Acquisition of the Microsoft Surface™ RT



Author:	Darren Freestone
	Lock and Code Pty Ltd
	darren@lockandcode.com
Date:	7 April 2013
Revision	1.01

Contents

Acquisition of the Microsoft Surface™ RT1
Step-by-Step Acquisition Instructions3
Step 1 – Requirements
Step 2 – Prepare Target Device
Adjust Power Settings3
Determine Storage Capacity4
Step 3 – Select Destination Media5
Step 4 – Forensic Software5
Acquisition Tools for ARM5
Soft Jail-Breaking the Device5
Step 5 – Prepare Destination Media6
Step 6 – Acquisition & Verification7
Jail Break7
Acquire Physical Drive and/or Logical Volume8
Step 7 –Bit-Locker Recovery Key10
Step 8 – Final Step10

Step-by-Step Acquisition Instructions

Step 1 - Requirements

In order to attempt the acquisition of a Microsoft Surface Windows RT device ("Surface RT") the specialist will first require user access to the device. If the device is pass-code locked and the pass-code is unknown then the specialist cannot proceed with the following approach.

If the device does not come with a keyboard dock/cover then the same result can be achieved with a USB hub, USB keyboard and USB mouse. The remainder of these instructions will assume the device has keyboard and mouse support.

To ensure there are as few unwanted interruptions as possible during the acquisition, connect the Surface RT to an AC outlet using the Surface RT power adapter.



Step 2 – Prepare Target Device

Figure 2 - Desktop Screen

The "Modern" screen is usually the first to confront the user. It is easier to prepare the target device from the traditional desktop screen. To show the desktop screen, click the "desktop" window of the "Modern" screen.

Adjust Power Settings

After many false starts, it became apparent that the Surface RT likes to go to sleep and the act of doing so will interfere with the acquisition progress. Access the power configuration page and make a note of the existing power settings. Set the **Put the computer to sleep** when **Plugged in** to **Never** as shown.

a	Edit Plan Settin	gs	- 🗆 🗙	
🔄 🄄 👻 🕈 🗃 « Power Opti	ons → Edit Plan Settings	× ٢	Search Co 🔎	
Change settings for the plan: Balanced Choose the sleep and display settings that you want your computer to use.				
Oim the display:	1 minute v	1 minute v		
Put the computer to sleep:	2 minutes 🗸 🗸	Never 🗸		
🔆 Adjust plan brightness:	•	•		
			¥	

Figure 3 - Power Plan Settings (Control Panel)

Determine Storage Capacity

The easiest way to determine the size of the internal storage of the device is to look under the foldout stand on the rear of the device. The capacity (eg. 32GB) will be clearly displayed. An alternate way is to open up a command prompt and issue the following command:

wmic diskdrive where index=0 list brief

Make a note of the storage capacity of the device for later reference.

Step 3 - Select Destination Media

The specialist should be careful to select an appropriate destination media. It should be greater in size than the target media and double the size if possible. An appropriately sized USB flash drive is ideal due to the lack of current on the device's USB port. If a suitably sized USB flash drive is not available then a USB Hard Disk Drive (HDD) can be used in some circumstances. A USB HDD which can be powered by AC is the next best choice.

In testing with USB devices other than the above the results were less than favourable with the USB disk disappearing/reappearing often.

Step 4 – Forensic Software

One of the challenges of working with the Surface RT is the inability to run standard x86 (32-bit) Windows programs on the device. In order to execute programs on the device they need to be :

- 1. Compiled for the ARM processor
- 2. Digitally signed by Microsoft

Acquisition Tools for ARM

To help facility acquisitions of Surface RT devices, Lock and Code Pty Ltd has released a few basic acquisition tools for Windows with binaries that will run on x86, x64 and ARM processors. There are also batch files to fully automate the acquisition progress. These tools are available from:

lockandcode.com

Soft Jail-Breaking the Device

Unfortunately the aforementioned acquisition tools are not digitally signed by Microsoft. In order to execute these tools, the Surface RT device needs to be "Jail-Broken". This jail break adjusts the point in kernel memory which governs the requirement for programs to be digitally signed, allowing non-Microsoft code to be executed. The jail-break is available from:

http://forum.xda-developers.com/showthread.php?t=2092158

Step 5 – Prepare Destination Media

The following can be performed on any computer and do not need to be performed on the Surface RT device itself.

Format your media and give it an appropriate volume name so that it can be clearly identified when used with the target device. Any Windows file system eg. NTFS, FAT, exFAT is work fine.

