DETERMINE RANSOMWARE TIMELINE

Before I go into demo for ransomware timeline. I would like to refresh info on file system tunneling first.

Below mention article from Microsoft mention Windows NT contains file system tunneling capabilities

- https://support.microsoft.com/en-us/help/172190/windows-nt-contains-file-system-tunneling-capabilities

KEY INFORMATION WITHIN ARTICLE

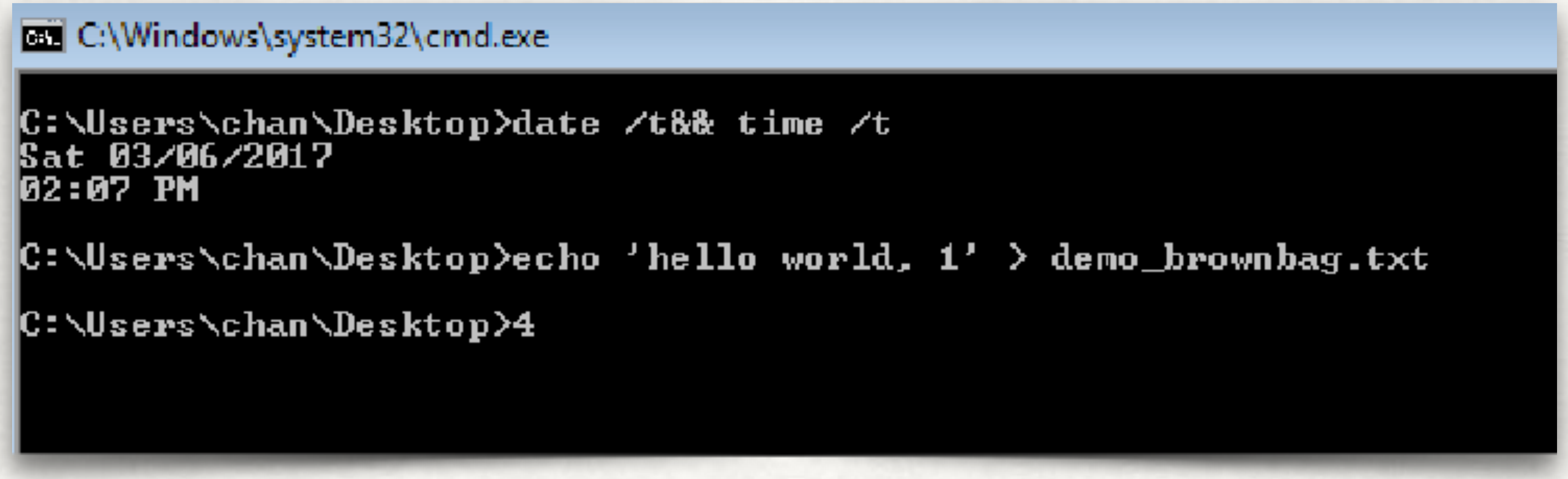
The Microsoft Windows products listed at the beginning of this article contain file system tunneling capabilities to enable compatibility with programs that rely on file systems being able to hold onto file meta-info for a short period of time. This occurs after **deletion** or **renaming** and re-introducing a new directory entry with that meta-info (if a **create** or **rename** occurs to cause a file of that name to appear again in a short period of time).

When a name is removed from a directory (**rename** or **delete**), its short/ long name pair and creation time are **saved in a cache**, keyed by the name that was removed. **When a name is added to a directory (rename or create), the cache is searched to see if there is information to restore. The cache is effective per instance of a directory. If a directory is deleted, the cache for it is removed.**

WHAT IS FILE TUNNELING

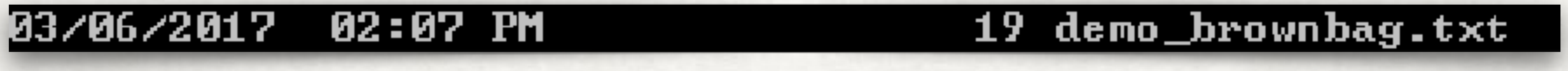
File delete and recreate with same file name within same directory

At 02:07 PM UTC +8 on 03rd of June 2017, a file call demo_brownbag.txt was created with the following content “hello world, 1”



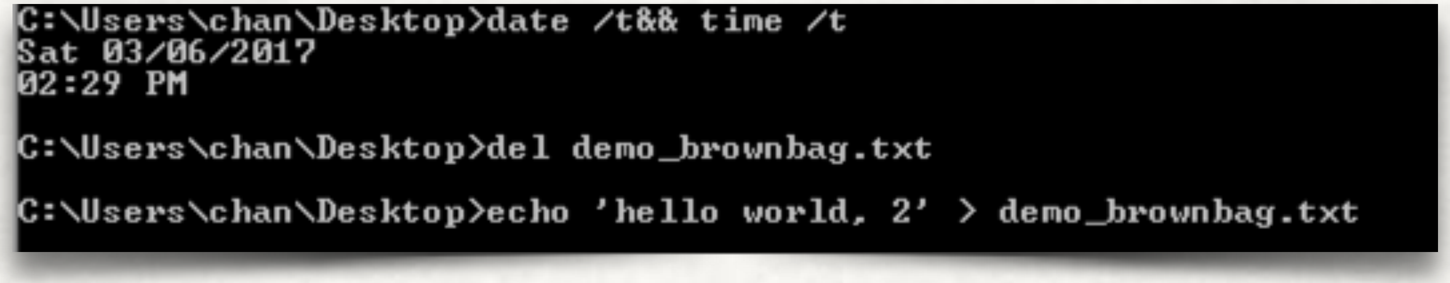
```
C:\Users\chan\Desktop>date /t&& time /t
Sat 03/06/2017
02:07 PM

C:\Users\chan\Desktop>echo 'hello world, 1' > demo_brownbag.txt

C:\Users\chan\Desktop>4
```

