Fight crime.
Unravel incidents... one byte at a time.

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?
Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (FOR508)
Insider Threat
The Theft of Intellectual Property in Windows 10

GIAC (GCFE) Gold Certification

Author: Eduard du Plessis, duplessiseduard@gmail.com
Advisor: Hamed Khiabani, Ph.D.
Accepted: March 7th 2021

Abstract

The prevalence of the theft of intellectual property investigations has grown over the past years and when investigated it will most likely be on a Windows 10 machine. It is important to have a clear framework on how to approach and execute such an investigation accurately and timeously. In this paper we will identify and analyse important Windows 10 artefacts that will reveal the user, the file and folders opened, applications used and the location of the files and folders. These artefacts are LNK (Link) Files, Jump Lists, Shell Bags, Prefetch files, USB connections and Network Mappings. We will demonstrate how to acquire and analyse these artefacts using a set of lightweight and powerful digital forensic software tools that are also affordable. The reader will find that by systematically analysing and correlating artefact events a timeline can be build that tells a story.
1. Introduction

In the five years since the release of Microsoft Windows 10 in July 2015, its market share has grown to almost 60% of the global operating system market and 68% of the Windows computer market (Keizer, 2020). The chance of investigating a Windows 10 computer during any investigation is therefore high.

Clients and management are usually anxious about the outcome of these investigations as internal disciplinary processes and legal action such as Anton Piller orders depends on the findings. The aim of this paper is to present to the reader the knowledge to investigate the theft of intellectual property on a Windows 10 computer when there are time and budget constraints.

To timeously get results when presented with an ever-growing data landscape that includes operating system artefacts, logs, internet history, user files, clouds can be difficult. The focus of the analysis will therefore be on a selection of six Windows artefacts called LNK (Link) Files, Jump Lists, Shell Bags, Prefetch files, USB connections and Network Mappings. These artefacts will be explained, acquired, analysed and finally correlated into a timeline.

Selective acquisitions of a Windows Server and a Windows 10 workstation will be done as well as the full forensic imaging of a USB drive. X-Ways Forensics will be used for a selective live acquisition of the Windows 10 workstation and in combination with F-Response Consultant for the remote acquisition of the Windows Server. X-Way Forensics is the main software tool used for the analysis and will be complemented by two specialised tools called ShellBag Explorer and USB Detective.

2. Incident

Company X’s CEO resigned and there were serious doubts about his motive for leaving the company. Company X’s IT reported that server logs showed the ex-employee logging into the company server late in the afternoon on his last day at work and working until after 17h00.
A digital forensic consultancy was appointed to investigate the incident. Management insisted that a preliminary report be issued within 48 hours as the ex-employee had access to sensitive information that threatened the future of the company.

The appointed digital forensic consultancy decided to make selective acquisitions of data from the ex-employee’s Windows 10 workstation as well as from the Windows Server 2019.

3. Digital Forensic Tools used in this investigation

X-Ways Forensics was used in combination with F-Response Consultant to acquire data from the Windows Server 2019 over the local network and for the live acquisition of files and artefacts from the Windows 10 workstation. X-Ways Forensics was also the main tool for the recovery and analysis of all acquired data. X-Ways Forensics has been described as a Swiss army knife for digital forensic investigations. It can run from a USB drive and its speed in acquiring and analysing data makes it the preferred tool. X-Ways Forensics 20.1 SR-4 x64 was used in this paper

F-Response Consultant Version 8.0.1.77 was used to establish an encrypted and compressed read-only connection to the Windows Server. It provides read-only access to physical disks, RAM/Volatile Memory, Cloud, Email and Database storage over IP networks. It is easy to use and works very well with X-Ways Forensics.

USB Detective Version 1.6 is a tool that specializes in the recovery of USB device history as well as the parsing of Jump Lists, LINK files and Shell Bags. It gives you more USB device history than most tools and its Verbose Report makes it easy to identity USB devices. In this investigation it was used to do an initial triage of the Windows 10 Workstation to determine if Intellectual Property was stolen.

ShellBags Explorer v1.4.0.0 is an excellent tool written and supported by Eric Zimmerman and is the go-to Shell Bag history recovery tool for many forensic examiners. It was used to recover Shell Bag history from the Windows 10 workstation by parsing registry hives.

Eduard du Plessis, duplessiseduard@gmail.com
4. Windows artefacts analysed

Various Microsoft Windows artefacts are important when determining:

- which files and folders were opened, accessed or copied,
- when they were opened, accessed or copied,
- and where they were located when opened, accessed or copied, for example:
  - on the local computer storage device,
  - on a computer server/network drive or
  - on an external storage device.

One of the more important aspects of these Windows artefacts is that we can track file and folder activity even after the files and folders were deleted. The Windows operating system artefacts we are going to focus on to determine if the theft of intellectual property took place are:

(Please see Appendix A for more information on the above artefacts.)

**Jump Lists** which have been found on Windows systems since Windows 7. They present to the user a listing of recently accessed files grouped per application. Jump lists can be found at the following location (Anisetti, 2015):

```
“%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations”
```

**Shell Bags** holds historic information of folders that were traversed with Windows Explorer. This is also true for folders opened on externally connected USB devices and network drives. It is necessary to parse the NTUSER.dat (Desktop) and USRCLASS.dat (Explorer) registry hives to get the Shell Bag information. Shell Bags can be found at the following registry hive locations (Lee, 2018):

Explorer Access:

```
“USRCLASS.DAT\Local\Settings\Software\Microsoft\Windows\Shell\Bags”
“USRCLASS.DAT\Local\Settings\Software\Microsoft\Windows\Shell\BagMRU”
```

Desktop Access:

```
“NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU”
“NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags”
```

Eduard du Plessis, duplessiseduard@gmail.com
Network connections made by the user can be found at the following locations in the SOFTWARE registry hive for Windows 7, 8 and 10 (Lee, 2018):

“SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Signatures\Unmanaged”
“SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Signatures\Managed”
“SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\NetLd\Cache”

USB media devices connected to the computer by the user leaves information in various places in the Windows operating system with too much information to list here. Please see Appendix A for detailed information.

LNK (link) files that are created by the user or automatically by the operating system when a file is opened. In this paper we will specifically analyse LNK files to determine which files the user opened. LNK files are found at the following locations (Lee, 2018):

Windows XP: “%USERPROFILE%\Recent”
Windows 7, 8 and 10:

“%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\”
“%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\”

Prefetch files are created by the operating system whenever a program is executed. Prefetch files can be found at (Lee, 2018):

Windows 7, 8 and 10: “\Windows\Prefetch\”

5. IT environment

The operating systems on the Windows Server 2019 and the Windows 10 workstation were the most current version and were newly installed for this paper.

Company X’s Server that was investigated:


Investigated workstation: “Windows 10 Pro, Version 20H2, OS build 19042.746”

Digital Forensic Lab computer 1: “Windows 10 Pro, Version 20H2, OS build 19042.746”

Digital Forensic Lab computer 2: “Windows 10 Pro, Version 20H2, OS build 19042.746”

Sandisk Ultra USB drive: “NTFS formatted”

Eduard du Plessis, duplessiseduard@gmail.com
6. Acquisition

As the client did not want a lengthy and expensive process of acquiring and analysing full forensic images of the Windows Server and the employee’s Windows 10 workstation it was decided to do selective acquisitions. This was done using X-Ways Forensics and F-Response Consultant.

