1-1-2014

Windows surface RT tablet forensics

Asif Iqbal
Zayed University

Hanan Al Obaidli
Zayed University

Andrew Marrington
Zayed University

Andy Jones
Edith Cowan University

Recommended Citation

Iqbal, Asif; Al Obaidli, Hanan; Marrington, Andrew; and Jones, Andy, "Windows surface RT tablet forensics" (2014). *All Works*. 4004.
https://zuscholars.zu.ac.ae/works/4004

Digital Investigation 11 (2014) S87–S93

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Windows Surface RT tablet forensics

Asif Iqbal [a,b,*], Hanan Al Obaidli [a], Andrew Marrington [b,*], Andy Jones [c,d]

[a] Athena Labs, Dubai, UAE
[b] Zayed University, Dubai, UAE
[c] Edith Cowan University, Australia
[d] University of South Australia, Australia

Keywords:
Windows RT
Tablet
Surface
Small scale digital device forensics
Acquisition

ABSTRACT

Small scale digital device forensics is particularly critical as a result of the mobility of these devices, leading to closer proximity to crimes as they occur when compared to computers. The Windows Surface tablet is one such device, combining tablet mobility with familiar Microsoft Windows productivity tools. This research considers the acquisition and forensic analysis of the Windows Surface RT tablet. We discuss the artifacts of both the Windows RT operating system and third-party applications. The contribution of this research is to provide a road map for the digital forensic examination of Windows Surface RT tablets.

Introduction

The proliferation of smartphones and tablet computers has significant implications for digital investigations. As the usage of mobile devices continues to expand, so will the proportion of digital evidence retrieved from these devices as compared to computer hard disks. According to Marturana et al. (2011) and the National Institute of Standards and Technology (NIST) (2001) it is more likely that law enforcement will encounter a suspect with a mobile device in his/her possession than a PC or laptop. Hence studying these devices from a forensic perspective is an essential task for both researchers and practitioners in digital forensics. Casey (2013) discussed smartphone forensic R&D and training, and indicated that the variety of hardware and operating systems in smartphones makes the forensic acquisition and analysis of these devices significantly different from the computers with which most forensic practitioners are familiar. This equally applies to tablets and other small scale devices, which are equally heterogeneous as their smartphone cousins. The variety of file systems, data structures and the number of third party applications available on some of these devices makes the realm of digital forensic research a significantly more complicated environment. This complication is highlighted by the diversity of research done on different devices as well as the changes in the operating systems or hardware of previously studied devices.

This research addresses Windows RT tablets, such as the Surface RT, from a digital forensic acquisition and analysis perspective. Windows RT is a variant of the Windows 8 operating system designed for mobile devices that utilize the ARM architecture. It is optimized for thin and light PCs that have extended battery life. It is only available pre-installed on selected tablets and PCs such as the ASUS VivoTab RT, Dell XPS 10, Lenovo IdeaPad Yoga 11, Samsung ATIV Tab, and Surface RT. Windows RT only runs built-in apps or apps that are downloaded from the Windows Store, while other apps such as Adobe Photoshop, and legacy programs that run on the regular Windows operating system cannot run on it. However, Windows RT still has a limited desktop mode where the user can use redesigned office applications such as Word, Excel and PowerPoint as well as exploring and arranging folders in a manner similar to the regular desktop mode.

[*] Corresponding authors. Zayed University, Dubai, UAE.
E-mail addresses: asif@babariqbal.com (A. Iqbal), andrew.marrington@zu.ac.ae (A. Marrington).

http://dx.doi.org/10.1016/j.diin.2014.03.011

This paper identifies a forensically sound acquisition method for a Windows RT device, and describes the file system structure and potential forensic artifacts. It is organized as follows: in the next section, we discuss related research in small scale digital device forensics, and then in the Methodology section we discuss our general methodology. Followed by the Acquisition section which describes Windows RT acquisition, then in the Analysis section we discuss analysis of acquired Windows RT images. This paper concludes with a synopsis of findings and planned future work in this area.

Related work

The field of small scale device forensics has challenged researchers because the diversity of hardware and operating systems of these devices requires different methods of forensic acquisition and analysis. According to Casey (2013) this is shown in "The effects of switching the camera module from Blackberry Curve 9360 devices" by Gisolf et al., which deals with the changes in the hardware of Blackberry Curve 9360 devices. As well with the work of Quick & Choo who investigated the artifacts left by Dropbox on a Windows 7 computer and an Apple iPhone 3G hence study the effect of a third party application and its relation to the cloud (Casey, 2013 Gisolf et al., 2013, Quick and Choo, 2013).

As a new tablet operating system, Windows RT has gained the interest of a number of researchers. According to reports, a hacker named C.L. Rokr (clrokr) has found a way to bypass the code integrity checking in Windows RT which allows users to run unsigned code on Surface tablets and other devices, effectively jailbreaking the platform (Windows RT jailbroken, 2013). This approach could also be utilized for forensic acquisition of these devices. The method is possible because most of the Windows RT code has been ported directly from Windows 8. This porting included a byte in the kernel that sets the minimum signing level for code execution. On Windows 8, this is set to 0 so that any code can be run, but on Windows RT, it is set to 8, meaning that code must be signed by Microsoft in order to run. Lock and Code Pty Ltd have developed software that will jailbreak the Windows RT device using the method described by clrokr, then use a set of acquisition tools to acquire an image of the device (Freestone, 2013).

