# A COMPREHENSIVE FORENSIC CASE REPORT WITH THE UNIVERSITY OF SINGAPORE TEAM #6

## UNIVERSITY OF SINGAPORE CASE #1: SUSPICIOUS EMPLOYEE

By

| Investigator Name | Matric Number | Contact Information |
|---|---|---|
| Haziq Hakim Bin Abdul Rahman | A0216481H | e0540038@u.nus.edu |
| Musfirah Wani Bte Abdul Rahim | A0221404Y | e0556596@u.nus.edu |
| Ng Jong Ray, Edward | A0216695U | e0540252@u.nus.edu |
| Sim Ting Yu Emily | A0221094N | e0556286@u.nus.edu |

March 2023

## Contribution Details

All team members contributed equally to this case.

# Table of Contents

# 1 Executive Summary

In this report, our forensics team will go through the provided evidence belonging to a suspicious employee, Mark. In this case, we looked through all of the evidence which consists of 3 registry files and an event log that was obtained from Mark's work laptop. After a thorough analysis of the evidence provided, the team have come up with 2 hypotheses. Firstly, Mark is suspicious as he had downloaded confidential documents and subsequently created his own admin account on his laptop. However, we found evidence that could show that Mark may not be guilty fully. Hence, our second hypothesis is that Mark is not guilty as there was evidence such as his account being created on the same day as the occurrence of the suspicious activity. As the evidence is quite polarising, more information is needed to come to a concise conclusion on which hypothesis is more plausible.

# 2 Objectives

## 2.1 Case Description

Mark is a former employee of the company and the subject of investigation in this case. Just before he left, another employee, John, reported a lost USB storage drive and his suspicions about Mark. It was observed that Mark was working irregular hours and browsing websites that are irrelevant to work. Therefore, our team has been approached by the Human Resources department of the company to conduct a forensics investigation on the registry hives and other files recovered from Mark's computer in response to these concerns.

## 2.2 Hypothesis

Our team has come out with two hypotheses for this case and they are (ranked in order):

1. He is **suspicious** as he had accessed confidential documents from an internal FTP server, accessed a thumb drive and created an Admin account on his laptop at an unusual hour.

2. He is **NOT suspicious** as someone is pretending to be Mark and is trying to sabotage him by creating a computer account under his name and performing all the aforementioned suspicious actions.

## 3 Evidence Analysed

In the forensics investigation, the following evidence files were given to the team.

| Evidence Number | Evidence Name | Hash Values (MD5) | Size |
|---|---|---|---|
| 00 | Event_Logs.evtx | 14ac1ef1a31aa42cf5fd3a4eac942f90 | 1092 KiB |
| 01 | Mark-NTUSER.DAT | 1a5a665b3f3cfb6dc150b26b87c1f17b | 512 KiB |
| 02 | SAM | 297d8a862ad079f7c5da48f96a71151d | 32 KiB |
| 03 | SYSTEM | e64992f9baaca0a728050677bac38ca4 | 9272 KiB |

## 4 Steps Taken

Since this investigation is initiated by the Human Resource team, the registry hives and other evidence files from Mark’s computer are directly provided to our forensic team and not acquired by our team. Hence, we are not able to determine if the acquisition process is performed in a way that ensures the integrity of the data being collected.

However, upon receiving the files, we computed the hash values of each of the files and created copies of it so that the team members would be able to analyse the evidence separately. To ensure the integrity of the evidence, we conducted hash value checks every time we worked with the copied files, thus preventing any potential modification or compromise of the original data.

The following is a list of software tools that were used to analyse the evidence:

| Software Used | Version Numbers |
|---|---|
| Registry Editor | Version 21H2 (OS Build 22000. 1455) |
| RegRipper | RegRipper3.0 |
| Event Viewer | Version: 1.0 |
| Windows Registry Recovery x64 (WRR64) | Version 3.1.1.0 |

# 5 Relevant Findings

## 5.1 System Information

The following information were found in the evidence #03 (SYSTEM), Mark's SYSTEM registry hive:

| Field | Values |
|---|---|
| Computer Name | WIN-8NQK06IH20A |
| Processor's architecture | AMD64 |
| Computer Time Zone | Eastern Standard Time |
| Computer's DHCP-based IP address | 192.168.67.145 |
| Network Mask | 255.255.255.0 |

## 5.2 Group and Users

### 5.2.1 Users

The following users were found in evidence #02 (SAM), Mark's SAM registry hive:

| Users | Last Logon Time (UTC) | SID |
|---|---|---|
| Administrator | 21/8/2013 9:47:09 PM | S-1-5-21-4115010050-4293081376-766057376-500 |
| Guest | - | S-1-5-21-4115010050-4293081376-766057376-501 |
| Mark | 7/3/2016 11:40:56 PM | S-1-5-21-4115010050-4293081376-766057376-1001 |
| Admin | 7/3/2016 11:41:12 AM | S-1-5-21-4115010050-4293081376-766057376-1002 |

### 5.2.2 Relevant Built-In Groups

The following important and relevant built-in groups were found in evidence #02 (SAM), Mark's SAM registry hive:

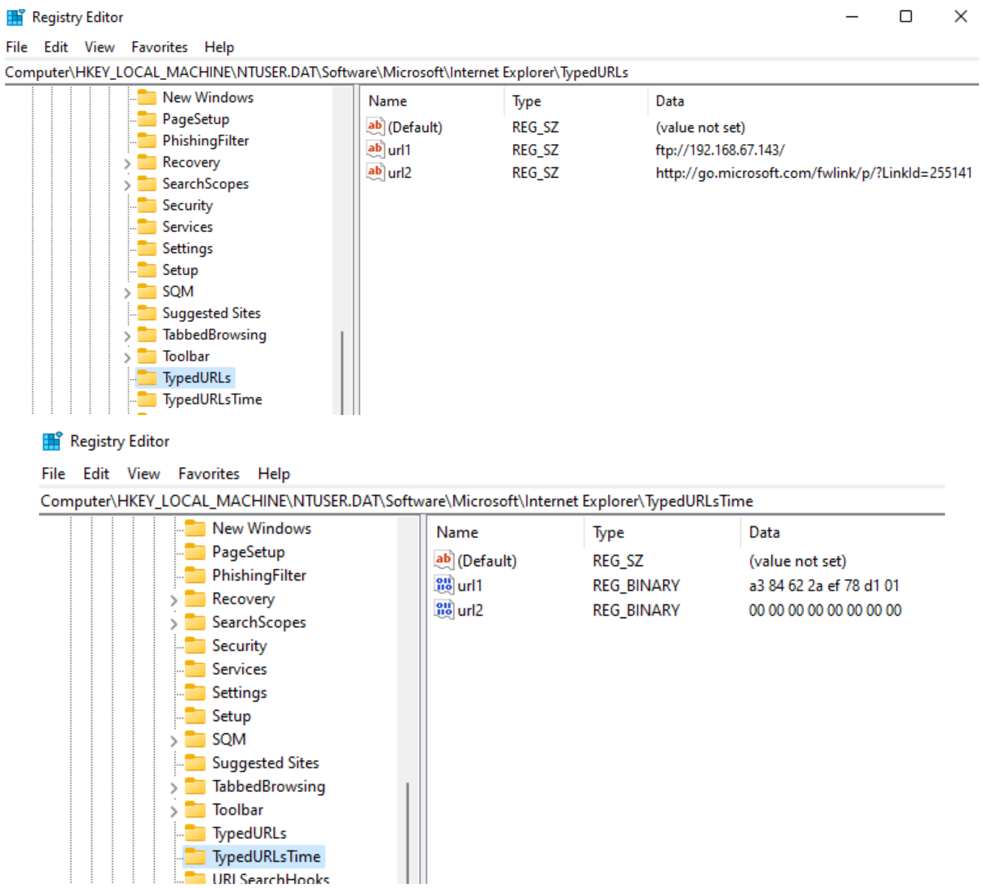
| **Built-in groups** | **Role description** |
|---|---|
| Administrator | Administrators have complete and unrestricted access to the computer/domain. |
| Users | Users are prevented from making accidental system-wide changes and can run most applications. |

## 5.3 Website Visited

Using Registry Editor, our team analysed the software registry keys from evidence #01 (MARK-NTUSER.DAT), and observed two URLs that were typed into the URL field and their typed times:

| **Typed URL** | **Typed URL Time** |
|---|---|
| ftp://192.168.67.143/ | Mon 7 March 2016 11:01:17 PM EST |
| http://go.microsoft.com/fwlink/p/?LinkId=255141 | - |

Furthermore, we performed a dual-tool technique to ensure that our findings are consistent. We used RegRipper and managed to obtain the same finding:



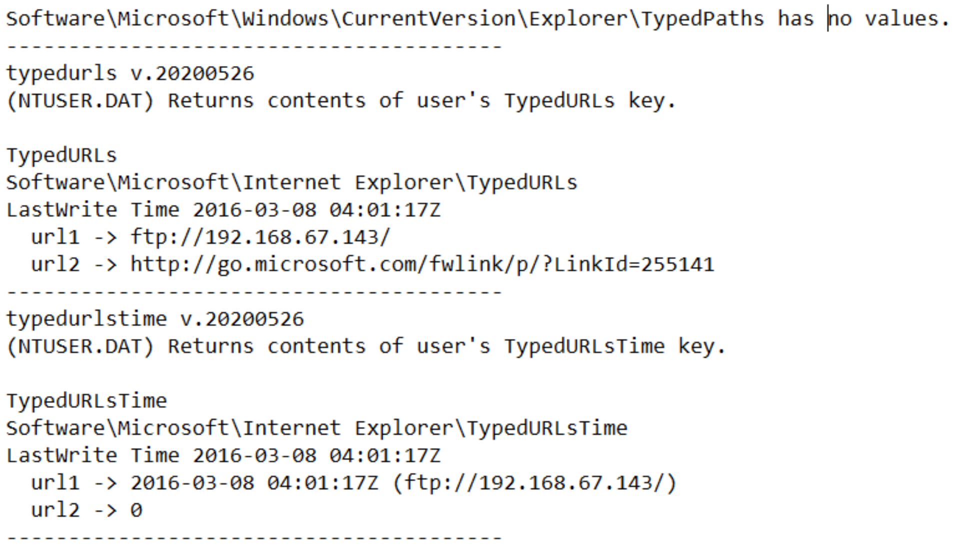
Computer\HKEY_LOCAL_MACHINE\NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| url1 | REG_SZ | ftp://192.168.67.143/ |
| url2 | REG_SZ | http://go.microsoft.com/fwlink/p/?LinkId=255141 |

Computer\HKEY_LOCAL_MACHINE\NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLsTime

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| url1 | REG_BINARY | a3 84 62 2a ef 78 d1 01 |
| url2 | REG_BINARY | 00 00 00 00 00 00 00 00 |

Fig 1. Using Registry Editor



```
Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths has no values.
----------------------------------------
typedurls v.20200526
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time 2016-03-08 04:01:17Z
  url1 -> ftp://192.168.67.143/
  url2 -> http://go.microsoft.com/fwlink/p/?LinkId=255141
----------------------------------------
typedurlstime v.20200526
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

TypedURLsTime
Software\Microsoft\Internet Explorer\TypedURLsTime
LastWrite Time 2016-03-08 04:01:17Z
  url1 -> 2016-03-08 04:01:17Z (ftp://192.168.67.143/)
  url2 -> 0
----------------------------------------
```

Fig 2. Using RegRipper

We believe that the typed URL (http://go.microsoft.com/fwlink/p/?LinkId=255141) does not have a typed URL time because this is the default homepage that is loaded when Mark opens his Internet Explorer browser. Thus, the team determined that this is not a suspicious activity.