It was further verified when issue with the command `dir /tc`



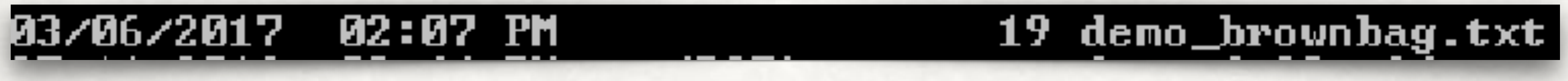
```
03/06/2017  02:07 PM                19 demo_brownbag.txt
```

Now at 02:29 PM UTC +8 on 03rd of June 2017, i deleted "demo_brownbag.txt" follow by creating a new file with the same name "demo_brownbag.txt" but with different content call "hello world, 2"



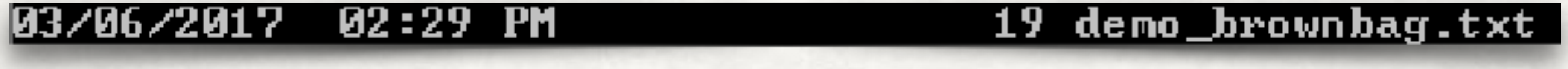
```
C:\Users\chan\Desktop>date /t&& time /t
Sat 03/06/2017
02:29 PM

C:\Users\chan\Desktop>del demo_brownbag.txt

C:\Users\chan\Desktop>echo 'hello world, 2' > demo_brownbag.txt
```

When doing a `dir /tc`, the newly created file still reflects 02:07 PM UTC +8 on 3rd of June 2017



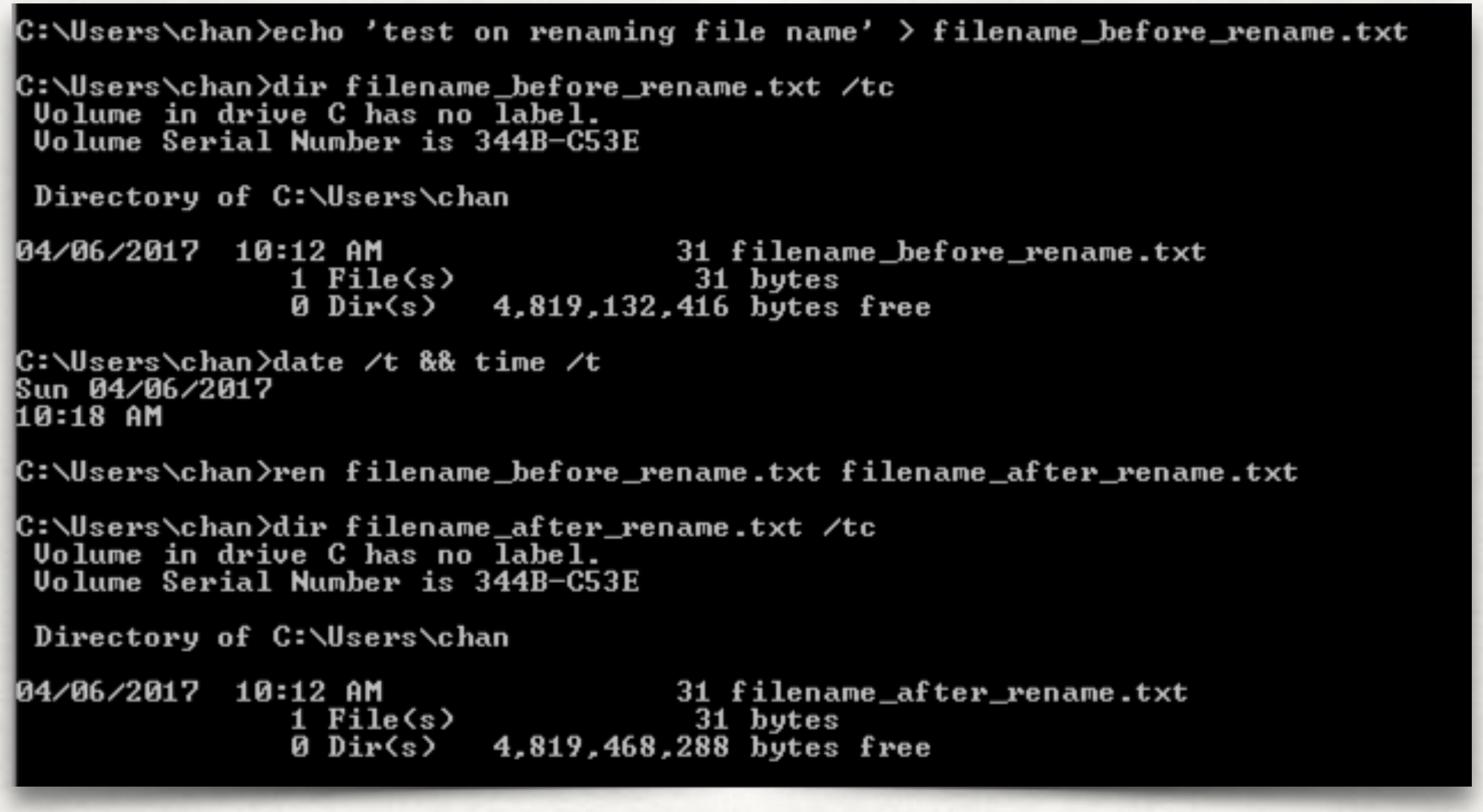
```
03/06/2017  02:07 PM                19 demo_brownbag.txt
```