Table 1: F-Response’s presentation of the Subject Targets of the acquired server.

Using Remote Desktop Protocol (RDP), the digital forensic workstation connected to the server with administrator rights. F-Response generated a small executable connection agent that was copied over to the target machine and then executed. This created an encrypted and compressed read-only connection between the forensic workstation and the target computer. The target drives were then seen as local drives on the forensic workstation. F-Response added the server’s primary (operating system) and secondary (Active Directory) drives to the forensic workstation as physical drives HD3 and HD4 and logical drives F and G as shown in Table 3.

After a X-Ways Forensics case was created the relevant target drive(s) were added to the case as shown in Table 4. The drives can be added to the X-Ways case as logical or physical drives. Apart from connecting the server’s primary and secondary drives it

Eduard du Plessis, duplessiseduard@gmail.com
would have also been possible to add the server’s RAM/volatile memory to the forensic examiner’s workstation.

![F-Response Management Console](image)

**Table 2: F-Response Console after connections were made to the server’s drives.**

![X-Ways Forensics](image)

**Table 3: Server drives being added to the X-Ways Forensics case.**

The selective acquisition of data from the Windows Server was done after adding the target drives to the X-Ways Forensics case. A forensic X-Ways Evidence File Container (EFC) was created for each acquisition.

The X-Ways Forensics’ Manuel describes the Evidence File Container as follows: “Most file-system level metadata (name, path, size, attributes/file mode, timestamps, deletion status, classification as alternate data stream or virtual file or e-mail message or attachment, ...) and especially the contents of the file are fully retained in

Eduard du Plessis, duplessiseduard@gmail.com
an evidence file container. Also, when a conventional (physical, sector-wise) image is overkill because you need to acquire only selected files and not entire media, containers are recommended.” (Fleischmann, 2020).

Each drive was traversed and filtered to show only files and artefacts that were needed for this investigation. These files and artefacts were then added to the Evidence File Container after which the Evidence File Container was closed and imaged creating an E01 forensic image. The read-only drives were removed from X-Ways and disconnected from F-Response.

![Image of X-Ways Forensics interface](image)

Table 4: The read-only server drives after being added to the X-Ways case.

The selective acquisition made of the Windows 10 workstation was done by running X-Ways Forensics live on the workstation from an externally connected USB drive. A case was created and the local C drive was added to the case. Further steps were performed in the same manner as done with the acquisition of the server.

7. Recovery and Analysis

7.1. Windows Server 2019

After the server’s E01 forensic image was loaded into the X-Ways case, a Refine Volume Snapshot process was run and the Active Directory folders to which the ex-employee had access rights to were scrutinised. The client was concerned that files relating to a Secret Project was stolen. Table 5 shows the Active Directory folders and files that the ex-employee could have accessed. The ex-employee’s username on Active Directory was jdoe.

Eduard du Plessis, duplessiseduard@gmail.com
A total of eighteen Secret Project files were found as listed in Table 5 of which 17 were existing files that were located in the sub-folders of the folder “\X_Folders\Secret Project Data\”. One deleted file was located in the deleted folder called “\X_Folders\jdoe\design”. We therefore know that the user jdoe copied the file called “[secret_project]_detailed_design.pptx” to his Active Directory share and then deleted it.

### 7.2. The ex-employee’s personal USB drive

The company IT department found a USB drive that was handed over to the examiner. The USB drive was imaged and processed with X-Ways Forensics. We can see from a file listing that a 7-Zip file containing all the secret files was found on the USB drive. The listing in Table 6 shows X-Ways traversing the zip file after it was parsed. The listing is of the 7-Zip archive as well as the contents of the 7-Zip archive. At this stage the owner of the USB drive is unknown.

**Table 5: Secret Project files found on the server.**

<table>
<thead>
<tr>
<th>Name</th>
<th>Exists</th>
<th>Path</th>
<th>SHA-256</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>secret_project\detailed_design.pptx</td>
<td>✓</td>
<td>Documents\7z\design</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\final_meeting.pptx</td>
<td>✓</td>
<td>Documents\7z\final</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\market_share_analysis.xlsx</td>
<td>✓</td>
<td>Documents\7z\market_share_analysis</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\price_analysis_1.xlsx</td>
<td>✓</td>
<td>Documents\7z\price_analysis</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\price_analysis_2.xlsx</td>
<td>✓</td>
<td>Documents\7z\price_analysis</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\pricing_decision.xlsx</td>
<td>✓</td>
<td>Documents\7z\pricing_decision</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\progress_1.docx</td>
<td>✓</td>
<td>Documents\7z\progress</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\progress_2.docx</td>
<td>✓</td>
<td>Documents\7z\progress</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\technical_review_1.docx</td>
<td>✓</td>
<td>Documents\7z\technical_review</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\technical_review_2.docx</td>
<td>✓</td>
<td>Documents\7z\technical_review</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>secret_project\technical_review_3.docx</td>
<td>✓</td>
<td>Documents\7z\technical_review</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
</tbody>
</table>

**Table 6: Secret Project files found on the server.**

<table>
<thead>
<tr>
<th>Name</th>
<th>Exists</th>
<th>Path</th>
<th>SHA-256</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents\7z\design</td>
<td>✓</td>
<td>Documents\7z\design</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>Documents\7z\final</td>
<td>✓</td>
<td>Documents\7z\final</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>Documents\7z\market_share_analysis</td>
<td>✓</td>
<td>Documents\7z\market_share_analysis</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>Documents\7z\price_analysis</td>
<td>✓</td>
<td>Documents\7z\price_analysis</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>Documents\7z\pricing_decision</td>
<td>✓</td>
<td>Documents\7z\pricing_decision</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>Documents\7z\progress</td>
<td>✓</td>
<td>Documents\7z\progress</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
<tr>
<td>Documents\7z\technical_review</td>
<td>✓</td>
<td>Documents\7z\technical_review</td>
<td>46231573510407642013694574212010</td>
<td>20210109 10:30:46</td>
</tr>
</tbody>
</table>

Eduard du Plessis, duplessiseduard@gmail.com
7.3. Comparing the Server and USB drive files

It was noticed that the USB drive contained files belonging to the Secret Project. Therefore, the Secret Project files on the server were compared to the files found on the USB drive. In Table 7 we can see seventeen files acquired from the server and the 7-Zip file called “Documents.7z” that was recovered from the USB drive. Table 7 also shows the seventeen individual files located in the 7-Zip archive. We can see by comparing the SHA-256 hash values that the files on the server are exactly the same as those found in the 7-Zip archive located on the USB drive. The creation time of the “Document.7z” file which X-Ways gives as “2021/01/25 17:32:05 +2” is important to the investigation as it will be used when correlating different events into a timeline.