As mentioned above Windows RT has some similarities with Windows 8 and as a result, we looked at some of the work done with regard to this operating system. Amanda Thomson studied forensic artifacts left on Windows 8 Consumer Preview 32-bit Edition in order to create a guide book for forensic examiners (Thomson, 2012). Using FTK Imager v3.0.1 Thomson imaged the VM where Windows 8 is installed and then utilized EnCase Forensic v6.17 for examination and analysis. The artifacts described by Thomson included information about Apps that are displayed on the Metro interface, as well as web cache and cookies specific to Metro Apps. Around the same time, Ethan Fleisher investigated the effect of Reset and Refresh function in Windows 8 (Fleisher, 2012). This feature allows a user to choose whether or not to reinstall the OS, quickly reset their entire computer, or thoroughly reset their entire computer. Hence, the reset operation may cause the machine to be wiped of all data and for that reason it is important for digital forensic researchers to investigate the artifacts left after utilizing this feature. Fleisher was able to find artifacts indicating that this feature was utilized as well as other artifacts about the reset or refreshed system.

Kaart, Klaver and van Baar stated that Windows 8, which is developed to run on mobile devices, such as tablets and phones, as well as on traditional devices such as laptops and desktop computers, might still have some of the files from the Windows Phone 7 operating system (Kaart et al., 2013). In their work they reverse-engineered significant parts of the EDB (Microsoft Embedded Database) volume format and extensively analyzed the pim.vol file that contains information related to contacts, appointments, call history, speed-dial settings and tasks. They also implemented a parser for the EDB volume format structure and compared their results to the traditional approach using an emulator and the API provided by the Windows CE operating system. The parser was able to recover additional databases, additional properties per record and unallocated records. Schaefer, Höfken and Schuba discussed the acquisition and analysis of a Windows Phone 7 device (Schaefer et al., 2012). Their work explains the main characteristics of the platform, the problems that forensic investigators face, methods to circumvent those problems and a set of tools to get data from the phone. Data that can be acquired from the phone include the file system, the registry and active tasks. Based on the file system, further information such as SMSs, Emails and Facebook data can be extracted (Schaefer et al., 2012).

From this initial search we identified that there is not sufficient scientific work that discusses Windows RT tablets from a digital forensic perspective. The main aim of our work will be to investigate the artifacts left on the device as well as acquiring an image of it.

Methodology

The main purpose of this research is to forensically investigate the Surface RT tablet which runs the Windows RT operating system. This tablet may contain valuable forensic artifacts, as it combines the traditional tablet application environment with common office productivity applications such as Word, PowerPoint and Excel. Alongside this is the use of the traditional Windows Explorer (File Explorer) available in the regular Windows Operating System. These desktop-style features in conjunction with the mobility and the availability of a full size USB port and MicroSD card, mean that this device may contain a wealth of forensic artifacts.

As the main purpose of this research is to forensically investigate the device, ensuring the integrity of the gathered artifacts is an essential requirement. This requirement is important not only in the case of a forensic investigation but also for forensic researchers to validate the acquisition that has been undertaken and the analysis of the acquired image. For that reason the test and examination procedure was derived from the Computer Forensics Tool Testing program guidelines established by the National Institute of Standards and Technology (NIST) (2001).

Table 1
Information used for the creation of the account.

Input	Value
First Name	John
Last Name	Doe
Email Address	m80003052@zu.ac.ae
Password	Testing1

This section of the paper will discuss the test environment for this research as well as the requirements to create such an environment and perform the test. Along with that, a discussion of the preformed scenario will be detailed which will assist in determining the expected artifacts that could be found on the device.

Test environment and requirements

As stated in the NIST guidelines, all the tools and devices used to create the test environment should be listed. Detailed below is a list of devices and analysis tools used in this investigation:

- Microsoft Surface RT device (32 GB)
- Custom data acquisition tool (compiled for Windows RT on ARM platform)
- Ophcrack (Version 3.6.0)
- Cafae
- Vim Text Editor (Version 7.4a.001)
- Yaru (Version 1.25)
- Mitec Structured Storage Viewer (Version 3.3.1)
- IrfanView (Version 4.36)

Prior to conducting the experiment a lab computer was set up to run all the analysis tools listed above. All system applications running on the Surface RT device were updated after the user account setup. The configuration was not modified during the setup of the device.

Test procedure

The test procedure consisted of three stages which were creating a fictional scenario, acquiring an image of the device and finally analyzing that image.

Scenario

This stage involves conducting common user activity such as browsing the Internet, using the camera and uploading images to SkyDrive.

A fictional scenario was developed for the purpose of conducting the investigation. A Microsoft account was created using fictional information. This account was created because installing applications, using SkyDrive features and sync features require a Microsoft Account. Table 1 contains the information used for creation of the account.

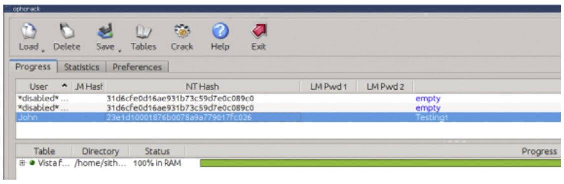
After the creation of the account, we performed a number of “normal” activities on the tablet. Selecting activities which we supposed were typical for the device based on the available applications, we simulated user activity on the device. Table 2 shows the simulated user activity on the device.

Acquisition

This stage involved the acquisition of an image of the device using a custom data acquisition tool that was compiled for Windows RT on the ARM platform. A base image was acquired after the creation of user account and this was analyzed for system related artifacts. Our acquisition technique is discussed in section four, below. After each activity a new image was acquired from the device

