Tamil CTF 2021 - Ransomware

TITLE - Ransomware

DESC

Tamil CTF is planning to organize their work, they are formatting a document. But a hacker got into their PC and installed a malware to jeopardize some important information and strip into pieces

Your senior analyst sends you to use your DFIR skills to analyse this

AUTHOR - aidenpearce369

Lets downlad the file,

```
aidenpearce369@amun:~/Ransomware$ ls
ransomeware.zip
aidenpearce369@amun:~/Ransomware$ file ransomeware.zip
ransomeware.zip: Zip archive data, at least v2.0 to extract
aidenpearce369@amun:~/Ransomware$ unzip ransomeware.zip
Archive:  ransomeware.zip
  inflating: ransomeware.raw
```

Its just a `zip` file, but when we extract it, we get a `memory image`

Analysing it in `volatility`

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1

...

INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/aidenpearce369/Ransomware/ransomeware.raw)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x8295c378L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x83941000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-09-24 09:40:03 UTC+0000
     Image local date and time : 2021-09-24 15:10:03 +0530
```

So its running in a profile `Win7SP1x86_23418`

Lets see the process running in the RAM,

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 pslist
Volatility Foundation Volatility Framework 2.6.1

...

Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
- ------------------------------
0x84233878 System                    4      0     90      554 ------      0 2021-09-24 09:33:17 UTC+0000
0x851fa8a8 smss.exe                272      4      2       29 ------      0 2021-09-24 09:33:17 UTC+0000
0x8697c030 csrss.exe               352    344      8      416      0      0 2021-09-24 09:33:22 UTC+0000
0x869cba58 csrss.exe               404    396     11      390      1      0 2021-09-24 09:33:23 UTC+0000
0x869cc6f0 wininit.exe             412    344      3       77      0      0 2021-09-24 09:33:23 UTC+0000
0x86a0b3a0 winlogon.exe            448    396      5      114      1      0 2021-09-24 09:33:23 UTC+0000
0x85349330 services.exe            508    412      9      201      0      0 2021-09-24 09:33:24 UTC+0000
0x85351030 lsass.exe               516    412      8      754      0      0 2021-09-24 09:33:24 UTC+0000
0x85350b60 lsm.exe                 524    412     10      148      0      0 2021-09-24 09:33:24 UTC+0000
0x8538a1d8 svchost.exe             632    508     10      355      0      0 2021-09-24 09:33:26 UTC+0000
0x8539d180 VBoxService.ex          692    508     13      124      0      0 2021-09-24 09:33:26 UTC+0000
0x853aeaa8 svchost.exe             748    508      8      283      0      0 2021-09-24 09:33:27 UTC+0000
0x86b4c8f0 svchost.exe             840    508     23      574      0      0 2021-09-24 09:33:27 UTC+0000
0x86b4b718 svchost.exe             888    508     27      538      0      0 2021-09-24 09:33:27 UTC+0000
0x86b5a8a0 svchost.exe             912    508     18      492      0      0 2021-09-24 09:33:27 UTC+0000
0x86b5b030 svchost.exe             936    508     38     1038      0      0 2021-09-24 09:33:27 UTC+0000
0x86b6e8a0 audiodg.exe            1028    840      6      130      0      0 2021-09-24 09:33:29 UTC+0000
0x86ba0d20 svchost.exe            1184    508     14      377      0      0 2021-09-24 09:33:30 UTC+0000
0x8c0183d8 spoolsv.exe            1348    508     14      289      0      0 2021-09-24 09:33:33 UTC+0000
