com.microsoft.rdc.macos.plist - PROPERTIES

Property	Description
ClientSettings.FirstRunExperienceLaunchedVersion	Version of application when first launched.
Developer.removedHomeFolderRedirection	Undetermined. True in all test scenarios.
kMSAnalyticsIsEnabledKey	
MSInstallId	Undetermined. GUID related to Microsoft App Center.
NSWindow Frame MainWindow	Defines the position and size of the main application window [10].
pastDevicesKey	NSKeyedArchiver encoded binary data containing list of devices used by application. It is likely that if the application is used across multiple systems with iCloud sync, this property would list all used devices. However, the author did not have the hardware required to test this theory.
SessionIdHistory	NSKeyedArchiver encoded binary data containing list of sessions. Each entry includes a session ID and a timestamp.
TelemetryDeviceId	Unique ID used to identify device for telemetry purposes.
TelemetryPreviousAppLaunchVersion	Version of application when last launched.
TelemetryPreviousDailyEventsTimeKey	
TelemetryPreviousSendDiagnostics	Whether or not application should send diagnostic data to Microsoft.
UserIdHistory	NSKeyedArchiver encoded binary data containing TODO.

IV. QUICK REFERENCE

A. *First Application Launch Time*

Rerefence section III-B1. The file `{source2}/offlinestorageHigh.dat` contains a ISO 8601 formatted date that represents the first time the application was launched.

B. *Saved Connections*

Reference section III-A2. The *ZBOOKMARKENTITY* table tracks all saved connections. Information available includes hostname/IP address, last connection time, credential to be used, and more. Analysis of the SQLite WAL may reveal deleted connections and past connection history.

C. *Quick Connect Usage*

Reference section III-A2. The *ZBOOKMARKENTITY* contains a row with *ZID* "QuickConnectBookmark" which tracks information related to the last quick connect system. Note that this row does not exist if no quick connection attempt has been made. Analysis of the SQLite WAL may reveal past quick connection attempts. Note that the presence of this row in the table is not on its own indicative of the connection having succeeded.

D. *Application Usage*

Reference section III-B2. The `{source2}/FirstStartTime.dat` file contains telemetry logs that may provide insight into the date/time the application was in use.

V. ACCOMPANYING PYTHON MODULE

This white paper is accompanied by a Python module named mRDPf [11]. The Python module is capable of automaticallty parsing all available data from sources 2 and 3. For source 1, the module dumps all SQLite tables once with inclusion of the WAL, and once without. For more detailed analysis of the WAL, a dedicated WAL-forensics tool should be used. See this website for complete documentation of the module as well as it's command line interface. See this GitHub repository for the source code for both the Python module and this white paper.

VI. Appendix

A. *ZBOOKMARKENTITY - Columns*

TABLE IX
ZBOOKMARKENTITY - Columns

Property	Description
ZADMINMODE	TODO
ZAUDIOCAPTUREENABLED	TODO
ZAUDIOPLAYBACKENUM	User Defined. 0 if sound should be played on host computer, 1 if sound should be played on remote computer, 2 if sound should never be played.
ZAUTORECONNECTENABLED	TODO
ZCAMERAREDIRECTIONENABLED	User Defined. True if the host camera should be redirected to the remote system.
ZCOLORDEPTH- ENUM	User Defined. Color depth to be used for the connection.
ZDYNAMICRESOLUTIONENABLED	User Defined. 1 if resolution should be adjusted dynamically to fit the window, 0 otherwise.
ZENABLERETINA	User Defined. 1 if retina support is enabled, 0 otherwise.
ZINPUTMODEENUM	TODO
ZPASTEBOARDREDIRECTIONENABLED	User Defined. 1 if clipboard should be shared, 0 otherwise.
ZPRINTERREDIRECTIONENABLED	User Defined. 1 if host printers should be redirected to remote system, 0 otherwise.
ZSCREENTYPEALLMONITORS	User Defined. 1 if all monitors connected to host should be used for connection, 0 if only one monitor should be used.
ZSCREENTYPEENUMTYPE	TODO
ZSCREENTYPEHEIGHT	User Defined. Height component of custom resolution to use, -1 if not set or using pre-defined resolution.
ZSCREENTYPERESOLUTIONTYPE	1 if a custom resolution is set, 0 if a preset resolution is selected.
ZSCREENTYPESCALE	TODO
ZSCREENTYPEWIDTH	User Defined. Width component of custom resolution to use, -1 if not set or using pre-defined resolution.
ZSMARTCARDREDIRECTIONENABLED	User Defined. 1 if smart cards connected to host should be shared with remote system, 0 otherwise.
ZSWAPMOUSEBUTTON	User Defined. 1 if left and right mouse buttons should be swapped, 0 otherwise.
ZBOOKMARKFOLDER	Z_PK of bookmark folder entity this bookmark is associated with. Folders are defined in ZBOOKMARKORDERENTITY.
ZCREDENTIAL	Z_PK of credential entity this bookmark is associated with. Credentials are defined in ZCREDENTIALENTITY.
ZGATEWAY	Z_PK of gateway entity this bookmark is associated with. Gateways are defined in ZGATEWAYENTITY.
Z_FOK_BOOKMARK- FOLDER	TODO
ZAUTHORINGTOOL	TODO
ZCREATIONSOURCEENUM	TODO
ZFRIENDLYNAME	User Defined. Display name for connection or ZHOSTNAME if not set.
ZHOSTNAME	User Defined. Hostname or IP address of the remote system.
ZID	Unique ID (GUID) assigned to bookmark or "QuickConnectBookmark" if bookmark represents a quick connect item.
ZRDPSTRING	RDP string used in .rdp files on Windows to define a connection.
ZFOLDERREDIRECTIONCOLLECTION	Binary PLIST defining what host folders, if any, should be made available to the remote system over RDP. Stores path to folder, name of folder, whether or not folder is read only, and an ID.
ZLASTCONNECTED	Binary PLIST indicating the time at which this bookmark was last used to connect to a remote system.
ZTHUMBNAILIMAGE	A GUID related to the thumbnail stored for his connection, if one exists. See the "Connection Thumbnails" section (III-A14) for more details.

References

[1] Deland-Han. Understanding remote desktop protocol (RDP) - windows server. [Online]. Available: https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

[2] openspecs office. [MS-RDPBCGR]: Remote desktop protocol: Basic connectivity and graphics remoting. [Online]. Available: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/5073f4ed-1e93-45e1-b039-6e30c385867c

[3] Microsoft remote desktop. [Online]. Available: https://apps.apple.com/us/app/microsoft-remote-desktop/id1295203466?mt=12

[4] About app sandbox. [Online]. Available: https://developer.apple.com/library/archive/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html

[5] SQLite documentation. [Online]. Available: https://sqlite.org/docs.html

[6] What is keychain access on mac? [Online]. Available: https://support.apple.com/guide/keychain-access/what-is-keychain-access-kyca1083/mac

[7] ISO - ISO 8601 — date and time format. [Online]. Available: https://www.iso.org/iso-8601-date-and-time-format.html

[8] K. of Spades. Upload crashes via API - visual studio app center. [Online]. Available: https://docs.microsoft.com/en-us/appcenter/diagnostics/upload-crashes

[9] ——. App center crashes for macOS - visual studio app center. [Online]. Available: https://docs.microsoft.com/en-us/appcenter/sdk/crashes/macos

[10] frame | apple developer documentation. [Online]. Available: https://developer.apple.com/documentation/appkit/nswindow/1419697-frame

[11] jholtmann/mrdpf. [Online]. Available: https://github.com/jholtmann/mrdpf