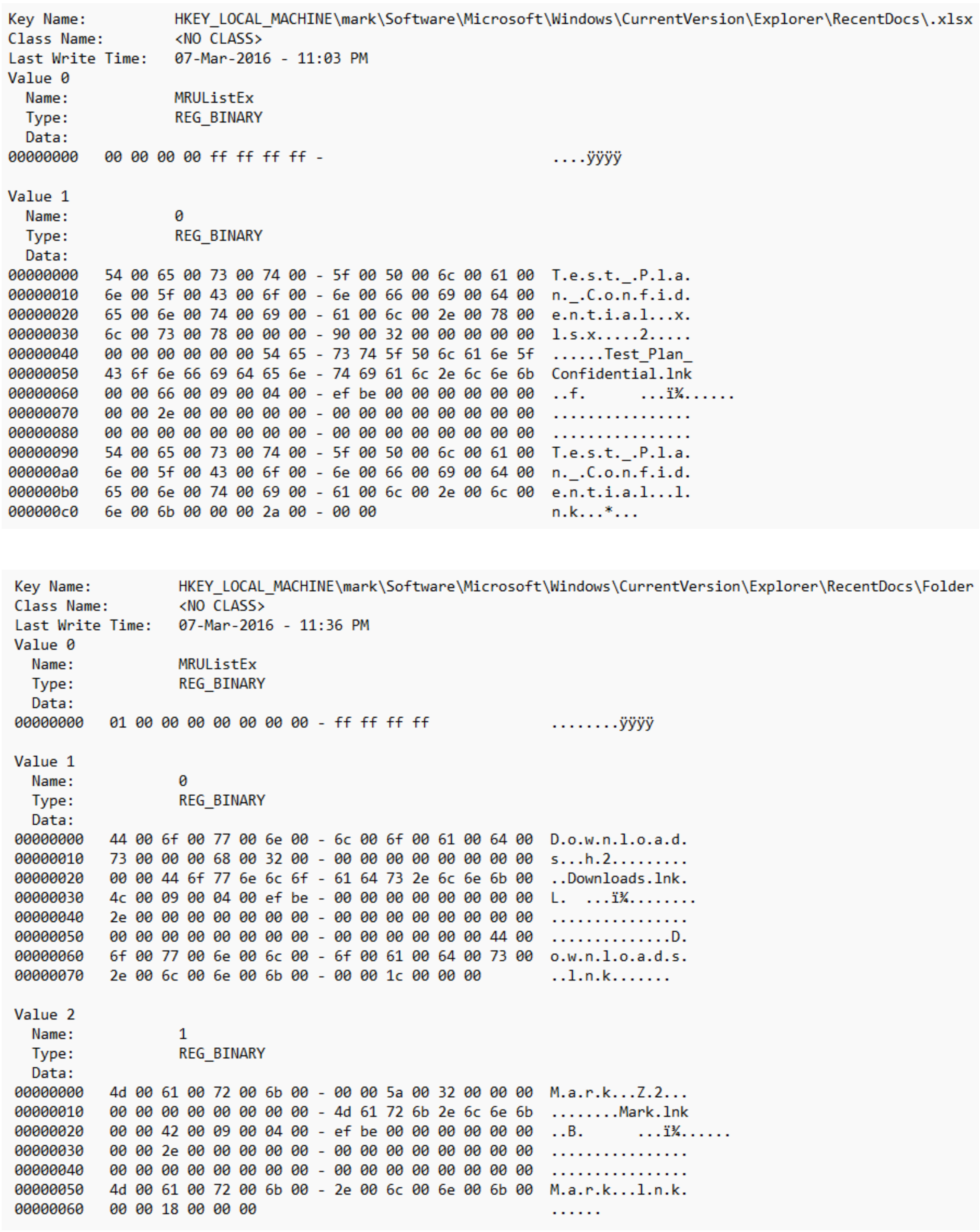
However, the above evidence shows that Mark accessed a FTP host on Mon 7 March 2016 11:01:17 PM EST. We believe that this could be an internal FTP server belonging to the company as Mark's computer has an IP address of 192.168.67.145 (network mask: 255.255.255.0) and the FTP server is on 192.168.67.143. Depending on the secrecy of this FTP server, we believe this could be suspicious, especially if Mark should not have access to this FTP server.

## 5.4 Files Accessed

To analyse the recently accessed documents, the team inspected evidence #01 (MARK-NTUSER.DAT) and observed the RecentDocs subkey at Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs. The Test_Plan_Confidential.xlsx is one notable document that was opened on the system with a last write time of 7/3/2016 - 11:03 PM (EST).

Additionally, the Mark and Downloads folder were also listed as the recently accessed folders.

| **Recent Accessed Document** | **Last Write Time (EST)** |
|---|---|
| Test_Plan_Confidential.xlsx | 7/3/2016 - 11:03 PM |
| Downloads Folder | 7/3/2016 - 11:36 PM |
| Mark Folder | 7/3/2016 - 11:36 AM |

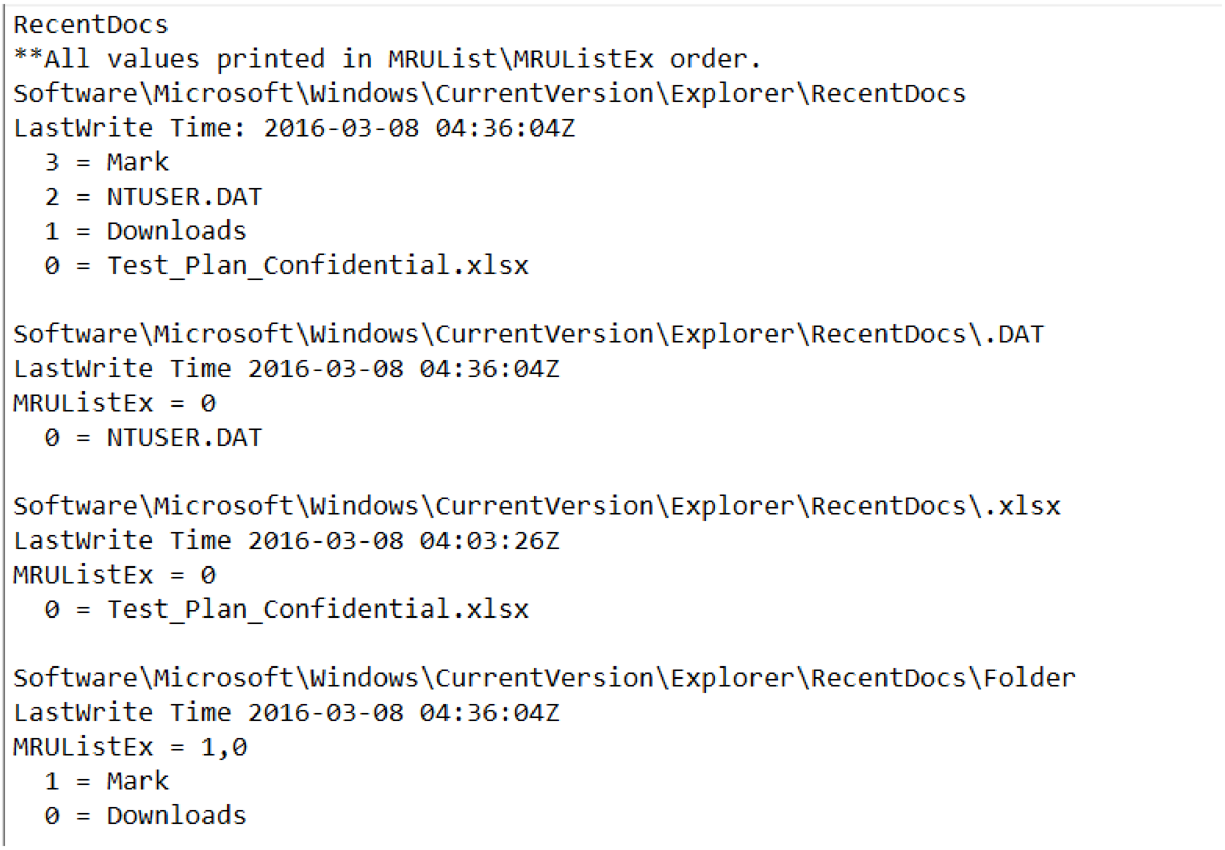


```
Key Name:          HKEY_LOCAL_MACHINE\mark\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx
Class Name:        <NO CLASS>
Last Write Time:   07-Mar-2016 - 11:03 PM
Value 0
  Name:            MRUListEx
  Type:            REG_BINARY
  Data:
00000000   00 00 00 00 ff ff ff ff -                           ....ÿÿÿÿ

Value 1
  Name:            0
  Type:            REG_BINARY
  Data:
00000000   54 00 65 00 73 00 74 00 - 5f 00 50 00 6c 00 61 00  T.e.s.t._.P.l.a.
00000010   6e 00 5f 00 43 00 6f 00 - 6e 00 66 00 69 00 64 00  n._.C.o.n.f.i.d.
00000020   65 00 6e 00 74 00 69 00 - 61 00 6c 00 2e 00 78 00  e.n.t.i.a.l...x.
00000030   6c 00 73 00 78 00 00 00 - 90 00 32 00 00 00 00 00  l.s.x.....2.....
00000040   00 00 00 00 00 00 54 65 - 73 74 5f 50 6c 61 6e 5f  ......Test_Plan_
00000050   43 6f 6e 66 69 64 65 6e - 74 69 61 6c 2e 6c 6e 6b  Confidential.lnk
00000060   00 00 66 00 09 00 04 00 - ef be 00 00 00 00 00 00  ..f.      ...ï¾......
00000070   00 00 2e 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
00000080   00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
00000090   54 00 65 00 73 00 74 00 - 5f 00 50 00 6c 00 61 00  T.e.s.t._.P.l.a.
000000a0   6e 00 5f 00 43 00 6f 00 - 6e 00 66 00 69 00 64 00  n._.C.o.n.f.i.d.
000000b0   65 00 6e 00 74 00 69 00 - 61 00 6c 00 2e 00 6c 00  e.n.t.i.a.l...l.
000000c0   6e 00 6b 00 00 00 2a 00 - 00 00                    n.k...*...
```

```
Key Name:          HKEY_LOCAL_MACHINE\mark\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
Class Name:        <NO CLASS>
Last Write Time:   07-Mar-2016 - 11:36 PM
Value 0
  Name:            MRUListEx
  Type:            REG_BINARY
  Data:
00000000   01 00 00 00 00 00 00 00 - ff ff ff ff              ........ÿÿÿÿ

Value 1
  Name:            0
  Type:            REG_BINARY
  Data:
00000000   44 00 6f 00 77 00 6e 00 - 6c 00 6f 00 61 00 64 00  D.o.w.n.l.o.a.d.
00000010   73 00 00 00 68 00 32 00 - 00 00 00 00 00 00 00 00  s...h.2.........
00000020   00 00 44 6f 77 6e 6c 6f - 61 64 73 2e 6c 6e 6b 00  ..Downloads.lnk.
00000030   4c 00 09 00 04 00 ef be - 00 00 00 00 00 00 00 00  L.  ...ï¾........
00000040   2e 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
00000050   00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 44 00  ..............D.
00000060   6f 00 77 00 6e 00 6c 00 - 6f 00 61 00 64 00 73 00  o.w.n.l.o.a.d.s.
00000070   2e 00 6c 00 6e 00 6b 00 - 00 00 1c 00 00 00        ..l.n.k.......

Value 2
  Name:            1
  Type:            REG_BINARY
  Data:
00000000   4d 00 61 00 72 00 6b 00 - 00 00 5a 00 32 00 00 00  M.a.r.k...Z.2...
00000010   00 00 00 00 00 00 00 00 - 4d 61 72 6b 2e 6c 6e 6b  ........Mark.lnk
00000020   00 00 42 00 09 00 04 00 - ef be 00 00 00 00 00 00  ..B.      ...ï¾......
00000030   00 00 2e 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
00000040   00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
00000050   4d 00 61 00 72 00 6b 00 - 2e 00 6c 00 6e 00 6b 00  M.a.r.k...l.n.k.
00000060   00 00 18 00 00 00                                  ......
```

Fig 3. Using Registry Editor to check RecentDocs.