0x8c03a770 svchost.exe            1420    508     18      298      0      0 2021-09-24 09:33:33 UTC+0000
0x8c040aa0 taskhost.exe           1468    508      9      246      1      0 2021-09-24 09:33:33 UTC+0000
0x8c064710 dwm.exe                1524    888      3       91      1      0 2021-09-24 09:33:33 UTC+0000
0x8c07c030 explorer.exe           1564   1488     31      951      1      0 2021-09-24 09:33:33 UTC+0000
0x8c0cd030 AnyDesk.exe            1660    508      9      221      0      0 2021-09-24 09:33:34 UTC+0000
0x8c114af8 VBoxTray.exe           1856   1564     15      150      1      0 2021-09-24 09:33:37 UTC+0000
0x8c1172d0 AnyDesk.exe            1868   1564      9      180      1      0 2021-09-24 09:33:37 UTC+0000
0x8c137d20 svchost.exe            1936    508     10      147      0      0 2021-09-24 09:33:38 UTC+0000
0x8c143580 svchost.exe            1980    508     20      281      0      0 2021-09-24 09:33:38 UTC+0000
0x8c07f9d8 SearchIndexer.         2236    508     13      612      0      0 2021-09-24 09:33:45 UTC+0000
0x8c299030 wmpnetwk.exe           2372    508     14      421      0      0 2021-09-24 09:33:46 UTC+0000
0x8c206030 svchost.exe            2552    508      8      348      0      0 2021-09-24 09:33:48 UTC+0000
0x8c34e688 WmiPrvSE.exe           2776    632      7      120      0      0 2021-09-24 09:33:52 UTC+0000
0x989cb5f0 calc.exe               2964   1564      4       77      1      0 2021-09-24 09:34:09 UTC+0000
0x850e8030 chrome.exe             3108   1564     32      974      1      0 2021-09-24 09:34:23 UTC+0000
0x98a26030 chrome.exe             3128   3108      9       90      1      0 2021-09-24 09:34:23 UTC+0000
0x869d6d20 chrome.exe             3284   3108     12      195      1      0 2021-09-24 09:34:25 UTC+0000
0x86b7cd20 chrome.exe             3320   3108      5      123      1      0 2021-09-24 09:34:25 UTC+0000
0x85359d20 chrome.exe             3556   3108     10      180      1      0 2021-09-24 09:34:28 UTC+0000
0x8539fa58 chrome.exe             3784   3108      5      108      1      0 2021-09-24 09:34:35 UTC+0000
0x8c38c790 chrome.exe             3816   3108     13      190      1      0 2021-09-24 09:34:36 UTC+0000
0x8c0cbd20 chrome.exe             2132   3108     13      220      1      0 2021-09-24 09:34:46 UTC+0000
0x8c069bb0 chrome.exe             2284   3108      9      171      1      0 2021-09-24 09:34:50 UTC+0000
```

```
0x86b95678 chrome.exe             3276   3108     13      257      1      0 2021-09-24 09:35:00 UTC+0000
0x8c3567d8 chrome.exe             3680   3108     12      191      1      0 2021-09-24 09:35:02 UTC+0000
0x843af4e0 AnyDesk.exe            4080   1564      9      204      1      0 2021-09-24 09:35:22 UTC+0000
0x843a7d20 sppsvc.exe             2428    508      4      141      0      0 2021-09-24 09:35:46 UTC+0000
0x843ac900 svchost.exe            2952    508     13      342      0      0 2021-09-24 09:35:47 UTC+0000
0x84421850 notepad.exe            1516   1564      5      262      1      0 2021-09-24 09:35:56 UTC+0000
0x84400680 notepad.exe            2852   1564      5      259      1      0 2021-09-24 09:36:37 UTC+0000
0x843d8d20 cmd.exe                1636   1564      1       22      1      0 2021-09-24 09:37:31 UTC+0000
0x843f5680 conhost.exe            3652    404      2       52      1      0 2021-09-24 09:37:31 UTC+0000
```

