Abstract

Microsoft OneNote is a powerful data management tool. In the past it has been an obscure component of the Microsoft Office suite. Today it is a cross platform PC, MAC, mobile, and web based application that integrates with Microsoft SkyDrive. However, there is no substantial research on the topic of OneNote forensics. This body of research explores the forensic artifacts that may be recovered during investigations involving Microsoft OneNote. The research explains the relevance of OneNote artifacts for today's electronic investigations, describes techniques for examiners to become familiar with OneNote and its files, and offers insight into the many artifacts that can be located for the various installations and usage of OneNote. A hypothetical case scenario involving the usage of OneNote to steal company secrets is presented. The subsequent walk-through style examination demonstrates how OneNote could be exploited for criminal purposes and how an examiner might proceed with the examination. The forensic artifacts of OneNote's structure, file header, internal paging and caching system, and its recycle bin are all discussed and analyzed. This body of research will allow others to investigate OneNote artifacts and to conduct further research.

THE FORENSIC ARTIFACTS OF MICROSOFT ONENOTE

By

Cynthia Gonnella

A Capstone Project Submitted to the Faculty of

Utica College

August 2012

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Cybersecurity

Table of Contents

List of Illustrative Material

Acknowledgement

Having spent my entire career in law enforcement, over half of it in computer forensics, I was ready for a challenge. I had spent years working cases in dead forensics and was ready to take it to the next level. I am pleased to acknowledge Utica College for providing a challenging and encompassing Cybersecurity Program. From the candidate selection process to the talented staff delivering the program, I always had assistance when there were difficulties. Many family and job related situations arose that would have made it nearly impossible to complete this program, had it not been for the dedication of the Utica professors and their concern for my success. I would like to acknowledge Professor Chris Riddell who has mentored me through the capstone process and Professor Leonard Popyack who graciously served as my second, technical reader. Both have provided professional and timely assistance as needed to ensure my successful completion of the program. I must acknowledge my family who has sacrificed much allowing me to complete the Cybersecurity Master's Program on top of a busy family life, a family business, and a full-time traveling job instructing computer forensic classes across the country. In fact, finishing what I started and validating my family's precious sacrifices, has been my main driving force to see this through. I am grateful for my numerous mentors over the years who have helped shape my successful career in computer forensics. I looked forward to the day, I too, could give something back to the forensic community. Having completed this program, I am able to deliver a foundational and crucial body of research. I am both pleased and excited to present the *Forensic Artifacts of Microsoft OneNote* to the forensic community. My hope is that others will pick up where I have left off and continue researching the forensic artifacts of OneNote.

The Forensic Artifacts of Microsoft OneNote

The purpose of this research was to explore the forensic artifacts that may be recovered during investigations involving Microsoft OneNote. OneNote is a powerful data management application that integrates with other Microsoft Office products and can be run on a local machine or from the web without installation. This research explains the relevance of OneNote artifacts for today's electronic investigations, describes techniques for examiners to become familiar with OneNote and its files, and offers insight into the many artifacts that can be located for the various installations and usage of OneNote. This body of research will allow others to investigate OneNote artifacts and conduct further research.

The Relevance of OneNote Artifacts

Experienced examiners learn to keep themselves abreast of the latest trends in hardware and software. Increased usage of software applications such as OneNote, tips them off to the types of files they can expect to see in future examinations. As the new releases of OneNote applications become more popular, examiners know it will not be long until requested to recover artifacts associated with OneNote files. While once an obscure component of the Microsoft Office suite, today OneNote is gaining in popularity. The newfound interest may be due to Microsoft's releasing OneNote as a cross platform app for desktop and mobile users alike. In June 2010, Microsoft released *web apps*, a lighter version of its Office products, including OneNote. Web apps require users to create a Windows Live account. Each live account provides the user seven gigabytes of personal storage space in Microsoft's cloud, *SkyDrive*. In January 2011, Microsoft released a mobile app for OneNote, to the Apple market. In February 2012, the mobile

app was also released to the Android market. Packed with features that serve today's instant technology needs, users who have discovered its versatility and powerful data organization abilities claim they would not part with it. Edwards and Edwards (2012), in their blog posted a comment about how integrated OneNote has become in their lives, "These days, I live and die by OneNote." (para. 1) Some even call it Microsoft's "best kept secret." Numoto (2011), the Corporate Vice President of Microsoft Office, called OneNote, "the unsung hero of Office." (para. 2)

OneNote has actually been available for years as a standalone install or as an optional component of Microsoft Office. Creative OneNote users have found several ways to capitalize on its data organization and management capabilities. In fact, several educational institutions, students, police officers and others have already put OneNote to use organizing data, collaborating on projects, scheduling events, and managing case information. Not all users will put OneNote to use for positive purposes. Crafty cyber criminals will undoubtedly exploit the unique features of OneNote for nefarious purposes.

Microsoft is reaching out to almost every user in the world, from PCs to Macs, from iPhones to Androids and tablets in between, regardless of the platform or browser they choose to operate. Surprisingly, an exhaustive Internet search yielded no documentation on the subject of the forensic artifacts of OneNote. Further researching of scholarly resources and forensic manuals also yielded no substantial research on the topic of conducting forensic investigations involving OneNote artifacts. The deficiency in research is disproportionate to the renewed interest in OneNote. The lack of

documentation prolongs the investigation while the examiner takes time to conduct new research.

When examiners are presented with unfamiliar file types, they must determine the origin and structure before understanding what artifacts may be collected. In some cases, the learning curve is so extensive that it precludes a timely report of the findings. Predictive research presented to the forensic community is a valuable resource. As the OneNote app has become a part of all markets, examiners can expect to see an increase in cases involving OneNote artifacts. This research serves as both an interim document for examiners who encounter OneNote files and a catalyst for further research.

Literature Review

Research of the installation methods, storage locations, and data structures of Microsoft OneNote, particularly as it pertains to computer forensics, is especially limited. Though the research into the forensic artifacts is limited, OneNote's developers and users have published several resources that offer the forensic examiner a foundation on which to build a working knowledge of OneNote. A study of these resources exposes the benefits and difficulties that may be encountered in a forensic examination involving OneNote files. The information contained in this literature review is presented in three sections; those who feel information is not flowing well enough in the forensic community, an example of how OneNote could be used for nefarious purposes, and the steps an examiner could take to collect OneNote forensic artifacts.

In the forensic community it is not uncommon for an examiner to be faced with new data types and unfamiliar applications that are clearly relevant to the case at hand. To complete a thorough analysis, the examiner must overcome the learning obstacle this

situation presents. Using investigative skills and forensic tools, the examiner often overcomes the obstacle. A series of testing and validation produces a working knowledge that can be applied to gather artifacts in the current case, and any similar cases in the future. In April 2012, in an interview with *Forensic Interviews*, a web site dedicated to interviewing computer forensic professionals, Harlan Carvey (2012), author of Windows computer forensic books, open source computer forensic books, and RegRipper forensic software, expressed his feelings that analysts seldom document the forensic problem solving process, depriving others in the forensic community of the lessons learned and the foundation on which to build more research.

> For some reason, analysts within the community seem to think that any problem that they've encountered, no one else has ever seen, so they won't ask for assistance. When an exam is over, analysts take the opposite view and tend not share their findings, thinking that everyone else has already seen what they've seen and therefore wouldn't be interested in their findings or thoughts. In the long run, this reticence to engage with the community is going to have a significant, detrimental impact on the community ("Yuri: Please give some predictions," para. 1).