Table 2
Activities that were carried out on the device

Application	Activity
Internet Explorer (Immersive)	• Internet Explorer (Immersive) • Navigated to link “About ZU” (http://www.zu.ac.ae/main/en/explore_zu/index.aspx) • Opened a new tab and navigated to slashdot.org • Favorite the page slashdot.org
Internet Explorer (Desktop)	• Browsed to google.com • Browsed to microsoft.com • Add microsoft.com to favorites
Camera	• Took 2 different photos and a video clip. • Uploaded the photos and video clips to Skydrive
Mail	• Setup email access to m80003052@zu.ac.ae • Accessed an email message • Composed and sent an email to asif@babariqbal.com • Subject: My Surface RT, Message: Hello from surface RT
SkyDrive	• Created and uploaded a document titled “Document2” • Downloaded and accessed “Document1.doc” previously uploaded to Skydrive from a different PC
Photos	• Downloaded pic1, pic2 and pic3 previously uploaded to Skydrive • Viewed pic1, pic2, pic3
Music	• Listened to a radio station, Artist “coldplay” • Note: During the process a Microsoft Xbox account was automatically created.
Calendar	• Added a new calendar event
Weather	• Added a new weather city “Seoul, South Korea”
Bing	• Searched for keywords “security”, “forensics” and “digital forensics”
Skype	• Added contact “asifiqbal.ai” • Initiated a text chat session with “asifiqbal.ai” • Initiated a video chat with “asifiqbal.ai”
Store	• Searched for and installed Skype app from the Windows Store



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	
disabled ...		31d6cfe0d16ae931b73c59d7e0c089c0			empty
disabled ...		31d6cfe0d16ae931b73c59d7e0c089c0			empty
John		23e1d10001876b0078a9a779017fc026			Testing1

Table	Directory	Status	Progress
Vista f...	/home/sith...	100% in RAM	

Fig. 1. Ophcrack being used to crack the password of user John's local and online account password.

Table 3
The structure of metro application data directory.

Directory	Content
AC	
INetCache	The cache file is stored in randomly named sub-directories. Cache files retain their original filename and extension.
INetCookies	Cookies are stored in this Directory with cookies for each website stored in a single textfile with random name
LocalState	This directory can be directly accessed by the application and can be used to permanently store any type of data.
Settings	Application settings are stored in this directory as Registry Hive (regf) files. These files can be analyzed using yaru

and compared to the base image, the changes were then analyzed and reported.

Analysis

This stage involved the analysis of the image acquired during the acquisition stage. As mentioned above, several images were created and analyzed, and compared to a base image. A description of the analysis and associated findings is provided in the analysis section below.

Acquisition

One of the first steps in any forensic investigation is acquiring an image of the device. A forensic image is acquired to ensure the integrity of the original evidence.

The acquisition process we employed was accomplished utilizing a kernel-level vulnerability in the Windows Driver Signature Enforcement mechanism, which has existed in Microsoft Windows on the PC for some time now. Since Windows RT is a port of Windows 8 to the ARM platform. This vulnerability was also ported to the Surface RT tablet and was employed by CL Rokr (aka 'clrokr') in order to jailbreak Windows RT (Windowsjailbroken et al., 2013).

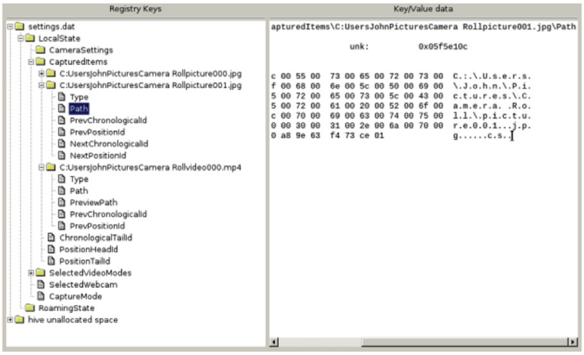
The minimum signing level determines how trusted an executable's signature is on the scale: Unsigned (0), Authenticode (4), Microsoft (8), and Windows (12). The default value on x86 machines is 0, to allow a user to run anything they like on their computer. On ARM machines, the default is set to 8. This is not a user setting, but a hardcoded global value in the kernel itself. It cannot be changed permanently on devices with UEFI's (Unified Extensible Firmware Interface) Secure Boot enabled. It can, however, be changed in memory.

By adapting the technique mentioned above, the value of signing level is set to Unsigned (0). This allows execution of unsigned applications.

We used the Windows Volume Shadow Copy service to acquire an image of the device's disk. For this purpose a C++ program was written to use VSS (Volume Shadow Copy Service) APIs to copy all of the disk's content.

Analysis

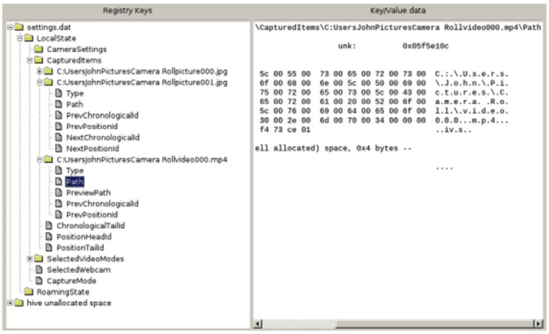
After setting up the user account on the device, a base image of the device was created. A predefined set of activities were then performed on the device, as detailed in



```
settings.dat
  LocalState
    CameraSettings
    CapturedItems
      C:UsersjohnPicturesCamera Rollpicture000.jpg
      C:UsersjohnPicturesCamera Rollpicture001.jpg
        Type
        Path
        PrevChronologicalId
        PrevPositionId
        NextChronologicalId
        NextPositionId
      C:UsersjohnPicturesCamera Rollvideo000.mp4
        Type
        Path
        PreviewPath
        PrevChronologicalId
        PrevPositionId
      ChronologicalTailId
      PositionHeadId
      PositionTailId
    SelectedVideoModes
    SelectedWebcam
    CaptureMode
  RoamingState
hive unallocated space
```

```
apturedItems\C:UsersJohnPicturesCamera Rollpicture001.jpg\Path

                unk:          0x05f5e10c


c 00 55 00  73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
f 00 68 00  6e 00 5c 00 50 00 69 00  \.J.o.h.n.\.P.i.
5 00 72 00  65 00 73 00 5c 00 43 00  c.t.u.r.e.s.\.C.
5 00 72 00  61 00 20 00 52 00 6f 00  a.m.e.r.a. .R.o.
c 00 70 00  69 00 63 00 74 00 75 00  l.l.\.p.i.c.t.u.
0 00 30 00  31 00 2e 00 6a 00 70 00  r.e.0.0.1...j.p.
0 a8 9e 63  f4 73 ce 01              g......c.s..
```

