

Report 6

For this week's lab, we used PowerShell to collect volatile information that was in our Microsoft Windows virtual machine. In my case, I used the host operating system since it was a Windows Operating system. The first task was to collect time and data. This can be done using the **date /t & time /t** command. The "&" executes the first command followed by the second one. Not using the **t/** parameter will result in you having to input a new date. Here below is the using the date and time commands for today's date.

```
C:\Users\garci>date /t & time /t
Wed 10/05/2022
07:16 PM
```

The second task was listing the users who where had logged in. In order to do that, you need to use the **psloggedon** command. This command can only be utilized if you had previously installed the Sysinternals Suite package in your system. Since I had already installed this package, I changed my directory to access those tools by using **cd Desktop\SysinternalsSuite**. Here below is the list of users that are logged on.

```
C:\Users\garci\Desktop\SysinternalsSuite>psloggedon

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
    10/5/2022 1:36:24 PM          EDUARDO-PC\garci

No one is logged on via resource shares.
```

You can also list the number of logged-on sessions using the **logonsessions** command.

```

C:\Users\garci\Desktop\SysinternalsSuite>logonsessions

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name:      WORKGROUP\EDUARDO-PC$
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            S-1-5-18
    Logon time:     10/5/2022 1:36:22 PM
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:00015b44:
    User name:
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            (none)
    Logon time:     10/5/2022 1:36:22 PM
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:00015f2e:
    User name:      Font Driver Host\UMFD-0
    Auth package:   Negotiate
    Logon type:     Interactive
    Session:        0
    Sid:            S-1-5-96-0-0
    Logon time:     10/5/2022 1:36:22 PM
    Logon server:

```

Using the **logonsessions** | **findstr "logon session"** command you list the logon session ID.

```

C:\Users\garci\Desktop\SysinternalsSuite>logonsessions | findstr "logon session"
LogonSessions v1.41 - Lists logon session information
[0] Logon session 00000000:000003e7:
[1] Logon session 00000000:00015b44:
[2] Logon session 00000000:00015f2e:
[3] Logon session 00000000:000003e4:
[4] Logon session 00000000:0001cbae:
[5] Logon session 00000000:0001d586:
[6] Logon session 00000000:0001d5ad:
[7] Logon session 00000000:000003e5:
[8] Logon session 00000000:0003530c:
[9] Logon session 00000000:00036058:

```

The **logonsessions -p** command displays the processes that are running in each session. Here below are the processes were running for the 9th logon session.

```

[9] Logon session 00000000:00036058:
    User name:      EDUARDO-PC\garci
    Auth package:   CloudAP
    Logon type:     Interactive
    Session:        1
    Sid:            S-1-5-21-2061162394-2380904589-191770230-1001
    Logon time:     10/5/2022 1:36:23 PM
    Logon server:
    DNS Domain:
    UPN:
    4792: sihost.exe
    4832: svchost.exe
    4840: svchost.exe
    4892: svchost.exe
    5072: taskhostw.exe
    5244: ctfmon.exe
    5536: explorer.exe
    6568: svchost.exe
    7620: StartMenuExperienceHost.exe
    7648: SearchHost.exe

```

Below we are using the `-c` parameter to display the information below.

```

C:\Users\garci\Desktop\SysinternalsSuite> logonsessions -c

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

Logon Session,User Name,Auth Package,Logon Type,Session,Sid,Logon Time,Logon Server,DNS Domain,UPN,Processes
00000000:000003e7,WORKGROUP\EDUARDO-PC$,NTLM,(none),0,S-1-5-18,10/5/2022 1:36:22 PM,,,,,
00000000:00015b44,,NTLM,(none),0,(none),10/5/2022 1:36:22 PM,,,,,
00000000:00015f2e,Font Driver Host\UMFD-0,Negotiate,Interactive,0,S-1-5-96-0-0,10/5/2022 1:36:22 PM,,,,,
00000000:000003e4,WORKGROUP\EDUARDO-PC$,Negotiate,Service,0,S-1-5-20,10/5/2022 1:36:22 PM,,,,,
00000000:0001cbae,Font Driver Host\UMFD-1,Negotiate,Interactive,1,S-1-5-96-0-1,10/5/2022 1:36:22 PM,,,,,
00000000:0001d586,Window Manager\DWM-1,Negotiate,Interactive,1,S-1-5-90-0-1,10/5/2022 1:36:22 PM,,,,,
00000000:0001d5ad,Window Manager\DWM-1,Negotiate,Interactive,1,S-1-5-90-0-1,10/5/2022 1:36:22 PM,,,,,
00000000:000003e5,NT AUTHORITY\LOCAL SERVICE,Negotiate,Service,0,S-1-5-19,10/5/2022 1:36:22 PM,,,,,
00000000:0003530c,EDUARDO-PC\garci,CloudAP,Interactive,1,S-1-5-21-2061162394-2380904589-191770230-1001,10/5/2022 1:36:23 PM,,,,,
00000000:00036058,EDUARDO-PC\garci,CloudAP,Interactive,1,S-1-5-21-2061162394-2380904589-191770230-1001,10/5/2022 1:36:23 PM,,,,,