Whereas if you issue just a `dir` command, it will reflect the time as 02:29 PM UTC +8 on 3rd of June 2017

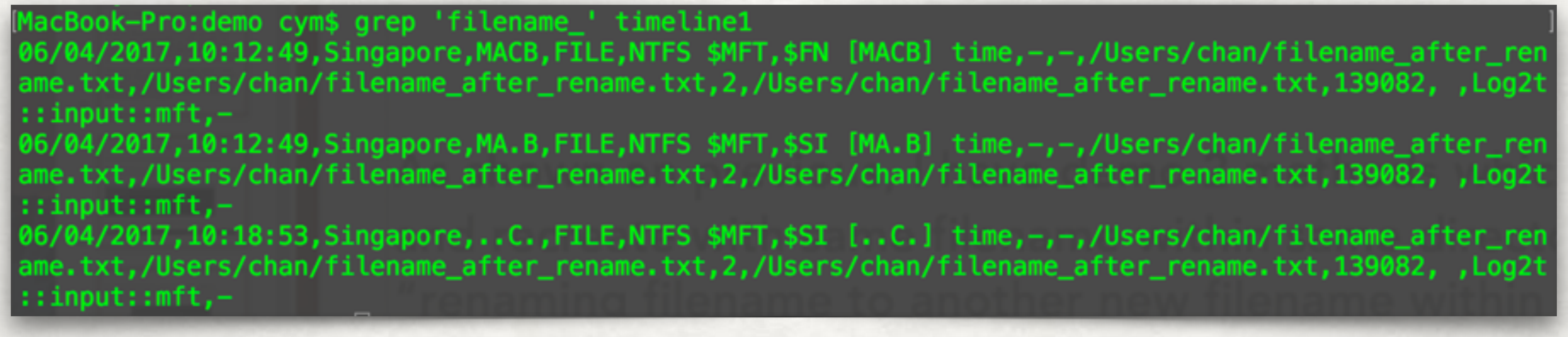


```
03/06/2017  02:29 PM                19 demo_brownbag.txt
```

Renaming filename to a new filename within same directory



```
C:\Users\chan>echo 'test on renaming file name' > filename_before_rename.txt

C:\Users\chan>dir filename_before_rename.txt /tc
 Volume in drive C has no label.
 Volume Serial Number is 344B-C53E

 Directory of C:\Users\chan

04/06/2017  10:12 AM                31 filename_before_rename.txt
               1 File(s)             31 bytes
               0 Dir(s)   4,819,132,416 bytes free

C:\Users\chan>date /t && time /t
Sun 04/06/2017
10:18 AM

C:\Users\chan>ren filename_before_rename.txt filename_after_rename.txt

C:\Users\chan>dir filename_after_rename.txt /tc
 Volume in drive C has no label.
 Volume Serial Number is 344B-C53E

 Directory of C:\Users\chan

04/06/2017  10:12 AM                31 filename_after_rename.txt
               1 File(s)             31 bytes
               0 Dir(s)   4,819,468,288 bytes free
```



```
MacBook-Pro:demo cym$ grep 'filename_' timeline1
06/04/2017,10:12:49,Singapore,MACB,FILE,NTFS $MFT,$FN [MACB] time,-,-,/Users/chan/filename_after_ren
ame.txt,/Users/chan/filename_after_rename.txt,2,/Users/chan/filename_after_rename.txt,139082, ,Log2t
::input::mft,-
06/04/2017,10:12:49,Singapore,MA.B,FILE,NTFS $MFT,$SI [MA.B] time,-,-,/Users/chan/filename_after_ren
ame.txt,/Users/chan/filename_after_rename.txt,2,/Users/chan/filename_after_rename.txt,139082, ,Log2t
::input::mft,-
06/04/2017,10:18:53,Singapore,..C.,FILE,NTFS $MFT,$SI [..C.] time,-,-,/Users/chan/filename_after_ren
ame.txt,/Users/chan/filename_after_rename.txt,2,/Users/chan/filename_after_rename.txt,139082, ,Log2t
::input::mft,-
```

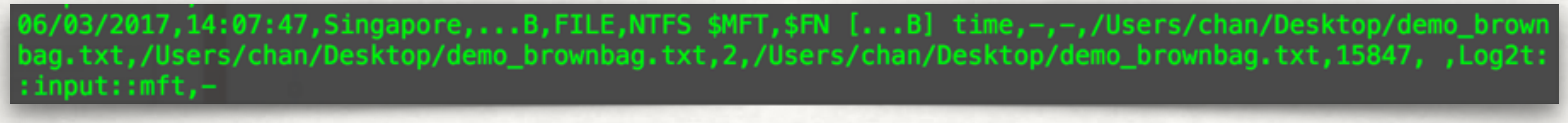
As shown on previous slides, I have demo 2 methods which are “delete and recreate with same filename within same directory” and “renaming filename to another new filename within same directory”

With regards to ransomware cases where files got encrypted with a extension added, it falls under the category of “renaming filename to another new filename within same directory” which I will show in later slide.