Carvey spoke about the lack of case notes available for examiners to educate themselves from each other's work. How then do examiners prepare themselves for the types of situations they may face? Many examiners consider different scenarios and think about how they would conduct an examination. A hypothetical, but realistic, scenario often helps examiners understand how certain software could be used to facilitate a crime. The following scenario leads in with the story of a manager who is accused of

leaking company secrets. A walk through of the forensic artifacts reveals how he used OneNote as a means to sneak a file out without being noticed. Many computer crime classes will use similar techniques to prepare examiners for the types of forensic examinations they will face throughout their career.

Scenario

The police department forensic unit was dispatched to the Rielitom Corporate office. Rielitom is a small business operated from a single office location. The computer users share information via file sharing over a simple Windows 7 home network. After suffering a costly virus, all computers had been configured to prevent the usage of removable media. The owner reported that an account manager and project team leader, Tom Terces, was reportedly leaking company secrets. As an account manager, Tom legitimately had access to all sensitive company files. He mainly used Microsoft Office 2010 to create and manage his team's projects. Tom was computer savvy and had unlimited use of the Internet from his work machine. He commonly used OneNote for data management. Tom allowed his team members to access the public documents folder he managed on his machine. All team members were regularly briefed on the sensitivity of data and clicked through a banner when logging on to remind them company data was never to be copied or disseminated in any way. One evening, a coworker observed Tom sitting in a bar with an unknown male. Tom was revealing company secrets to him about prototype P1-343, via a laptop computer. The coworker also overheard Tom complaining to the man about his salary and how he was overworked. The coworker reported the incident to the owner of the company, who immediately contacted the police. The forensic unit responded after hours and launched a covert investigation.

Only the coworker who reported the incident and the owner were aware of the investigation. When questioned about the laptop and what was displayed on the screen, the coworker said he remembered seeing OneNote open at the top of the screen, but it looked like a different version than Tom used at work. The employee stated he did not know the other party or who owned the laptop, but he did not think the laptop was Tom's. Using proper authority and forensic practices, a police forensic examiner acquired an image of the local hard drive from Tom's work PC and returned to the police department to perform a forensic analysis.

Analysis

Analysis of this hard drive image should include a search for any unauthorized copying of files or content related to prototype P1-343. The mere existence of related files would not be evidentiary, as Tom had authority to access all company files. The examiner would normally select a forensic suite to conduct the processing. In this study, AccessData's *Forensic Toolkit (FTK),* version 1.81.6, in demo mode (version 4.0 is current), was chosen to examine a Windows 7 x86 virtual machine with Microsoft Office 2010 installed (AccessData, 2012). The image file was mounted in FTK Imager 3.0.1.1467 (AccessData, 2012). FTK was set to index the contents of the hard drive image and to carve documents during its initial processing. The leaked prototype file was expected to be located in the public documents directory. Parts of the prototype file were also expected in the pagefile.sys where Windows swaps out memory to the hard drive for efficiency while working with files (Casey, 2010, Loc. 6334). These areas were checked and the expected items were found. Initially, nothing appeared out of the ordinary.

In this particular case however, several factors should lead the examiner to search for artifacts specific to OneNote. First, the reporting employee saw OneNote was open when Tom was showing secrets about prototype P1-343 to an acquaintance away from the office. Second, OneNote is a program Tom uses, yet the employee did not believe Tom was using his own laptop. Third, Tom could not copy the files to a thumb drive, as the company network policy prevented it. Finally, Tom had full use of Microsoft Office and unlimited Internet access, giving him opportunity to save data to a OneNote web notebook from work. He could then easily share it with another party away from work.

OneNote organizes data in a hierarchical structure similar to a file cabinet. Only instead of the cabinet, drawers, and folders, OneNote uses notebooks, sections, and pages. New users can think of a *notebook* as a file cabinet, a *section* as a drawer, and a *page* as an individual file folder in the drawer. The items on a page are like the loose sheets or notes that are stuffed in the folder. In a physical filing system, sometimes notes are written on the cover of the folder or on the inside of the folder. Pieces of paper and "post-its" are tossed in the folder to keep related ideas and notes together in one place. The file folder may even contain print outs of documents or a CD containing copies of related electronic files. OneNote is an electronic version of this data management. Like a file folder in the cabinet, but electronically, OneNote allows users to insert picture files, print outs of files, screen clippings, audio and video recordings, ink pad writings, and even copies of other files into a page within a section. Sections are stored as *.one* files.

If the examiner hypothesized that Tom inserted the prototype file into OneNote on the local machine, verifying the hypothesis could be as simple as viewing the contents of any .one files in the folder, *OneNote Notebooks*, under Tom's *Documents* folder.

However in checking this location, (C:\Users\<username>\Documents\OneNote Notebooks\), the folder contained no .one files. On the surface then, it appeared that Tom did not create any OneNote notebooks. However, OneNote also stores data in *AppData*. AppData is a system and hidden folder under the user profile's home folder. By default, as a safeguard to keep users from damaging the operating system, Windows is set not to show system or hidden folders. Fortunately, FTK and other forensic tools display all files and folders regardless of those settings. In the AppData folder, OneNote keeps backups of .one files, performs caching of notebook data, and stores server information. OneNote caches notebook sections in the file, *OneNoteOfflineCache.onecache*.

Figure 1 displays 8 search hit results obtained using FTK to search the entire OneNote AppData folder in FTK, for the unique prototype name, "P1-343", (Path searched: C:\Users\<username>\AppData\Microsoft\OneNote\).

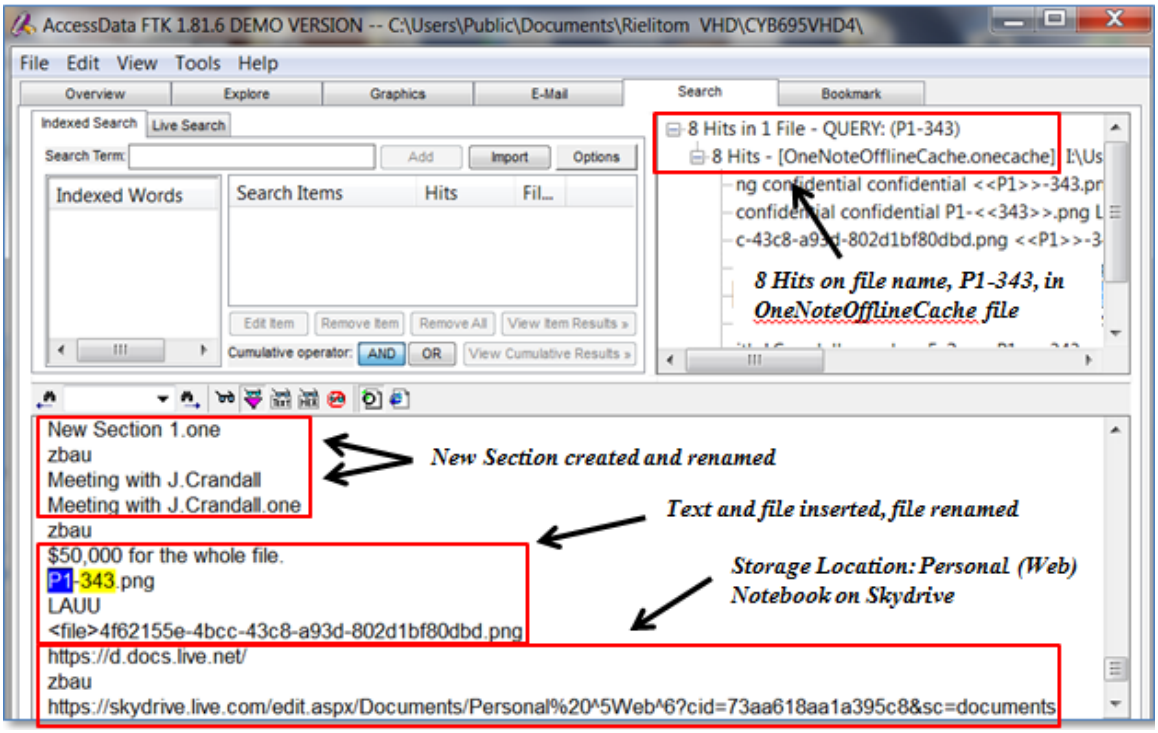

Figure 1. FTK search results of OneNoteOfflineCache.onecache.