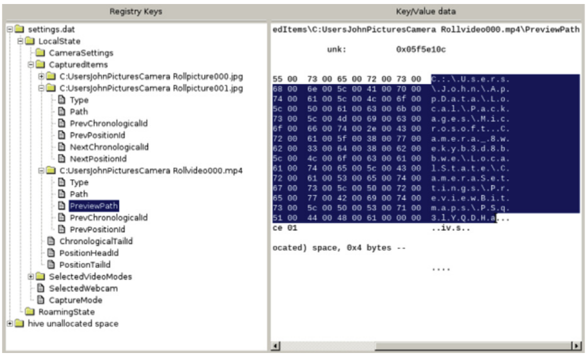
Fig. 2. Setting.db Registry hive file being analyzed in yaru. Path property of Picture001 is being highlighted.



```
settings.dat
  LocalState
    CameraSettings
    CapturedItems
      C:UsersjohnPicturesCamera Rollpicture000.jpg
      C:UsersjohnPicturesCamera Rollpicture001.jpg
        Type
        Path
        PrevChronologicalId
        PrevPositionId
        NextChronologicalId
        NextPositionId
      C:UsersjohnPicturesCamera Rollvideo000.mp4
        Type
        Path
        PreviewPath
        PrevChronologicalId
        PrevPositionId
      ChronologicalTailId
      PositionHeadId
      PositionTailId
    SelectedVideoModes
    SelectedWebcam
    CaptureMode
  RoamingState
hive unallocated space
```

```
\CapturedItems\C:UsersJohnPicturesCamera Rollvideo000.mp4\Path

                unk:          0x05f5e10c


5c 00 55 00  73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
6f 00 68 00  6e 00 5c 00 50 00 69 00  \.J.o.h.n.\.P.i.
75 00 72 00  65 00 73 00 5c 00 43 00  c.t.u.r.e.s.\.C.
65 00 72 00  61 00 20 00 52 00 6f 00  a.m.e.r.a. .R.o.
5c 00 76 00  69 00 64 00 65 00 6f 00  l.l.\.v.i.d.e.o.
30 00 2e 00  6d 00 70 00 34 00 00 00  0.0.0...m.p.4...
f4 73 ce 01                           ..iv.s..

ell allocated) space, 0x4 bytes --

                                      ....
```

Fig. 3. Setting.db Registry hive file being analyzed in yaru. Path property of Video000 is being highlighted.



```
settings.dat
  LocalState
    CameraSettings
    CapturedItems
      C:UsersjohnPicturesCamera Rollpicture000.jpg
      C:UsersjohnPicturesCamera Rollpicture001.jpg
        Type
        Path
        PrevChronologicalId
        PrevPositionId
        NextChronologicalId
        NextPositionId
      C:UsersjohnPicturesCamera Rollvideo000.mp4
        Type
        Path
        PreviewPath
        PrevChronologicalId
        PrevPositionId
      ChronologicalTailId
      PositionHeadId
      PositionTailId
    SelectedVideoModes
    SelectedWebcam
    CaptureMode
  RoamingState
hive unallocated space
```

```
edItems\C:UsersJohnPicturesCamera Rollvideo000.mp4\PreviewPath

          unk:          0x05f5e10c


55 00  73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
68 00  6e 00 5c 00 41 00 70 00  \.J.o.h.n.\.A.p.
74 00  61 00 5c 00 4c 00 6f 00  p.D.a.t.a.\.L.o.
5c 00  50 00 61 00 63 00 6b 00  c.a.l.\.P.a.c.k.
73 00  5c 00 4d 00 69 00 63 00  a.g.e.s.\.M.i.c.
6f 00  66 00 74 00 2e 00 43 00  r.o.s.o.f.t...C.
72 00  61 00 5f 00 38 00 77 00  a.m.e.r.a._.8.w.
62 00  33 00 64 00 38 00 62 00  e.k.y.b.3.d.8.b.
5c 00  4c 00 6f 00 63 00 61 00  b.w.e.\.L.o.c.a.
61 00  74 00 65 00 5c 00 43 00  l.S.t.a.t.e.\.C.
72 00  61 00 53 00 65 00 74 00  a.m.e.r.a.S.e.t.
67 00  73 00 5c 00 50 00 72 00  t.i.n.g.s.\.P.r.
65 00  77 00 42 00 69 00 74 00  e.v.i.e.w.B.i.t.
73 00  5c 00 50 00 53 00 71 00  m.a.p.s.\.P.S.q.
51 00  44 00 48 00 61 00 00 00  3.l.Y.Q.D.H.a...
ce 01                           ..iv.s..

ocated) space, 0x4 bytes --

                                ....
```

Fig. 4. Setting.db Registry hive file being analyzed in yaru. PreviewPath property of Video000 is being highlighted, this property hold full path to one frame of the video used for preview

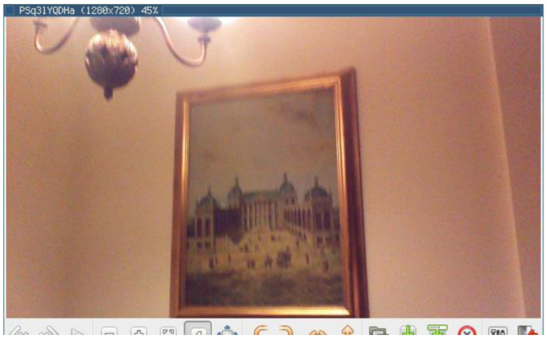
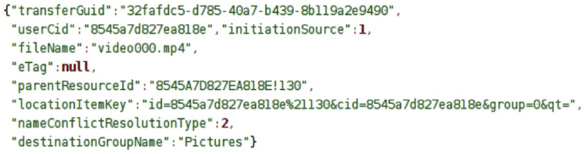


Fig. 5. Image recovered from the PreviewPath variable mentioned in above. The image is saved in JPEG format.