Here `cmd.exe` , `chrome.exe` and `notepad.exe` may be doubtful

You can search for any signs of `malware` using

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 malfind

...
```

But no clues

Lets find it with sessions,

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 sessions
Volatility Foundation Volatility Framework 2.6.1

...

**************************************************
Session(V): 80e3e000 ID: 0 Processes: 25

PagedPoolStart: 80000000 PagedPoolEnd ffbfffff
 Process: 352 csrss.exe 2021-09-24 09:33:22 UTC+0000
 Process: 412 wininit.exe 2021-09-24 09:33:23 UTC+0000
 Process: 508 services.exe 2021-09-24 09:33:24 UTC+0000
 Process: 516 lsass.exe 2021-09-24 09:33:24 UTC+0000
 Process: 524 lsm.exe 2021-09-24 09:33:24 UTC+0000
 Process: 632 svchost.exe 2021-09-24 09:33:26 UTC+0000
 Process: 692 VBoxService.ex 2021-09-24 09:33:26 UTC+0000
 Process: 748 svchost.exe 2021-09-24 09:33:27 UTC+0000
 Process: 840 svchost.exe 2021-09-24 09:33:27 UTC+0000
 Process: 888 svchost.exe 2021-09-24 09:33:27 UTC+0000
 Process: 912 svchost.exe 2021-09-24 09:33:27 UTC+0000
 Process: 936 svchost.exe 2021-09-24 09:33:27 UTC+0000
 Process: 1028 audiodg.exe 2021-09-24 09:33:29 UTC+0000
 Process: 1184 svchost.exe 2021-09-24 09:33:30 UTC+0000
 Process: 1348 spoolsv.exe 2021-09-24 09:33:33 UTC+0000
 Process: 1420 svchost.exe 2021-09-24 09:33:33 UTC+0000
 Process: 1660 AnyDesk.exe 2021-09-24 09:33:34 UTC+0000
 Process: 1936 svchost.exe 2021-09-24 09:33:38 UTC+0000
```

```
 Process: 1980 svchost.exe 2021-09-24 09:33:38 UTC+0000
 Process: 2236 SearchIndexer. 2021-09-24 09:33:45 UTC+0000
 Process: 2372 wmpnetwk.exe 2021-09-24 09:33:46 UTC+0000
 Process: 2552 svchost.exe 2021-09-24 09:33:48 UTC+0000
 Process: 2776 WmiPrvSE.exe 2021-09-24 09:33:52 UTC+0000
 Process: 2428 sppsvc.exe 2021-09-24 09:35:46 UTC+0000
 Process: 2952 svchost.exe 2021-09-24 09:35:47 UTC+0000
 Image: 0x8696f3f0, Address 90130000, Name: win32k.sys
 Image: 0x842a2a00, Address 903a0000, Name: TSDDD.dll
**********************************************
Session(V): 8a668000 ID: 1 Processes: 24

PagedPoolStart: 80000000 PagedPoolEnd ffbfffff
 Process: 404 csrss.exe 2021-09-24 09:33:23 UTC+0000
 Process: 448 winlogon.exe 2021-09-24 09:33:23 UTC+0000
 Process: 1468 taskhost.exe 2021-09-24 09:33:33 UTC+0000
 Process: 1524 dwm.exe 2021-09-24 09:33:33 UTC+0000
 Process: 1564 explorer.exe 2021-09-24 09:33:33 UTC+0000
 Process: 1856 VBoxTray.exe 2021-09-24 09:33:37 UTC+0000
 Process: 1868 AnyDesk.exe 2021-09-24 09:33:37 UTC+0000
 Process: 2964 calc.exe 2021-09-24 09:34:09 UTC+0000
 Process: 3108 chrome.exe 2021-09-24 09:34:23 UTC+0000
 Process: 3128 chrome.exe 2021-09-24 09:34:23 UTC+0000
 Process: 3284 chrome.exe 2021-09-24 09:34:25 UTC+0000
 Process: 3320 chrome.exe 2021-09-24 09:34:25 UTC+0000
 Process: 3556 chrome.exe 2021-09-24 09:34:28 UTC+0000
 Process: 3784 chrome.exe 2021-09-24 09:34:35 UTC+0000
 Process: 3816 chrome.exe 2021-09-24 09:34:36 UTC+0000
 Process: 2132 chrome.exe 2021-09-24 09:34:46 UTC+0000
 Process: 2284 chrome.exe 2021-09-24 09:34:50 UTC+0000
 Process: 3276 chrome.exe 2021-09-24 09:35:00 UTC+0000
 Process: 3680 chrome.exe 2021-09-24 09:35:02 UTC+0000
 Process: 4080 AnyDesk.exe 2021-09-24 09:35:22 UTC+0000
 Process: 1516 notepad.exe 2021-09-24 09:35:56 UTC+0000
 Process: 2852 notepad.exe 2021-09-24 09:36:37 UTC+0000
 Process: 1636 cmd.exe 2021-09-24 09:37:31 UTC+0000
 Process: 3652 conhost.exe 2021-09-24 09:37:31 UTC+0000
 Image: 0x869c0b88, Address 90130000, Name: win32k.sys
 Image: 0x851ab938, Address 903d0000, Name: cdd.dll
```