The entries in this file documented the user's activities. The user created a new OneNote section, "New Section 1.one," and renamed it, "Meeting with J.Crandall.one". The user added text, "$50,000 for the whole file." The user also inserted a possible graphic file, "P1-343.png". OneNote cached the file to its *OneNoteOfflineCache_Files* folder and references it as, "4f62155e-4bcc-43c8-a93d-802d1bf80dbd.png". *Personal (Web)* and the storage path indicates a web notebook stored in the Microsoft cloud, *Skydrive*.

The information gained in the "P1-343" search could lead the examiner to further hypothesize that the file inserted is a graphic of the prototype and the meeting was a sale to a "Mr. Crandall" for "$50,000." This hypothesis must be verified one step at a time, starting with the file that was inserted. One method to verify the contents of the file is to locate the file in OneNote's cached files folder. Similar to temporary Internet files and saved web pages, OneNote caches files related to its sections into a folder, *OneNoteOfflineCache_Files*
(Folder Path: C:\Users\<username>\AppData\Microsoft\OneNote\14.0).

The cache folder is helpful because a file name and extension are not enough to prove the file inserted into the OneNote section contained company secrets. Any file could be named "P1-343.png." By comparing the cached files with the results from the P1-343 search, the examiner could verify the contents of the specific P1-343.png file that was inserted. FTK explorer was used to browse the OneNote cache file folder and view the contents of each cached file. The results from the P1-343 search indicated that OneNote referenced the inserted file as, "4f62155e-4bcc-43c8-a93d-802d1bf80dbd.png". Sorting the list by file name in FTK explorer would make it easier to locate the file, "4f62155e-4bcc-43c8-a93d-802d1bf80dbd.png". Once located, selecting the file displays

the contents in the FTK viewing window. In this case, the expectation was that the file, "P1-343.png," that had been inserted into the OneNote section, would contain a graphic related to prototype P1-343. Figure 2 displays the contents of the OneNoteOfflineCache_Files folder as viewed in FTK. The file list was sorted by file name to find, "4f62155e-4bcc-43c8-a93d-802d1bf80dbd.png", the file name used by OneNote to reference, "P1-343.png."

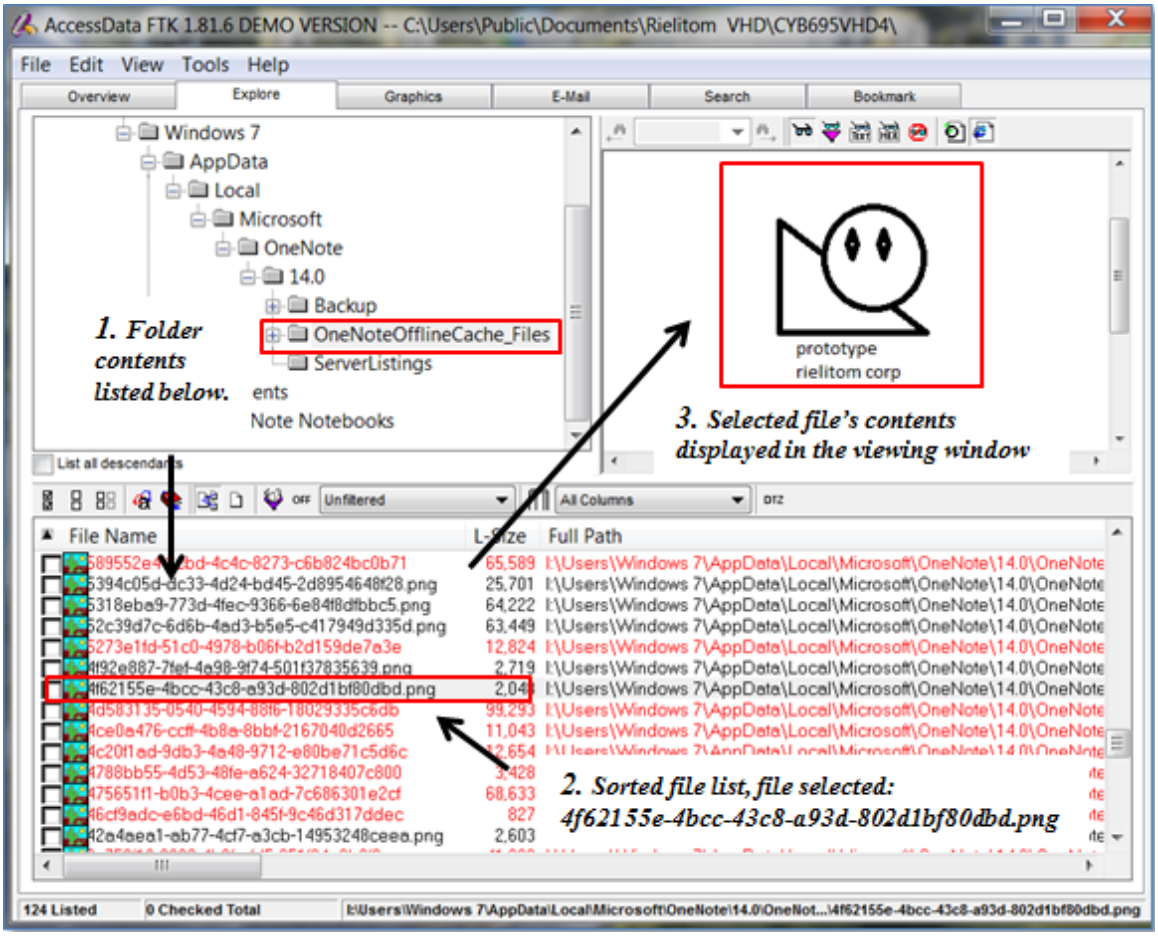

Figure 2. FTK Explorer display of *OneNoteOfflineCache_Files* folder.

Browsing the list allowed the file, "4f62155e-4bcc-43c8-a93d-802d1bf80dbd.png" to be easily located and displayed. The viewing window in FTK indicated the file contained a graphic of prototype P1-343. The Rielitom owner verified this was a sensitive file. He was also familiar with a male named Crandall. The next logical step to continue testing

the hypothesis would be for the examiner to determine the Skydrive account that was used and to issue a letter of preservation while a search warrant is crafted for the contents of the SkyDrive and Mr. Terces financial records.

Discussion

Tom had legitimate access to all prototype files, including P1-343.png. The existence of the file and references to the file name, were expected in all areas of the drive. The large number of legitimate file accesses and references that would be seen in a case such as the Rielitom case, could lead to complacency during the examination. However, a prudent examiner looks at all the details and puts together a hypothesis from which to investigate how the file could have been leaked from the company network. The examiner must test his or her hypothesis while keeping an open mind to all other possibilities. The details from the coworker and company owner coupled with OneNote's storage and caching systems, led the examiner to the conclusion that Tom used a personal (web) notebook to sneak the prototype file out of the company's network without using removable media. Tom was known to be a user of OneNote with unlimited Internet access at work, was considered to be computer savvy, had legitimate access to sensitive files, and could not use removable media to sneak a file out. Further, Tom was observed by a coworker showing the prototype to another person in a bar while talking about dissatisfaction with his salary. Had the examiner stopped at checking only the local storage folder for OneNote files, Tom might have been cleared, or at best, the situation would have been left to question.