Table 4
The data found inside the settings registry hive.

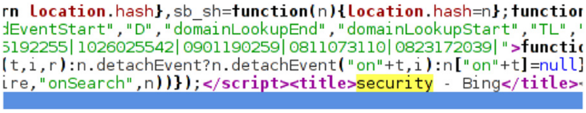
Tree	Content
Local State	
Captured Items	A list of all items captured with the Camera application.
%Path to image no slashes%	A single captured item
Path	The full path to the image file, images are stored in jpg format under %userprofile%\Pictures\Camera Roll\.
%Path to video no slashes%	
Path	Full path to video file, videos are stored in mp4 file format under %userprofile%\Pictures\Camera Roll\.
PreviewPath	Path to preview thumbnail to one frame of the captured video. These images are stored under %Application Package Directory%\LocalState\CameraSettings\PreviewBitmaps\ {random filename} in JPEG file format.

Table 2. Apart from activities performed on the device, a document titled “Document1.doc” was uploaded to the SkyDrive from a different computer. Three Pictures were also uploaded to SkyDrive with file names pic1.jpg, pic2.jpg and pic3.jpg.



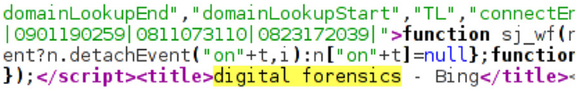
```
{"transferGuid":"32fafdc5-d785-40a7-b439-8b119a2e9490",
 "userCid":"8545a7d827ea818e","initiationSource":1,
 "fileName":"video000.mp4",
 "eTag":null,
 "parentResourceId":"8545A7D827EA818E!130",
 "locationItemKey":"id=8545a7d827ea818e%21130&cid=8545a7d827ea818e&group=0&qt=",
 "nameConflictResolutionType":2,
 "destinationGroupName":"Pictures"}
```

Fig. 6. File recovered indicating upload of video000.mp4 captured to Pictures directory on Skydrive



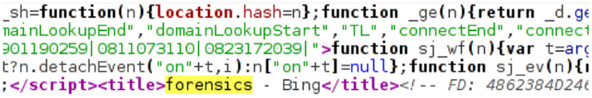
```
rn location.hash},sb_sh=function(n){location.hash=n};functior
dEventStart","D","domainLookupEnd","domainLookupStart","TL",'
5192255|1026025542|0901190259|0811073110|0823172039|">functic
(t,i,r):n.detachEvent?n.detachEvent("on"+t,i):n["on"+t]=null]
ire,"onSearch",n))});</script><title>security - Bing</title>
```

Fig. 7. Excerpt from cached file search.htm indicating search for term “security”.



```
domainLookupEnd","domainLookupStart","TL","connectEr
|0901190259|0811073110|0823172039|">function sj_wf(r
ent?n.detachEvent("on"+t,i):n["on"+t]=null};functior
});</script><title>digital forensics - Bing</title>
```

Fig. 8. Excerpt from cached file search.htm indicating search for term “digital forensics”.



```
_sh=function(n){location.hash=n};function _ge(n){return _d.ge
nainLookupEnd","domainLookupStart","TL","connectEnd","connect
901190259|0811073110|0823172039|">function sj_wf(n){var t=arg
t?n.detachEvent("on"+t,i):n["on"+t]=null};function sj_ev(n){
;</script><title>forensics - Bing</title><!-- FD: 4862384D24
```

Fig. 9. Excerpt from cached file search.htm indicating search for term “forensics”.

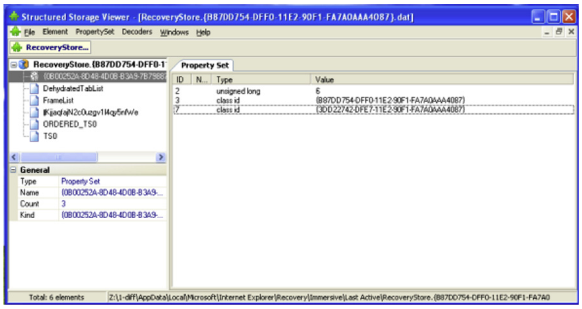
Non-Metro application artifacts recovered

One of the interesting artifacts recovered from the Surface RT tablet was the password of the user’s online and offline account. We were able to recover this artifact because the information from the user’s online Microsoft account is used in the local Windows user account. The local account also shares the password of the online account of the user. Since Windows stores password hashes of the local account in SAM file located in %WINDOWS%/System32/config directory, the content of this directory were investigated. The Ophcrack tool was used to decode the SAM file found on the device, where the password of the user’s online and offline account was successfully recovered (see Fig. 1). More complex passwords could be recovered using the Rainbow tables (Marechal, 2008).

Other useful non-Metro artifacts retrieved from the device were photos and videos taken on the device itself. All the photos and videos taken on the device itself were stored in the (%userprofile%\Pictures\Camera Roll\) directory, where the variable (%userprofile%) stands for

Table 5
The structure of “recovery” directory.