We used RegRipper and managed to obtain the same finding:

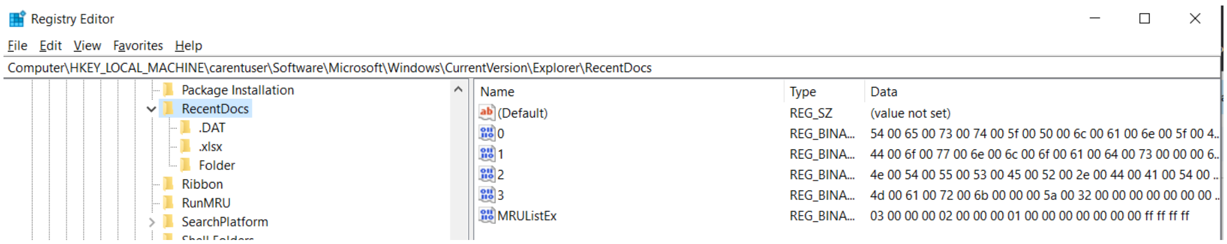


```
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2016-03-08 04:36:04Z
  3 = Mark
  2 = NTUSER.DAT
  1 = Downloads
  0 = Test_Plan_Confidential.xlsx

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.DAT
LastWrite Time 2016-03-08 04:36:04Z
MRUListEx = 0
  0 = NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx
LastWrite Time 2016-03-08 04:03:26Z
MRUListEx = 0
  0 = Test_Plan_Confidential.xlsx

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time 2016-03-08 04:36:04Z
MRUListEx = 1,0
  1 = Mark
  0 = Downloads
```

Fig 4. Using RegRipper to check RecentDocs

From Fig 3, .lnk files are Windows shortcuts files that are created to improve user access. These files can be created automatically when the user recently accessed a certain file. Hence the existence of Download.lnk and Mark.lnk indicates that these folders have been recently accessed.

We noted the order of file access via the MRUListEx (Most Recently Used list) value, which can be found under the same RecentDocs subkey:



Computer\HKEY_LOCAL_MACHINE\carentuser\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| 0 | REG_BINA... | 54 00 65 00 73 00 74 00 5f 00 50 00 6c 00 61 00 6e 00 5f 00 4.. |
| 1 | REG_BINA... | 44 00 6f 00 77 00 6e 00 6c 00 6f 00 61 00 64 00 73 00 00 00 6.. |
| 2 | REG_BINA... | 4e 00 54 00 55 00 53 00 45 00 52 00 2e 00 44 00 41 00 54 00 .. |
| 3 | REG_BINA... | 4d 00 61 00 72 00 6b 00 00 00 5a 00 32 00 00 00 00 00 00 00 .. |
| MRUListEx | REG_BINA... | 03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 ff ff ff ff |

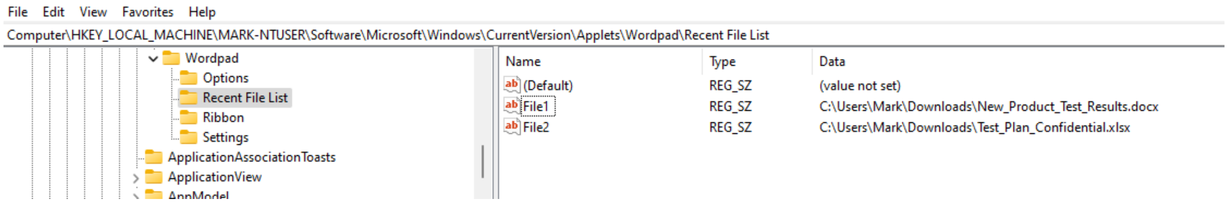
Fig 5. MRUListEx found under RecentDocs subkey

After viewing the MRUListEx value, the relevant notable access order is as follows:

Mark folder ⟶ Downloads folder ⟶ Test_Plan_Confidential.xlsx

This indicates that Test_Plan_Confidential.xlsx is stored under Mark's Downloads folder, which hints at the possibility that this file has been downloaded. By default, a file usually goes into the Downloads folder on a system if it gets downloaded.

And indeed, while browsing through Mark's NTUSER.DAT registry hive, we found that this file is stored under Mark's Downloads folder (C:\Users\Mark\Downloads\Test_Plan_Confidential.xlsx):



Computer\HKEY_LOCAL_MACHINE\MARK-NTUSER\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| File1 | REG_SZ | C:\Users\Mark\Downloads\New_Product_Test_Results.docx |
| File2 | REG_SZ | C:\Users\Mark\Downloads\Test_Plan_Confidential.xlsx |

Fig 6. Test_Plan_Confidential is stored under Mark's Downloads folder

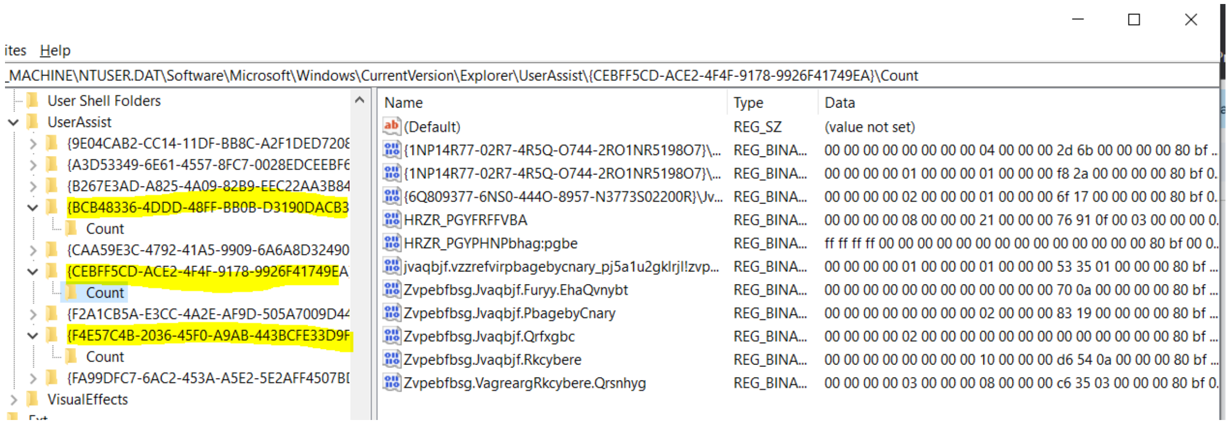
Since the Last Write Time of Test_Plan_Confidential.xlsx is 2 minutes after Mark accessed the FTP server and is in Mark's Downloads folder, we have a strong suspicion that he had downloaded Test_Plan_Confidential.xlsx from the internal FTP server and then possibly opened the file to read it or perform some changes to it.

## 5.5 Applications Accessed

In order to view the applications accessed, one of the ways is to view the UserAssist registry keys to view GUI-based programs launched from the desktop. We analysed evidence #01 (Mark-NTUSER.DAT) and observed the following registry:

\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

We found 3 UserAssist keys with valid values inside its 'Count' keys:



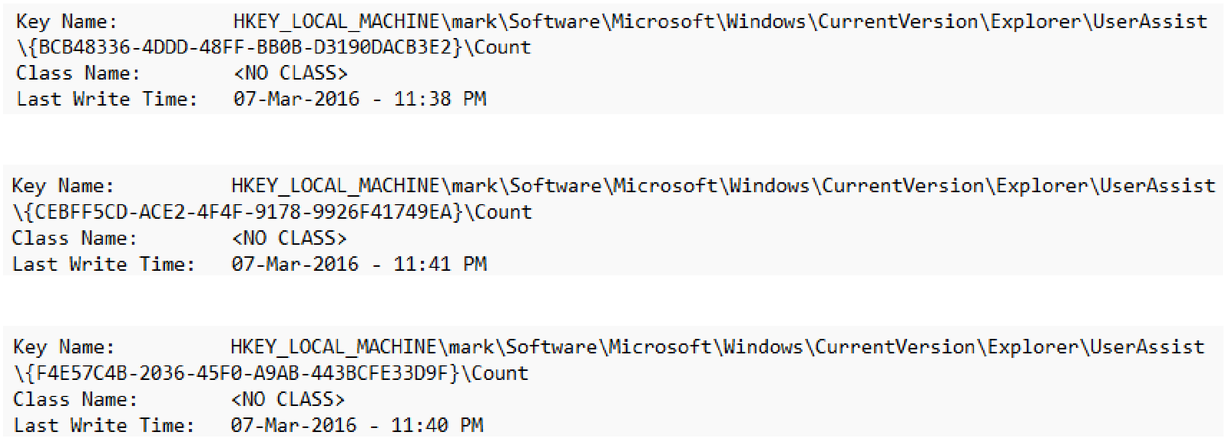
_MACHINE\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

```
User Shell Folders
UserAssist
  {9E04CAB2-CC14-11DF-BB8C-A2F1DED7208
  {A3D53349-6E61-4557-8FC7-0028EDCEEBF6
  {B267E3AD-A825-4A09-82B9-EEC22AA3B84
  {BCB48336-4DDD-48FF-BB0B-D3190DACB3
    Count
  {CAA59E3C-4792-41A5-9909-6A6A8D32490
  {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA
    Count
  {F2A1CB5A-E3CC-4A2E-AF9D-505A7009D44
  {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F
    Count
  {FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BI
VisualEffects
```

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| {1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\... | REG_BINA... | 00 00 00 00 00 00 00 00 04 00 00 00 2d 6b 00 00 00 00 80 bf ... |
| {1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\... | REG_BINA... | 00 00 00 00 01 00 00 00 01 00 00 00 f8 2a 00 00 00 00 80 bf 0... |
| {6Q809377-6NS0-444O-8957-N3773S02200R}\Jv... | REG_BINA... | 00 00 00 00 02 00 00 00 01 00 00 00 6f 17 00 00 00 00 80 bf 0... |
| HRZR_PGYFRFFVBA | REG_BINA... | 00 00 00 00 08 00 00 00 21 00 00 00 76 91 0f 00 03 00 00 00 0... |
| HRZR_PGYPHNPbhag:pgbe | REG_BINA... | ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 bf 00 0... |
| jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjl!zvp... | REG_BINA... | 00 00 00 00 01 00 00 00 01 00 00 00 53 35 01 00 00 00 80 bf ... |
| Zvpebfbsg.Jvaqbjf.Furyy.EhaQvnybt | REG_BINA... | 00 00 00 00 00 00 00 00 00 00 00 00 70 0a 00 00 00 00 80 bf ... |
| Zvpebfbsg.Jvaqbjf.PbagebyCnary | REG_BINA... | 00 00 00 00 00 00 00 00 02 00 00 00 83 19 00 00 00 00 80 bf ... |
| Zvpebfbsg.Jvaqbjf.Qrfxgbc | REG_BINA... | 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 80 bf ... |
| Zvpebfbsg.Jvaqbjf.Rkcybere | REG_BINA... | 00 00 00 00 00 00 00 00 10 00 00 00 d6 54 0a 00 00 00 80 bf ... |
| Zvpebfbsg.VagreargRkcybere.Qrsnhyg | REG_BINA... | 00 00 00 00 03 00 00 00 08 00 00 00 c6 35 03 00 00 00 80 bf 0... |

Fig 7. Notable UserAssist keys (highlighted in yellow)