We have now confirmed that somebody copied the secret server files onto a USB drive. The question is now who did it. As the ex-employee is under suspicion the investigating will now focus on his Windows 10 workstation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Evidence object</th>
<th>Hash*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents.7z</td>
<td>SanDisk USB Ultra, P1</td>
<td>7449ACBFED61C35E6553A7ED06106D56A45AC71A872F006ED51A53431</td>
</tr>
<tr>
<td>secret_project\technical_server_w2_v2.ppt</td>
<td>SanDisk USB Ultra, P1</td>
<td>0084C19C9771B304D1472001B6007FED60DD2B905A4DEB5B70A78354</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.ppt</td>
<td>SanDisk USB Ultra, P1</td>
<td>0084C19C9771B304D1472001B6007FED60DD2B905A4DEB5B70A78354</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.ppt</td>
<td>SanDisk USB Ultra, P1</td>
<td>0084C19C9771B304D1472001B6007FED60DD2B905A4DEB5B70A78354</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.ppt</td>
<td>SanDisk USB Ultra, P1</td>
<td>0084C19C9771B304D1472001B6007FED60DD2B905A4DEB5B70A78354</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.ppt</td>
<td>SanDisk USB Ultra, P1</td>
<td>0084C19C9771B304D1472001B6007FED60DD2B905A4DEB5B70A78354</td>
</tr>
<tr>
<td>secret_project\progress_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\progress_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
<tr>
<td>secret_project\technical_server_w2.doc</td>
<td>SanDisk USB Ultra, P1</td>
<td>47786BA141602D79D5BEBD4FA93B6C07B0B719B0D7678E81C91265EB13A49</td>
</tr>
</tbody>
</table>

Table 7: Files recovered from the server and USB drive.

Eduard du Plessis, duplessiseduard@gmail.com
7.4. Windows 10 Workstation

7.4.1. USB Detective

USB Detective was used to do a triage of the investigated workstation to determine if there were any signs that the workstation was used in the theft of Intellectual Property. USB Detective can gather USB connection information by processing a Live System, processing a Logical Drive or by Selecting individual Files and Folders. The latter was chosen in order to display the location of files that were parsed.

After the EO1 image of the Windows 10 workstation was mounted with Arsenal Image Mounter the various files and folders were chosen as shown in Table 8.

Table 8: USB Detective’s selection of files and folders that were parsed.

USB Detective parses the following registry hives, logs and artefacts as shown in Table 8 (Hale, 2017).

“\Windows\System32\config\SYSTEM”

The Windows SYSTEM Registry Hive.

“\Windows\System32\config\SOFTWARE”

The Windows SOFTWARE Registry Hive.

“\Users\Username\NTUSER.DAT”

Eduard du Plessis, duplessiseduard@gmail.com
ntuser.dat is a registry file that stores user profile information.

```
\Users\Username\AppData\Local\Microsoft\Windows\UsrClass.dat
```

The UsrClass.dat stores the Shell ag information for the Desktop, zip files, remote and local folders, Windows special folders and virtual folders.

```
Windows\INF\setupapi.dev.log
```

The setupapi.dev.log is a plain text log file that holds device installation information.

```
Windows\Appcompat\Programs\Amcache.hve
```

The Amcache.hve is a registry hive file that is created by Windows to store the Information related to execution of programs.

```
Windows\System32\winevt\Logs
```

Location of Windows event logs (.evtx files).

```
\Users\Username\AppData\Roaming\Microsoft\Windows\Recent
```

LNK files location.

```
\Users\Username\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
```

Jump Lists location.

The information in Table 9 regarding the Connect and Disconnect of the Sandisk USB Ultra Device was retrieved from the “SYSTEM” registry hive found at the following location: “\Windows\System32\config\SYSTEM”. The other information in the timeline was retrieved from the “UsrClass.dat” registry hive found at:

```
\Users\General Manager\AppData\Local\Microsoft\Windows\UsrClass.dat
```

<table>
<thead>
<tr>
<th>Timestamp (SAST/SAST)</th>
<th>Event Type</th>
<th>File Path</th>
<th>Serial</th>
<th>Description</th>
<th>Volume Name/Label</th>
<th>Drive Letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data design</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-final</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-final</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 16:22</td>
<td>Directory Interaction</td>
<td>My Computer\Y:\Secret Project Data-progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 17:31</td>
<td>Connect</td>
<td>VCS476150711015930800169: Sandisk USB Ultra USB Device</td>
<td>Personal Drive</td>
<td>D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021/01/25 17:33</td>
<td>Disconnect</td>
<td>VCS476150711015930800169: Sandisk USB Ultra USB Device</td>
<td>Personal Drive</td>
<td>D</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 9: USB and Network activity as found by The USB Detective.**

Eduard du Plessis, duplessiseduard@gmail.com
We can see that the user interacted with the Active Directory shared drive “Y:\” on 25 January 2021 at 16:22. He viewed various sub-folders under the shared folder called “Y:\Secret Project Data\”. Ten minutes later at 16:32 he interacted with his personal share called “Y:\jdoe\”. Notice that the sub-folders in the “jdoe” share have some of the same names as sub-folders found in the “Secret Project Data” share.

The user connected a “Sandisk USB Ultra USB Device” to the Windows 10 workstation at “2021/01/25 17:31” and disconnected the device at “2021/01/25 17:33”. We can correlate the connect and disconnect to the creation time of the “Document.7z” file which X-Ways gave as “2021/01/25 17:32:05 +2” as found on the UB drive. We can therefore confirm that the ex-employee connected the USB drive to the computer and copied the “Document.7z” file from the workstation to the USB drive.

From the USB Detective reports that gets automatically generated by the software we identify the USB device that was connected as follows:

```
“Serial/UID: VC0476150711013938000169
Description: Sandisk USB Ultra USB Device
First Connected (SAST/SAST): 2021/01/25 17:31:48 +2
Last Connected (SAST/SAST): 2021/01/25 17:31:49 +2
Last Disconnected (SAST/SAST): 2021/01/25 17:33:01 +2
Volume Name/Label: Personal Drive
Drive Letter(s): D
VSN: (Not available.)
Last User: General Manager”
```

### 7.4.2. X-Ways Forensics

It is already clear that the ex-employee copied the 7-Zip file to the external Sandisk USB device. To make our case stronger we will analyse various other Windows artefacts. As the suspect events all took place on 25 January 2021 between 16:22:01 +2 and 17:32:58 +2 on 25 January 2021 the focus will be on all events during that period.

Keyword searches were run against the E01 images of the Windows 10 workstation to find any activity involving the Secret Files as well as the existence of the
7-Zip file. Even though none of the files were found on the workstation as existing or deleted files there were a lot of references to the files in Jump Lists and LNK files. We will now use Jump Lists, LNK files, Shell Bags, Prefetch files, USB connections and network connections to further prove that the ex-employee is guilty of the theft of intellectual property.

After scrutinising the timeline of 25 January 2021 in X-Ways the following artefacts were found as being important to the investigation:

**Jump Lists**

To scrutinise the computer’s Jump Lists we navigate to the following location:
```
\Users\GeneralManager\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
```

Two Jump Lists of interest were found as shown by X-Ways Forensics. The two files were opened by the user using LibreOffice 5 and shown in Table 10.