The knowledge of how OneNote stores details about a user's actions, and the understanding of OneNote's file caching mechanism were paramount in discovering and

explaining Tom's activities to verify the examiner's hypotheses. OneNote's features are far more reaching than the simple example that was offered in the scenario. However, the scenario should provoke thought and further research on the topic. With the availability and cross platform apps today, OneNote usage will continue to rise. Examiners need research that will assist them as they are faced with cases involving OneNote.

History of OneNote from 2010 to 2012

Microsoft's bloggers touted in June 2010 about the release of web apps for its popular Office products. Web apps are components of SkyDrive and include lightweight versions of Word, PowerPoint, Excel, and OneNote. The web apps program manager for Microsoft blogged in June 2010, notifying users that the web apps featured the ability to open OneNote notebooks directly in the browser (Simons, 2010). Through a free Windows Live account, users can access limited storage in a private SkyDrive, and then create, store, and share Office documents via web apps, without having to open Office programs (Microsoft Support, 2012). On January 18, 2011, Microsoft released the first OneNote app for iPhone, through Apple's App Store (Numoto, 2011). Later that year, on December 12, 2011, Microsoft released version 1.3, geared for the iPad (Apple App Store, 2011). On February 7, 2012, Michael Oldenburg, a Technical Writer in the Office Division of Microsoft, announced the release of OneNote for Android, which could be downloaded through the Android Market app store (Oldenburg, 2012).

Figure 3 is a timeline of the significant OneNote and SkyDrive releases from 2010-2012 affecting the current availability of OneNote.

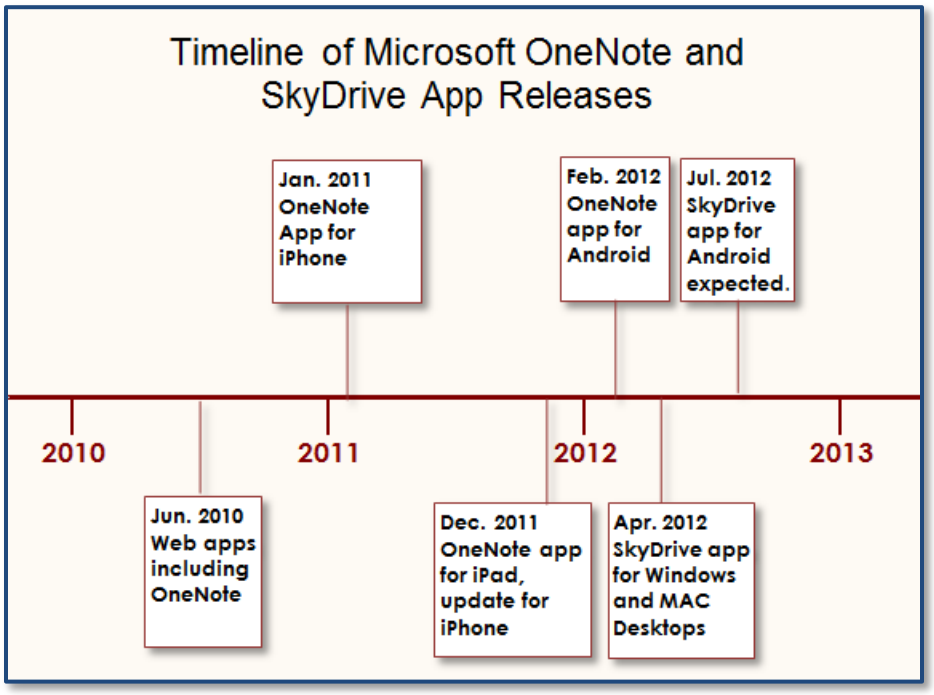

Figure 3. Timeline of Significant Microsoft OneNote and SkyDrive releases.

Today, tablet and cell phone users of all three leading mobile operating systems, Microsoft Windows, Apple iOS, and Android, can interact with OneNote files via their specific mobile apps or a browser using web apps in their SkyDrive. OneNote mobile may be the key for Microsoft to lure new users, connecting them to SkyDrive in the process. Microsoft's mobile app campaign appeared successful, resulting in thousands of OneNote app installs. For instance, according to Google Play's OneNote app page (2012), from April 12, 2012, to May 11, 2012, between 500,000-1,000,000 Android users installed OneNote mobile. The OneNote app page displays the statistics in a graphical trending chart showing the install history for the last 30 days ("About this app," chart).

Figure 4 displays screen clippings capturing the Google Play OneNote charts posted on May 11, 2012 (assuming installs between April 12-May 11) and June 23, 2012 (assuming installs between May 24-June 23) on Google Play.

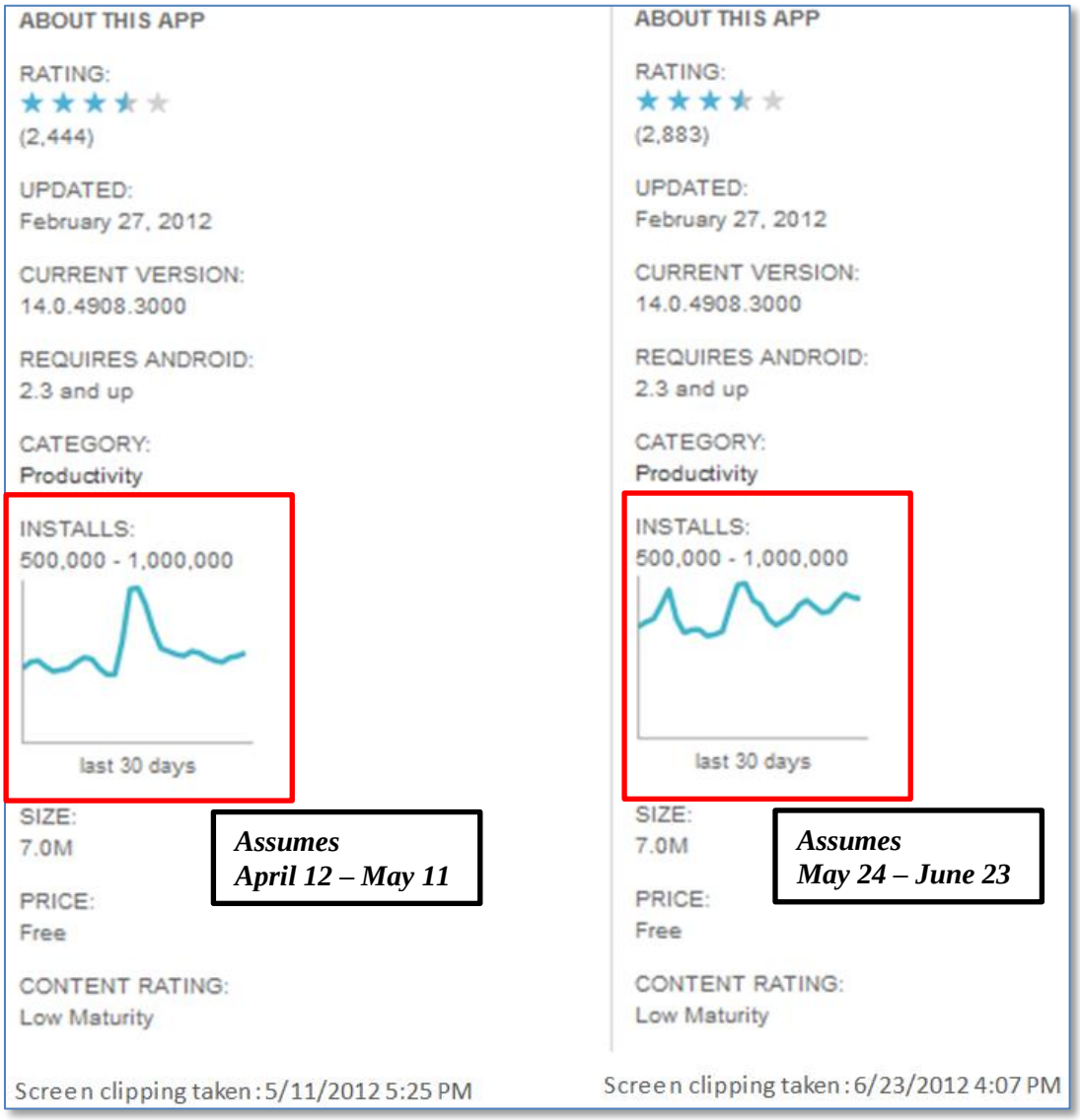

Figure 4. Google Play OneNote app installation trending charts.