So there is something definitely up with `chrome.exe` and `notepad.exe`,

Registry hives can give `IE explorer` history,

Now we cant see `chrome` history, but we can `grep` it in `strings`

Lets check for `http`,

After tries like, `http://google` , `http://127.0.0.1`

```
aidenpearce369@amun:~/Ransomware$ strings ransomeware.raw | grep http://192.168
```

```
http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87/
http://192.168.1.87/
    http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
Ahttp://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000,*
EGL_ANGLE_platform_ahttp://192.168.1.87:8000,*
http://192.168.1.87/
khttp://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
    http://192.168.1.87:8000/
http://192.168.1.87:8000/
J*http://192.168.1.87:8000/
    http://192.168.1.87/
http://192.168.1.87/
http://192.168.1.87/
http://192.168.1.87/
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/Directory listing for /
http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/
http://192.168.1.87:8000/Directory listing for /
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/
Hnamespace-f0265b5b_9b92_4ccf_9ee5_1835421d3964-http://192.168.1.87:8000/
Hnamespace-f0265b5b_9b92_4ccf_9ee5_1835421d3964-http://192.168.1.87:8000/
http://192.168.1.87:
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll(
6http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/Directory listing for /
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/
http://192.168.1.87/
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/http://192.168.1.87:8000/application/x-msdos-programapplication/x-msdos-program
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
```

```
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
http://192.168.1.87:8000/
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
http://192.168.1.87:8000
http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/
http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/
http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/
http://192.168.1.87/
http://192.168.1.87/
L9http://192.168.1.87:8000/original.txt.txt
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000
http://192.168.1.87:8000/
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87/
http://192.168.1.87:8000/h
http://192.168.1.87/
http://192.168.1.87:8000/
```

```
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
_dk_http://192.168.1.87 http://192.168.1.87 http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/
M_dk_http://192.168.1.87 http://192.168.1.87 http://192.168.1.87:8000/
[_dk_http://192.168.1.87 http://192.168.1.87 http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/Directory listing for /
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87/
http://192.168.1.87/
http://192.168.1.87:8000/http://192.168.1.87:8000/application/x-msdos-programapplication/x-msdos-program
/+P9].Nhttp://192.168.1.87:8000/http://192.168.1.87:8000/application/x-msdos-programapplication/x-msdos-
program
    http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000
http://192.168.1.87:8000/
http://192.168.1.87:8000/
e-f0265b5b_9b92_4ccf_9ee5_1835421d3964-http://192.168.1.87:8000/
Hnamespace-f0265b5b_9b92_4ccf_9ee5_1835421d3964-http://192.168.1.87:8000/
Hnamespace-f0265b5b_9b92_4ccf_9ee5_1835421d3964-http://192.168.1.87:8000/
Hnamespace-ddd5e499_9945_4a2f_ac68_ecffe17e797b-http://192.168.1.87:8000/
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
Pnamespace-f0265b5b_9b92_4ccf_9ee5_1835421d3964-http://192.168.1.87:8000/
Pnamespace-f0265b5b_9b92_4ccf_9ee5_1835421d3964-http://192.168.1.87:8000/
Pnamespace-ddd5e499_9945_4a2f_ac68_ecffe17e797b-http://192.168.1.87:8000/
http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/
|_dk_http://192.168.1.87 http://192.168.1.87 http://192.168.1.87:8000/notepad.exe
_dk_http://192.168.1.87 http://192.168.1.87 http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/
```

```
http://192.168.1.87:8000/
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
$http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
8http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll
http://192.168.1.87:8000/
http://192.168.1.87:8000/*
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87/
http://192.168.1.87:8000/
http://192.168.1.87/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/api-ms-win-core-path-l1-1-0.dll)
http://192.168.1.87:8000/notepad.exe,
http://192.168.1.87:8000/companyleaks.txt
fa583bea-7ca7-43fc-ae36-87c749cfe858192http://192.168.1.87:8000/
a52cbceb-318c-4453-87ab-496318bd9b5a192.168.1.87:8000http://192.168.1.87:8000/
http://192.168.1.87:8000/Directory listing for /
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/notepad.exe
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000BD1F630B479E7325E77504E9C908EB97
_---]---]---]lctf.com:443,*":{"expiration":"0","last_modified":"13276947761736356","model":0,"setting":
{"hasHighScore":false,"lastMediaPlaybackTime":0.0,"mediaPlaybacks":0,"visits":1}},"https://www.google.com
:443,*":{"expiration":"0","last_modified":"13276947316417682","model":0,"setting":
{"hasHighScore":false,"lastMediaPlaybackTime":0.0,"mediaPlaybacks":0,"visits":2}}},"media_stream_camera":
{},"media_stream_mic":{},"midi_sysex":{},"mixed_script":{},"nfc":{},"notifications":
{},"password_protection":{},"payment_handler":{},"permission_autoblocking_data":
{},"permission_autorevocation_data":{},"popups":{},"ppapi_broker":{},"protected_media_identifier":
{},"protocol_handler":{},"safe_browsing_url_check_data":{},"sensors":{},"serial_chooser_data":
{},"serial_guard":{},"site_engagement":{"http://192.168.1.87:8000,*":
{"expiration":"0","last_modified":"13276949677295228","model":0,"setting":
{"lastEngagementTime":1.3276949677295186e+16,"lastShortcutLaunchTime":0.0,"pointsAddedToday":5.1,"rawScor
e":5.1}},"https://anydesk.com:443,*":
{"expiration":"0","last_modified":"13276947383421526","model":0,"setting":
{"lastEngagementTime":1.3276947383421476e+16,"lastShortcutLaunchTime":0.0,"pointsAddedToday":2.1,"rawScor
```

