**一、情景概况**

前几日在某部委客户处协助办案，碰到了一个微软的Surface RT平板，案件要求对该设备做硬盘镜像（已掌握系统密码）。几经周折后，最终把该设备的硬盘镜像完整固定了下来。因感觉该设备较少碰到，并且一般没有现成的镜像工具，所以在这里略去与案件相关的敏感信息不表，把当时证据固定的大致情况做一个分享。

Surface RT也叫Surface，是微软2012年下半年推出的第一代平板设备，ARM架构，Windows RT操作系统。

Windows RT是微软在Windows 8的基础上，专门为ARM架构开发的操作系统，也叫Windows on ARM或WOA。其功能与Windows 8基本是一样的，只是微软故意设置了障碍让Windows RT不能兼容桌面应用。打个比方，Windows RT就像是Windows 8的妆后版，两者骨子里是相同的，只是微软使用代码完整性检查机制（Code Integrity Mechanism）人为地将这两个平台区分开来。

**二、难点解析**

这样一来，Windows RT就无法兼容x86/x64软件，也就是Windows RT环境下无法运行以往在PC上使用的一些软件，无法运行传统Windows应用程序。说直白一点就是：原来可以用的取证程序、镜像工具在Windows RT系统上统统都无法运行了。

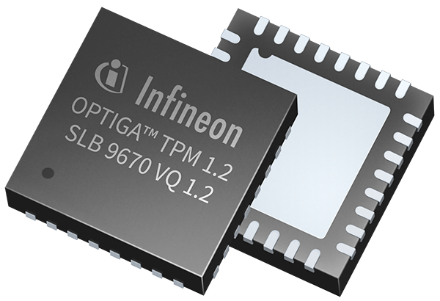
那么，能否通过取证引导盘引导Surface RT制作镜像呢？由于Surface RT默认启用了SecureBoot，所以没有经过电子签名的取证引导盘无法引导Surface RT。虽然可以通过禁用SecureBoot来实现引导，但因为Surface系列设备都默认开启了BitLocker加密，一旦禁用SecureBoot，系统引导过程中会要求输入BitLocker恢复密钥，所以这个方法行不通。

或许有人问：是否可以把硬盘拆下来直接作镜像？这条路也是不通的，Surface RT的存储部分以芯片形式焊接在主板上。下图橙色方框内的芯片即是用作存储的三星NAND芯片：



而且，即使能通过拆芯片的方式完成存储芯片镜像，最后在镜像解析环节依然会碰壁。原因如下：

首先，Surface全系列设备都内置了TPM安全芯片，用来保护设备、系统安全。



TPM全称Trusted Platform Module，即可信平台模块，TPM芯片是指符合TPM（可信赖平台模块）标准的安全芯片，它能有效地保护PC、防止非法用户访问。Surface RT采用的是英飞凌的OPTIGA™ TPM芯片。

其次，Surface设备默认启用设备加密（Device Encryption）来保护设备数据的安全，无需用户再额外设置即对系统分区进行加密。该功能使用了基于TPM安全芯片的BitLocker加密技术，从而有效防止了对系统密码的各种破解及密码绕过。