These charts were captured by screen clipping on May 11, 2012 and again on June 23, 2012. They show a trending pattern that appears to be increasing and leveling off to a steady stream of installs ("About this app," chart). As for Apple installs, according to the

Associated Press in the *Huffington Post*, *March 6th edition*, for the week ending March 5th, 2012, the Microsoft OneNote App for iPad made it to the top ten, ranked the 8th most installed free app, ahead of the apps for "Weather Channel Interactive" and "iBooks".

Some Examiners who have encountered OneNote files reported finding them difficult to work with during their examinations. One examiner in particular located files with an extension of *.one* that appeared to be case relevant and wished to view the contents. The examiner's research revealed the files were OneNote files. Lacking the knowledge to analyze OneNote files, the examiner solicited assistance by posting in a support portal forum for a popular forensic suite, *EnCase.*

> How can we access to the contents of the Microsoft OneNote files or How to decrypt this kind of files? …these kind of files have a "one" extension and in a case I'm dealing with, i have a lot of these files with relevant names, (interesting filenames). However, how can I access the content of the files or, in other words, how can I decrypt the file?
>
> Thanks in advance!
>
> 12-11-2009 05:38 PM (Guidance Software, 2009, para. 1)

Kindly, another user responded:

> the format is not supported (yet) by the Outside In viewer, and looks like the recommended approach is to download the trial version of OneNote:
>
> http://blogs.msdn.com/chris_pratley/...te-viewer.aspx
>
> The file format itself is documented by microsoft, and claims to be "a revision based format" which implies the files carry around older revisions with potentially

> interesting data, should you feel like tackling the decoding. (Guidance Software, 2009, para. 2)

In these 2009 posts, neither the initiator nor the responder was familiar with OneNote files. Now in 2012, OneNote is available as an app, downloaded daily in the mobile app stores. OneNote is also automatically included on Windows phones and in Microsoft Office suite. With OneNote so readily available and Microsoft's efforts to market OneNote mobile and web apps, it is only natural that users will try it out. New apps like OneNote that become popular create the need for examiners to become familiar with its associated files, reinforcing the relevance of this research.

Familiarization Techniques for Examiners

An accepted practice for examiners to become familiar with a new application and its files is to install and use it themselves. When users keep track of the changes that take place upon installation and usage and publish them in a document, it is a *whitepaper*. Examiners test and validate whitepapers by attempting to follow the steps described in the document, and comparing their own results to the results described in the paper. Once vetted, the whitepaper becomes a guide for examiners to follow as they conduct an examination involving the application and its data files. It is more efficient for examiners to build off of previously written whitepapers rather than starting from scratch. It perpetuates the cycle of testing and validation of previous and new research. In the literature review section of this study, the lack of whitepapers and instructional writings are what drove the research, resulting in the testing and documentation of methods used to investigate a case involving OneNote. Other researchers will test and validate the assertions in this study, in their future research projects.

Artifacts Associated With Various OneNote installations

The installation process and some operating system artifacts for OneNote are predictable for each device type and operating system. The artifacts will vary among the different installations and usage. For instance, variations in the artifacts occur when OneNote is installed on a local machine, rather than running it from the cloud. Thoroughly processing a case involving OneNote files, requires a forensic examiner to become familiar with the different installation methods, the OneNote file structure, and the tools and techniques to parse data from OneNote files.

OneNote may be installed on a PC as a standalone product or as an optional component of Office. This research used a full installation of OneNote as an Office 2010 component on a Windows 7, x64 PC platform. OneNote's mobile app may be installed on an iPhone, iPad, iPod, Windows Phone 7, or on various Android phones and tablets. This research used an ASUS Transformer Prime TF-201 tablet running the Android version 4.0, Ice Cream Sandwich (ICS) platform. The SkyDrive app, used to access OneNote files stored in the Microsoft cloud, may be installed on Windows or Mac computers. This research used a SkyDrive app installed on a Windows 7, x64 PC and a MacBook Pro running OS X (Lion), to access OneNote web notebooks stored in a user's SkyDrive. Once installed, OneNote notebooks accessed either locally or on a Microsoft SkyDrive, leave artifacts that may be collected to prove or disprove the usage of OneNote occurred. Artifacts collected from various installs and devices make up a large portion of this research. These examples will provide insight to examiners encountering cases involving OneNote.

OneNote Artifacts When Installed on a Windows PC

OneNote installations on a Windows PC leaves several artifacts that may help determine the install location, date, and time when the installation occurred. In Windows 7, the Windows event log files are at C:\Windows\System32\winEvt\Logs. These files should be extracted from an image of the subject hard drive. The files cannot be extracted while Windows is in use. Using the Windows native viewer in the Control Panel, the Application log can be opened by selecting the option to O*pen Saved log* from the A*ction* menu and navigating to the location where the extracted event log files were saved. The Application log file may be searched for "OneNote" to find entries relating to the date and time of the installation and whether it was successful.

The OneNote install date, time, and location details can also be determined in a Windows PC by enlisting the assistance of a tool that automatically parses and displays the contents of the *prefetch* folder. Windows keeps track of each executable file and its associated dependent files as they are run. In doing so, Windows creates a *.pf file* in the prefetch folder for future reference in case the user runs that program again, preloading the necessary components. Prefetch entries contain date, time, and location information about where the executable and dependent files are stored. Nir Sofer has published *WinPrefetchView*, a tool that parses and displays the prefetch files located in C:Windows/Prefetch. The resulting list can be sorted or just scrolled through, to search for "OneNote." The findings may help determine when the installation file was launched, where it was launched from, and where the dependent files are stored. The tool also has an option to create an HTML report of selected items (Sofer, 2010).

All changes made to the system by installing OneNote on a Windows PC can be documented through a process of capturing a baseline of the system state before installing OneNote, and then comparing the system state again after the installation. *WhatChanged* is a freeware utility from Vista Software that automates this process. With this tool, the user takes a system snapshot before an event, runs the event, and takes a second snapshot. The tool compares the two snapshots reporting the changes that have occurred since the first snapshot (Vista Software, 2011). Documenting the new or changed files and folders created before and after installation, will give the examiner a baseline of what to look for in a system where OneNote was installed.