Log2timeline uses MACB where “M” stands for last modify time, “A” stands for last accessed time, “C” stands for MFT entry modify time and “B” stands for born time which also mean creation time.

There is another way to reference them which is the MACE where“M” stands for last modify time, “A” stands for last accessed time, “C” stands for creation time and “E” stands for MFT entry modify time

When doing DFIR on collected artifacts, I will rely on the $FN attribute ‘B’ flag which stands for ‘born time’ on the timeline analysis of $MFT using log2timeline.



```
06/03/2017,14:07:47,Singapore,...B,FILE,NTFS $MFT,$FN [...B] time,-,-,/Users/chan/Desktop/demo_brown
bag.txt,/Users/chan/Desktop/demo_brownbag.txt,2,/Users/chan/Desktop/demo_brownbag.txt,15847, ,Log2t:
:input::mft,-
```

Sometimes I would rely on the $FN attribute “born time” to determine when any dropped file from a malware executable or any files were first created to determine the date when the malware was first executed.

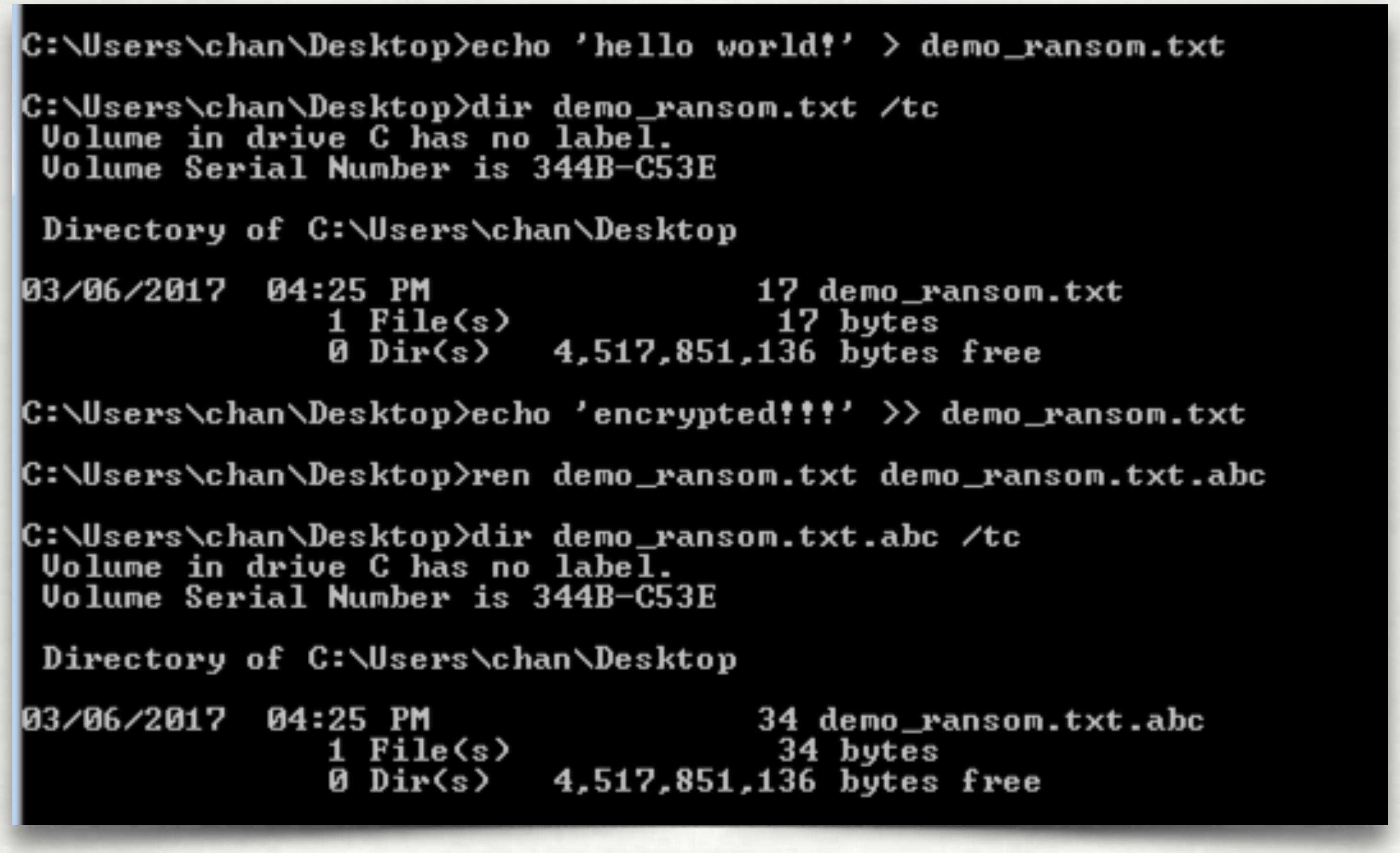
But depending on different scenario, this would throw me off track if the malware try to use the file tunneling approach on a **existing legitimate file**.