Directory	Comments
Active	
Last Active	Data related to tabs open in the last session of Internet Explorer Desktop version
Immersive	
Active	This directory is located under the Immersive directory
Last Active	This directory holds several files stored with filename %GUID%.dat. All of these files represent an open tab in last browsing session. Apart from these files there is a RecoveryState.{%GUID%}.dat file which serves to hold the GUID variable used in each of the files mentioned above. The files use Object Linking and Embedding (OLE) Compound File (CF) format and can be identified by the header D0 CF 11 E0 A1 B1 1A E1. These files can be analyzed by using the free tool “Mitec Structured Storage Viewer” or by utilizing open-source library libolecf (code.google.com/p/libolecf/)


Structured Storage Viewer - [RecoveryStore.{B87DD754-DFF0-11E2-90F1-FA7A0AAA4087}.dat]
File Element PropertySet Decoders Windows Help
RecoveryStore...
RecoveryStore.{B87DD754-DFF0-1
{0B00252A-8D48-4D0B-B3A9-7B7988
DehydratedTabList
FrameList
♯KjaqfajN2c0uzgv1l4qy5nfWe
ORDERED_TS0
TS0
Property Set

ID	N...	Type	Value
2		unsigned long	6
3		class id	{B87DD754-DFF0-11E2-90F1-FA7A0AAA4087}
7		class id	{3DD22742-DFE7-11E2-90F1-FA7A0AAA4087}

General

Type	Property Set
Name	{0B00252A-8D48-4D0B-B3A9-...
Count	3
Kind	{0B00252A-8D48-4D0B-B3A9-...

Total: 6 elements Z:\1-diff\AppData\Local\Microsoft\Internet Explorer\Recovery\Immersive\Last Active\RecoveryStore.{B87DD754-DFF0-11E2-90F1-FA7A0

Fig. 10. RecoveryState.{%GUID%}.dat file being analyzed in Mitec SSV. Two GUIDs can be seen that indicates that two tabs were open.

(C:\Users\%User Name%\). The retrieved photos were stored in JPEG format while the videos were stored in MP4 file format.

Analysis of Metro application artifacts

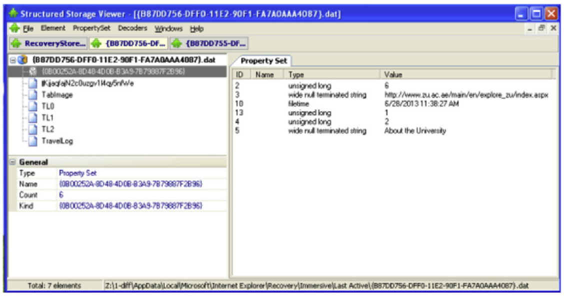
Metro applications do not have direct access to the file system and all of their content is stored under (%userprofile %\AppData\Local\Packages\%Application Name%_%id%). Table 3 details the structure of the Metro application data directory.

Camera Application

Artifacts left by the Camera Metro application were found in the directory "Microsoft.Camera_8wekyb3d8bbwe" under the package's directory. The Registry hive "settings.dat" was found under the Settings directory (see Figs. 2–5). Table 4 details the data found inside the settings registry hive.

Photo application

The photos application displays not only the local photos stored in the Pictures directory in the user's home directory but also online photos stored in user's SkyDrive. All the online SkyDrive photos are cached to the expected INetCache directory under the package directory (microsoft.windowsphotos_8wekyb3d8bbwe). As mentioned previously these files retain their original file-names. The photos uploaded during the case study phase of the experiment were recovered from randomly named directories under INETCache directory.


Structured Storage Viewer - [{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat]
File Element PropertySet Decoders Windows Help
RecoveryStore...
{B87DD756-DF...
{B87DD755-DF...
{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat
{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
♯KjaqfajN2c0uzgv1l4qy5nfWe
TabImage
TL0
TL1
TL2
TravelLog
Property Set

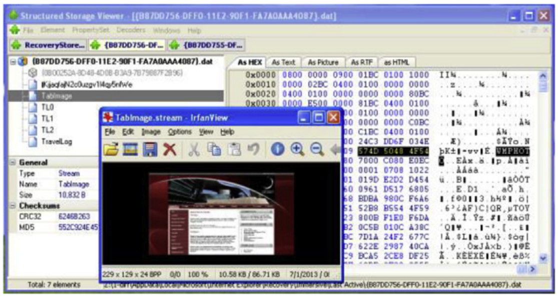
ID	Name	Type	Value
2		unsigned long	6
3		wide null terminated string	http://www.zu.ac.ae/main/en/explore_zu/index.aspx
10		filetime	6/28/2013 11:38:27 AM
13		unsigned long	1
4		unsigned long	2
5		wide null terminated string	About the University

General

Type	Property Set
Name	{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
Count	6
Kind	{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}

Total: 7 elements Z:\1-diff\AppData\Local\Microsoft\Internet Explorer\Recovery\Immersive\Last Active\{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat

Fig. 11. {B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat file being analyzed in Mitec SSV.


Structured Storage Viewer - [{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat]
File Element PropertySet Decoders Windows Help
RecoveryStore...
{B87DD756-DF...
{B87DD755-DF...
{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat
{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
♯KjaqfajN2c0uzgv1l4qy5nfWe
TabImage
TL0
TL1
TL2
TravelLog
As HEX
As Text
As Picture
As RTF
as HTML
TabImage.stream - IrfanView
File Edit Image Options View Help

```
0x0000 0800 0000 0900 01BC 0100 1000
0x0010 0000 02BC 0400 0100 0000 0000
0x0020 0400 0100 0000 0000 0000 80BC
0x0030 0000 E500 0000 81BC 0400 0100
```

General

Type	Stream
Name	TabImage
Size	10,832 B

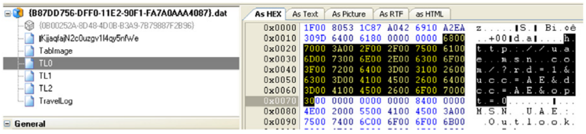
Checksums

CRC32	6246B263
MD5	552C924E45

229 x 129 x 24 BPP 0/0 100 % 10.58 KB / 86.71 KB 7/1/2013 / 0

Total: 7 elements

Fig. 12. TabImage stream in file {B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat. This file holds information about a single tab in browsing session.