综上，难点有三：

1、Windows RT系统上无法运行常用的取证工具；

2、很难找到可引导Surface RT的取证用启动盘；

3、Surface RT默认启用基于TPM芯片的BitLocker加密，无法制作可解析的全盘镜像。

**三、操作步骤**

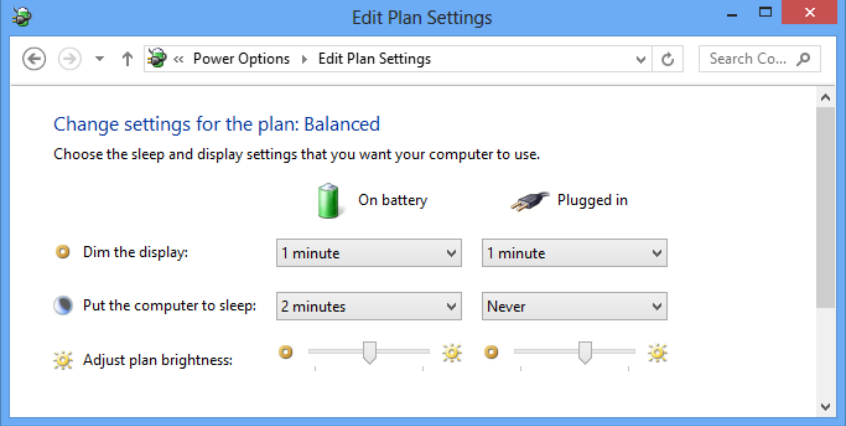
最终，在参考了国内外相关资料后制作镜像成功，在此表示感谢！操作步骤如下：

1. Surface RT只有一个USB2.0接口，为了方便操作，通过USB Hub连接了鼠标；





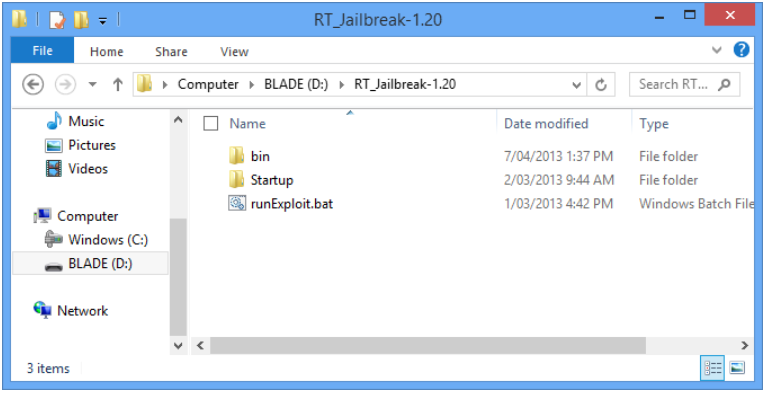
1. 修改电源项设置，以防在制作镜像的过程中嫌疑机进入睡眠模式；

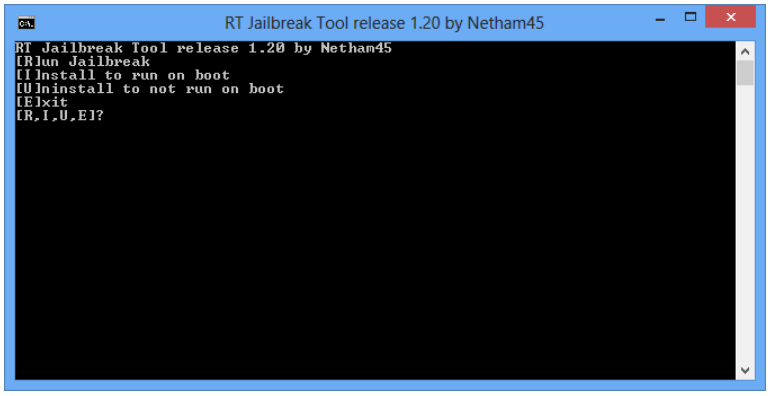


1. 把包含越狱、获取工具的大容量U盘接入Surface RT设备，并以管理员身份运行“runExploit.bat”文件；

越狱工具下载链接：

<https://dl.xda-developers.com/1/7/7/1/9/5/1/RT_Jailbreak-1.20.zip?key=9gvJShbv7M3GBeX6-x2OeQ&ts=1537887015>