However this approach still helps as most malware we observed have persistence mechanism and even though dropped files are being recreated daily when host is being turn on, the $FN attribute “born” time will still relate when the first time the file is being created on the host.

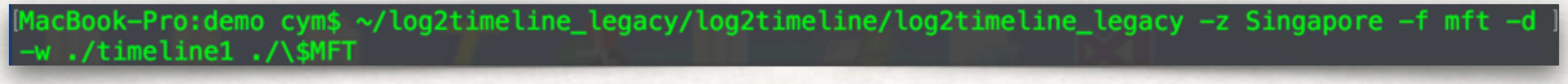
As you have recalled in my previous slide where I mention depending on different scenario.

We cannot use the $FN attribute born time to determine when a file was first encrypted in ransomware cases where initially i thought the $FN attribute “born time” should reflect the time the encrypted file was created since there a extension added.

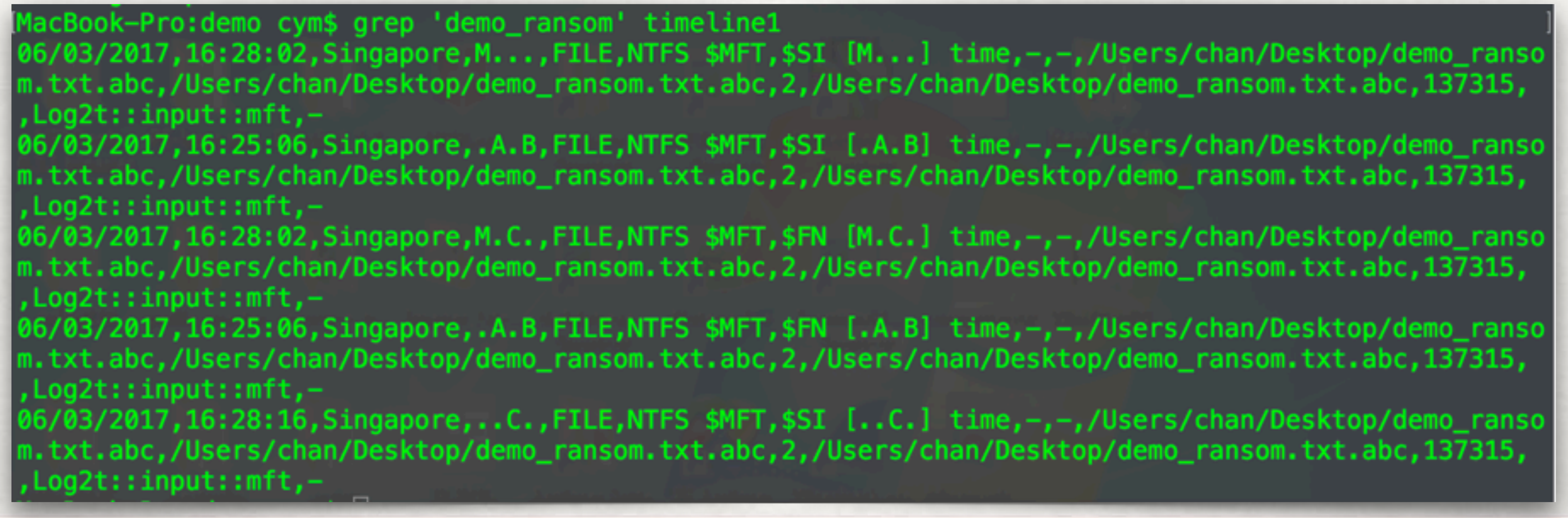
After some experiment, I realize ransomware encrypts and **rename** the file only as shown in next slide.



```
C:\Users\chan\Desktop>echo 'hello world!' > demo_ransom.txt

C:\Users\chan\Desktop>dir demo_ransom.txt /tc
 Volume in drive C has no label.
 Volume Serial Number is 344B-C53E

 Directory of C:\Users\chan\Desktop

03/06/2017  04:25 PM                17 demo_ransom.txt
               1 File(s)             17 bytes
               0 Dir(s)   4,517,851,136 bytes free

C:\Users\chan\Desktop>echo 'encrypted!!!' >> demo_ransom.txt

C:\Users\chan\Desktop>ren demo_ransom.txt demo_ransom.txt.abc

C:\Users\chan\Desktop>dir demo_ransom.txt.abc /tc
 Volume in drive C has no label.
 Volume Serial Number is 344B-C53E

 Directory of C:\Users\chan\Desktop

03/06/2017  04:25 PM                34 demo_ransom.txt.abc
               1 File(s)             34 bytes
               0 Dir(s)   4,517,851,136 bytes free
```