{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat
{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
♯KjaqfajN2c0uzgv1l4qy5nfWe
TabImage
TL0
TL1
TL2
TravelLog
General
As HEX
As Text
As Picture
As RTF
as HTML

```
0x0000 1F00 8053 1C87 A042 6910 A2EA  z.....▮S.▮ Bi.◊ê
0x0010 309D 6400 6180 0000 0000 6800  ..+00▮d.a▮....h.
0x0020 7000 3A00 2F00 2F00 7500 6100  t.t.p.:././.u.a.
0x0030 6D00 7300 6E00 2E00 6300 6F00  e...m.s.n...c.o.
0x0040 3F00 7200 6400 3D00 3100 2600  m./.?.r.d.=.1.&.
0x0050 6300 3D00 4100 4500 2600 6400  u.c.c.=.A.E.&.d.
0x0060 3D00 4100 4500 2600 6F00 7000  c.c.=.A.E.&.o.p.
0x0070 3000 0000 0000 0000 8400 0000  t.=.0.......▮...
0x0080 4E00 2000 5500 4100 4500 3A00  M.S.N. .U.A.E.:.
0x0090 7500 7400 6C00 6F00 6F00 6B00  .O.u.t.l.o.o.k.
```

Fig. 13. TL0 stream in file {B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat. URL is being highlighted.

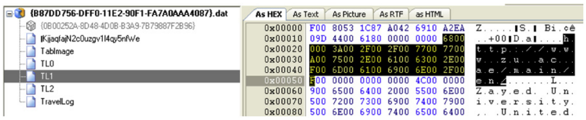
SkyDrive application

Data related to files uploaded to SkyDrive using the application was found in the directory (LocalState\bt\uploads\%User ID%\) under the package directory (microsoft.microsoftskydrive_ 8wekyb3d8bbwe). See Fig. 6. The data is stored in xml files with GUID as file-name. The following are the nodes that are of interest:

- transferGUID: Unique ID of the transaction, this id is also used in filename.
- UserCid: Unique ID of user's Microsoft account, this is previouly mentioned as variable %User ID%.
- FileName: Name of file on local system, this will also be used as name of the file on SkyDrive servers.
- destinationGroup: Name of the directory files is to be sent to on SkyDrive server.

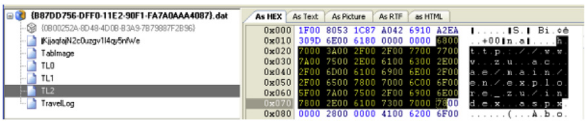
Bing search

Bing search artifacts were recovered from randomly named subdirectories of the INetCache directory in the Bing package directory (Microsoft.Bing_8wekyb3d8bbwe). The files recovered were cached files of page search.htm, which is called when a new search term is entered. The cache directories also held several image files that were


{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat
{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
♯KjaqfajN2c0uzgv1l4qy5nfWe
TabImage
TL0
TL1
TL2
TravelLog
As HEX
As Text
As Picture
As RTF
as HTML

```
0x00000 F00 8053 1C87 A042 6910 A2EA  Z.....▮S.▮ Bi.çê
0x00010 09D 4400 6180 0000 0000 6800  ..+00▮D.a▮....h.
0x00020 000 3A00 2F00 2F00 7700 7700  t.t.p.:././.w.w.
0x00030 A00 7500 2E00 6100 6300 2E00  w...z.u...a.c...
0x00040 F00 6D00 6100 6900 6E00 2F00  a.e./.m.a.i.n./.
0x00050 F00 0000 0000 0000 4C00 0000  e.n./.......L...
0x00060 900 6500 6400 2000 5500 6E00  Z.a.y.e.d. .U.n.
0x00070 500 7200 7300 6900 7400 7900  i.v.e.r.s.i.t.y.
0x00080 500 6E00 6900 7400 6500 6400  ,. .U.n.i.t.e.d.
```

Fig. 14. TL1 stream in file {B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat. URL is being highlighted.


{B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat
{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
IKjiaqfajN2c0uzgv1l4qy5nfWe
TabImage
TL0
TL1
TL2
TravelLog
As HEX
As Text
As Picture
As RTF
as HTML

```
0x000  1F00 8053 1C87 A042 6910 A2EA  I.....IS.I Bi.¢ê
0x010  309D 6E00 6180 0000 0000 6800  ..+00In.aI....h
0x020  7000 3A00 2F00 2F00 7700 7700  t.t.p.:././.w.w.
0x030  7A00 7500 2E00 6100 6300 2E00  v...z.u...a.c...
0x040  2F00 6D00 6100 6900 6E00 2F00  a.e./.m.a.i.n./.
0x050  2F00 6500 7800 7000 6C00 6F00  e.n./.e.x.p.l.o.
0x060  5F00 7A00 7500 2F00 6900 6E00  r.e._.z.u./.i.n.
0x070  7800 2E00 6100 7300 7000 7800  d.e.x...a.s.p.x.
0x080  0000 2800 0000 4100 6200 6F00  ......(...A.b.o.
```

Fig. 15. TL2 stream in file {B87DD755-DFF0-11E2-90F1 FA7A0AAA4087}.dat. URL has been highlighted.

displayed in the result of the search. These results reflected search terms used in the case study phase of the experiment see Figs. 7–9.

Analysis of Internet Explorer artifacts

Internet Explorer browser session artifacts were recovered from (%userprofile%\AppData\Local\Microsoft\Internet Explorer\Recovery\). Table 5 details the structure of "Recovery" directory.

Using the data found in these files, a timeline of the user's activity in the last browsing session was established see Fig. 10.

