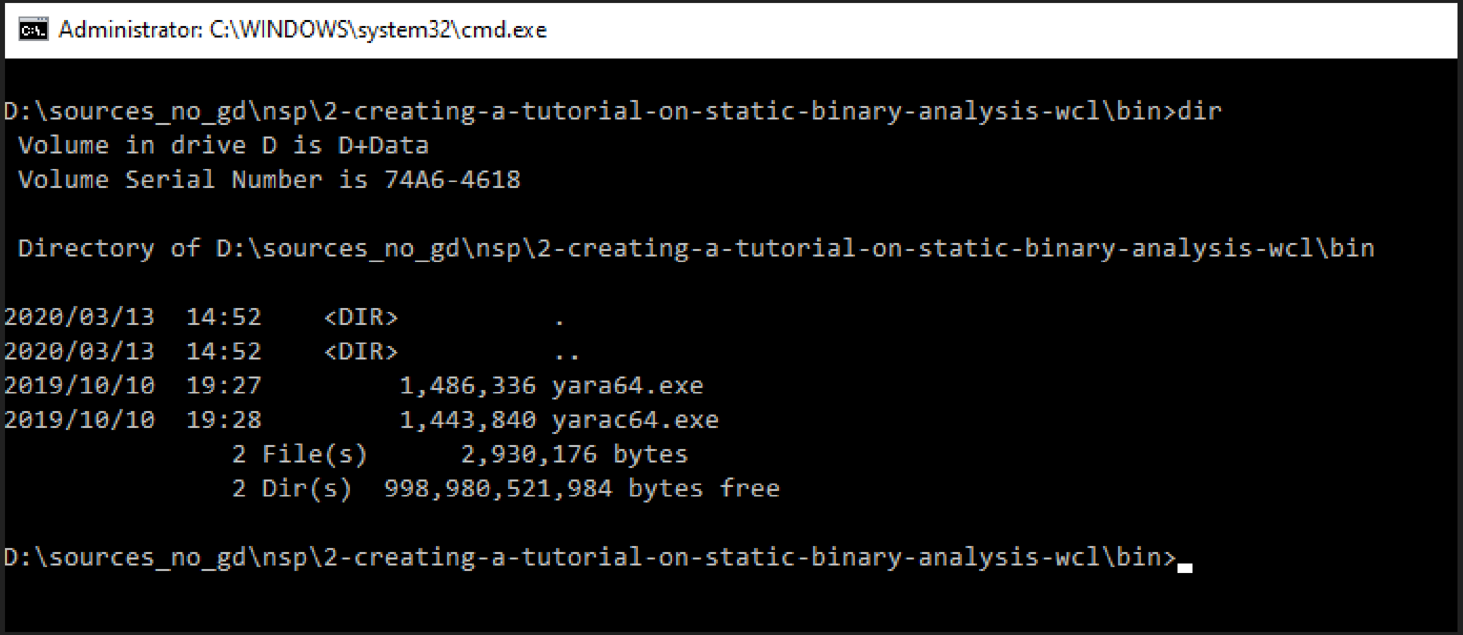
YARA Tutorial

0856069 Weichun, Lin

Installation

- Download yara binary from GitHub Release Page: https://github.com/VirusTotal/yara/releases and unzip it. *Files are already put at bin folder.*



```
D:\sources_no_gd\nsp\2-creating-a-tutorial-on-static-binary-analysis-wcl\bin>dir
 Volume in drive D is D+Data
 Volume Serial Number is 74A6-4618

 Directory of D:\sources_no_gd\nsp\2-creating-a-tutorial-on-static-binary-analysis-wcl\bin

2020/03/13  14:52    <DIR>          .
2020/03/13  14:52    <DIR>          ..
2019/10/10  19:27         1,486,336 yara64.exe
2019/10/10  19:28         1,443,840 yarac64.exe
               2 File(s)      2,930,176 bytes
               2 Dir(s)  998,980,521,984 bytes free

D:\sources_no_gd\nsp\2-creating-a-tutorial-on-static-binary-analysis-wcl\bin>
```