<table>
<thead>
<tr>
<th>Name</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>d38a3ea7ec79fbed.automaticDestinations-ms</td>
<td>2,00;C:\Program Files (x86)\LibreOffice 5\program\swriter.exe</td>
</tr>
<tr>
<td>ecd1a5e2c3af9c46.automaticDestinations-ms</td>
<td>1,00;C:\Program Files (x86)\LibreOffice 5\program\simpress.exe</td>
</tr>
</tbody>
</table>

**Table 10: Jump Lists showing that files located on the Active Directory share were opened**

Table 11 shows the Jump List called “d38a3ea7ec79fbed.automaticDestinations-ms” as parsed by X-Ways. The parsing of the Jump List shows that the user opened a file called “[secret_project]_technical_review_#1.docx” using LibreOffice’s swriter.exe application

<table>
<thead>
<tr>
<th>Application swriter's automaticdestination file parsed by X-Ways Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Path</td>
</tr>
<tr>
<td>Created</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Size</td>
</tr>
<tr>
<td>Modified</td>
</tr>
<tr>
<td>Record changed</td>
</tr>
<tr>
<td>Accessed</td>
</tr>
<tr>
<td>SHA-256</td>
</tr>
<tr>
<td>Type descr.</td>
</tr>
<tr>
<td>Child objects</td>
</tr>
<tr>
<td>Content created</td>
</tr>
<tr>
<td>Evidence object</td>
</tr>
</tbody>
</table>

Eduard du Plessis, duplessiseduard@gmail.com
Table 11: Opening of file located on the Active Directory share.

Table 12 shows the Jump List file called “ecd1a5e2c3af9c46fb6ed.automaticDestinations-ms” as parsed by X-Ways. The parsing shows that the user opened a file called “[secret_project\_detailed_design.pptx” using LibreOffice’s “simpress.exe” application.

Table 12: Opening of file located on the Active Directory share.

Eduard du Plessis, duplessiseduard@gmail.com
**LNK files**

To determine which files the user opened we scrutinised the LNK files found in the folder: “\Users\General Manager\AppData\Roaming\Microsoft\Windows\Recent\” (Belkasoft.com, 2021).

The following five LNK files of interest were found and analysed.

<table>
<thead>
<tr>
<th>No.</th>
<th>LNK File Name</th>
<th>Created</th>
<th>SHA-256</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>technical review.lnk</td>
<td>2021/01/25 16:22:22</td>
<td>950770D9ACD69A485S9A9694C3DFC808BADAA 41ED263C954F6B19F9EC11EE4C</td>
</tr>
<tr>
<td>3</td>
<td>[secret_project]_detailed_design.lnk</td>
<td>2021/01/25 16:23:05</td>
<td>D310F9D6D856742D476778B08120AABEFE0F8A6 DD01BC8DB421453812AD03859</td>
</tr>
<tr>
<td>4</td>
<td>design.lnk</td>
<td>2021/01/25 16:23:05</td>
<td>CE3ED30A9F7C89ED1281F2783FB1B801BC09 9FB814F763A6FA6E7CD2F07E</td>
</tr>
<tr>
<td>5</td>
<td>Documents.7z.lnk</td>
<td>2021/01/25 17:26:06</td>
<td>9E156ABEF9A5120550D86CAB9D2D123B95B056 9CF66168CC2234AFBAB135C</td>
</tr>
</tbody>
</table>

**Table 13: Listing of analysed LNK files found on the Workstation.**

The five LNK files shown in Table 13 represents three different types of events. A file being opened, navigating to a folder and a zip file being viewed. The LNK files analysed below were parsed and presented as shown by X-ways Forensics.

The parsed data of **LNK File 1** as shown in Table 13 shows us that the user “General Manager” opened a file called “[secret_project]_technical_review_#1.docx” that was located on the Active Directory “Y” share. The LNK file was created on 25 January 2021 at 16:22:22 +2 which is the date and time that the user opened the file. The Created, Modified, Record changed and Accessed dates all belong to the LNK file. The Target Created, Last Written and Last Accessed dates belong to the “.docx” file that was located and opened on the Active Directory “Y” share at the location (McQuaid, 2014): “\X_Folders\Secret Project Data\technical review\[secret_project]_technical_review_#1.docx”.

In Table 14 we can see that the Record Changed timestamp of the file “[secret_project]_technical_review_#1.docx” is the same date and time as when the LNK file was created. This tells us that when the user opened the file located on the sever from his workstation and that this action altered the Record changed date of the target file to

Eduard du Plessis, duplessiseduard@gmail.com
“2021/01/25 16:22:22 +2”. It also tells us that the target “.docx” file that was opened resided on the network share “\server\X_Folders$” with the working directory being “Y:\Secret Project Data\technical review”.

The Gateway MAC Address “D0 67 E5 40 5D 10” is the MAC address of the server’s ethernet device. Also provided is the size of the target file and the hash value of the LNK file.

Table 15 shows the metadata of LNK File 1’s target file, which is the file that was opened. The Path to the file on the Active Directory share has “f-switch...” at the beginning of the path. This is the path of the encrypted read-only connection that F-Response made to the server’s data drive. F-Switch is F-Response Consultant’s patented technology.

```
[secret_project]_technical_review_#1.lnk
```

Existence: ✓

Path: C:\Users\General\AppData\Roaming\Microsoft\Windows\Recent

Created: 2021/01/25 16:22:22 +2

Type: Link

Size: 0.9 KB

Modified: 2021/01/25 16:22:22 +2

Record changed: 2021/01/25 16:22:22 +2


Hash SHA-256: A1D223BDE7162D1145904BE33D72FD122990F9E96DC832054238DEFE64735E11

Metadata: Target attributes: A

Target file size: 121441

Target created: 2021/01/24 09:37:58 +2

Last written: 2015/01/05 23:01:06 +2

Last accessed: 2021/01/24 09:37:58 +2

Network share name: \server\X_Folders$

Drive letter: Y:

Target path: +

Working directory: Y:\Secret Project Data\technical review

Host name: server

Volume ID: {0D5FA4A2-A88E-4A8D-85D0-DFB0BBB7A9ED}

Object ID: {145509BD-5F11-11EB-BF1D-D067E5405D10}

MAC Address: D0 67 E5 40 5D 10

Timestamp: 2021/01/25 15:27:32 +2, Seq: 16336

Evidence object: Case_25_01_2021_Company X - Windows 10 Workstation

**Table 14: Information of LNK File 1 as parsed by X-Ways Forensics.**
Table 15: Metadata of the LNK File 1’s Target File taken from the server.

**LNK File 2** was created when the user navigated to the network share named “\server\X_Folders$” using Windows File Explorer. The Modified, Record Changed and Accessed timestamps are all “2021/01/24 at 16:22:22 +2” and refers to the moment when the user viewed the folder.