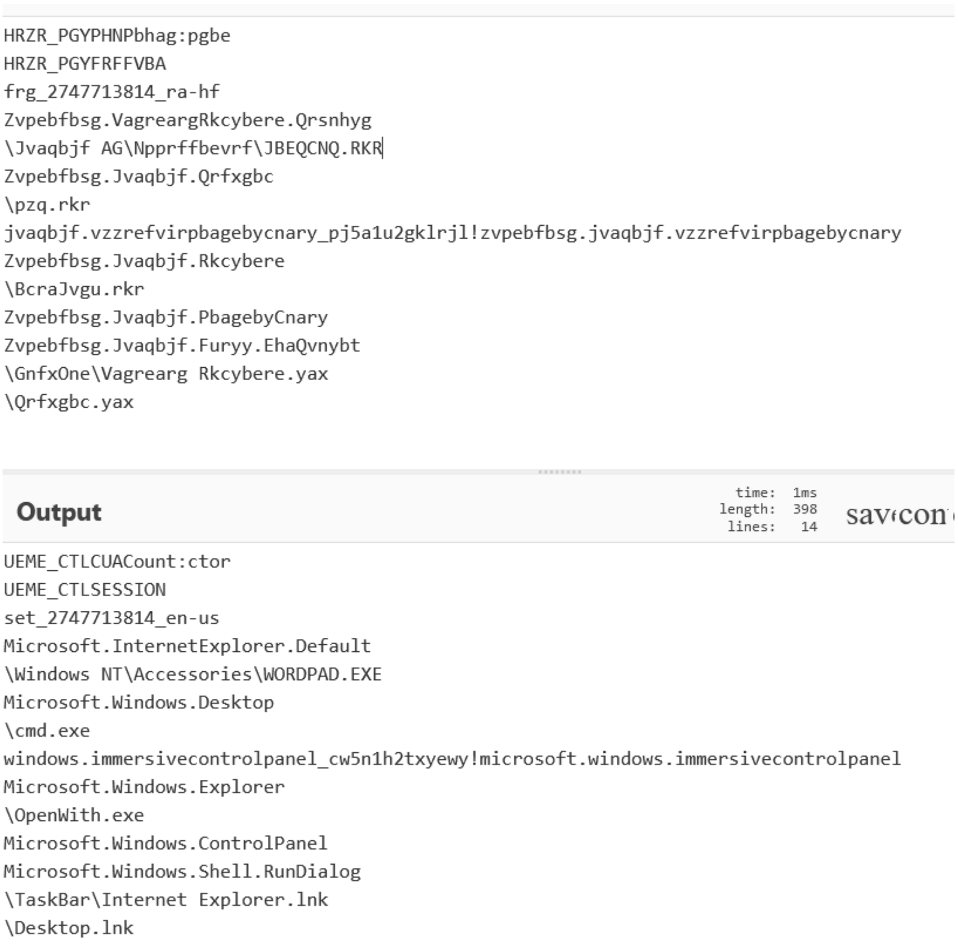
We checked the access times of these programs (by exporting the key from RegEdit and viewing the values in notepad) and they were indeed accessed on the same day and hour as the suspicious file, Test_Plan_Confidential.xlsx that was mentioned earlier:



```
Key Name:          HKEY_LOCAL_MACHINE\mark\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
\{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}\Count
Class Name:        <NO CLASS>
Last Write Time:   07-Mar-2016 - 11:38 PM


Key Name:          HKEY_LOCAL_MACHINE\mark\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
Class Name:        <NO CLASS>
Last Write Time:   07-Mar-2016 - 11:41 PM


Key Name:          HKEY_LOCAL_MACHINE\mark\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count
Class Name:        <NO CLASS>
Last Write Time:   07-Mar-2016 - 11:40 PM
```

Fig 8. The programs access date is the same as the suspicious file

Looking at the values inside the 3 notable UserAssist keys, they are ROT13 encoded names. Hence we converted the value into a readable format and get the following:



```
HRZR_PGYPHNPbhag:pgbe
HRZR_PGYFRFFVBA
frg_2747713814_ra-hf
Zvpebfbsg.VagreargRkcybere.Qrsnhyg
\Jvaqbjf AG\Nppr ffbevrf\JBEQCNQ.RKR
Zvpebfbsg.Jvaqbjf.Qrfxgbc
\pzq.rkr
jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjl!zvpebfbsg.jvaqbjf.vzzrefvirpbagebycnary
Zvpebfbsg.Jvaqbjf.Rkcybere
\BcraJvgu.rkr
Zvpebfbsg.Jvaqbjf.PbagebyCnary
Zvpebfbsg.Jvaqbjf.Furyy.EhaQvnybt
\GnfxOne\Vagrearg Rkcybere.yax
\Qrfxgbc.yax
```

**Output**

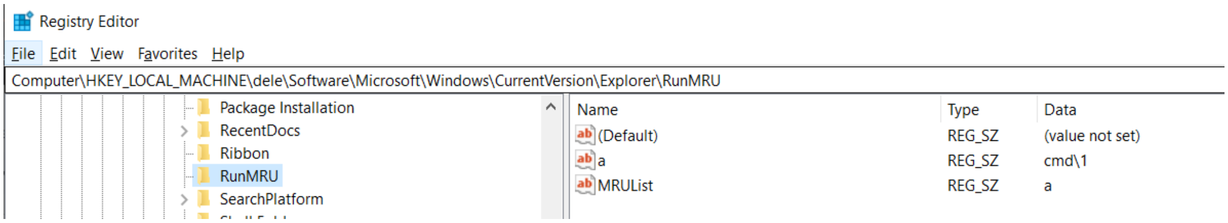
```
  time:  1ms
length:  398
 lines:   14
```

```
UEME_CTLCUACount:ctor
UEME_CTLSESSION
set_2747713814_en-us
Microsoft.InternetExplorer.Default
\Windows NT\Accessories\WORDPAD.EXE
Microsoft.Windows.Desktop
\cmd.exe
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
Microsoft.Windows.Explorer
\OpenWith.exe
Microsoft.Windows.ControlPanel
Microsoft.Windows.Shell.RunDialog
\TaskBar\Internet Explorer.lnk
\Desktop.lnk
```

Fig 9. Conversion of UserAssist ROT13 encoded value to readable value

From the output of the readable text conversion, applications Mark may have opened are **Internet Explorer, Windows Explorer, Wordpad and command prompt**.

As mentioned above, Internet Explorer was most likely used to access the FTP server. However, nothing notable was found for the command prompt application.

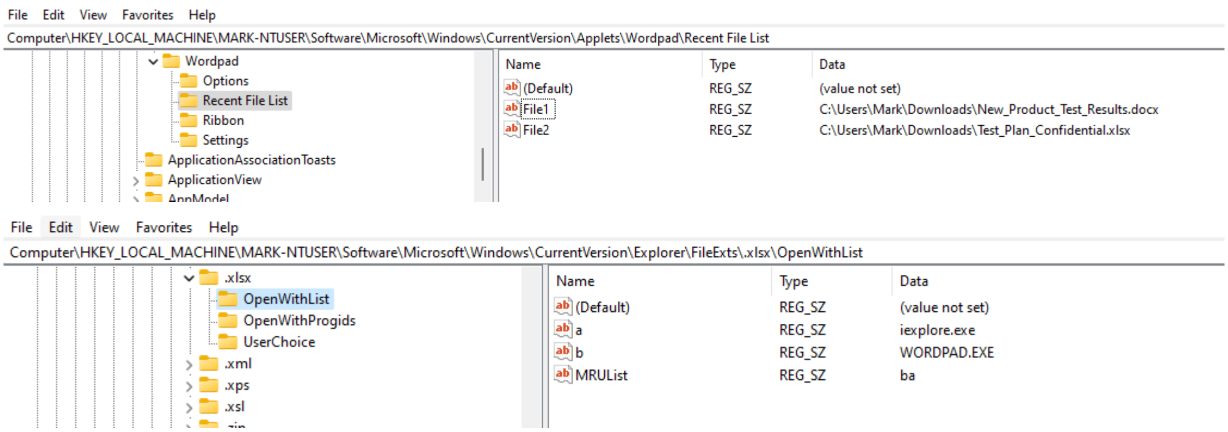


Computer\HKEY_LOCAL_MACHINE\dele\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| a | REG_SZ | cmd\1 |
| MRUList | REG_SZ | a |

Fig 10. Command prompt is run through Run Utility.

However, we observed that Test_Plan_Confidential.xlsx could have been accessed via Wordpad, including another document called New_Product_Test_Result.docx:



Computer\HKEY_LOCAL_MACHINE\MARK-NTUSER\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| File1 | REG_SZ | C:\Users\Mark\Downloads\New_Product_Test_Results.docx |
| File2 | REG_SZ | C:\Users\Mark\Downloads\Test_Plan_Confidential.xlsx |

Computer\HKEY_LOCAL_MACHINE\MARK-NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\OpenWithList

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| a | REG_SZ | iexplore.exe |
| b | REG_SZ | WORDPAD.EXE |
| MRUList | REG_SZ | ba |

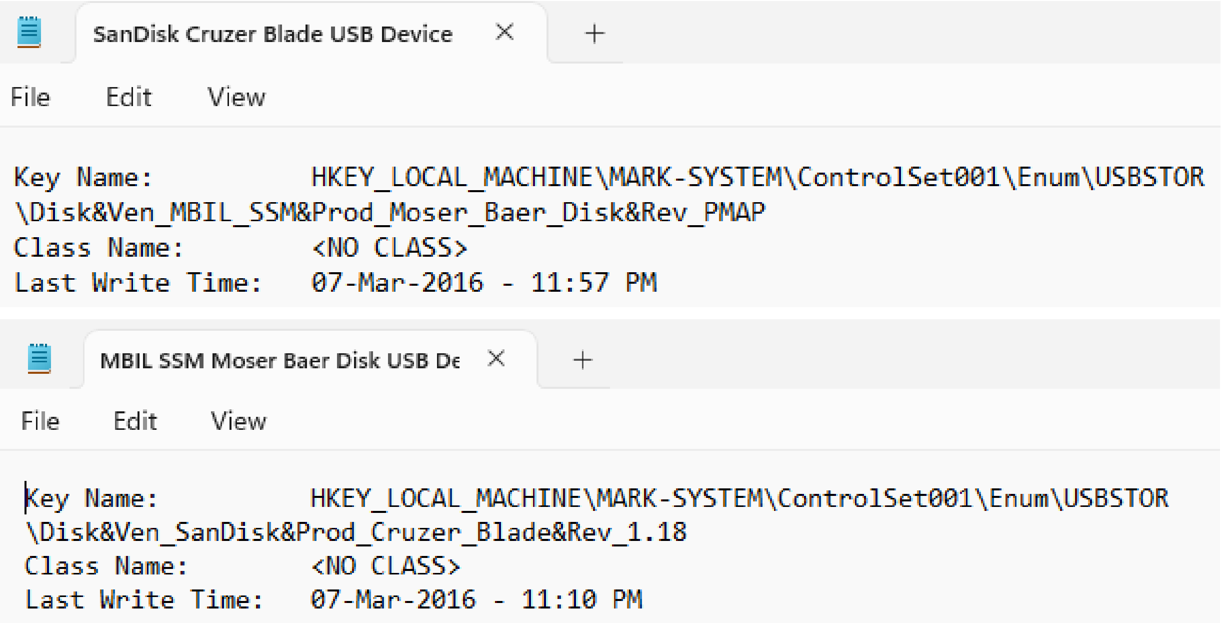
Fig 11. Looking at what Wordpad has opened

Unfortunately, that was the only place that we could find the New_Product_Test_Result.docx. Moreover, it did not appear in the RecentDocs key, more will be discussed in Section 7.3.

## 5.5 USB Devices

Using the Registry Editor, our team observed that there were two USB devices that had been connected to Mark's computer before.

| USB Device | Last Write Time (EST) |
|---|---|
| SanDisk Cruzer Blade USB Device | 7/3/2016 - 11:10 PM |
| MBIL SSM Moser Baer Disk USB Device | 7/3/2016 - 11:57 PM |



SanDisk Cruzer Blade USB Device
File
Edit
View
MBIL SSM Moser Baer Disk USB De
File
Edit
View

```
Key Name:          HKEY_LOCAL_MACHINE\MARK-SYSTEM\ControlSet001\Enum\USBSTOR
\Disk&Ven_MBIL_SSM&Prod_Moser_Baer_Disk&Rev_PMAP
Class Name:        <NO CLASS>
Last Write Time:   07-Mar-2016 - 11:57 PM
```

```
Key Name:          HKEY_LOCAL_MACHINE\MARK-SYSTEM\ControlSet001\Enum\USBSTOR
\Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.18
Class Name:        <NO CLASS>
Last Write Time:   07-Mar-2016 - 11:10 PM
```

Fig 12. USB devices recently connected to Mark's computer

From our analysis, we noticed that the last write time of the Test_Plan_Confidential.xlsx is at 7/3/2016 - 11:03 PM and within that same hour, both of the USB devices have also been written to. The last write time is updated whenever files or data are written to or removed from the USB device. It can also be updated when a USB device is connected or disconnected from the machine.