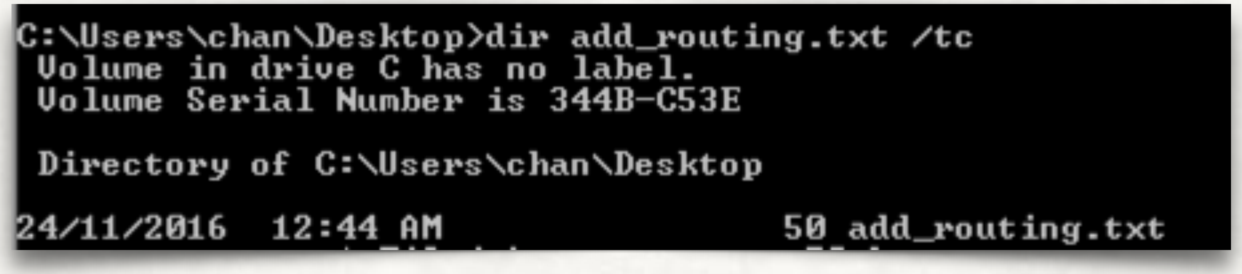


```
MacBook-Pro:demo cym$ ~/log2timeline_legacy/log2timeline/log2timeline_legacy -z Singapore -f mft -d
-w ./timeline1 ./\$MFT
```



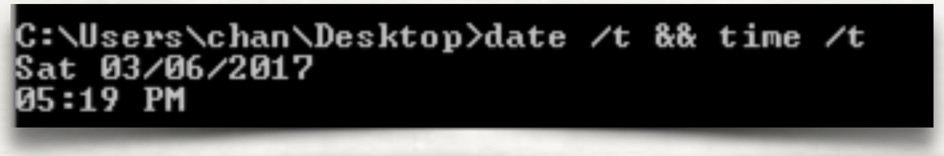
```
MacBook-Pro:demo cym$ grep 'demo_ransom' timeline1
06/03/2017,16:28:02,Singapore,M...,FILE,NTFS $MFT,$SI [M...] time,-,-,/Users/chan/Desktop/demo_ranso
m.txt.abc,/Users/chan/Desktop/demo_ransom.txt.abc,2,/Users/chan/Desktop/demo_ransom.txt.abc,137315,
,Log2t::input::mft,-
06/03/2017,16:25:06,Singapore,.A.B,FILE,NTFS $MFT,$SI [.A.B] time,-,-,/Users/chan/Desktop/demo_ranso
m.txt.abc,/Users/chan/Desktop/demo_ransom.txt.abc,2,/Users/chan/Desktop/demo_ransom.txt.abc,137315,
,Log2t::input::mft,-
06/03/2017,16:28:02,Singapore,M.C.,FILE,NTFS $MFT,$FN [M.C.] time,-,-,/Users/chan/Desktop/demo_ranso
m.txt.abc,/Users/chan/Desktop/demo_ransom.txt.abc,2,/Users/chan/Desktop/demo_ransom.txt.abc,137315,
,Log2t::input::mft,-
06/03/2017,16:25:06,Singapore,.A.B,FILE,NTFS $MFT,$FN [.A.B] time,-,-,/Users/chan/Desktop/demo_ranso
m.txt.abc,/Users/chan/Desktop/demo_ransom.txt.abc,2,/Users/chan/Desktop/demo_ransom.txt.abc,137315,
,Log2t::input::mft,-
06/03/2017,16:28:16,Singapore,..C.,FILE,NTFS $MFT,$SI [..C.] time,-,-,/Users/chan/Desktop/demo_ranso
m.txt.abc,/Users/chan/Desktop/demo_ransom.txt.abc,2,/Users/chan/Desktop/demo_ransom.txt.abc,137315,
,Log2t::input::mft,-
```

To verify, I will monitor the timeline of the file "add_routing.txt" which was created on 24th Nov 2016 at 12:44 AM UTC +8

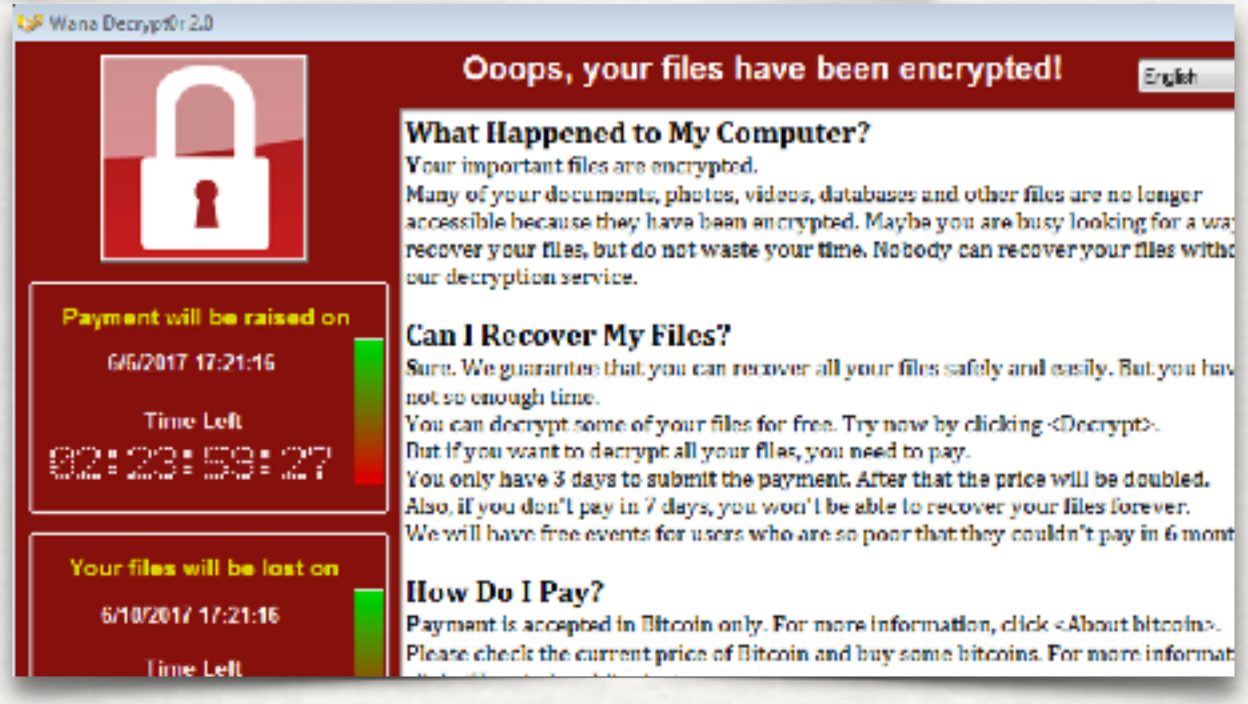


```
C:\Users\chan\Desktop>dir add_routing.txt /tc
 Volume in drive C has no label.
 Volume Serial Number is 344B-C53E

 Directory of C:\Users\chan\Desktop

24/11/2016  12:44 AM                50 add_routing.txt
```