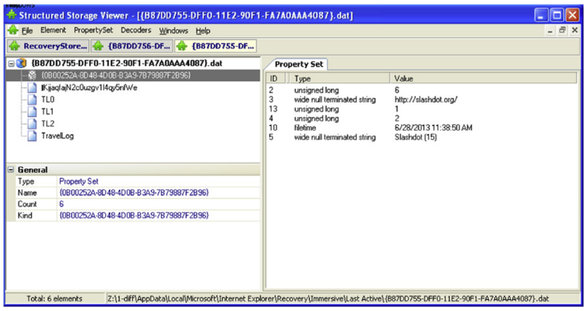
Analysis of the Property Set in the file {B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat indicated the last destination of the user was the page titled "About the University" with a corresponding URL www.zu.ac.ae/main/en/explore_zu/index.aspx see Fig. 11.

The stream titled TabImage held the thumbnail preview image. This image was stored in Microsoft's proprietary format "Windows Media Photo" (WMPHOTO). This stream was saved as binary data and was viewed using image viewing software IrfanView see Fig. 12

By analyzing the streams (TL%Number%) it was found that on opening the browser, the user was directed to the default page MSN UAE (http://uae.msn.com/?rd=1&dcc=AE&opt=0). The user then navigated to Zayed University website's main page (http://www.zu.ac.ae/main/en). And from there, finally, to Zayed University website's "About University" page (http://www.zu.ac.ae/main/en/explore_zu/index.aspx) see Figs. 13–15.

Similar analysis was done on second file {B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat which represented a second browser tab see Fig. 16.

All the information recovered during this analysis was found to be consistent with the case study conducted in the first stage of the experiment.


Structured Storage Viewer - [{B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat]
File
Element
PropertySet
Decoders
Windows
Help
RecoveryStore...
{B87DD756-DF...
{B87DD755-DF...
{B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat
{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
IKjjaqfajN2c0uzgv1l4qy5nfWe
TL0
TL1
TL2
TravelLog
Property Set

ID	Type	Value
2	unsigned long	6
3	wide null terminated string	http://slashdot.org/
13	unsigned long	1
4	unsigned long	2
10	filetime	6/28/2013 11:38:50 AM
5	wide null terminated string	Slashdot (15)

General

Type	Property Set
Name	{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}
Count	6
Kind	{0B00252A-8D48-4D0B-B3A9-7B79887F2B96}

Total: 6 elements Z:\1-diff\AppData\Local\Microsoft\Internet Explorer\Recovery\Immersive\Last Active\{B87DD755-DFF0-11E2-90F1-FA7A0AAA4087}.dat

Fig. 16. B87DD756-DFF0-11E2-90F1-FA7A0AAA4087}.dat file being analyzed in Mitec SSV.

Conclusion and future work

The field of digital forensics is developing with the innovation of new devices. In this research we have studied the forensics of the Windows Surface RT tablet, which runs the Windows RT operating system. Utilizing a vulnerability in Windows RT code, we were able to perform the acquisition of the device.[1] There are a range of artifacts that could be considered as evidence when forensically investigating a Surface RT device. These artifacts can be divided as non-Metro application artifacts and Metro application artifacts. In terms of non-Metro application artifacts, an interesting artifact that was retrieved was the user's online and offline account password. In terms of Metro Application artifacts, we were able to retrieve information about, for example, the Camera Application, the Photos Application, SkyDrive and Bing Searches.

With regard to future work, we plan to utilize the information gathered in this research to develop a tool that will automate the process of acquisition and analysis of a Surface RT device. Other possible future work is to compare the artifacts from the Surface RT with those from other Windows RT devices to determine whether there are any differences in the data stored on the device and their structure.

References

Casey Eoghan. Smartphone incident response. Digit Investig June, 2013; 10(1). ISSN: 1742-2876:1–2. http://dx.doi.org/10.1016/j.diin.2013.04.004.

Fleisher Ethan. Windows 8 Forensics: Reset and Refresh Artifacts, infosecisland [Retrieved from], www.infosecisland.com/blogview/22353-Windows-8-Forensics-Reset-and-Refresh-Artifacts.html; September 24, 2012.

Freestone D. Acquisition of the Microsoft Surface™ RT. Lock and Code Pty Ltd; April, 2013.

Gisolf Floris, Geradts Zeno, Verhoeven Dennie, Klaver Coert. The effects of switching the camera module from BlackBerry Curve 9360 devices. Digital Investigation 2013;10(1):56–61.

Kaart M, Klaver C, van Baar RB. Forensic access to Windows Mobile pim.vol and other Embedded Database (EDB) volumes. Digit Investig February, 2013;9(3–4). ISSN: 1742-2876:170–92. http://dx.doi.org/10.1016/j.diin.2012.12.002.

Marechal Simon. Advances in password cracking. J Comput Virol 2008; 4(1):73–81.

Marturana F, Me G, Berte R, Tacconi S. A quantitative approach to Triaging in Mobile Forensics. In: Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 10th International Conference on; 2011. pp. 582–8 [16–18 Nov.].

National Institute of Standards and Technology. General test methodology for computer forensic tools [Retrieved from], http://www.cftt.nist.gov/documents.htm; 2001 [2001].

Quick Darren, Choo Kim-Kwang Raymond. Dropbox analysis: Data remnants on user machines. Digital Investigation 2013;10(1):3–18.

Schaefer T, Höfken H, Schuba M. Windows phone 7 from a digital forensics perspective. In: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Digital Forensics and Cyber Crime, Springer Berlin Heidelberg, vol. 88; 2012. pp. 62–76.

Thomson Amanda CF. Windows 8 forensic guide; 2012 [Retrieved from] https://propellerheadforensics.files.wordpress.com/2012/05/thomson_windows-8-forensic-guide2.pdf.

Windows RT jailbroken. Comput Fraud Secur 20 January, 2013;(1):3–20.

[1] It should be mentioned that this particular vulnerability, allowing root access, no longer exists in the updated Windows 8.1 version on current Surface devices.