e":2.1}},"https://ctf.tamilctf.com:443,*":
{"expiration":"0","last_modified":"13276949690187694","model":0,"setting":
{"lastEngagementTime":1.327694969018768e+16,"lastShortcutLaunchTime":0.0,"pointsAddedToday":4.5,"rawScore
":4.5}},"https://tamilctf.com:443,*":
{"expiration":"0","last_modified":"13276949701450965","model":0,"setting":
{"lastEngagementTime":1.3276949701450912e+16,"lastShortcutLaunchTime":0.0,"pointsAddedToday":4.5,"rawScor
e":4.5}},"https://www.google.com:443,*":
{"expiration":"0","last_modified":"13276947314512119","model":0,"setting":
{"lastEngagementTime":1.327694731451208e+16,"lastShortcutLaunchTime":0.0,"pointsAddedToday":4.5,"rawScore
":4.5}}},"sound":{},"ssl_cert_decisions":{},"storage_access":{},"subresource_filter":
{},"subresource_filter_data":{},"usb_chooser_data":{},"usb_guard":{},"vr":{},"webid_request":
{},"webid_share":{},"window_placement":
{}},"pref_version":1},"created_by_version":"94.0.4606.61","creation_time":"13276947282795333","exit_type"
:"Crashed","icon_version":7,"last_engagement_time":"13276949701450912","last_time_obsolete_http_credentia
ls_removed":1632473742.790966,"managed_user_id":"","name":"Person 1","password_account_storage_settings":
{},"were_old_google_logins_removed":true},"protection":{"macs":{}},"safebrowsing":{"event_timestamps":
{"0":{"5":["13276949694"]}},"metrics_last_log_time":"13276947283"},"sessions":{"event_log":
[{"crashed":false,"time":"13276947283301600","type":0},
{"did_schedule_command":true,"first_session_service":true,"tab_count":0,"time":"13276947387272331","type"
:2,"window_count":1},{"crashed":false,"time":"13276947417453634","type":0},
{"did_schedule_command":true,"first_session_service":true,"tab_count":0,"time":"13276947470565153","type"
:2,"window_count":1},{"crashed":false,"time":"13276947736535675","type":0},
{"did_schedule_command":true,"first_session_service":true,"tab_count":2,"time":"13276947761735387","type"
:2,"window_count":1},
{"crashed":false,"time":"13276949665600698","type":0}],"session_data_status":1},"signin":
{"DiceMigrationComplete":true,"allowed":true},"spellcheck":{"dictionaries":["en-
US"],"dictionary":""},"sync":{"requested":false},"token_service":
{"dice_compatible":true},"translate_site_blacklist_with_time":{},"unified_consent":
{"migration_state":10},"updateclientdata":{"apps":{"nmmhkkegccagdldgiimedpiccmgmieda":
{"cohort":"1::","cohortname":"","dlrc":5380,"pf":"e6ea06b8-e107-4a66-99b5-4816d9496a63"}}},"web_apps":
{"did_migrate_default_chrome_apps":
[],"last_preinstall_synchronize_version":"94","system_web_app_failure_count":0,"system_web_app_last_attem
pted_language":"en-
US","system_web_app_last_attempted_update":"94.0.4606.61","system_web_app_last_installed_language":"en-
US","system_web_app_last_update":"94.0.4606.61"},"zerosuggest":{"cachedresults":")]}'\n[\"\",[],[],[],
{\"google:clientdata\":{\"bpc\":false,\"tlw\":false},\"google:suggesttype\":
[],\"google:verbatimrelevan:yM
http://192.168.1.87:8000/
2http://192.168.1.87:8000/favicon.ico
http://192.168.1.87:8000/malware
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
_http://192.168.1.87:8000
f8c6a31http://192.168.1.87:8000/companyleaks.txt
bae027c1-282a-4061-93aa-e76e257c40961http://192.168.1.87:8000/K
eef2a613-4455-41fa-9ce4-855ff07c4f5419http://192.168.1.87:8000/
d1c47ccc-62c7-4bd9-a5b8-368250bb587419http://192.168.1.87:8000/companyleaks.txt
xsoftware\borland\delphi\tserverinfol9177445423947044046829540174911270.0.0.1:(net
disk)software\microsoft\windows\currentversion\runsoftware\microsoft\windows\currentversion\policies\wino
ldapptoolhelp32readprocessmemorychangeserviceconfig2ahttp://ip.aq138.com/getip.asp?
aquser=http://ip.aq138.com/setip.asphttp://192.168.1.5/get.asp?user=http://192.168.1.5/set.asp

```
http://192.168.1.87:8000/
http://192.168.1.87:8000/
5   http://192.168.1.87/p
.http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
0ed96e6b-7467-4e50-ae86-
20a38860d148192192.168.1.87:8000http://192.168.1.87:8000/192.168.1.87:80000,1Directory listing for /0,0