The install location and various settings can also be obtained by viewing the associated entries in the Windows Registry. A tool such as *Registry Viewer* from AccessData is helpful to parse and browse the software hive from the Windows registry at the path, Software\Microsoft\Office\14.0\OneNote\InstallRoot (Access Data Corp., 2006). Another registry file that contains user settings, *NTUSER.DAT*, is located in the user's home profile account folder. In Windows 7, the NTUSER.DAT is located at C:\Users\<ProfileName>\. NTUSER.DAT contains the individual user preferences and activity settings. The file must be opened using a registry file viewer such as the Registry Viewer or Windows native registry viewer, *Regedit*. A rather significant artifact that can be obtained from the NTUSER.DAT file is the location of recently accessed, saved and backed up notebooks. These values may help determine if a user stored a OneNote notebook locally, on a network share, on a Sharepoint server, or in a SkyDrive. If a user had notebooks open at the time of forensic imaging, then Software\Microsoft\Office\14.0\

OneNote\OpenNotebooks in the registry might offer clues about any offsite notebook accesses.

The concept of SkyDrive notebooks connected over the Internet suggests the analysis of Internet history may uncover additional artifacts. Internet history files should be extracted from the user account within the acquired image. An alternative is to mount the image using AccessData's FTK *Imager version 3+*, and use a tool such as Digital Detective's *NetAnalysis* to parse the Internet history (AccessData, 2012; Digital Detective, 2012). All of the installation artifacts change, or will not be present, if OneNote is used in an alternative method like through the SkyDrive app, mobile apps, or directly from the web app.

OneNote Artifacts: SkyDrive App on Desktops

Windows 7. According to information on the Microsoft website (2012), *SkyDrive System-Requirements* page, users can download and install the SkyDrive app for systems meeting the following requirements:

> 32- or 64-bit version of either Windows 8 Consumer Preview,Windows 7, or Windows Vista with Service Pack 2 and the Platform Update for Windows Vista, or Windows Server 2008 R2, or Windows Server 2008 with Service Pack 2 and the Platform Update for Windows Server 2008, or Mac OS X 10.7 Lion. (para. 1)

Installing the app will create a SkyDrive folder that can be accessed just like any other folder through Windows Explorer at the folder path, "C:\Users\<ProfileName>\." Using OneNote in conjunction within the SkyDrive, users can create, edit, share, and delete web notebooks. If available, OneNote automatically synchronizes changes to the SkyDrive. If

not, OneNote stores the changes and synchronizes when the SkyDrive connection becomes available again.

MAC OS X Lion. Similar to Windows, SkyDrive can be downloaded and installed on MAC OS X (10.7) Lion (Microsoft, 2012). The installation creates a "SkyDrive" folder that can be accessed from the MAC just like any other folder, but the files are stored on the user's SkyDrive. OneNote itself is not available as a full installation for MAC. However, with the OneNote web app used in conjunction with the SkyDrive, MAC users can create, edit, share, and delete notebooks.

It is imperative that examiners consider the role of forensic artifacts when OneNote is used in conjunction with SkyDrive or any cloud services. In cases where the user stores OneNote files directly to the cloud, obvious artifacts may be scarce. However, a deeper examination may uncover helpful artifacts. For instance, operating systems keep track of network connections, update Internet history, and recent file lists. Operating systems may also store temporary Internet files, as well as snippets of files, in RAM and the page file. Examiners do themselves a service when they include a memory capture (take a snapshot of RAM before shutting the machine down) as part of their routine data collection. The memory may contain remnants of files opened from SkyDrive, or details of the running processes, showing the usage of web apps and accesses to the SkyDrive. Knowing what to search for requires an understanding of the OneNote file structure and its features. Examiners who lack experience with OneNote files will seek whitepapers and previously conducted studies, drawing upon the experience of other examiners.

OneNote Artifacts: OneNote Mobile Apps

The forensic implications of artifacts left by OneNote installed as an app on a mobile device or tablet are starkly different from a PC. There is no Windows application event log or familiar Windows registry to glean OneNote details. These devices often have no removable storage and can only be accessed by connecting them to a computer over a cable. Specialized skills are needed to work with these mobile devices.

iDevices. The OneNote App from the Apple Store (iTunes) can be installed on iDevices. According to its documentation on the App Store (2011), users who install OneNote can create searchable text notes, which are always available on their SkyDrive. Installation requires iPhone, iPod, or iPad with iOS 4.3 (Requirements section).

Android Devices. OneNote mobile may be downloaded from the Google Play store for Android devices running 2.3 or newer. Once installed, an icon for OneNote Mobile appears on the Android's desktop. When clicked, OneNote opens a local cache of notebooks and attempts to sync with the SkyDrive.

OneNote Artifacts: Browser Web App

Groups of users who are all using HTML5-compatible browsers like Firefox 4, Google Chrome, Internet Explorer 9, Opera, or Safari can work together at the same time in a shared OneNote Web notebook (Matthews, 2011). Using this method, when any of the users makes changes, SkyDrive is able to save them online in one place. Each user's updates or additions to the notebook are recorded. The *view authors* feature allows all users to see each other's updates in near real-time. SkyDrive keeps track of the previous 25 versions automatically. Changes are easy to undo by restoring or downloading an older version using the *Show Page Versions* feature (Microsoft, 2012). The actions a user

performs in OneNote apps still have to be run through the processor and memory. Operating systems commonly use some form of swapping data between virtual memory (pagefile) and RAM (Random Access Memory) for efficiency. These areas should not be overlooked when searching for OneNote artifacts. They should be searched for OneNote files by signature (file header, and sometimes footer).

OneNote File Structure

File Header

Sometimes it is necessary for an examiner to search for a deleted, damaged, or partial file. A thorough search of a hard drive includes all areas including the system files, unused disk areas, and a search of the memory. All or part of a file may be recoverable using an advanced searching technique which requires locating the file by recognizing its contents. Examining several OneNote *.one* files for the common first few bytes establishes the pattern that is common at the beginning of all .one files. The first 16 bytes are always the same hexadecimal codes, "E4 52 5C 7B 8C D8 A7 4D AE B1 53 78 D0 29 96 D3." These bytes are called the file *header*, or *signature*. Forensic tools can be used to search for a file's signature. This is a common technique used by analysts, to locate and carve files. As a method of testing the file header to see if it could be used successfully to locate OneNote files, EnCase Forensic version 6.18 by Guidance Software (now available in version 7) was configured with a new file signature to search for OneNote file headers (Guidance Software, 2012). EnCase Forensic comes with Microsoft Office file signatures built-in, but OneNote was not among them.

Figure 5 shows the results of searching by the added file signature in EnCase (set up as a Grep, case sensitive expression, \xE4\x52\x5C\x7B\x8C\xD8\xA7\x4D\xAE\xB1\x53\x78\xD0\x29\x96\xD3). EnCase located several instances of the OneNote file header.

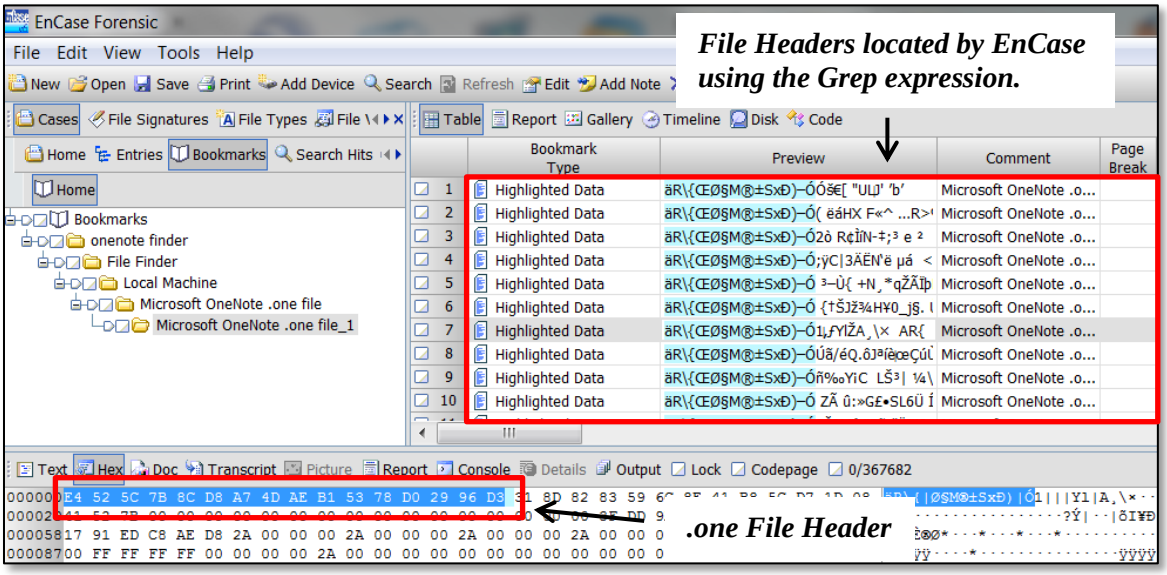

Figure 5. OneNote files located by file header in Guidance Software EnCase.