```

The next step was to collect information on network connections using the **netstat** command. To collect all the information, you can use the **netstat -a** command to display all the connections.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -a

Active Connections

    Proto Local Address           Foreign Address         State
    TCP    0.0.0.0:135             Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:445             Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:554             Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:1042            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:1043            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:2869            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:3389            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:5040            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:5357            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:7680            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:9012            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:9013            Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:10243           Eduardo-PC:0            LISTENING
    TCP    0.0.0.0:17500           Eduardo-PC:0            LISTENING
```

Using the **netstat -p tcp** command will display a protocol that uses TCP. Here below are the active connections using TCP. You also select other protocols as well.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -p tcp

Active Connections

    Proto Local Address           Foreign Address         State
    TCP    127.0.0.1:1042          Eduardo-PC:49789        ESTABLISHED
    TCP    127.0.0.1:1042          Eduardo-PC:49795        ESTABLISHED
    TCP    127.0.0.1:1042          Eduardo-PC:49807        ESTABLISHED
    TCP    127.0.0.1:1042          Eduardo-PC:49866        ESTABLISHED
    TCP    127.0.0.1:9012          Eduardo-PC:49828        ESTABLISHED
    TCP    127.0.0.1:9013          Eduardo-PC:49808        ESTABLISHED
    TCP    127.0.0.1:9013          Eduardo-PC:49867        ESTABLISHED
    TCP    127.0.0.1:17532         Eduardo-PC:49818        ESTABLISHED
    TCP    127.0.0.1:27060         Eduardo-PC:57392        ESTABLISHED
```

The **netstat -r** command will display the routing table. Here below you can see the routing table.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -r

=====
Interface List
12...04 42 1a 06 2a 44 .....Realtek Gaming GbE Family Controller
22...00 ff ed 1c 6a 65 .....TAP-NordVPN Windows Adapter V9
23...0a 00 27 00 00 17 .....VirtualBox Host-Only Ethernet Adapter
19...e8 f4 08 de 07 92 .....Intel(R) Wireless-AC 9260 160MHz
15...e8 f4 08 de 07 93 .....Microsoft Wi-Fi Direct Virtual Adapter #3
3...ea f4 08 de 07 92 .....Microsoft Wi-Fi Direct Virtual Adapter #4
6...e8 f4 08 de 07 96 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.254    192.168.1.198    25
127.0.0.0                  255.0.0.0         On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255   On-link          127.0.0.1        331
127.255.255.255            255.255.255.255   On-link          127.0.0.1        331
192.168.1.0                255.255.255.0     On-link          192.168.1.198    281
192.168.1.198              255.255.255.255   On-link          192.168.1.198    281
192.168.1.255              255.255.255.255   On-link          192.168.1.198    281
192.168.56.0               255.255.255.0     On-link          192.168.56.1     281
192.168.56.1               255.255.255.255   On-link          192.168.56.1     281
192.168.56.255             255.255.255.255   On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0         On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0         On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0         On-link          192.168.1.198    281
255.255.255.255            255.255.255.255   On-link          127.0.0.1        331
255.255.255.255            255.255.255.255   On-link          192.168.56.1     281
255.255.255.255            255.255.255.255   On-link          192.168.1.198    281
=====
Persistent Routes:
None
```

The `netstat -b` command will display an executable involved with the connection. Here below are the executables that are involved in my PC.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -b

Active Connections

    Proto Local Address           Foreign Address         State
    TCP    127.0.0.1:1042          Eduardo-PC:49789        ESTABLISHED
    [asus_framework.exe]
    TCP    127.0.0.1:1042          Eduardo-PC:49795        ESTABLISHED
    [asus_framework.exe]
    TCP    127.0.0.1:1042          Eduardo-PC:49807        ESTABLISHED
    [asus_framework.exe]
    TCP    127.0.0.1:1042          Eduardo-PC:49866        ESTABLISHED
    [asus_framework.exe]
    TCP    127.0.0.1:9012          Eduardo-PC:49828        ESTABLISHED
    [ArmourySocketServer.exe]
    TCP    127.0.0.1:9013          Eduardo-PC:49808        ESTABLISHED
    [ArmourySocketServer.exe]
```