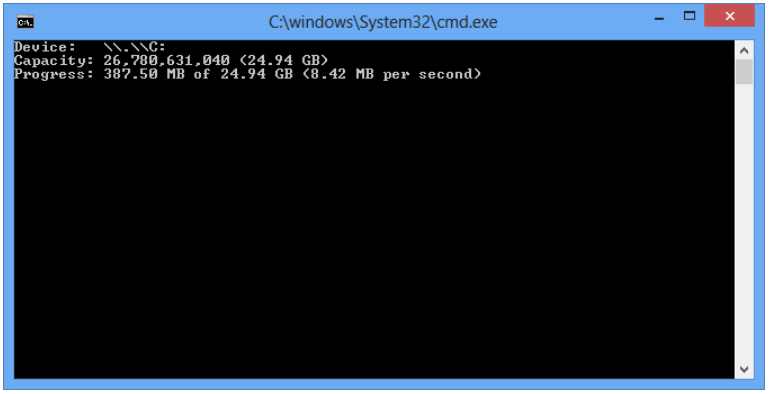
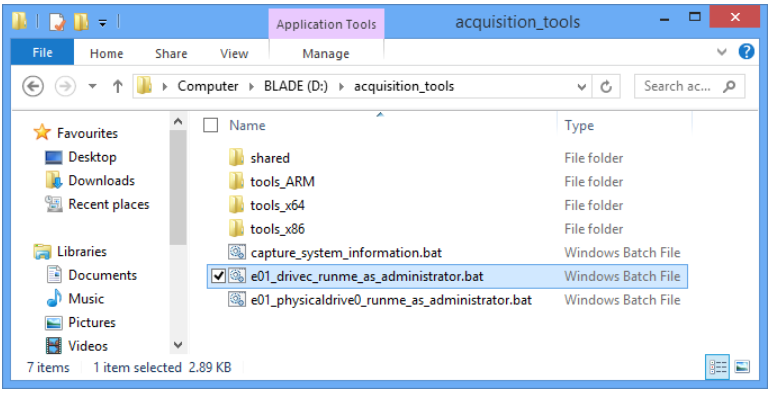




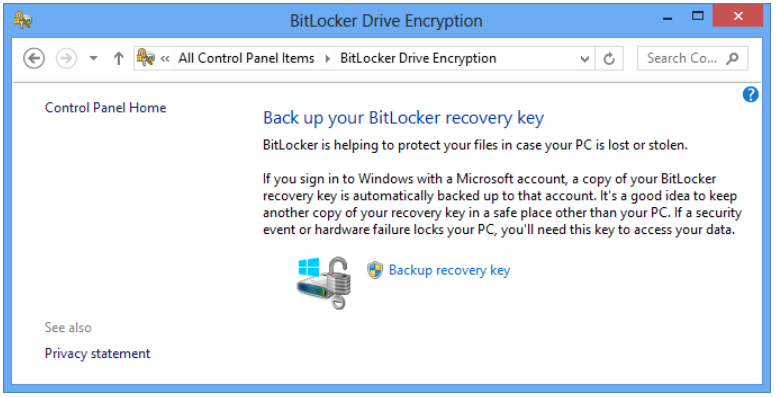
1. 以管理员身份运行运行“e01\_drivec\_runme\_as\_administrator.bat”文件制作C盘的分区镜像（Surface RT除引导和备份分区外只有C盘），镜像完成后，进行MD5哈希校验；

获取工具下载链接：

<http://lockandcode.com/download/acquisition_tools/win32/acquisition_tools.zip>



1. 以管理员身份运行运行“e01\_physicaldrive0\_runme\_as\_administrator.bat”文件制作全盘镜像，并备份BitLocker恢复密钥到外置U盘中以备解密BitLocker加密磁盘；



网络上有资料说基于TPM芯片的BitLocker磁盘加密镜像借助恢复密钥无法解密，笔者实际测试Surface Pro 1796的结果是可以的。这里要注意的是：需要先确认能否备份到BitLocker密钥，如果不显示密钥备份项的话可以通过设置更改。

基于ARM架构的Windows RT系统现在比较少见了，但除了微软的Surface RT外也还有一些，像华硕的VivoTab RT、戴尔的XPS 10、联想的Idea-Pad Yoga 11、三星的ATIV Tab等等，希望读者在碰到这些偏门的设备时这篇小文能起到一个参考的作用。

本文属于事后总结，因此借用了网络资料的部分英文截图，各部分可对照中文版Windows RT进行参考。