At below time, i ran wannacry on my vm



```
C:\Users\chan\Desktop>date /t && time /t
Sat 03/06/2017
05:19 PM
```



Ooops, your files have been encrypted!

Payment will be raised on

6/6/2017 17:21:16

Time Left

02:23:59:27

Your files will be lost on

6/10/2017 17:21:16

Time Left

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a wa
recover your files, but do not waste your time. Nobody can recover your files witho
our decryption service.

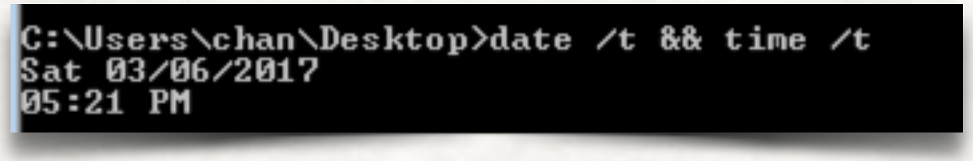
Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you hav
not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 mont

How Do I Pay?

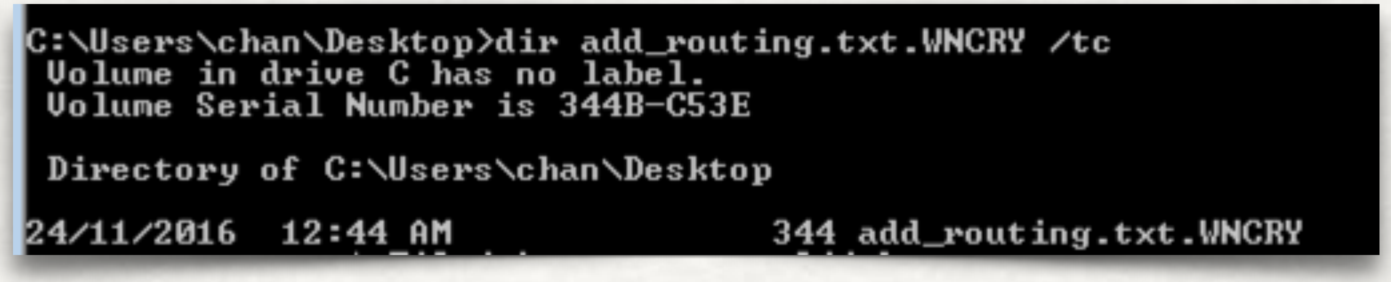
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more informat