Data carving is helpful to recover deleted, damaged, or partial files.

Recycle Bin, Backup and Cache

OneNote keeps its own type of recycle bin and backup system. Though a user may have deleted a page, it could be stored in the OneNote recycle bin. A user can configure the frequency of backups and the storage location for backups and other important files. The settings are accessed by the user within OneNote in the *File*, *Options* menu. The user can select the location for *Unfiled Notes Section*, the *Backup Folder*, and the *Default Notebook*. The frequency and number of backups to keep on file can be customized as well. How much unused space to allow in files before optimizing occurs, can be set to a percentage. Even the *Cache file location* can be chosen by the user. David

Rasmussen (2006) blogged about OneNote synchronization and how to use a OneNote file between multiple computers. He explained that OneNote writes everything to a cache file location and then later quietly synchronizes with the actual file data. This way, if a network file is in use, and the network becomes unavailable, the user can continue working. When the connection is restored, the file will be synchronized. Rasmussen added that this feature is also handy for those who store their OneNote notebooks on a removable media because they can work between computers (Rasmussen, 2006).

Any notebook that has been opened on a local machine will have parts of it cached. Sometimes the whole notebook section is cached. Even web notebooks may have parts cached in OneNote's internal caching system or the operating system's paging file. Given this feature, analysts should always conduct a search by file header and unique keywords to find all OneNote files, or remnants of cached data, within the hard drive from the local machine. OneNote stores deleted pages for up to 60 days before actually deleting them. It has its own built in recycle bin, *OneNote_DeletedPages.one* (Pierce, 2011). Figure 6 displays OneNote headers that were detected in the operating system's page file and in OneNote_DeletedPages.one.

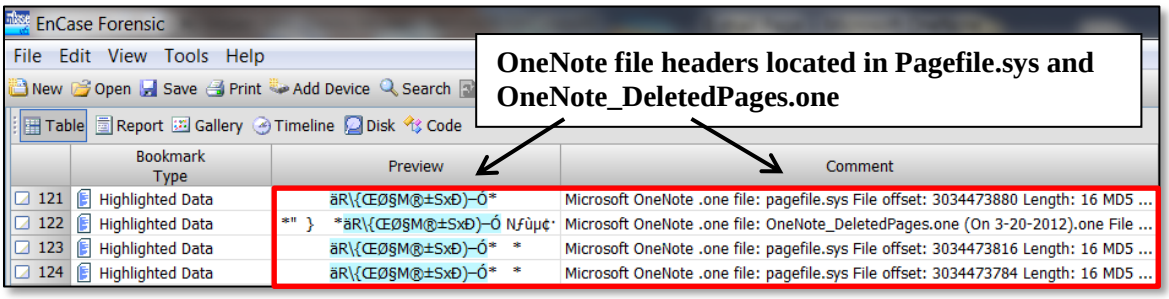

Figure 6. Encase .one header search of pagefile.sys and OneNote_DeletedPages.one.

With its own built-in recycle bin and paging system, OneNote has the potential to contain a large amount of case relevant data. Typical users will be unaware of the continued

existence of data they have deleted, or never intentionally saved to the local machine. Examiners who are familiar with the forensic artifacts of OneNote will know where to start looking for deleted .one files and backup copies. They will also know how to discover the deeper OneNote artifacts hidden within the files themselves. As new cases involving OneNote emerge, many examiners will be forced to study the forensic artifacts of OneNote all at once. They will reach out to other examiners or conduct Internet searches, trying to understand this complex application, having its own internal recycle bin, backup, and caching system. This body of research will be a starting place for them.

Recommendations for the Future

Develop OneNote Forensic Guidelines

A guideline of protocols should be developed that examiners may follow when conducting an investigation involving OneNote. The research will require many tedious hours of testing and validation. The researcher's time is largely spent documenting steps taken and the results, and recreating the work to validate the results. It is a project worthy of its burden. Many forensic examiners will benefit from the published results, saving countless hours of on-the-fly learning when working a critical case involving OneNote. More documentation of actual cases involving OneNote and the techniques used to discover evidence are important steps to developing these guidelines.

Persuade Mainstream Forensic Suites to Recognize OneNote

OneNote and its files may appear obscure when compared to the files examiners see in daily examinations. However, the simple but not uncommon, Rielitom scenario presented in the *literature review* section in this study, demonstrates the need for the OneNote file type to be recognized by the mainstream forensic suites. The fact that

OneNote is likely to emerge in more examinations (cross platform – PC, MAC, and mobile apps), it makes sense that the most common forensic suites should include file headers to search for the OneNote file types. The Mainstream forensic suite providers should be urged to include the OneNote file headers in their default set or as an update. The software providers including the OneNote header would cut down on the time an examiner must devote to determining the proper hexadecimal code and adding the file header (a skill that requires training initially and must be developed over time), as demonstrated in *File Structure: File Header*, in this study. It would also help examiners who are unfamiliar with OneNote to find hidden .one files and to recover lost, damaged, or partial files.

Research SkyDrive Artifacts

In addition to understanding OneNote, a new topic of concern became apparent. All Office apps, not just OneNote, integrate easily with SkyDrive. Research needs to be conducted on the artifacts created by interaction with SkyDrive. Areas of research that deserve attention are 1) SkyDrive as a repository of data, 2) SkyDrive as an instrument used with web apps, 3) SkyDrive's network sharing permissions, and 4) The network traffic generated when connected to a SkyDrive. In the Rielitom scenario in this study, a user was able to sneak data from the company network to a SkyDrive, bypassing local security measures (prohibited removable media). Even the web apps of the Office applications leave some trace on the computer used to access those files. These areas need research and testing to document where examiners should begin when there is an indication that SkyDrive was used.

Conclusion

Relevance of OneNote Artifacts

Microsoft OneNote is a powerful data management application that integrates with other Microsoft Office products. It can even be run from the web without installation on the local machine. Since 2010, Microsoft has released free web versions of its Office apps for PC and MAC, including OneNote. In addition to the desktop version of OneNote and the SkyDrive desktop app, starting in 2011, mobile apps were also released for all mainstream mobile devices including iOS and Android (Simons, 2010; Microsoft Support, 2012). Forensic examiners can now expect to start seeing OneNote files during their investigations. There is so little awareness and documentation for examiners about the forensics of OneNote that its artifacts could easily go ignored or improperly analyzed. Yet, those artifacts could be the smoking gun in the investigation.