{"NewTabPage":
{"PrevNavigationTime":"13276949696939785"},"account_id_migration_state":2,"account_tracker_service_last_u
pdate":"13276947285226249","alternate_error_pages":
{"backup":true},"announcement_notification_service_first_run_time":"13276947283316571","autocomplete":
{"retention_policy_last_version":94},"autofill":{"orphan_rows_removed":true},"browser":
{"has_seen_welcome_page":true,"navi_onboard_group":"","window_placement":
{"bottom":718,"left":10,"maximized":false,"right":1014,"top":10,"work_area_bottom":728,"work_area_left":0
,"work_area_right":1024,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":
{"daily_original_length":
["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",
"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","
0","0","0","0","0","0","0","1466030"],"daily_received_length":
["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",
"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","
0","0","0","0","0","0","0","1466030"],"last_update_date":"13276895400000000","this_week_number":2699,"thi
s_week_services_downstream_foreground_kb":
{"112189210":60,"115188287":28,"117649486":441,"125522256":3,"21145003":707,"35473769":0,"35565745":4,"47
815025":6,"49601082":1,"5151071":3,"54845618":6,"67052219":0,"73107389":33,"7687691":0,"78917933":280,"88
863520":0,"99279418":1}},"default_apps_install_state":3,"domain_diversity":
{"last_reporting_timestamp":"13276947286762942"},"download":{"directory_upgrade":true},"extensions":
{"alerts":{"initialized":true},"chrome_url_overrides":
{},"last_chrome_version":"94.0.4606.61"},"gaia_cookie":
{"changed_time":1632473690.063605,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"
[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":
{"signin_scoped_device_id":"58476a58-350f-442c-a546-
0fe671c88bb5"}},"http_original_content_length":"1466030","http_received_content_length":"1466030","intl":
{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":
{},"8181035976":{}}},"language_model_counters":{"en":2},"media":
{"device_id_salt":"FD519CD7D7308B9C8938060F4FDC58F3","engagement":{"schema_version":4}},"media_router":
{"receiver_id_hash_token":"AJbK9TVEf0/WIfjQ7dPs6Xj5B249CjRQkKFYbmWX/K26w2jbuo2fL5zFWF1FficAp1LtyAaNDHxBt1
Haz4fU5A=="},"ntp":{"num_personal_suggestions":4},"plugins":{"plugins_list":[]},"profile":
{"avatar_bubble_tutorial_shown":2,"avatar_index":26,"content_settings":
{"enable_quiet_permission_ui_enabling_method":{"notifications":1},"exceptions":{"accessibility_events":
{},"app_banner":{},"ar":{},"auto_select_certificate":{},"automatic_downloads":{},"autoplay":
{},"background_sync":{},"bluetooth_chooser_data":{},"bluetooth_guard":{},"bluetooth_scanning":
{},"camera_pan_tilt_zoom":{},"client_hints":{},"clipboard":{},"cookies":{},"durable_storage":
{},"file_handling":{},"file_system_access_chooser_data":{},"file_system_last_picked_directory":
{},"file_system_read_guard":{},"file_system_write_guard":{},"font_access":{},"geolocation":
{},"hid_chooser_data":{},"hid_guard":{},"http_allowed":{},"idle_detection":{},"images":
{},"important_site_info":{},"insecure_private_network":{},"installed_web_app_metadata":
{},"intent_picker_auto_display":{},"javascript":{},"javascript_jit":{},"legacy_cookie_access":
{},"media_engagement":{"http://192.168.1.87:8000,*":
{"expiration":"0","last_modified":"13276947470563558","model":0,"setting":
{"hasHighScore":false,"lastMediaPlaybackTime":0.0,"mediaPlaybacks":0,"visits":1}},"https://anydesk.com:44
```

```
3,*":{"expiration":"0","last_modified":"13276947387247814","model":0,"setting":
{"hasHighScore":false,"lastMediaPlaybackTime":0.0,"mediaPlaybacks":0,"visits":1}},"https://ctf.tamilctf.c
om:443,*":{"expiration":"0","last_modified":"13276947761744925","model":0,"setting":
{"hasHighScore":false,"lastMediaPlaybackTime":0.0,"mediaPlaybacks":0,"visits":1}},"https://tami
http://192.168.1.87:8000/
http://192.168.1.87:8000/companyleaks.txt
http://192.168.1.87:8000/companyleaks.txt
```