At below timing, wannacry finish running



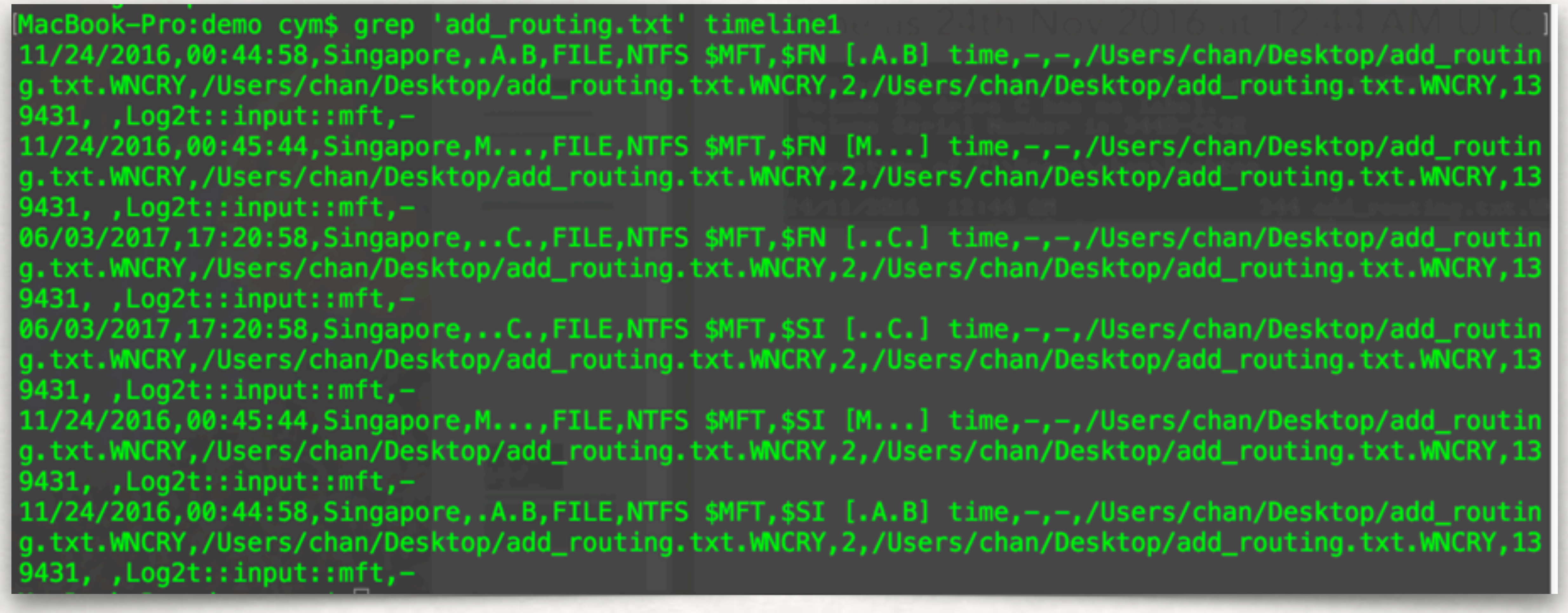
```
C:\Users\chan\Desktop>date /t && time /t
Sat 03/06/2017
05:21 PM
```

Checking the encrypted file date and time, it still reflected creation date and time as 24th Nov 2016 at 12:44 AM UTC +8



```
C:\Users\chan\Desktop>dir add_routing.txt.WNCRY /tc
 Volume in drive C has no label.
 Volume Serial Number is 344B-C53E

 Directory of C:\Users\chan\Desktop

24/11/2016  12:44 AM               344 add_routing.txt.WNCRY
```

Checking out the born time for both $FN and $SI attribute, it reflects the date and timing as 24th Nov 2016 at 12:44 AM UTC +8



```
[MacBook-Pro:demo cym$ grep 'add_routing.txt' timeline1
11/24/2016,00:44:58,Singapore,.A.B,FILE,NTFS $MFT,$FN [.A.B] time,-,-,/Users/chan/Desktop/add_routin
g.txt.WNCRY,/Users/chan/Desktop/add_routing.txt.WNCRY,2,/Users/chan/Desktop/add_routing.txt.WNCRY,13
9431, ,Log2t::input::mft,-
11/24/2016,00:45:44,Singapore,M...,FILE,NTFS $MFT,$FN [M...] time,-,-,/Users/chan/Desktop/add_routin
g.txt.WNCRY,/Users/chan/Desktop/add_routing.txt.WNCRY,2,/Users/chan/Desktop/add_routing.txt.WNCRY,13
9431, ,Log2t::input::mft,-
06/03/2017,17:20:58,Singapore,..C.,FILE,NTFS $MFT,$FN [..C.] time,-,-,/Users/chan/Desktop/add_routin
g.txt.WNCRY,/Users/chan/Desktop/add_routing.txt.WNCRY,2,/Users/chan/Desktop/add_routing.txt.WNCRY,13
9431, ,Log2t::input::mft,-
06/03/2017,17:20:58,Singapore,..C.,FILE,NTFS $MFT,$SI [..C.] time,-,-,/Users/chan/Desktop/add_routin
g.txt.WNCRY,/Users/chan/Desktop/add_routing.txt.WNCRY,2,/Users/chan/Desktop/add_routing.txt.WNCRY,13
9431, ,Log2t::input::mft,-
11/24/2016,00:45:44,Singapore,M...,FILE,NTFS $MFT,$SI [M...] time,-,-,/Users/chan/Desktop/add_routin
g.txt.WNCRY,/Users/chan/Desktop/add_routing.txt.WNCRY,2,/Users/chan/Desktop/add_routing.txt.WNCRY,13
9431, ,Log2t::input::mft,-
11/24/2016,00:44:58,Singapore,.A.B,FILE,NTFS $MFT,$SI [.A.B] time,-,-,/Users/chan/Desktop/add_routin
g.txt.WNCRY,/Users/chan/Desktop/add_routing.txt.WNCRY,2,/Users/chan/Desktop/add_routing.txt.WNCRY,13
9431, ,Log2t::input::mft,-
```

The only time we can rely on the file is encrypted for ransomware is the “MFT entry modify time” which is the “C” flag where from the above it reflect the file was encrypted on 03rd of June 2017 at 17:20 UTC +8

CONCLUSION

- For ransomware cases especially for wannacry, look out for the mft entry modify time if you use log2timeline.

- So far, the mft entry modify time can be used to determine when the file was encrypted (and renamed to xxxxx.wncry)

- Using the date and time found, we could produce a timeline to look into file related activities in $MFT where we might even found the executable file causing the encryption.