OneNote Forensic Techniques

The only documentation found offering a method for examiners to work with .one files, suggested just opening the files in the native application, OneNote (Guidance Software, 2009). This method does allow limited access to the artifacts, but does not address the entries in the cache file, which may contain the smoking gun or clues to offsite storage locations. When a user stores OneNote files directly to a SkyDrive web notebook, the cache file may contain clues that will assist in the investigation explaining not only the method used, but may show intent. The literature review in this study used a scenario to demonstrate how OneNote might be used to facilitate a crime. A web notebook was created on a SkyDrive and accessed from OneNote installed on a local machine. A new section was created in the web notebook. Text and a graphic file were

inserted into the section. The cache file, "OneNoteOfflineCache.onecache," was immediately analyzed and artifacts were collected. Supplemental research and testing are needed to determine when the cache file is overwritten. This study does not address how long an examiner can expect data to remain in the cache file.

Lack of Foundational Research

Examiners test and validate whitepapers by attempting to follow the steps described in the document and comparing their own results to the results described in the paper. The lack of whitepapers on OneNote forensics was an obstacle for this study that propelled the research forward and confirmed its necessity. Through lengthy testing and analysis, the OneNote file structure and its features were examined to determine how OneNote could be exploited to perpetrate a crime.

The findings were delivered through the use of a hypothetical criminal case scenario where OneNote was central to the crime. In the scenario, a computer savvy employee used OneNote to leak company secrets. A walk-through delivery style was used to present the examination of the employee's work computer. OneNote's internal file caching system contained the keys to solving how the suspect leaked the company secrets by inserting a file into a OneNote web notebook. The web notebook was stored in his SkyDrive on the Internet. On the surface it appeared there were no OneNote notebooks on the computer. However, an in depth examination of specific system files within OneNote revealed evidence of how the secret was leaked.

The scenario was designed as evidence based persuasion to demonstrate why examiners need to become familiar with OneNote and its capabilities. Conscientious examiners will read the scenario and recognize that it was due to the understanding of

OneNote's caching features, and how it integrates with the cloud, that the examiner did not overlook the smoking gun. Examiners who are not familiar with OneNote could easily have missed the smoking gun.

Bridging the Gap

Though it has been around for years, OneNote is still in its infancy, having only been available freely in SkyDrive since 2010 and to the mobile app stores since 2011. Understandably, there is no foundational research for examiners to draw upon. Prudent examiners tenaciously research any unfamiliar file. However, at the present time, their efforts would be unfruitful when searching for forensic details about .one files. The current lack of available whitepapers or any substantial research on the forensics of OneNote could be devastating to an investigation. Examiners have little or no guidance in place for finding OneNote artifacts. The scarcity of documented research, coupled with the relatively "new" OneNote, could result in the guilty remaining free to harm again, or the innocent suffering injustice for lack of uncovering the keys to exoneration.

This study was intended to produce an understanding of the significant artifacts created by OneNote, and to inspire researchers to conduct more in depth testing and analysis. Pioneering this type of foundational research is based in part on experience, and in part on investigative instinct. Providing it to the forensic community bridges the gap in available research on the forensic artifacts of Microsoft OneNote. The artifacts offered in this study are only a starting place. Hopefully more researchers and investigators will devote time to studying the forensic artifacts of OneNote, providing their findings to the forensic community as well. In doing so, they make an exciting contribution to the body

of knowledge for others to draw upon when they need it most, during an important investigation involving OneNote.

Bibliography

Access Data Corp. (2006). *adownloads.* Retrieved April 16, 2012, from http://accessdata.com/support: http://accessdata.com/support/adownloads

AccessData. (2012). *ftk.* Retrieved July 5, 2012, from accessdata.com: http://accessdata.com/products/computer-forensics/ftk

AccessData. (2012, March 21). *FTKImager_UserGuide.pdf.* Retrieved July 9, 2012, from accessdata.com: http://accessdata.com/downloads/current_releases/imager/FTKImager_UserGuide.pdf

Apple App Store. (2011, December 11). *Microsoft OneNote.* Retrieved May 22, 2012, from itunes.apple.com: http://itunes.apple.com/us/app/onenote/id410395246

Associated Press. (2012, March 6). *The top iPhone and iPad apps on App Store.* Retrieved May 12, 2012, from Huffington Post: http://www.huffingtonpost.com/huff-wires/20120306/us-itunes-apps-top-10/

Carvey, H. (2012, April). *Interview with Harlan Carvey.* Retrieved June 13, 2012, from f-interviews.com: http://f-interviews.com/2012/04/11/interview-with-harlan-carvey/

Digital Detective. (2012). *netanalysis.asp.* Retrieved July 9, 2012, from digital-detective.co.uk: http://www.digital-detective.co.uk/netanalysis.asp

Edwards, T., & Edwards, L. (2012, April 4). *OneNote 2010 Sort Utility.* Retrieved June 4, 2012, from sqlservertimes2.com: http://sqlservertimes2.com/?p=804

Google Play. (2012, Apr-May). *OneNote Mobile.* Retrieved May 10, 2012, from Google Play: https://play.google.com/store/apps/details?id=com.microsoft.office.onenote

Guidance Software. (2009, December 4). *Support Portal.* Retrieved May 11, 2012, from Guidance Software: https://support.guidancesoftware.com/forum/showthread.php?t=36548&highlight=onenote

Guidance Software. (2012). *encase-forensic.* Retrieved July 5, 2012, from guidancesoftware.com: http://www.guidancesoftware.com/encase-forensic.htm

Matthews, L. (2011, June 21). *SkyDrive update brings HTML5-powered awesomeness.* Retrieved May 25, 2012, from www.geek.com: http://www.geek.com/articles/news/skydrive-update-brings-html5-powered-awesomeness-20110621/

Microsoft. (2012). *SkyDrive and Office work together.* Retrieved May 24, 2012, from windows.microsoft.com: http://windows.microsoft.com/en-US/skydrive/work-together-online

Microsoft. (2012). *SkyDrive system requirements.* Retrieved May 22, 2012, from windows.microsoft.com: http://windows.microsoft.com/en-US/skydrive/system-requirements

Microsoft Support. (2012). *Using Office Web Apps in Skydrive.* Retrieved May 22, 2012, from office.microsoft.com: http://office.microsoft.com/en-us/web-apps-help/using-office-web-apps-in-skydrive-HA101231889.aspx

Numoto, T. (2011, January 18). *Starting today, OneNote Mobile for iPhone helps free your ideas.* Retrieved May 22, 2012, from blogs.office.com: http://blogs.office.com/b/office-exec/archive/2011/01/18/onenote-mobile-for-iphone-helps-you-free-your-ideas.aspx

Oldenburg, M. C. (2012, February 7). *OneNote Mobile for Android is now available worldwide.* Retrieved May 22, 2012, from blogs.office.com: http://blogs.office.com/b/microsoft-onenote/archive/2012/02/07/onenote-mobile-for-android-is-now-available-worldwide.aspx

Pierce, J. (2011). *MOS 2010 Study Guide for Microsoft OneNote* (Kindle Edition ed.). OReilly Media.

Rasmussen, D. (2006, June 29). *David Rasmussen's Blog.* Retrieved April 16, 2012, from http://blogs.msdn.com: http://blogs.msdn.com/b/david_rasmussen/archive/2006/06/29/650705.aspx

Simons, N. (2010, June 7). *Office Web Apps Blog.* Retrieved May 22, 2012, from http://blogs.office.com: http://blogs.office.com/b/officewebapps/archive/2010/06/07/office-web-apps-now-available-on-windows-live.aspx

Sofer, N. (2010). *win_prefetch_view.html.* Retrieved April 16, 2012, from http://www.nirsoft.net: http://www.nirsoft.net/utils/win_prefetch_view.html

Vista Software. (2011). *Whatchanged.* Retrieved June 11, 2012, from http://www.vtaskstudio.com: http://www.vtaskstudio.com/support.php