The **netstat -e** command will display the network statistics. You see my network stats below.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -e

Interface Statistics

           Received           Sent
Bytes      1133807869      1073364033
Unicast packets      14895013      5071213
Non-unicast packets      1051050      50435
Discards           469           0
Errors             0           0
Unknown protocols      0
```

The next task involved using the **tasklist**, **listdlls**, and **handle** commands to collect process information. The tasklist will display the list of tasks that are currently running. The information displayed is the Image name, PID number, Session name, Session#, and Memory Usage. You can see below the list of tasks on my PC.

```
C:\Users\garci\Desktop\SysinternalsSuite>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	3,732 K
Registry	320	Services	0	93,436 K
smss.exe	792	Services	0	1,368 K
csrss.exe	988	Services	0	6,676 K
wininit.exe	1124	Services	0	7,272 K
csrss.exe	1132	Console	1	7,164 K
services.exe	1196	Services	0	11,308 K
lsass.exe	1204	Services	0	14,640 K
svchost.exe	1332	Services	0	21,528 K
fontdrvhost.exe	1360	Services	0	64 K
svchost.exe	1424	Services	0	13,228 K
svchost.exe	1480	Services	0	4,860 K
winlogon.exe	1532	Console	1	1,656 K

You can also filter tasks based on a specific parameter. You can use the **tasklist /FI "PID gt 320"** to display tasklists that are greater than 320. Note that you can specify the parameters that you want to filter out as well. Here below I display the list of tasks that contains a PID number less than 320.

```
C:\Users\garci\Desktop\SysinternalsSuite>tasklist /FI "PID lt 320"
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	3,732 K

The **handle** command displays the information about open handles for any process in the system. Here below you can see some open handles for my PC.

```
backgroundTaskHost.exe pid: 3204 EDUARDO-PC\garci
 48: File (RW-) C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2209.1071.0_x64__8wekyb3d8bbwe
120: Section \BaseNamedObjects\_ComCatalogCache_
204: Section \Sessions\1\AppDataContainerNamedObjects\S-1-15-2-930279079-3258969966-1203931420-3379063298-1496040207-3203565093-3038441310\Appli
cationService:c841d8d932b5a213d9
2A4: File (R-D) C:\Windows\System32\en-US\KernelBase.dll.mui

-----
RuntimeBroker.exe pid: 25064 EDUARDO-PC\garci
 50: File (RW-) C:\Windows\System32
17C: Section \BaseNamedObjects\_ComCatalogCache_
1F0: Section \BaseNamedObjects\_ComCatalogCache_
1F4: File (R--) C:\Windows\Registration\R000000000000d.clb
224: File (R-D) C:\Windows\System32\en-US\KernelBase.dll.mui

-----
handle.exe pid: 28292 EDUARDO-PC\garci
 4C: File (RW-) C:\Windows
A0: File (RW-) C:\Users\garci\Desktop\SysinternalsSuite
E4: File (RW-) C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.22000.1_none_6ec7c6847ea94424
```


The **listdlls** command will display the DLLs loaded into processes. Here you can the processes that are loaded with DLLs below.