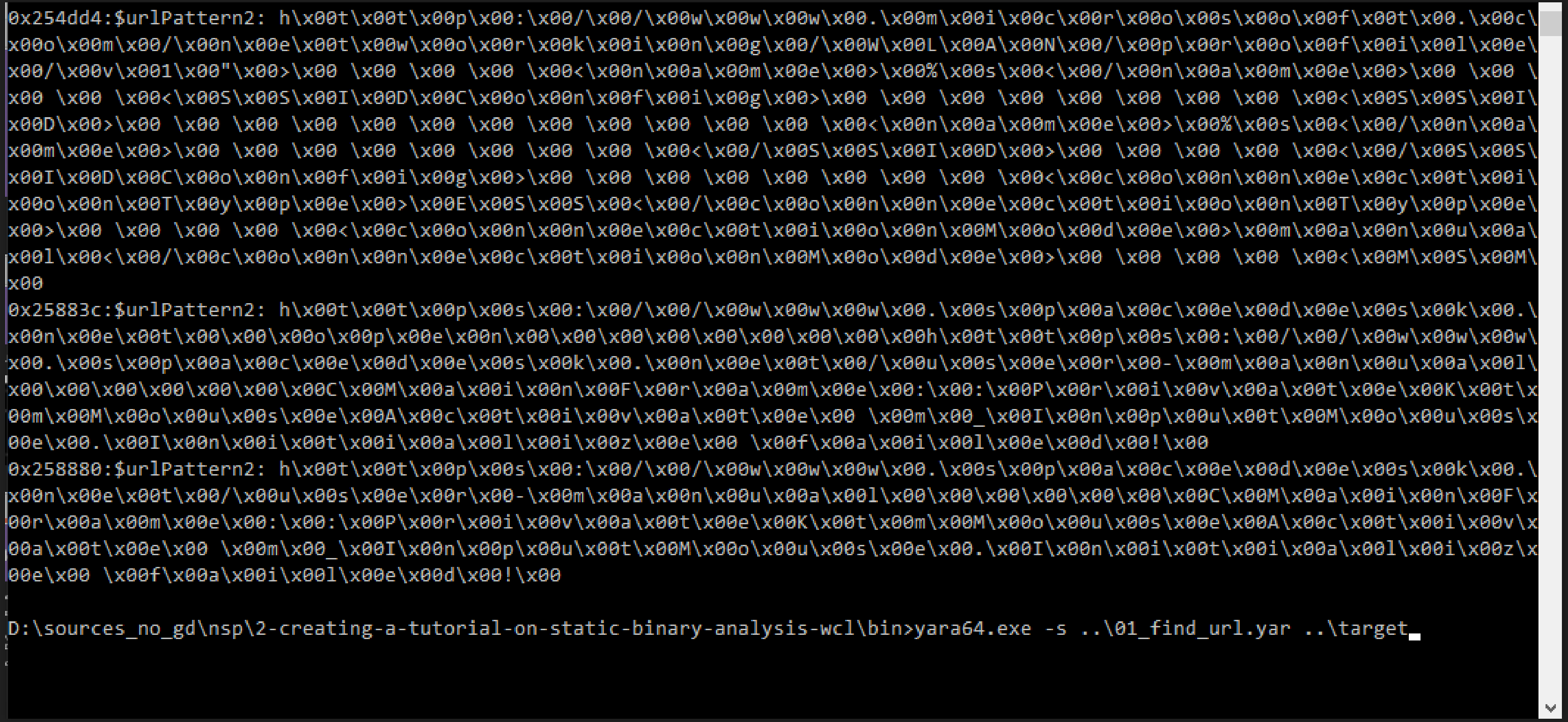
Try find any URL in file

- Execute yara64.exe ..\01_find_url.yar ..\target to check if files in target folder is matched rule: 01_find_url.yar
- Some string contains \x00 since strings are store in UTF–16LE format. Just replace \x00 in string make it readable.
- If you want to see matched pattern, add –s parameter in yara64

```
rule MatchUrl
{
    strings:
        $urlPattern1 = /https?:\/\/([^\x00-\x0A]*)/
        $urlPattern2 =
/h\x00t\x00t\x00p\x00(s\x00)?:\x00\/\x00\/\x00([^
\x01-\x0A]*)/

    condition:
        $urlPattern1 or $urlPattern2
}
```