<table>
<thead>
<tr>
<th>technical review.lnk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exist:</strong> √</td>
</tr>
<tr>
<td><strong>Path:</strong> Drive C:/Users/General Manager/AppData/Roaming/Microsoft/Windows/Recent</td>
</tr>
<tr>
<td><strong>Created:</strong> 2021/01/25 16:22:22 +2</td>
</tr>
<tr>
<td><strong>Type:</strong> Lnk</td>
</tr>
<tr>
<td><strong>Size:</strong> 0.6 KB</td>
</tr>
<tr>
<td><strong>Modified:</strong> 2021/01/25 16:22:22 +2</td>
</tr>
<tr>
<td><strong>Record changed:</strong> 2021/01/25 16:22:22 +2</td>
</tr>
<tr>
<td><strong>Accessed:</strong> 2021/01/25 16:22:22 +2</td>
</tr>
<tr>
<td><strong>Hash SHA256:</strong> 950770DPACD6948909AB96914C3DFC9B09BDA8AA41ED26C95456B19F9EC1EE4C</td>
</tr>
<tr>
<td><strong>Metadata:</strong> Target attributes: (Directory)</td>
</tr>
<tr>
<td><strong>Target file size:</strong> 4096</td>
</tr>
<tr>
<td><strong>Target created:</strong> 2021/01/24 09:37:58 +2</td>
</tr>
<tr>
<td><strong>Last written:</strong> 2021/01/24 09:37:59 +2</td>
</tr>
<tr>
<td><strong>Last accessed:</strong> 2021/01/24 09:38:06 +2</td>
</tr>
<tr>
<td><strong>Network share name:</strong> \server\X_Folders$</td>
</tr>
<tr>
<td><strong>Drive letter:</strong> Y</td>
</tr>
<tr>
<td><strong>Host name:</strong> server</td>
</tr>
<tr>
<td><strong>Volume ID:</strong> [03FA4A2-A88E-4A8D-85D0-DFE0BBB7A9ED]</td>
</tr>
<tr>
<td><strong>Object ID:</strong> [145509BE-5F11-11EB-BFD0-D0675405D10] MAC</td>
</tr>
<tr>
<td><strong>Address:</strong> D0 87 E5 40 5D 10</td>
</tr>
<tr>
<td><strong>Timestamp:</strong> 2021/01/25 15:27:32 +2, Seq: 16336</td>
</tr>
<tr>
<td><strong>Evidence object:</strong> Case_25_01_2021_Company X - Windows 10 Workstation</td>
</tr>
</tbody>
</table>

Table 16: Information of LNK File 2 as parsed by X-Ways Forensics.
LNK File 3 was identified as suspect as the events relating to the 7-Zip software occurred at the same time as when the user were navigating to and opening the secret files located on the server. The LNK file parsed results shown in Table 17 confirms that an archive file called “Documents.7z” was viewed.

A Google search was done for the term “best free zip program” using the Microsoft Edge browser at “2021/01/25 17:07:02 +2”. X-Ways retrieved the information by parsing the Microsoft Edge SQLite History file located at: “\Users\General Manager\AppData\Local\Microsoft\Edge\User Data\Default\History”.

The X-Ways timeline shows the following: “Start download, source: https://www.7-zip.org/a/7z1900.exe (target:\Users\General Manager\Downloads\7z1900-x64.exe)”. Scrutinising the workstation’s directory structure confirmed that the file “7z1900-x64.exe” existed in the “Download” folder of the user “General Manager” with the creation date being “2021/01/25 17:07:43 +2”.

Table 17: Information of LNK File 3 as parsed by X-Ways Forensics.
Prefetch file history recovered from the location “\Windows\Prefetch” and parsed by X-Ways confirms the installation date as “Name: 7Z1900-X64.EXE; Run Count: 1; Last Run: 2021/01/25 17:08:04 +2” and the first and only time 7-Zip was run as “Name: 7ZG.EXE; Run Count: 1; Last Run: 2021/01/25 17:21:58 +2”.

USB Device Information: To generate a registry report using X-Ways all files are filtered to only show the registry hives SYSTEM, SOFTWARE, SECURITY, SAM, NTUSER.DAT and UsrClass. Selecting the relevant registry hives and pressing enter opens the selected files in the X-Ways Registry Viewer where the hives can be manually scrutinised. Right clicking on the registry viewer presents different options. Selecting Create Report generated a HTML report that was searched for the USB device information “Serial/UID VC0476150711013938000169” as found in the USB Detective report.

X-Ways gave us the following results. We can therefore confirm that the USB history as parsed by USB Detective is correct and the Sandisk Ultra USB drive was connected to the Windows 10 workstation.

\Windows\System32\config\SYSTEM

<table>
<thead>
<tr>
<th>USB Storage VC0476150711013938000169&amp;0</th>
<th>Sandisk USB Ultra USB Device</th>
<th>2021/01/25 17:31:49 +2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Arrival VC0476150711013938000169&amp;0</td>
<td>(Default): 2021/01/25 17:31:48 +2</td>
<td>2021/01/25 17:31:48 +2</td>
</tr>
<tr>
<td>Last Removal VC0476150711013938000169&amp;0</td>
<td>(Default): 2021/01/25 17:32:58 +2</td>
<td>2021/01/25 17:32:58 +2</td>
</tr>
</tbody>
</table>

Mounted devices

<table>
<thead>
<tr>
<th>DosDevices</th>
<th>2021/01/25 17:31:49 +2</th>
</tr>
</thead>
<tbody>
<tr>
<td>????USBSTOR#Disk &amp; Ven_Sandisk &amp; Prod_USB_Ultra &amp; Rev_1100 &amp; VC0476150711013938000169 &amp; 0 &amp; \53f6307-b6bf-11d0-94f2-00a0c91ef88b &amp; 0</td>
<td></td>
</tr>
<tr>
<td>????Volume [27835c30-5e19-11eb-9b95-5c5673cc0a2]</td>
<td>\77_USBSTOR#Disk &amp; Ven_Sandisk &amp; Prod_USB_Ultra &amp; Rev_1100 &amp; VC0476150711013938000169 &amp; 0 &amp; \53f6307-b6bf-11d0-94f2-00a0c91ef88b &amp; 0</td>
</tr>
</tbody>
</table>

\Windows\System32\config\SOFTWARE

Portable device

| SWD\WPDHUSENUM\??_USBSTOR\DISK & VEN_SANDISK & PROD_USB_Ultra & REV_1100 & VC0476150711013938000169 & 0 & \\53f6307-b6bf-11d0-94f2-00a0c91ef88b & 0 | 2021/01/25 17:31:49 +2 |

\Windows\System32\config\SECURITY

<table>
<thead>
<tr>
<th>Drive</th>
<th>Last access</th>
<th>Name</th>
<th>Serial</th>
</tr>
</thead>
<tbody>
<tr>
<td>D:</td>
<td>2021/01/25 17:31:49 +2</td>
<td>Disk &amp; Ven_Sandisk &amp; Prod_USB_Ultra &amp; Rev_1100</td>
<td>VC0476150711013938000169 &amp; 0</td>
</tr>
</tbody>
</table>

Eduard du Plessis, duplessiseduard@gmail.com
Network Connection information as found in the X-Ways registry report is as follows:

Found in: `\Users\General Manager\NTUSER.DAT`

<table>
<thead>
<tr>
<th>Type of network drive</th>
<th>Path of mapped network drive</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td><code>\server\X_Folders$</code></td>
<td>2021/01/24 09:53:56 +2</td>
</tr>
</tbody>
</table>

The MAC Address “D0 67 E5 40 5D 10” was already identified in the LNK file section as the MAC address of the server’s ethernet device. We therefore know that the Windows 10 workstation connected to the server.