Therefore, there is a high possibility that the file (Test_Plan_Confidential.xlsx) could have been saved on either of the USB devices.

## 5.6 Event Logs

The event logs file is one of the critical pieces of evidence that the team analysed to formulate the timeline for the case.

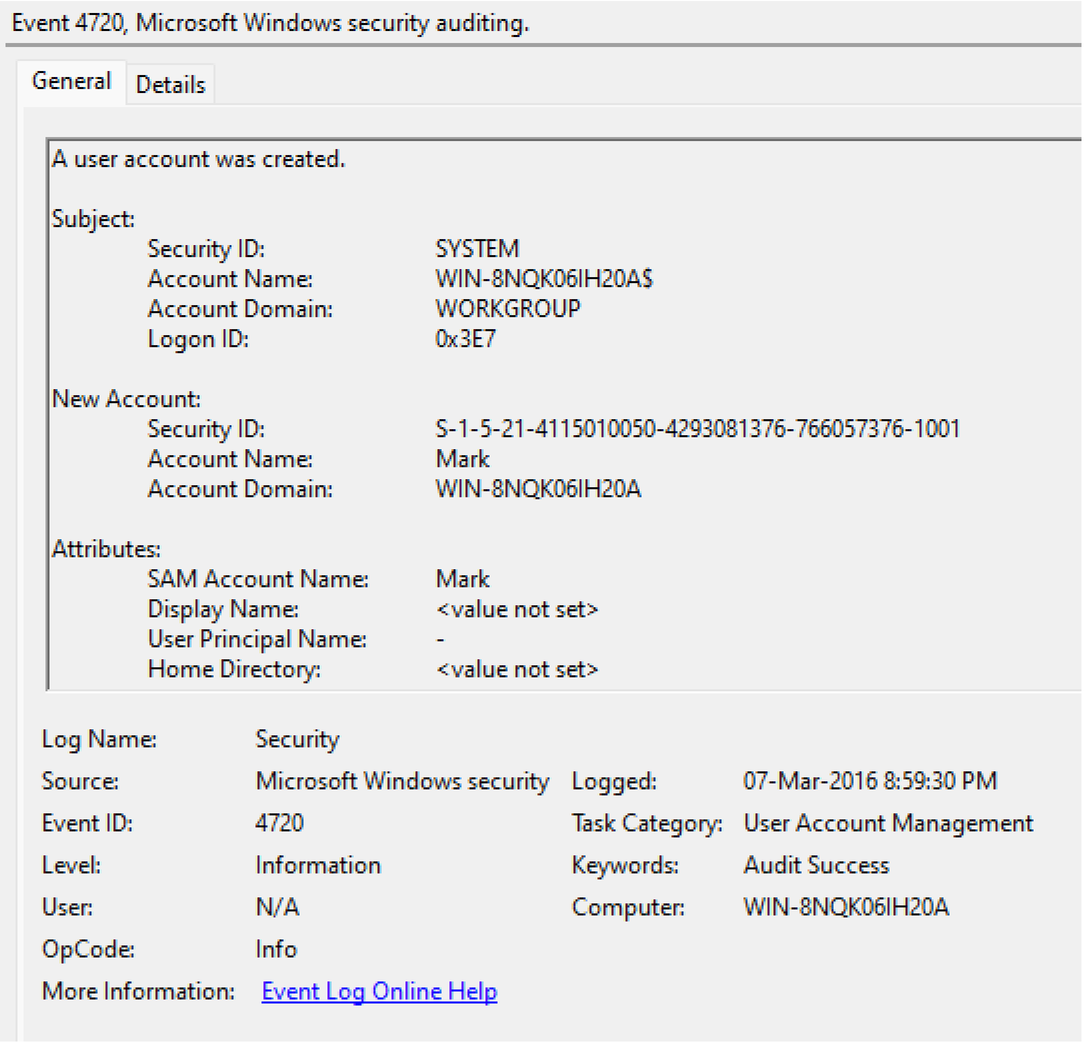
### 5.6.1 Mark Account Creation

At 8:59:30 PM (EST) on 7 March 2016, an account called "Mark" was created. The other subsequent logs show changes to this new user account (e.g. changes to User Access Control). The team found that the creation time for Mark's account is suspicious. Given that this event log file was seized from Mark’s computer, our team finds it unusual that Mark’s account was created on the same day as the other suspicious event logs were generated.

We are able to rule this out as a legitimate account creation because being an employee in the company, Mark should have already had his account created much earlier on his first day of work. Moreover, this would have been done during normal work hours. This account is created 2 hours before all the suspicious activities happened could be a sign that someone else was trying to frame Mark.

Thus, our team has derived two conclusions for this account creation. Firstly, the account is created by the case creator which explains the creation of Mark's account on the same day. If this is true, then the case would follow the claim that Mark is suspicious as all the activities found would be performed by Mark himself.

Alternatively, someone may have impersonated Mark and performed suspicious activities on the computer to sabotage him.

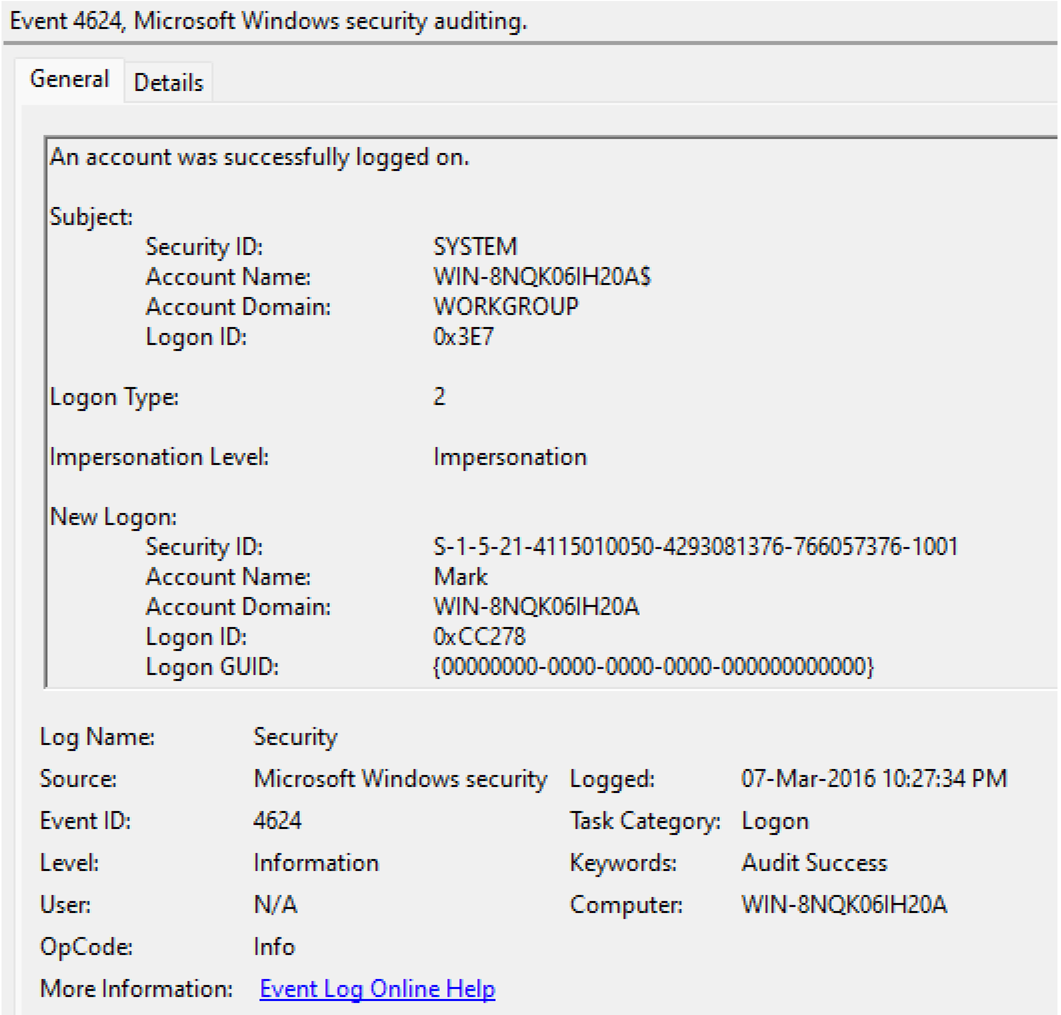


Event 4720, Microsoft Windows security auditing.

```
A user account was created.

Subject:
        Security ID:            SYSTEM
        Account Name:           WIN-8NQK06IH20A$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

New Account:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-1001
        Account Name:           Mark
        Account Domain:         WIN-8NQK06IH20A

Attributes:
        SAM Account Name:       Mark
        Display Name:           <value not set>
        User Principal Name:    -
        Home Directory:         <value not set>
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          07-Mar-2016 8:59:30 PM
Event ID:          4720                         Task Category:   User Account Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        WIN-8NQK06IH20A
OpCode:            Info
More Information:  Event Log Online Help
```

Fig 13. Mark Account Created



Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           WIN-8NQK06IH20A$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     2