Try find any URL in file



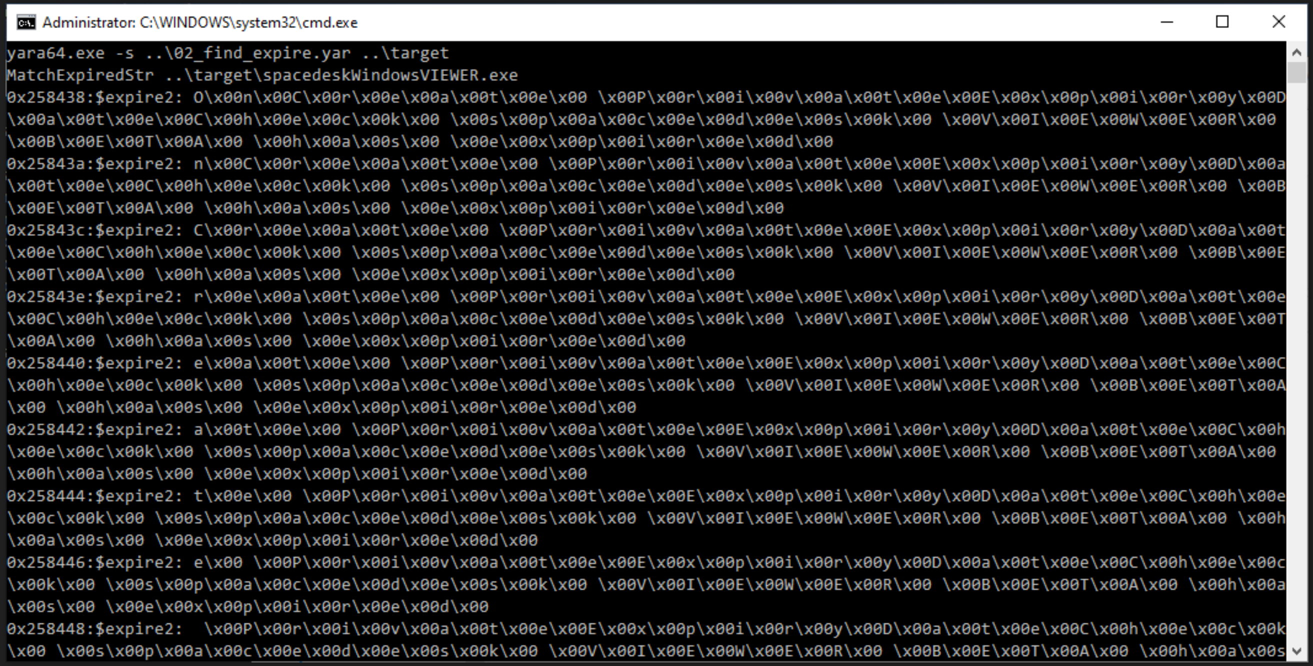
```
0x254dd4:$urlPattern2: h\x00t\x00t\x00p\x00:\x00/\x00/\x00w\x00w\x00w\x00.\x00m\x00i\x00c\x00r\x00o\x00s\x00o\x00f\x00t\x00.\x00c\
x00o\x00m\x00/\x00n\x00e\x00t\x00w\x00o\x00r\x00k\x00i\x00n\x00g\x00/\x00W\x00L\x00A\x00N\x00/\x00p\x00r\x00o\x00f\x00i\x00l\x00e\
x00/\x00v\x001\x00"\x00>\x00 \x00 \x00 \x00 \x00<\x00n\x00a\x00m\x00e\x00>\x00%\x00s\x00<\x00/\x00n\x00a\x00m\x00e\x00>\x00 \x00 \
x00 \x00 \x00<\x00S\x00S\x00I\x00D\x00C\x00o\x00n\x00f\x00i\x00g\x00>\x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00<\x00S\x00S\x00I\
x00D\x00>\x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00<\x00n\x00a\x00m\x00e\x00>\x00%\x00s\x00<\x00/\x00n\x00a\
x00m\x00e\x00>\x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00<\x00/\x00S\x00S\x00I\x00D\x00>\x00 \x00 \x00 \x00 \x00<\x00/\x00S\x00S\
x00I\x00D\x00C\x00o\x00n\x00f\x00i\x00g\x00>\x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00<\x00c\x00o\x00n\x00n\x00e\x00c\x00t\x00i\
x00o\x00n\x00T\x00y\x00p\x00e\x00>\x00E\x00S\x00S\x00<\x00/\x00c\x00o\x00n\x00n\x00e\x00c\x00t\x00i\x00o\x00n\x00T\x00y\x00p\x00e\
x00>\x00 \x00 \x00 \x00 \x00<\x00c\x00o\x00n\x00n\x00e\x00c\x00t\x00i\x00o\x00n\x00M\x00o\x00d\x00e\x00>\x00m\x00a\x00n\x00u\x00a\
x00l\x00<\x00/\x00c\x00o\x00n\x00n\x00e\x00c\x00t\x00i\x00o\x00n\x00M\x00o\x00d\x00e\x00>\x00 \x00 \x00 \x00 \x00<\x00M\x00S\x00M\
x00