Found in: `\Windows\System32\config\SOFTWARE`

<table>
<thead>
<tr>
<th>Default Gateway MAC (Managed)</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>D0 67 E5 40 5D 10</td>
<td>2021/01/23 10:00:24 +2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default Gateway MAC</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>D0 67 E5 40 5D 10</td>
<td>2021/01/23 09:38:32 +2</td>
</tr>
</tbody>
</table>

7.4.3. ShellBags Explorer

ShellBags Explorer is an excellent forensic software tool to use when investigating Shell Bag history. It parses the `NTUSER.dat` and `UsrClass.dat` registry hives on a live system by loading an active registry or on an offline hive by selecting and loading the relevant hives (Zimmerman, 2017).

<table>
<thead>
<tr>
<th>Absolute Path</th>
<th>First Interacted</th>
<th>Last Interacted</th>
<th>Last Write Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop\My Computer\Secret Project\Data design</td>
<td>25-01-2021 16:22:01</td>
<td>25-01-2021 16:32:11</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Secret Project\Data final</td>
<td>25-01-2021 16:22:02</td>
<td>25-01-2021 16:32:11</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Secret Project\Data pricing decision</td>
<td>25-01-2021 16:22:04</td>
<td>25-01-2021 16:32:11</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Secret Project\Data progress</td>
<td>25-01-2021 16:22:05</td>
<td>25-01-2021 16:32:11</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Secret Project\Data proposal</td>
<td>25-01-2021 16:22:07</td>
<td>25-01-2021 16:32:11</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Secret Project\Data technical review</td>
<td>25-01-2021 16:22:13</td>
<td>25-01-2021 16:32:11</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Y:\Files</td>
<td>25-01-2021 16:32:11</td>
<td>25-01-2021 16:32:11</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Y:\Files design</td>
<td>25-01-2021 16:32:28</td>
<td>25-01-2021 16:32:32</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Y:\Files technical review</td>
<td>25-01-2021 16:32:32</td>
<td>25-01-2021 16:32:32</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Users\Desktop</td>
<td>25-01-2021 17:07:50</td>
<td>25-01-2021 17:07:50</td>
<td></td>
</tr>
<tr>
<td>Desktop\My Computer\Users\General Manager\Downloads</td>
<td>25-01-2021 17:07:50</td>
<td>25-01-2021 17:07:50</td>
<td></td>
</tr>
</tbody>
</table>

Table 18: Shell Bags shown in a directory structure by ShellBags Explorer
The offline method will give you more information and is also the method being used in this paper (Zimmerman, 2017). ShellBags Explorer presents the results of the parsed registry hives in a directory structure as can be seen in Table 18. We can easily identify the folders that the user opened on the workstation’s local C drive, the externally connected D drive as well as those opened on the Microsoft Server’s Active Directory share mapped as drive “Y”. The directory view as shown in Table 18 already showed us the First Interacted, Last Interacted and the Last Write Time. A right-click on “My Computer” expands all nodes on the computer and shows all Shell Bags under each node. Left clicking on the shell bag “Y:\SecretProjectData\technical review” shows the Shell Bag’s Table 19: Node View information in three tabs: “Summary”, “Details” and “Hex”. Table 20 shows the Summary tab information. The Details tab shows more information for example “File System Hint”, which can be the useful if you are looking for a USB drive formatted with FAT32. Table 21 is a screenshot of some of “Detail tab” information not shown in the Summary tab.

<table>
<thead>
<tr>
<th>Name: technical review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute path: Desktop\My Computer\Y:\Secret Project Data\technical review</td>
</tr>
<tr>
<td>Key-Value name path: BagMRU\1\23-5</td>
</tr>
<tr>
<td>Registry last write time: 25-01-2021 16:32:10.840</td>
</tr>
</tbody>
</table>

Target timestamps

- Created on: 24-01-2021 09:38:00.000
- Modified on: 24-01-2021 09:38:00.000
- Last accessed on: 24-01-2021 09:38:08.000

Miscellaneous

- Shell type: Directory
- Node slot: 37
- MRU position: 0
- # of child bags: 0
- First interacted with: 25-01-2021 16:22:12.809
- Last interacted with: 25-01-2021 16:32:10.840

Table 20 – Summary Tab view of the Shell Bag

Table 21 – Detail Tab (Partially shown)
8. Correlation of data

The comparison of the secret files on the Windows Server 2019 server with those found on the Sandisk USB Ultra Drive confirmed that someone stole files from the company’s Secret Project. The server’s Secret Project files were found on the USB drive in a 7-Zip archive file. After acquiring and analysing data from the ex-employee’s Windows 10 workstation we successfully confirmed the following.

An initial triage of the Windows 10 workstation using USB Detective confirmed the suspicion that the ex-employee was involved in copying the secret files to the USB drive. On 25 January 2021 from “2021/01/25 16:22:01 +2” and “2021/01/25 17:32:32 +2” he explored the server’s “Y” share and viewed the Secret Project’s folders as well as folders in his personal “jdoe” share. The names of some of the folders in the “jdoe” share had the same names as sub-folders found in the Secret Project share. He then connected a USB drive to the computer at “2021/01/25 17:31:48 +2” and disconnected at “2021/01/25 17:32:58 +2”.

Analysing Jump Lists for the user “General Manager” on the Windows 10 workstation confirms that two files located on the “Y” share was opened by the user from the Windows 10 workstation.

LNK file analyses confirms the opening of the files as found in the Jump List history. Furthermore, LNK file analyses shows suspect 7-Zip activity. Further analysis found that the user downloaded the 7-Zip executable at “2021/01/25 17:07:43 +2” and installed it at “2021/01/25 17:08:06 +2”. Recovered Prefetch files confirms the installation of the downloaded executable as well as the first and only run of the installed 7-Zip application.

The opening of folders as initially showed by USB Detective was recovered and showed in detail by ShellBag Explorer.

A timeline of the 25 January 2021 events are as follows:
17:07:02 +2   Google search for “best free zip program”.

Eduard du Plessis, duplessiseduard@gmail.com
17:07:43 +2 Download the 7-Zip installation executable.
17:07:50 +2 Accessed the Windows 10 workstation “Download” folder.
17:08:04 +2 Installed the downloaded 7-Zip software.
17:21:58 +2 Run 7-Zip at and created the zip file containing the Secret Project files.
17:31:48 +2 USB device connection to the Windows 10 workstation.
17:32:05 +2 The file Documents.7z is created on the USB drive.
17:32:58 +2 USB device disconnect from the Windows 10 workstation.