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-1001
        Account Name:           Mark
        Account Domain:         WIN-8NQK06IH20A
        Logon ID:               0xCC278
        Logon GUID:             {00000000-0000-0000-0000-000000000000}
```

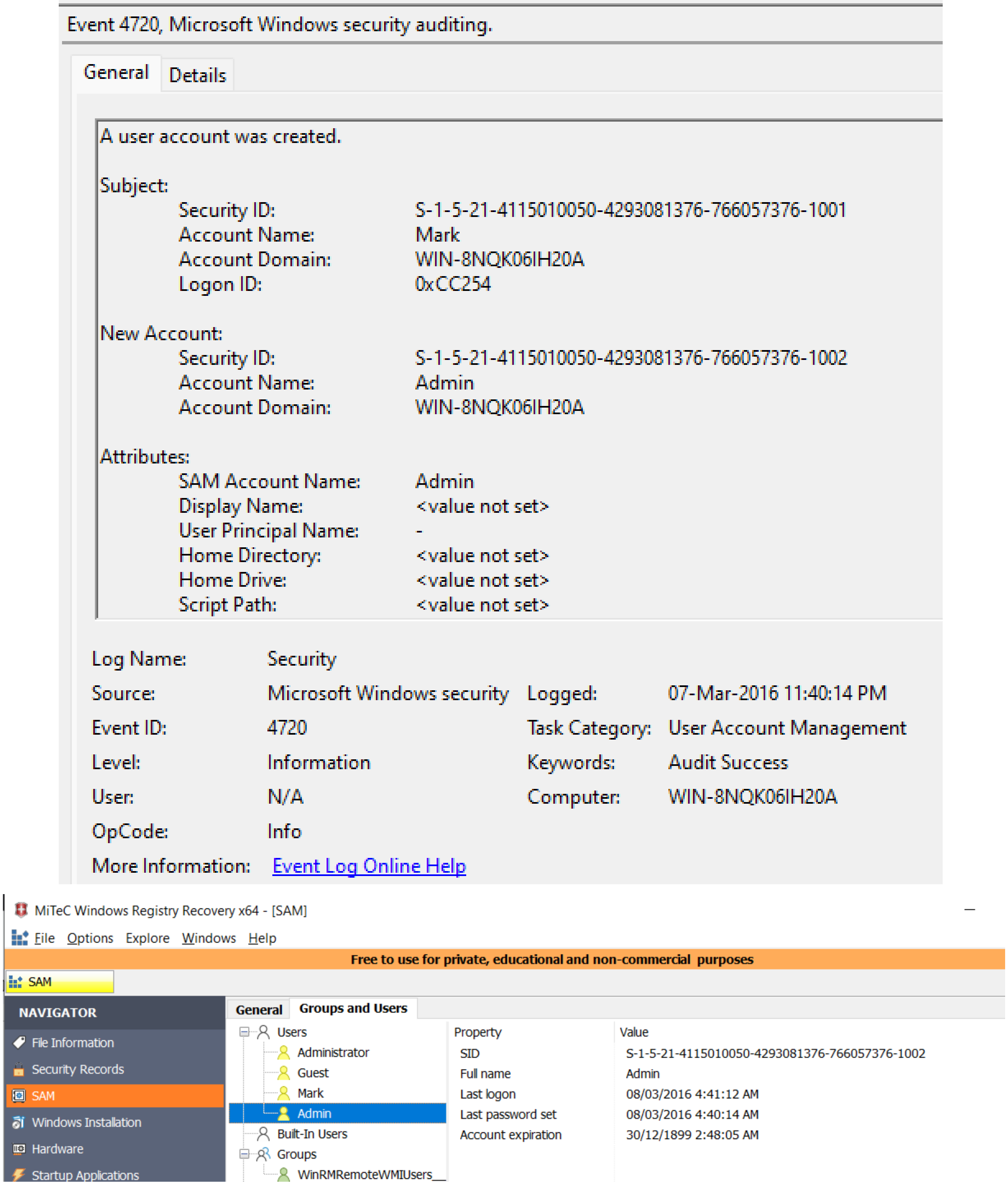
```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          07-Mar-2016 10:27:34 PM
Event ID:          4624                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        WIN-8NQK06IH20A
OpCode:            Info
More Information:  Event Log Online Help
```

Fig 14 Mark account was login

### 5.6.2 Admin Account Creation

Apart from Mark's account creation, we also noticed that Mark created an "Admin" account at 7 Mar 2016 11:40:14PM (EST). After the creation of the Admin account, Mark enabled the account and set a password for that account. He also performed a series of actions to the account such as adding the "Admin" account into the built-in administrator group, which gives the account in that group super privileges.

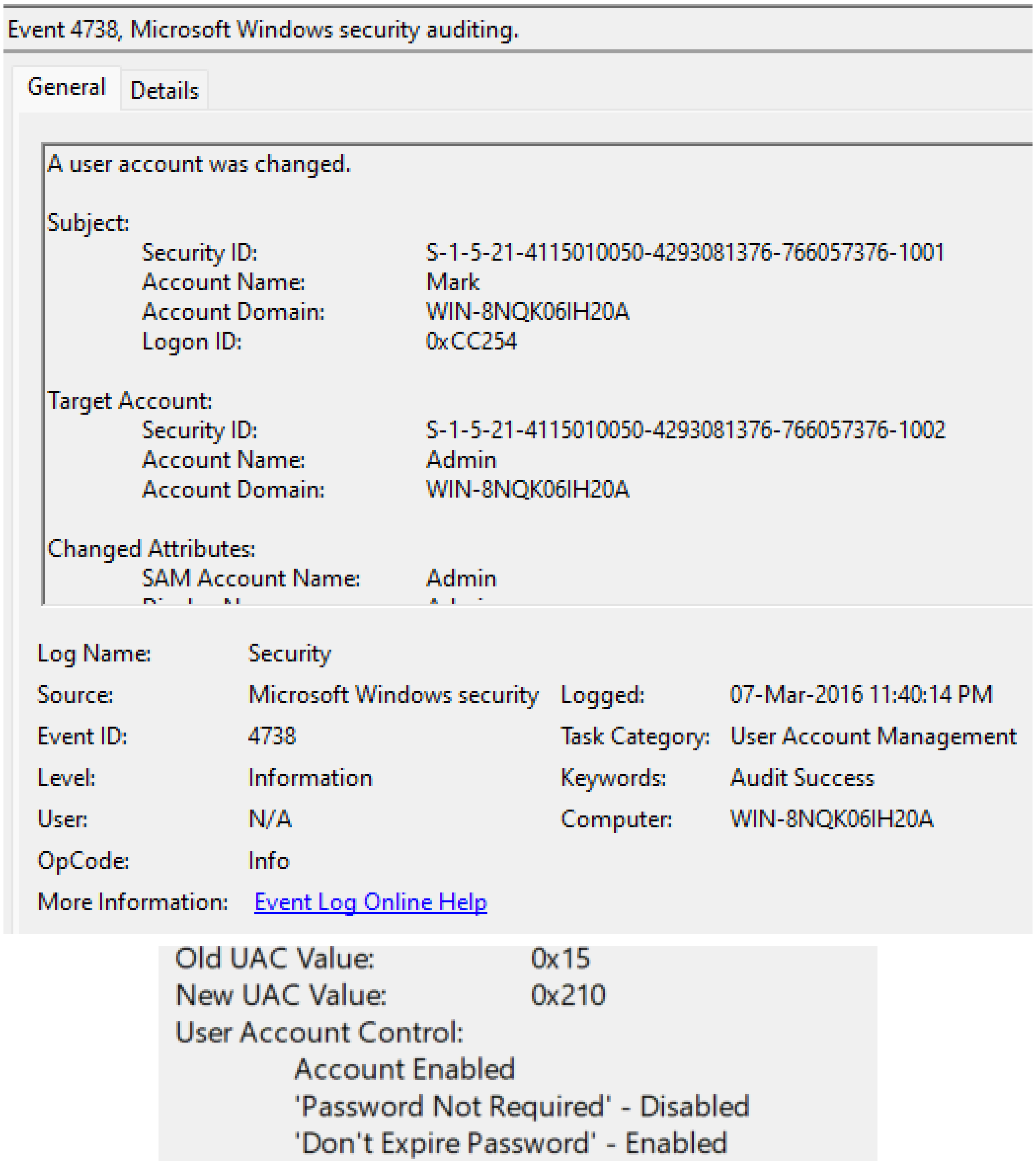
The "Admin" account was also created at a suspicious time as it was created at the same hour after Mark had accessed the sensitive file (Test_Plan_Confidential at 7 Mar 2016 11:03 PM).



```
Event 4720, Microsoft Windows security auditing.

General   Details

A user account was created.

Subject:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-1001
        Account Name:           Mark
        Account Domain:         WIN-8NQK06IH20A
        Logon ID:               0xCC254

New Account:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-1002
        Account Name:           Admin
        Account Domain:         WIN-8NQK06IH20A

Attributes:
        SAM Account Name:       Admin
        Display Name:           <value not set>
        User Principal Name:    -
        Home Directory:         <value not set>
        Home Drive:             <value not set>
        Script Path:            <value not set>

Log Name:          Security
Source:            Microsoft Windows security   Logged:         07-Mar-2016 11:40:14 PM
Event ID:          4720                         Task Category:  User Account Management
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       WIN-8NQK06IH20A
OpCode:            Info
More Information:  Event Log Online Help
```

| Property | Value |
|---|---|
| SID | S-1-5-21-4115010050-4293081376-766057376-1002 |
| Full name | Admin |
| Last logon | 08/03/2016 4:41:12 AM |
| Last password set | 08/03/2016 4:40:14 AM |
| Account expiration | 30/12/1899 2:48:05 AM |

Fig 15. Mark created Admin Account



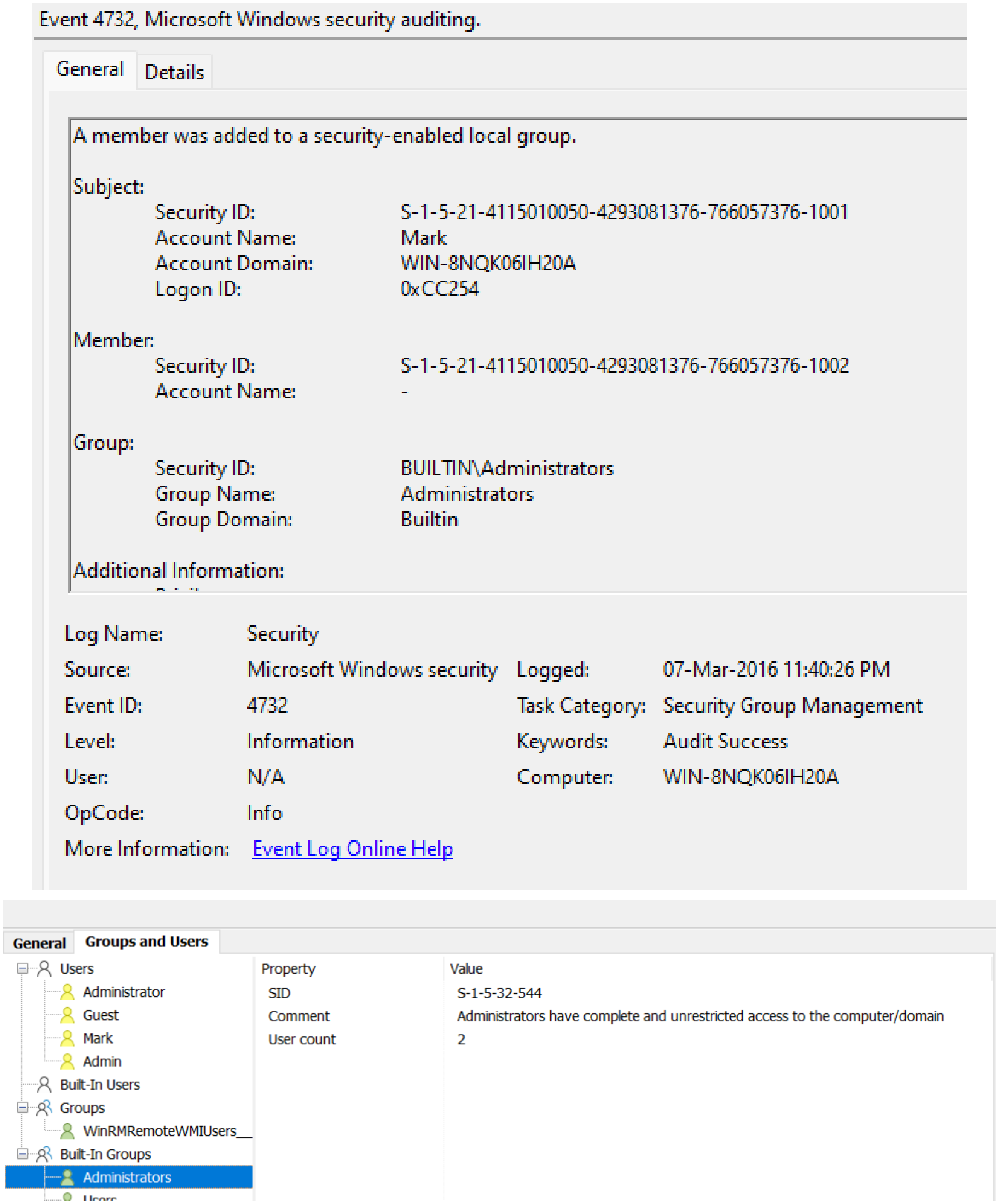
Event 4738, Microsoft Windows security auditing.

```
A user account was changed.