0x25883c:$urlPattern2: h\x00t\x00t\x00p\x00s\x00:\x00/\x00/\x00w\x00w\x00w\x00.\x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00.\
x00n\x00e\x00t\x00\x00\x00o\x00p\x00e\x00n\x00\x00\x00\x00\x00\x00\x00\x00\x00h\x00t\x00t\x00p\x00s\x00:\x00/\x00/\x00w\x00w\x00w\
x00.\x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00.\x00n\x00e\x00t\x00/\x00u\x00s\x00e\x00r\x00-\x00m\x00a\x00n\x00u\x00a\x00l\
x00\x00\x00\x00\x00\x00\x00C\x00M\x00a\x00i\x00n\x00F\x00r\x00a\x00m\x00e\x00:\x00:\x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00K\x00t\x
00m\x00M\x00o\x00u\x00s\x00e\x00A\x00c\x00t\x00i\x00v\x00a\x00t\x00e\x00 \x00m\x00_\x00I\x00n\x00p\x00u\x00t\x00M\x00o\x00u\x00s\x
00e\x00.\x00I\x00n\x00i\x00t\x00i\x00a\x00l\x00i\x00z\x00e\x00 \x00f\x00a\x00i\x00l\x00e\x00d\x00!\x00
0x258880:$urlPattern2: h\x00t\x00t\x00p\x00s\x00:\x00/\x00/\x00w\x00w\x00w\x00.\x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00.\
x00n\x00e\x00t\x00/\x00u\x00s\x00e\x00r\x00-\x00m\x00a\x00n\x00u\x00a\x00l\x00\x00\x00\x00\x00\x00\x00C\x00M\x00a\x00i\x00n\x00F\x
00r\x00a\x00m\x00e\x00:\x00:\x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00K\x00t\x00m\x00M\x00o\x00u\x00s\x00e\x00A\x00c\x00t\x00i\x00v\x
00a\x00t\x00e\x00 \x00m\x00_\x00I\x00n\x00p\x00u\x00t\x00M\x00o\x00u\x00s\x00e\x00.\x00I\x00n\x00i\x00t\x00i\x00a\x00l\x00i\x00z\x
00e\x00 \x00f\x00a\x00i\x00l\x00e\x00d\x00!\x00

D:\sources_no_gd\nsp\2-creating-a-tutorial-on-static-binary-analysis-wcl\bin>yara64.exe -s ..\01_find_url.yar ..\target
```