9. Software performance

X-Ways Forensics is a lightweight but powerful and versatile forensic software tool that is unmatched. The inexperienced examiner might find X-Ways intimidating at first but there are very good resources available to assist with learning its full capability. The X-Ways Forensics Practitioner’s Guide by Brett Shavers and Eric Zimmerman is an excellent book that teaches you step by step on how to use the tool constructively. Ted Smith’s website www.xwaysclips.co.uk has more than 60 training videos covering most important tasks.

F-Response is an extremely easy and reliable tool to use and pairing it with X-Ways prepares the examiner for most assignments.

USB Detective is good for triage and should be part of any digital forensic analyst’s toolkit. Few other forensic software tools parses USB drive connection information from so many different data points like it does. The recently added LNK file and Shell Bag information makes it even more powerful especially when used for the quick triage of a device.

ShellBags Explorer is many people’s obvious choice for Shell Bag analysis and an added bonus is that it is a free tool.
10. Conclusion

Digital forensic examiners are under pressure to provide results and often have to meet impossible deadlines. This paper provided a framework which will help the examiner to quickly get to critical results to determine if further investigation is necessary.

It is important that the examiner knows which process to follow, where to look for information and which software tools to use.

Acquiring and analysing a wider variety of devices and data points will provide more thorough and accurate results. To this paper’s server, workstation and external storage device we can add mobile devices and clouds. Depending on the severity of the crime and what is legally possible personal devices can also be added to an investigation.

As Windows stores a diverse variety of artefacts and logs it is important that only the necessary and minimum set of artefacts are recovered and analysed. The set of artefacts in this theft of intellectual property investigation are all easy to recover and analyse.

The digital forensic tool set chosen are all lightweight, powerful and affordable. Focused use will make sure that results are presented timeously and with the least amount of effort.

Eduard du Plessis, duplessiseduard@gmail.com
References


Eduard du Plessis, duplessiseduard@gmail.com
Appendix
Windows Artefacts
(As per the SANS DFIR Windows Forensic Analysis Poster)

LNK (Link) files

Description
- LNK files are generated when a user opens files or documents. These files and documents can be located on the local machine or on a remote machine and created by a user’s actions or automatically by the Windows operating system.
- LNK files are shortcut files that link to an application or file commonly found on a user’s desktop, or throughout a system and end with a .LNK extension.

Location
- Windows XP:
  - \%USERPROFILE%\Recent
- Windows 7, 8 and 10:
  - \%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\n  - \%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\n
Interpretation of LNK artefact
- Date/Time file of that name was first opened
  - Creation Date of Shortcut (LNK) File
- Date/Time file of that name was last opened
  - Last Modification Date of Shortcut (LNK) File
- LNK Target File (Internal LNK File Information) Data:
  - Modified, Access, and Creation times of the target file
  - Volume Information (Name, Type, Serial Number)
  - Network Share information
  - Original Location
  - Name of System

Eduard du Plessis, duplessiseduard@gmail.com
Jump Lists

Description
- Jump Lists present the user with links to recently accessed files. Jump lists have been part of Windows since being introduced in Windows 7. It provides a list of recently accessed files and documents associated with a given application. Before Windows 7 forensic examiners were only presented with a short list of recently accessed files. Jump list artifacts provide details on recent files for each application giving a lot of information and timestamps on a user’s actions.

Location
- Win7/8/10:
  ° %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation of Jump List artefact
- An AutomaticDestination Jump List file can be opened by using the Structured Storage Viewer.
- Each one of these files is a separate LNK file that are numerically stored in order from the earliest one (usually 1) to the most recent (largest integer value)

Shell bags

Description
- Shell Bags are Microsoft Windows artefacts that stores the information of folders that were recently browsed by the user on a local machine, the network, and/or removable devices.
- It gives you information on previously existing folders.
- When folders were accessed.

Location
- Explorer Access:
  ° USRCLASS.DAT\Local\Settings\Software\Microsoft\Windows\Shell\Bags

Eduard du Plessis, duplessiseduard@gmail.com
USRCALSS.DAT\Local\Settings\Software\Microsoft\Windows\Shell\BagMRU

- Desktop Access:
  - NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
  - NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

**Interpretation**

- Stores information about which folders were most recently browsed by the user

**Prefetch files**

**Description**

- Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.

- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8
- (exename)-(hash).pf

**Location**

- WinXP/7/8/10:
  - Windows\Prefetch

**Interpretation**

- Each .pf will include last time of execution, number of times run, and device and file handles used by the program
- Date/Time file by that name and path was first executed - Creation Date of .pf file (-10 seconds)
- Date/Time file by that name and path was last executed
  - Embedded last execution time of .pf file
  - Last modification date of .pf file (-10 seconds)
  - Win8-10 will contain last 8 times of execution

Eduard du Plessis, duplessiseduard@gmail.com
Network connections

Description
- Identify networks that the computer has been connected to
- Networks could be wireless or wired
- Identify domain name/intranet name
- Identify SSID
- Identify Gateway MAC Address

Location
- Win7/8/10 SOFTWARE HIVE:
  - SOFTWARE\Microsoft\Windows\NT\CurrentVersion\NetworkList\Signatures\Unmanaged
  - SOFTWARE\Microsoft\Windows\NT\CurrentVersion\NetworkList\Signatures\Managed
  - SOFTWARE\Microsoft\Windows\NT\CurrentVersion\NetworkList\Nla\Cache

Interpretation
- Identifying intranets and networks that a computer has connected to is incredibly important
- Not only can you determine the intranet name, you can determine the last time the network was connected to it based on the last write time of the key
- This will also list any networks that have been connected to via a VPN
- MAC Address of SSID for Gateway could be physically triangulated

USB Device Connections

To determine if any USB attached storage devices were connected to the computer and if any which Windows user connected the USB devices to the computer.

Key Identification
- Description
  - Track USB devices plugged into a machine.
- Location
  - SYSTEM\CurrentControlSet\Enum\USBSTOR
- \textit{SYSTEM\CurrentControlSet\Enum\USB}

\textbf{Interpretation}

- Identify vendor, product, and version of a USB device plugged into a machine
- Identify a unique USB device plugged into the machine
- Determine the time a device was plugged into the machine
- Devices that do not have a unique serial number will have an “&” in the second character of the serial number

\textbf{First & Last Connection Times}

\textbf{Description}

- Determine temporal usage of specific USB devices connected to a Windows Machine.

\textbf{Location for First Time Connections}

- Plug and Play Log Files
  - XP: \texttt{\Windows\setupapi.log}
  - Win7/8/10: \texttt{\Windows\inf\setupapi.dev.log}

\textbf{Interpretation}

- Search for Device Serial Number
- Log File times are set to local time zone

\textbf{Location First, Last, and Removal Times (Win7/8/10 Only)}

- System Hive:
  \texttt{\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial\Properties\83da6326-97a6-4088-9453-a19231573b29\####}
  - 0064 = First Install (Win7-10)
  - 0066 = Last Connected (Win8-10)
  - 0067 = Last Removal (Win8-10)
User identification

- **Description**
  - Find User that used the Unique USB Device.