Subject:
	Security ID:		S-1-5-21-4115010050-4293081376-766057376-1001
	Account Name:		Mark
	Account Domain:		WIN-8NQK06IH20A
	Logon ID:		0xCC254

Target Account:
	Security ID:		S-1-5-21-4115010050-4293081376-766057376-1002
	Account Name:		Admin
	Account Domain:		WIN-8NQK06IH20A

Changed Attributes:
	SAM Account Name:	Admin
```

| | | | |
|---|---|---|---|
| Log Name: | Security | | |
| Source: | Microsoft Windows security | Logged: | 07-Mar-2016 11:40:14 PM |
| Event ID: | 4738 | Task Category: | User Account Management |
| Level: | Information | Keywords: | Audit Success |
| User: | N/A | Computer: | WIN-8NQK06IH20A |
| OpCode: | Info | | |
| More Information: | Event Log Online Help | | |

```
Old UAC Value:		0x15
New UAC Value:		0x210
User Account Control:
	Account Enabled
	'Password Not Required' - Disabled
	'Don't Expire Password' - Enabled
```

Fig 16. Password is enabled and required for Admin account



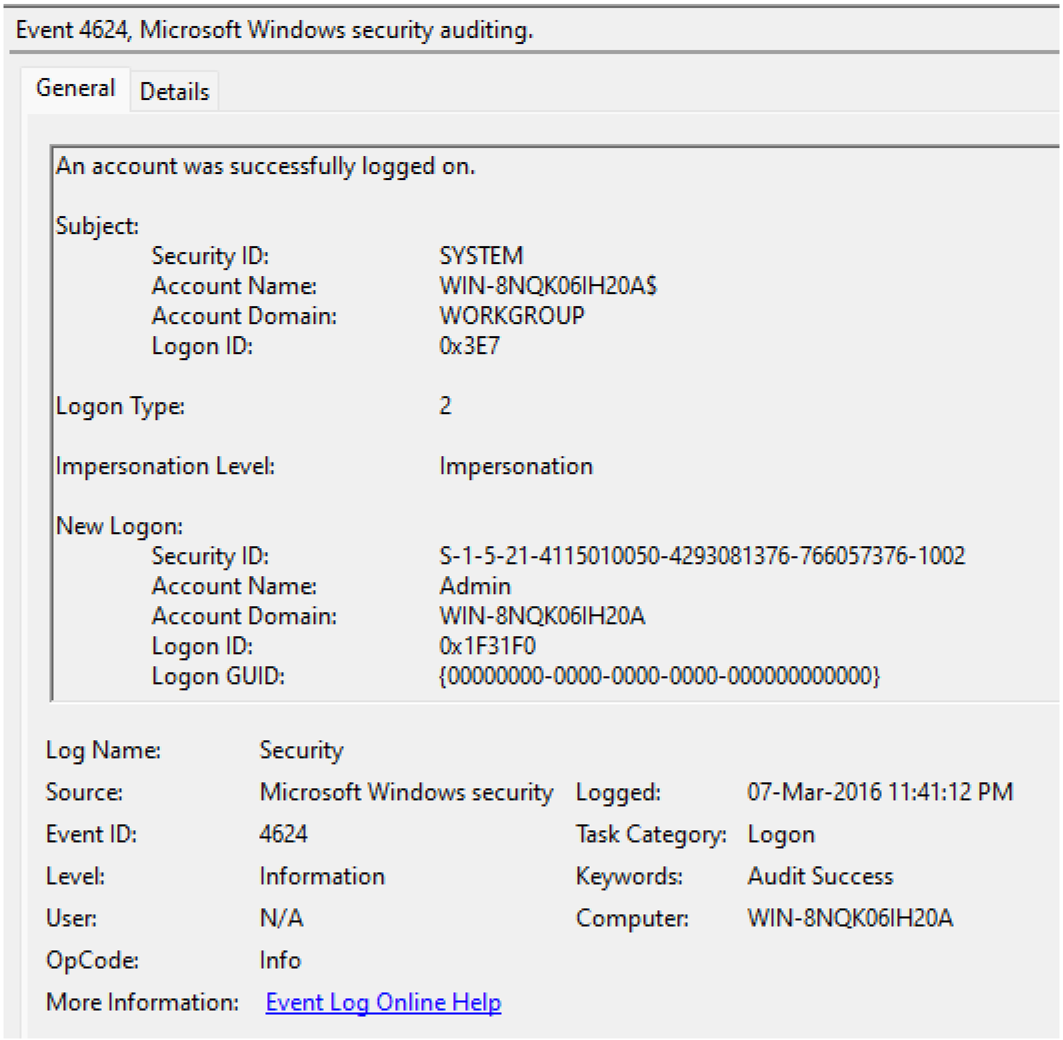
Event 4732, Microsoft Windows security auditing.

```
A member was added to a security-enabled local group.

Subject:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-1001
        Account Name:           Mark
        Account Domain:         WIN-8NQK06IH20A
        Logon ID:               0xCC254

Member:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-1002
        Account Name:           -

Group:
        Security ID:            BUILTIN\Administrators
        Group Name:             Administrators
        Group Domain:           Builtin

Additional Information:
```

```
Log Name:          Security
Source:            Microsoft Windows security    Logged:          07-Mar-2016 11:40:26 PM
Event ID:          4732                          Task Category:   Security Group Management
Level:             Information                   Keywords:        Audit Success
User:              N/A                           Computer:        WIN-8NQK06IH20A
OpCode:            Info
More Information:  Event Log Online Help
```

| Property | Value |
|---|---|
| SID | S-1-5-32-544 |
| Comment | Administrators have complete and unrestricted access to the computer/domain |
| User count | 2 |

Fig 17. The Admin account was added into the built in Administrators group

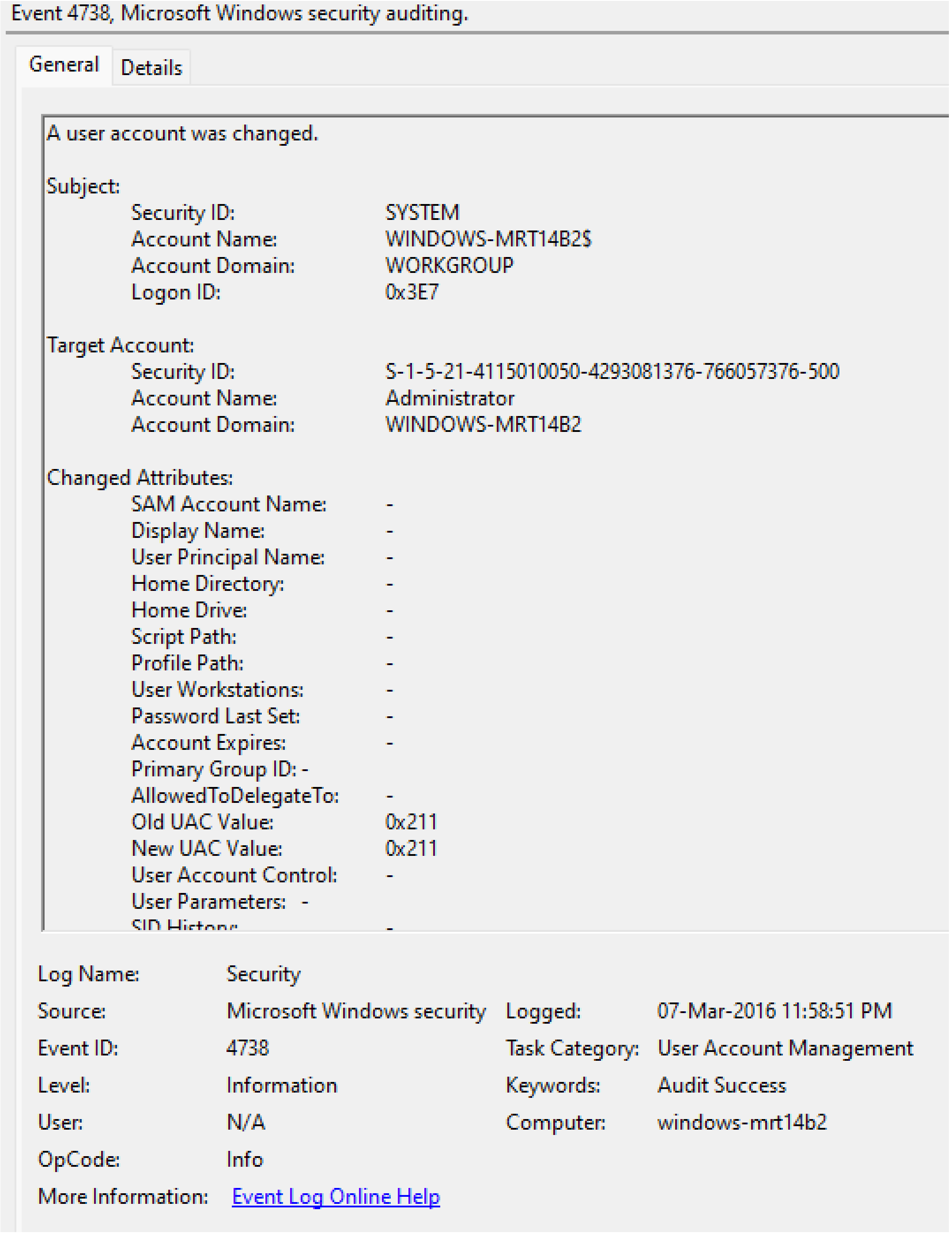


```
Event 4624, Microsoft Windows security auditing.

General   Details

An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           WIN-8NQK06IH20A$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     2

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-1002
        Account Name:           Admin
        Account Domain:         WIN-8NQK06IH20A
        Logon ID:               0x1F31F0
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Log Name:          Security
Source:            Microsoft Windows security   Logged:          07-Mar-2016 11:41:12 PM
Event ID:          4624                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        WIN-8NQK06IH20A
OpCode:            Info
More Information:  Event Log Online Help
```

Fig 18. The Admin account was logged into

### 5.6.3 Administrator Account Disabled

At 7 Mar 2016 11:58:51 PM (EST), after the Admin account was added to the built-in Administrators group, the real Administrator account was disabled. As seen in the event logs, the UAC value has been changed to 0x211: Account Disabled, Password Never Expires. Our team found this action suspicious as the creation of an “Admin” account could potentially be created to replace the legitimate “Administrator” account. Furthermore, if this action is performed by Mark, this might indicate that he might have malicious intent to access the company’s resources even after he leaves the company as he still has a way to access the resources via a different privileged account.



Event 4738, Microsoft Windows security auditing.

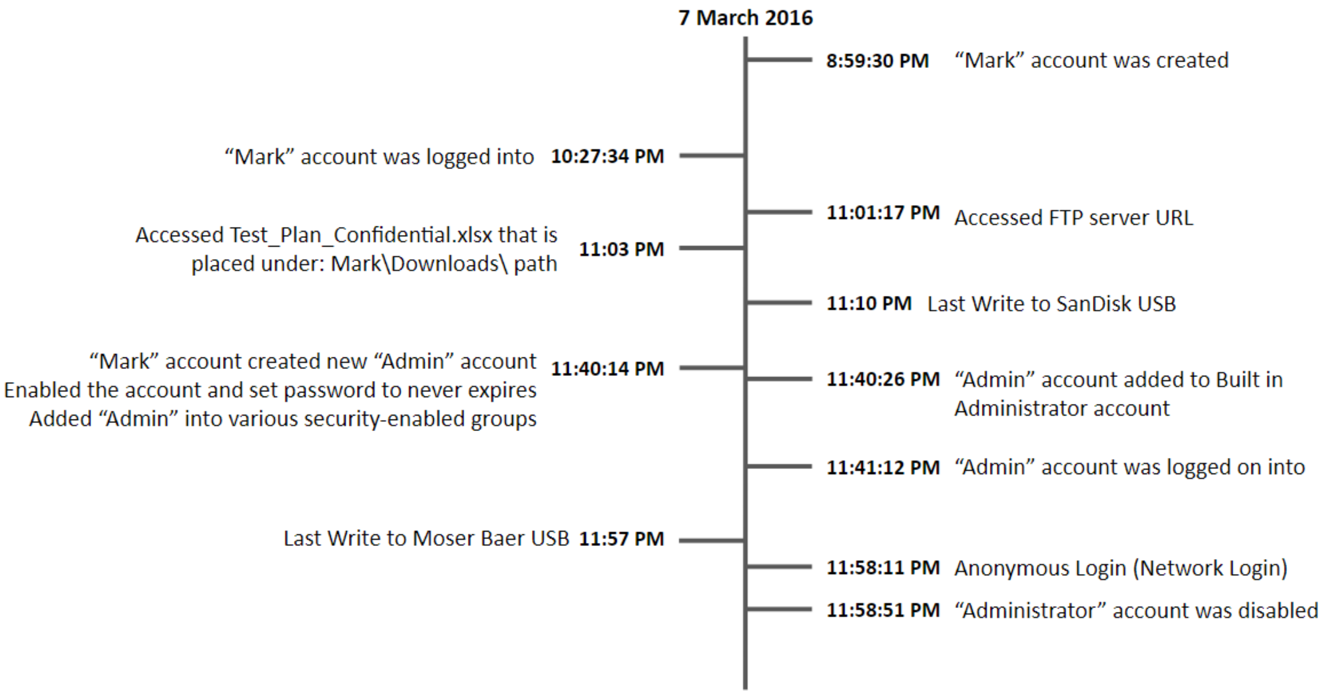
```
A user account was changed.