It seems like he viewed `companyleaks.txt` , downloaded `notepad.exe` and `DLLs`,

`notepad.exe` ??

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 filescan | grep
notepad.exe
Volatility Foundation Volatility Framework 2.6.1
0x0000000000e4c988      1      1 R--r-d \Device\HarddiskVolume2\Windows\System32\en-US\notepad.exe.mui
0x0000000007d4dae0      1      1 R--r-d \Device\HarddiskVolume2\Windows\System32\en-US\notepad.exe.mui
0x00000000381b2a80      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\en-US\notepad.exe.mui
0x00000000384f3038      4      0 R--r-d \Device\HarddiskVolume2\Windows\System32\notepad.exe
0x000000003d746738      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\notepad.exe
```

Everything seems legit

Lets check for command history,

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 cmdscan
Volatility Foundation Volatility Framework 2.6.1

...

**************************************************
CommandProcess: conhost.exe Pid: 3652
CommandHistory: 0x420588 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 11 LastAdded: 10 LastDisplayed: 10
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x41e328: dir
Cmd #1 @ 0x41dd18: cd ../..
Cmd #2 @ 0x41dd38: net user
Cmd #3 @ 0x4164d0: whoami
Cmd #4 @ 0x41dd98: cd Windows
Cmd #5 @ 0x41ddb8: cd system
Cmd #6 @ 0x41e358: dir
Cmd #7 @ 0x4181e8: .\malware.exe
Cmd #8 @ 0x402190: echo "Yay Got flag!!"
Cmd #9 @ 0x4206f0: echo "Congrats(Evil Smile)"
Cmd #10 @ 0x464b80: type .\malware.exe
Cmd #19 @ 0x310030: ???.??????????.??????????.??????????.??????????.??????????.??????????.??
Cmd #29 @ 0xff82a6bc: ???????????
```

```
Cmd #36 @ 0x3f00c4: B?F??????
Cmd #37 @ 0x41d158: B?B???????A
```

So he ran `malware.exe` renamed from `notepad.exe`,

Lets find that,

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 filescan | grep
malware.exe
Volatility Foundation Volatility Framework 2.6.1
0x0000000016b6aac8      9      0 R--rwd \Device\HarddiskVolume2\Windows\system\malware.exe
0x000000003fee21c8      8      0 R--rwd \Device\HarddiskVolume2\Windows\system\malware.exe
```

Lets dump that `malware.exe`,

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 dumpfiles -Q
0x0000000016b6aac8 -D .
Volatility Foundation Volatility Framework 2.6.1

...

ImageSectionObject 0x16b6aac8   None   \Device\HarddiskVolume2\Windows\system\malware.exe
DataSectionObject 0x16b6aac8   None   \Device\HarddiskVolume2\Windows\system\malware.exe
```

Checking the `file` type,

```
aidenpearce369@amun:~/Ransomware$ ls
file.None.0x850e3768.dat  file.None.0x8c235008.img  ransomeware.raw  ransomeware.zip
aidenpearce369@amun:~/Ransomware$ file file.None.0x850e3768.dat
file.None.0x850e3768.dat: PE32 executable (console) Intel 80386, for MS Windows
aidenpearce369@amun:~/Ransomware$ file file.None.0x8c235008.img
file.None.0x8c235008.img: PE32 executable (console) Intel 80386, for MS Windows
```

Trying to run it,

```
aidenpearce369@amun:~/Ransomware$ wine file.None.0x850e3768.dat
TamilCTF{v0lat1lity_1s_n0t_2_3a5y}
```

After trying many attempts, it displays the same ...

Applying little bit of reversing skills to (BTW Forensics is not only about using tools, you need a little bit of reversing too, If you are not.. you need to tune up)

```
aidenpearce369@amun:~/Ransomware$ strings file.None.0x850e3768.dat | grep company
companyleaks.txt
```

So it does some operation with `companyleaks.txt`

On reversing the `ELF` in `Ghidra`, you would get

```
undefined4 FUN_00401639(void)

{
  undefined *puVar1;
  undefined auStack279 [255];
  int iStack24;
  int iStack20;

  FUN_00401840();
  puVar1 = &DAT_00411044;
  iStack20 = FUN_0040ea98();
  if (iStack20 == 0) {
    FUN_004015fd("TamilCTF{v0lat1lity_1s_n0t_2_3a5y}",puVar1);
    FUN_0040eaa0();
  }
  FUN_004015d0(iStack20,&DAT_0041107b,auStack279);
  iStack24 = FUN_0040ea08();
  if (iStack24 == 0x13) {
    toupper(0x66);
    FUN_0040ea28();
  }
  else {
    FUN_004015fd("TamilCTF{v0lat1lity_1s_n0t_2_3a5y}");
  }
  return 0;
}
```