- **Location**
  - Look for GUID from `SYSTEM\MountedDevices`
  - `NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2`

- **Interpretation**
  - This GUID will be used next to identify the user that plugged in the device. The last write time of this key also corresponds to the last time the device was plugged into the machine by that user. The number will be referenced in the user’s personal mountpoints key in the NTUSER.DAT

PnP Events

- **Description**
  - When a Plug and Play driver install is attempted, the service will log an ID 20001 event and provide a Status within the event. It is important to note that this event will trigger for any Plug and Play-capable device, including but not limited to USB, Firewire, and PCMCIA devices.

- **Location** System Log File
  - Win7/8/10: `%system root%\System32\winevt\logs\System.evtx`

- **Interpretation**
  - Event ID: 20001 – Plug and Play driver install attempted
  - Event ID 20001
  - Timestamp
  - Device information
  - Device serial number
  - Status (0 = no errors)
Volume Serial Number

- **Description**
  - Discover the Volume Serial Number of the Filesystem Partition on the USB. (NOTE: This is not the USB Unique Serial Number, which is hardcoded into the device firmware.)

- **Location**
  - SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt
  - Use Volume Name and USB UniqueSerial Number to:
    - Find last integer number in line
    - Convert Decimal Serial Number into Hex Serial Number

- **Interpretation**
  - Knowing both the Volume Serial Number and the Volume Name, you can correlate the data across SHORTCUT File (LNK) analysis and the RECENTDOCs key.
  - The Shortcut File (LNK) contains the Volume Serial Number and Name
  - RecentDocs Registry Key, in most cases, will contain the volume name when the USB device is opened via Explore

Drive Letter & Volume Name

- **Description**
  - Discover the last drive letter of the USB Device when it was plugged into the machine.

- **Location XP**
  - Find ParentIdPrefix - SYSTEM\CurrentControlSet\Enum\USBSTOR
  - Using ParentIdPrefix Discover Last Mount Point
    - SYSTEM\MountedDevices

- **Location Windows 7, 8 and 10**
  - SOFTWARE\Microsoft\Windows Portable Devices\Devices
  - SYSTEM\MountedDevices

Eduard du Plessis, duplessiseduard@gmail.com
Examine Drive Letters looking at Value Data Looking for Serial Number

- Interpretation
  - Identify the USB device that was last mapped to a specific drive letter. This technique will only work for the last drive mapped. It does not contain historical records of every drive letter mapped to a removable drive.
## Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Date/Time Details</th>
<th>Location</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Security West 2021</td>
<td>May 10, 2021 - May 15, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam May 2021</td>
<td>May 17, 2021 - May 22, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Stockholm May 2021</td>
<td>May 31, 2021 - Jun 05, 2021</td>
<td>Virtual - Central European Summer Time, Sweden</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS FOR500 In Italian June 2021</td>
<td>Jun 07, 2021 - Jun 12, 2021</td>
<td>Virtual - Central European Summer Time, Italy</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Security Central: June 2021</td>
<td>Jun 07, 2021 - Jun 12, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Hurlburt DCO/H 21-05</td>
<td>Jun 14, 2021 - Jun 19, 2021</td>
<td>Hurlburt Field, FL</td>
<td>CyberCon</td>
</tr>
<tr>
<td>State of Wisconsin-Dept of Admin (WI DOA) FOR508</td>
<td>Jun 14, 2021 - Jun 19, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Paris June 2021</td>
<td>Jun 14, 2021 - Jun 19, 2021</td>
<td>Virtual - Central European Summer Time, France</td>
<td>CyberCon</td>
</tr>
<tr>
<td>MPO/W Columbia CNODP FY21 (FOR610) 6-day format</td>
<td>Jun 14, 2021 - Jun 19, 2021</td>
<td>Columbia, MD</td>
<td>CyberCon</td>
</tr>
<tr>
<td>South By SE Asia PenTest 2021</td>
<td>Jun 21, 2021 - Jun 26, 2021</td>
<td>Virtual - India Standard Time, India</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Miami: Virtual Edition 2021</td>
<td>Jun 21, 2021 - Jun 26, 2021</td>
<td>Virtual - Central Eastern Time, India</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Fort Gordon Cyber Protection Brigade (CPB/ARCYBER) (FOR572)</td>
<td>Jun 21, 2021 - Jun 26, 2021</td>
<td>Augusta, GA</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defence Australia 2021</td>
<td>Jun 28, 2021 - Jul 10, 2021</td>
<td>Canberra, Australia</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Digital Forensics en Espanol: June 2021</td>
<td>Jun 28, 2021 - Jul 03, 2021</td>
<td>Virtual - Central Eastern Standard Time, Australia</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defence Australia 2021 - Live Online</td>
<td>Jun 28, 2021 - Jul 10, 2021</td>
<td>Virtual - Central Eastern Standard Time, Australia</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defence Japan 2021</td>
<td>Jun 28, 2021 - Jul 10, 2021</td>
<td>Virtual - Japan Standard Time, Japan</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London July 2021</td>
<td>Jul 05, 2021 - Jul 10, 2021</td>
<td>Virtual - British Summer Time, United Kingdom</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Stay Sharp Summer 2021</td>
<td>Jul 07, 2021 - Jul 09, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Cyber Defence Singapore July 2021 - Live Online</td>
<td>Jul 12, 2021 - Jul 24, 2021</td>
<td>Singapore, Singapore</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANSFIRE 2021</td>
<td>Jul 12, 2021 - Jul 17, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Cyber Defence Singapore July 2021</td>
<td>Jul 12, 2021 - Jul 17, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam July 2021</td>
<td>Jul 19, 2021 - Jul 24, 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>CyberCon</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2021</td>
<td>Jul 22, 2021 - Jul 31, 2021</td>
<td>Virtual - US Eastern, Central Europe</td>
<td>CyberCon</td>
</tr>
<tr>
<td>MPO/W Columbia CMIP FY21 (FOR508) 5-day format</td>
<td>Jul 26, 2021 - Jul 30, 2021</td>
<td>Columbia, MD</td>
<td>CyberCon</td>
</tr>
<tr>
<td>USMC-MARFORCYBER / UKI - Live In-Person (FOR518)</td>
<td>Jul 26, 2021 - Jul 31, 2021</td>
<td>Columbia, MD</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Wellington August 2021</td>
<td>Aug 02, 2021 - Aug 07, 2021</td>
<td>Wellington, New Zealand</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Wellington August 2021 - Live Online</td>
<td>Aug 02, 2021 - Aug 07, 2021</td>
<td>Virtual - New Zealand Standard Time, New Zealand</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Cyber Defence India August 2021</td>
<td>Aug 09, 2021 - Aug 28, 2021</td>
<td>Virtual - India Standard Time, India</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS NOVA: Virtual Edition 2021</td>
<td>Aug 09, 2021 - Aug 14, 2021</td>
<td>Virtual - Central European Summer Time, Italy</td>
<td>CyberCon</td>
</tr>
</tbody>
</table>