Download the Jail-Break and unzip the archive. Copy the **RT_Jailbreak-1.20** folder into the root directory of your USB destination media.

Download the Acquisition Tools and unzip the archive. Copy the **acquisition_tools** folder into the root directory of your USB destination media.

Open the **acquisition_tools** folder and locate the three batch files. As the names suggest, one is for acquisition of the PhysicalDriveO and another is for the acquisition of the C drive. If space permits on your destination media then performing both acquisitions is recommended. If not, there are two choices.

- 1. Acquire the physical drive and capture the bit-locker recovery keys.
- 2. Acquire the logical drive C only. Other volumes such as the recovery volume and EFI volume will be missed. The bit-locker keys are not required for this option.

The final batch file will capture the system's metadata into a log file.

Next, edit the acquisition batch file/s you wish to run on the Surface RT. Inside you will see variables being "set" with default values such as "Case Number". Modify the fields as appropriate and save the changes. If no changes are made the acquisition will still operate correctly, however the resulting image file will not contain the case specific metadata.

The destination media is now ready to be used in an acquisition of a Surface RT device.

🛶 l ⊋ 🕕 = l	Drive Tools	BLADE (D:)	- 🗆 🗙	
File Home SI	are View Manage		~ ()	
J Music	↑ □ Name	Date modified	Туре	
Pictures	acquisition_tools	7/04/2013 8:48 AM	File folder	
Videos	📗 RT_Jailbreak-1.20	7/04/2013 1:37 PM	File folder	
P Computer Windows (C:) BLADE (D:)				
👊 Network				
2 items	V C			



Step 6 - Acquisition & Verification

Insert the USB media into the USB port of the Surface RT device.



Figure 4 - Side Profile of Surface RT showing USB Port

Jail Break

Locate the USB media using Windows Explorer. Explorer may open automatically. Open the **RT_Jailbreak-1.20** folder.



Figure 5 - Jail Break Folder



Execute the **runExploit.bat** file. Select the first option and jail break for this session only.

Figure 2 - Jail Break Menu

Follow the remaining instructions and the result will be a soft jail-broken device. Note: the device needs to be connected to the Internet in order for the Jail Break to complete successfully.

Acquire Physical Drive and/or Logical Volume

Next, navigate back and into the **acquisition_tools** folder. Locate the batch file you wish to execute. **Right-click -> Run as Administrator**.



Figure 6 - Acquisition Tools

 C:\windows\System32\cmd.exe

 ×

 Device:
 \.\\C: Capacity: 26.780.631.040 (24.94 GB) Progress: 387.50 MB of 24.94 GB (8.42 MB per second)
 ^

A few seconds after the batch files executes you will see a progress indicator which refreshes often.

Figure 7 – Logical Acquisition of Device "//./C:" (Drive C)

Once the acquisition is complete, it will automatically launch a verification process on the image. If time permits, allow this process to finish. The result will be matching MD5 hash values.

If required, execute the second batch file.

The resulting forensic images will be stored in the root directory of the USB media and will be named appropriately as per the settings in the batch files. Each forensic image is broken into multiple E01 image files which can be opened with all popular Forensic Software Suites.

It's recommended to also run the **capture_system_information_runme_as_administrator.bat** file. On some systems, administration mode is required. It takes only a few moments to run and will capture system related metadata into a log file.

Wir	ndowsSystemInformation.txt - Notepad – 🗖	×
File Edit Format View Help		
		~
System Information		
Host Name:	SURFACE_TEST	
OS Name:	Microsoft Windows RT	
OS Version:	6.2.9200 N/A Build 9200	
OS Manufacturer:	Microsoft Corporation	
OS Configuration:	Standalone Workstation	
OS Build Type:	Multiprocessor Free	
Registered Owner:	Arm_port	
Registered Organization:		
Product ID:	00186-50018-09082-AAOEM	
Original Install Date:	18/03/2013, 9:52:02 AM	
System Boot Time:	31/03/2013, 12:25:10 AM	
		~
<		>



Step 7 –Bit-Locker Recovery Key

If due to time or space limitations, the PhysicalDrive0 was the only option chosen then the bit-locker recovery key for the C drive needs to be captured before the process is complete. Open the **Control Panel -> BitLocker Drive Encryption -> Backup Recovery Key** and save the resulting recovery key to the root directory of the USB media.



Figure 9 - BitLocker Drive Encryption (Control Panel)

Step 8 – Final Step

Before completing work with the Surface RT device, remember to revisit the power settings page and change the power settings back as per the recorded notes.