This `if (iStack24 == 0x13)` condition checks for the length of the variable whether its size should be `19` or not

If `true` perform some operation, if `false` return `fake flag`

So it reads `companyleaks.txt` which contains 19 chars

Lets confirm it,

```
aidenpearce369@amun:~/Ransomware$ cat companyleaks.txt
aidenpearce369
aidenpearce369@amun:~/Ransomware$ wine file.None.0x850e3768.dat
TamilCTF{v0lat1lity_1s_n0t_2_3a5y}

...
```

```
aidenpearce369@amun:~/Ransomware$ cat companyleaks.txt
aidenpearce369foren
aidenpearce369@amun:~/Ransomware$ wine file.None.0x850e3768.dat
lvnnAz9n3éf0réDFIc}X²f
aidenpearce369@amun:~/Ransomware$
```

The user would have copied the text from `http://192.168.1.87:8000/companyleaks.txt` and would have pasted in `Notepad` , since it can be viewed only

Lets try dumping the `memorydump` of `notepad.exe`,

Since there are two `notepad.exe` process,

```
aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 memdump -p 1516 --
dump-dir .
Volatility Foundation Volatility Framework 2.6.1

...

************************************************************************
Writing notepad.exe [  1516] to 1516.dmp

aidenpearce369@amun:~/Ransomware$ vol.py -f ransomeware.raw --profile=Win7SP1x86_23418 memdump -p 2852 --
dump-dir .
Volatility Foundation Volatility Framework 2.6.1

...

************************************************************************
Writing notepad.exe [  2852] to 2852.dmp
```

Finding any useful data in it..

```
aidenpearce369@amun:~/Ransomware$ strings 1516.dmp | grep Tam
Tam%Tam0Tam
TamQTamQTam;TamFTam
ExGetLicenseTamperState
ExSetLicenseTamperState
TamilCTF{  I deleted it :(
Tamil_Default
Tamil_Default
Tampa1
ExSetLicenseTamperState
ExGetLicenseTamperState
TamilCTF{RaM_1s_t00
_dk_https://tamilctf.com https://tamilctf.com https://tamilctf.com/assets/TamilCTF/TAMIL-CTF-
LOGO_BGTRNS_CRP.png
```

```
M_dk_https://tamilctf.com https://tamilctf.com https://tamilctf.com/assets/TamilCTF/TAMIL%20CTF.png
_dk_https://tamilctf.com https://tamilctf.com https://tamilctf.com/assets/TamilCTF/favicon.ico
```

So there seems a part of flag (hint)

`TamilCTF{RaM_1s_t00`

Its length is of 19 bytes

Lets try using it,

```
aidenpearce369@amun:~/Ransomware$ echo "TamilCTF{RaM_1s_t00" > test.txt
aidenpearce369@amun:~/Ransomware$ ls
1516.dmp  2852.dmp  file.None.0x850e3768.dat  file.None.0x8c235008.img  ransomeware.raw  ransomeware.zip
test.txt
aidenpearce369@amun:~/Ransomware$ wine file.None.0x850e3768.dat
TamilCTF{v0lat1lity_1s_n0t_2_3a5y}
aidenpearce369@amun:~/Ransomware$ mv test.txt companyleaks.txt
aidenpearce369@amun:~/Ransomware$ wine file.None.0x850e3768.dat
_v0l4z1l3_f0r_DFIR}X²f
```

So this `malware.exe` simply performs some operations and gives the second part of the flag out from the first part where the user copied `companyleaks.txt` from website

You would get the first part of the flag here itself

```
aidenpearce369@amun:~/Ransomware$ strings ransomeware.raw | grep TamilCTF{
TamilCTF{  I deleted it :(
TamilCTF{  I deleted it :(
TamilCTF{RaM_1s_t00
TamilCTF{v0lat1lity_1s_n0t_2_3a5y}
TamilCTF{v0lat1lity_1s_n0t_2_3a5y}
TamilCTF{v0lat1lity_1s_n0t_2_3a5y}
```

Completing the whole flag for this challenge,

`TamilCTF{RaM_1s_t00_v0l4z1l3_f0r_DFIR}`

I made this challenge to prove that a Good forensic analyst must have little bit of reversing skills too...

Its not always about Forensic tools you use