Subject:
        Security ID:            SYSTEM
        Account Name:           WINDOWS-MRT14B2$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Target Account:
        Security ID:            S-1-5-21-4115010050-4293081376-766057376-500
        Account Name:           Administrator
        Account Domain:         WINDOWS-MRT14B2

Changed Attributes:
        SAM Account Name:       -
        Display Name:           -
        User Principal Name:    -
        Home Directory:         -
        Home Drive:             -
        Script Path:            -
        Profile Path:           -
        User Workstations:      -
        Password Last Set:      -
        Account Expires:        -
        Primary Group ID: -
        AllowedToDelegateTo:    -
        Old UAC Value:          0x211
        New UAC Value:          0x211
        User Account Control:   -
        User Parameters:  -
        SID History:            -
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          07-Mar-2016 11:58:51 PM
Event ID:          4738                         Task Category:   User Account Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        windows-mrt14b2
OpCode:            Info
More Information:  Event Log Online Help
```

Fig 17. The real Administrator account was disabled

# 6 Timeline

The following is a timeline that our team have drafted based on our knowledge of the events that happen in this case:



7 March 2016

8:59:30 PM “Mark” account was created

10:27:34 PM “Mark” account was logged into

11:01:17 PM Accessed FTP server URL

11:03 PM Accessed Test_Plan_Confidential.xlsx that is placed under: Mark\Downloads\ path

11:10 PM Last Write to SanDisk USB

11:40:14 PM “Mark” account created new “Admin” account  
Enabled the account and set password to never expires  
Added “Admin” into various security-enabled groups

11:40:26 PM “Admin” account added to Built in Administrator account

11:41:12 PM “Admin” account was logged on into

11:57 PM Last Write to Moser Baer USB

11:58:11 PM Anonymous Login (Network Login)

11:58:51 PM “Administrator” account was disabled

# 7 Other Interesting Findings

The team have observed some interesting findings that might be relevant to the case.

## 7.1 Time Modification

The event logs showed that there were changes made to the system time at different timings. The table below displays the occurrence of system time change in sequence from first to last.

| Time (EST) | Performed By | Process Information |
|---|---|---|
| Previous Time:<br>2016-03-07, 17:59:30<br>New Time:<br>2016-03-07, 20:59:30 | Security ID: SYSTEM<br>Account Name:<br>WIN-8NQK06IH20A$<br>Account Domain:<br>WORKGROUP<br>Logon ID: 0x3E7 | Process ID: 0x334<br>Name:<br>C:\Windows\System32\rundll32.exe |
| Previous Time:<br>2016-03-07, 23:13:12<br>New Time:<br>2016-03-07, 23:32:11 | | Process ID: 0x538<br>Name: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe |
| Previous Time:<br>2016-03-08, 00:00:44<br>New Time:<br>2016-03-26, 22:24:26 | | |
| Previous Time:<br>2016-03-26, 22:29:01<br>New Time:<br>2016-03-26, 22:37:11 | | |
| Previous Time:<br>2016-03-26, 22:38:49<br>New Time:<br>2016-03-27, 10:09:51 | | |

The first occurrence of the system time change is made on the host system, this event log is being captured prior to all other computer’s activity that is performed by Mark. The team is unable to determine the motive for this action but we feel that this action is not necessarily a cause for concern.

The subsequent system time change is triggered by the “vmtoolsd.exe” process. This process is associated with VMware Tools, a set of utilities that are installed on virtual machines running on VMware virtualization software. Our team was not able to give definite reasoning for these events but we came to two possible conclusions.

It could be possible that Mark is running a virtual machine on his computer and possibly performing some activities.

However, our team's main conclusion is that it could also be a result of the case creator trying to create different scenarios at different timing, hence, explaining the sudden change of system time and missing event logs from 8 Mar 2016 to 26 Mar 2016.

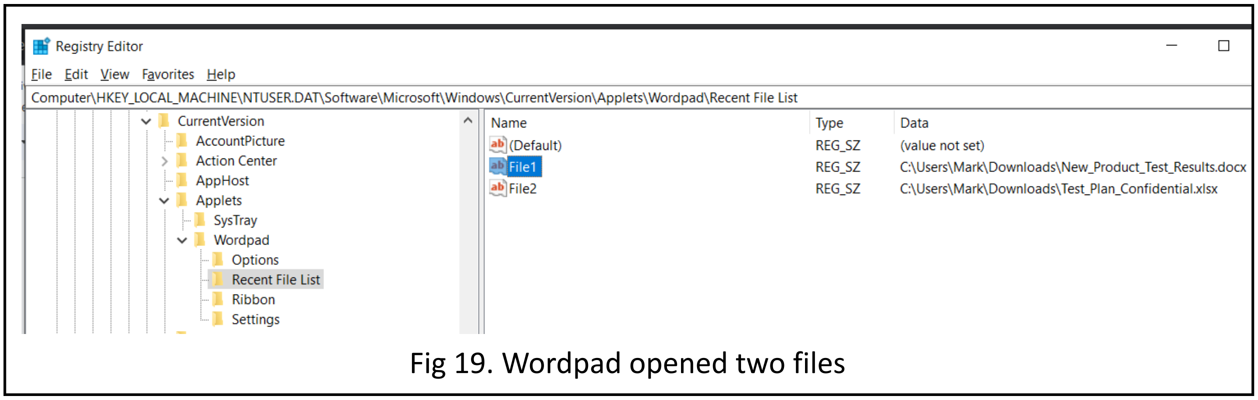
More evidence (section 9.3) is needed for the team to deduce the purpose of the time changes and the use of the virtual machine.

## 7.2 Change of Computer Name

In addition, we noticed that there are different computer names found in the Event Log. For instance, WIN-8NQK06IH20A and windows-mrt14b2. We know for certain that WIN-8NQK06IH20A belongs to Mark’s computer, however, we are unsure of what windows-mrt14b2 is as we are unable to find more supporting evidence to justify the appearance of that computer.

## 7.3 Notable file(s) accessed

As mentioned in section 5.5, **Wordpad.exe** was used to open **TWO** files - a .docx file and .xlsx file:



Computer\HKEY_LOCAL_MACHINE\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| File1 | REG_SZ | C:\Users\Mark\Downloads\New_Product_Test_Results.docx |
| File2 | REG_SZ | C:\Users\Mark\Downloads\Test_Plan_Confidential.xlsx |

Fig 19. Wordpad opened two files

However, New_Product_Test_Result.docx wasn't found in the RecentDocs registry key for recently accessed files even though it's under RecentFileList for Wordpad. Hence, we suspect that this file could have been possibly deleted or renamed.

# 8 Conclusion

After analysing the evidence, based on the team's knowledge, we have arrived at a tentative conclusion that Mark may be suspicious, but additional evidence is required to reach a more definitive conclusion. Given the limited scope of the evidence currently in possession, it is challenging to establish whether or not Mark has stolen any company data or confidential material.

## 8.1 Mark is Suspicious

The team is certain and able to corroborate the claim that Mark has been working during unusual hours based on the evidence timestamp generated from his computer activities. These odd hours started with Mark's account logging in at 7 Mar 2016 10:27 pm (EST) and only ended at 7 Mar 2016 11:58 pm (EST).

Additionally, the computer activities revealed that during the odd hours, Mark accessed an FTP server and highly likely downloaded confidential files to his computer as the Downloads folder was accessed at the same hour. Mark could have also read or even modified the files as he has used the Wordpad application to access the files "Test_Plan_Confidential.xlsx". During that same hour, from the computer's registry, we are able to observe that two USB devices were accessed. By analysing the timeline, we observed that the access time on the USB devices at 7 Mar 2016 11:10 pm (EST) and 7 Mar 2016 11:57 pm (EST) is later than the "Test_Plan_Confidential.xlsx" file at 7 Mar 2016 11:03 pm (EST). This suggests that the files could have been saved on these USB devices.

Furthermore, the creation of an "Admin" account on Mark's computer further increases our suspicion of him. This account was created with a password and was added to various groups such as the built-in user and administrator groups. It is highly possible that Mark planned to use this account as a backdoor to gain access to the company's resources after leaving the company. The fact that the account possesses super privileges, similar to those of the original administrator, in addition to disabling the real administrator account further reinforces the possibility of trying to disguise his newly created "Admin" account as the real one. Also, it was noted that there was a login to this "Admin" account at 7 Mar 2016 11:41 pm (EST). This could be Mark testing his 'backdoor' access into the "Admin" account.

Although these actions highly suggest that Mark might have ill intentions, additional evidence would be necessary to reach a more definitive conclusion.

## 8.2 Mark is not suspicious

This hypothesis stems largely from a single piece of evidence at 7 Mar 2016, 8:59:30 pm (EST) which is when Mark's account was created.

However, we also acknowledge that this log could have been recorded by accident and was generated by the case creator when creating this specific case. Due to lack of sufficient information, we are hence unable to come to a definitive conclusion and hence created these 2 main hypotheses.

# 9 Recommendations

Below are some recommendations and other evidence we think should be obtained to help reach a more definitive conclusion.

## 9.1 Obtaining the physical USB device

The physical USB devices (SanDisk Cruzer Blade USB Device and MBIL SSM Moser Baer Disk USB Device) in this forensic investigation are critical pieces of evidence that could yield valuable insights into Mark's culpability.

Obtaining the USB device would enable the team to create an identical image file of the data on the USB. The team would be able to analyse the data saved on the USB device and even retrieve any potentially deleted or concealed data.

Having access to the data on the detected USB devices would provide a more conclusive answer to the case. If the “Test_Plan_Confidential.xlsx” file is found on the USB (could use a hash lookup), it concludes that Mark is definitely suspicious.

## 9.2 USB Devices Interpretation

Our team has two interpretations of the sentence “employee, John, reported a missing USB storage drive and was also suspicious about Mark.” from the case description. The first interpretation is that the USB belongs to the company and John is tracking these USBs. The second interpretation is that the missing USB belongs to John. Depending on the interpretation, the recommendations would be different.

### 9.2.1 Inventory List of Company’s USB devices

Having access to the inventory list can help us to determine if the 2 USB devices belong to the company. As a USB drive has been reported missing, this could help prove whether Mark has stolen a USB device to copy the confidential files.

### 9.2.2 John’s SYSTEM registry hive

Having access to John’s SYSTEM registry hive could allow us to compare the values of the USBSTOR plugged into Mark’s system. If the values match, it would mean that there is a high possibility that Mark has access to the thumb drive that John had reported missing.

## 9.3 Image file of Mark’s laptop

Mark’s laptop is a critical piece of evidence since most of the evidence is stored there. Having an image file of Mark’s laptop can reveal critical data such as any potentially deleted or concealed data. Moreover, it can help give more information about what the document Test_Plan_Confidential.xlsx (and also New_Product_Test_Result.docx) is and if it has been modified or deleted.

## 9.4 More details on Mark’s resignation date and the company’s SOP for disemployment

It is important to obtain the exact date of Mark’s departure from the company as having this information will allow the team to establish a more precise timeline of events and eventually have a better conclusion on the motivation for any suspicious activity found on Mark’s computer.

Furthermore, investigating the company’s standard operating procedures for disemployment can provide insights to the forensic team on the process for revoking access to the company’s system and resources. The team would be able to determine if the computer event found on Mark’s laptop is a violation of the SOP, hence gaining stronger evidence to show that Mark had performed illegal activities.

## 9.5 More event logs

The event log file given for this case seems limited and is for security events. More event logs that provide information about PnP (Plug and Play devices) like USB plug-ins could be provided.