↓ \x00 Removed

0x25883c:$urlPattern2:
https://www.spacedesk.netopenhttps://www.spacedesk.net/user-manualCMainFrame::PrivateKtmMouseActivatem_InputMouse.Initialize failed!
0x258880:$urlPattern2:
https://www.spacedesk.net/user-manualCMainFrame::PrivateKtmMouseActivatem_InputMouse.Initialize failed!

Another try: find keyword: “expired”

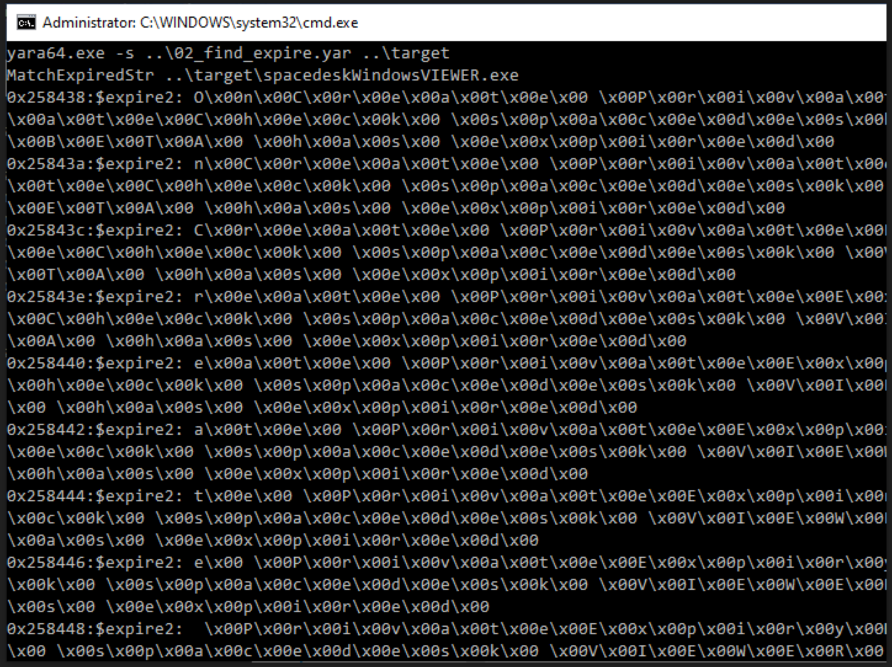


```
yara64.exe -s ..\02_find_expire.yar ..\target
MatchExpiredStr ..\target\spacedeskWindowsVIEWER.exe
0x258438:$expire2: O\x00n\x00C\x00r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D
\x00a\x00t\x00e\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00
\x00B\x00E\x00T\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x25843a:$expire2: n\x00C\x00r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a
\x00t\x00e\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B
\x00E\x00T\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x25843c:$expire2: C\x00r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a\x00t
\x00e\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B\x00E
\x00T\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x25843e:$expire2: r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a\x00t\x00e
\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B\x00E\x00T
\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258440:$expire2: e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a\x00t\x00e\x00C
\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B\x00E\x00T\x00A
\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258442:$expire2: a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a\x00t\x00e\x00C\x00h
\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B\x00E\x00T\x00A\x00
\x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258444:$expire2: t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a\x00t\x00e\x00C\x00h\x00e
\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B\x00E\x00T\x00A\x00 \x00h
\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258446:$expire2: e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a\x00t\x00e\x00C\x00h\x00e\x00c
\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B\x00E\x00T\x00A\x00 \x00h\x00a
\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258448:$expire2:  \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00D\x00a\x00t\x00e\x00C\x00h\x00e\x00c\x00k
\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00 \x00B\x00E\x00T\x00A\x00 \x00h\x00a\x00s
```

```
rule MatchExpiredStr
{
    strings:
        $expire1 = /expired/i
        $expire2 =
/([\w\s]\x00)+e\x00x\x00p\x00i\x
00r\x00e\x00d\x00/i

    condition:
        $expire1 or $expire2
}
```

Another try: find keyword: “expired”



```
yara64.exe -s ..\02_find_expire.yar ..\target
MatchExpiredStr ..\target\spacedeskWindowsVIEWER.exe
0x258438:$expire2: O\x00n\x00C\x00r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00
\x00a\x00t\x00e\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00
\x00B\x00E\x00T\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x25843a:$expire2: n\x00C\x00r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00
\x00t\x00e\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00
\x00E\x00T\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x25843c:$expire2: C\x00r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00
\x00e\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00
\x00T\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x25843e:$expire2: r\x00e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00
\x00C\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00
\x00A\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258440:$expire2: e\x00a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00
\x00h\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00
\x00 \x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258442:$expire2: a\x00t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00
\x00e\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00
\x00h\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258444:$expire2: t\x00e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00
\x00c\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00
\x00a\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258446:$expire2: e\x00 \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00
\x00k\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00
\x00s\x00 \x00e\x00x\x00p\x00i\x00r\x00e\x00d\x00
0x258448:$expire2:  \x00P\x00r\x00i\x00v\x00a\x00t\x00e\x00E\x00x\x00p\x00i\x00r\x00y\x00
\x00 \x00s\x00p\x00a\x00c\x00e\x00d\x00e\x00s\x00k\x00 \x00V\x00I\x00E\x00W\x00E\x00R\x00
```

```
MatchExpiredStr ..\target\spacedeskWindowsVIEWER.exe
0x258438:$expire2: OnCreate PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x25843a:$expire2: nCreate PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x25843c:$expire2: Create PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x25843e:$expire2: reate PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x258440:$expire2: eate PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x258442:$expire2: ate PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x258444:$expire2: te PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x258446:$expire2: e PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
0x258448:$expire2:  PrivateExpiryDateCheck spacedesk VIEWER BETA has expired
...
0x2584ce:$expire2: spacedesk VIEWER BETA has expired
0x2584d0:$expire2: pacedesk VIEWER BETA has expired
...
0x258500:$expire2:  expired
```