```
listdlls64.exe pid: 26548
Command line: listdlls

Base          Size      Path
0x000000002d030000 0x38000 C:\Users\garci\Desktop\SysinternalsSuite\Listdlls64.exe
0x0000000022240000 0x209000 C:\WINDOWS\SYSTEM32\ntdll.dll
0x0000000021210000 0xbd000 C:\WINDOWS\System32\KERNEL32.DLL
0x000000001f9d0000 0x37c000 C:\WINDOWS\System32\KERNELBASE.dll
0x00000000207a0000 0x1f000 C:\WINDOWS\System32\imagehlp.dll
0x000000001ffb0000 0x111000 C:\WINDOWS\System32\ucrtbase.dll
0x0000000017640000 0xa000 C:\WINDOWS\SYSTEM32\VERSION.dll
0x0000000020d70000 0xa3000 C:\WINDOWS\System32\msvcrt.dll
0x000000001f7f0000 0x162000 C:\WINDOWS\System32\CRYPT32.dll
0x0000000020390000 0x1ad000 C:\WINDOWS\System32\USER32.dll
0x000000001f720000 0x26000 C:\WINDOWS\System32\win32u.dll
0x0000000021c20000 0x29000 C:\WINDOWS\System32\GDI32.dll
0x000000001fdd0000 0x119000 C:\WINDOWS\System32\gdi32full.dll
0x000000001f750000 0x9d000 C:\WINDOWS\System32\msvc_p_win.dll
0x0000000020f10000 0xec000 C:\WINDOWS\System32\COMDLG32.dll
0x0000000021cc0000 0x379000 C:\WINDOWS\System32\combase.dll
0x00000000200d0000 0x120000 C:\WINDOWS\System32\RPCRT4.dll
0x0000000021000000 0xea000 C:\WINDOWS\System32\shcore.dll
0x00000000213f0000 0x5d000 C:\WINDOWS\System32\SHLWAPI.dll
0x0000000021460000 0x7b8000 C:\WINDOWS\System32\SHELL32.dll
0x00000000f840000 0x2a5000 C:\WINDOWS\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.22000.120_none_9d947278b86cc467\COMCTL32.dll
0x0000000020e20000 0xae000 C:\WINDOWS\System32\ADVAPI32.dll
0x0000000020cd0000 0x9e000 C:\WINDOWS\System32\sechost.dll
0x00000000201f0000 0xd6000 C:\WINDOWS\System32\OLEAUT32.dll
0x0000000020ed0000 0x31000 C:\WINDOWS\System32\IMM32.DLL
0x0000000016ba0000 0x221000 C:\WINDOWS\System32\dbghe1p.dll
0x000000001fd50000 0x7f000 C:\WINDOWS\System32\bcryptPrimitives.dll
```

The **pslist** command displays the list of processes that are running in the system.

```
C:\Users\garci\Desktop\SysinternalsSuite>pslist

PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for EDUARDO-PC:

Name          Pid Pri Thd  Hnd  Priv      CPU Time  Elapsed Time
Idle           0   0  48   0    60    208:36:49.593  8:53:06.781
System         4   8  347 6750   44     0:17:14.328  8:53:06.781
Registry       320  8   4   0  11452    0:00:00.718  8:53:08.927
smss           792 11   2   57  1136    0:00:00.140  8:53:06.778
csrss          988 13  14  851  2456    0:00:01.781  8:53:03.725
wininit        1124 13   1  148  1432    0:00:00.078  8:53:01.671
csrss         1132 13  16  921 16828    0:00:04.203  8:53:01.668
services       1196  9   9  800  6228    0:00:12.671  8:53:01.625
lsass          1204  9  11 1935 11536    0:00:21.687  8:53:01.597
svchost        1332  8  19 1630 12468    0:00:19.015  8:53:01.470
fontdrvhost    1360  8   5   37  1680    0:00:00.015  8:53:01.461
svchost        1424  8  11 1619 10312    0:00:58.953  8:53:01.414
svchost        1480  8   4  386  3508    0:00:01.296  8:53:01.400
winlogon       1532 13   6  267  2752    0:00:00.140  8:53:01.379
fontdrvhost    1584  8   5   37  5216    0:00:00.625  8:53:01.362
```

You can also use several other process information such as **pslist -d** command to view information on threads, the **pslist -m** command to view memory information, and the **pslist -x** command to view memory and thread information. Here below is the list of memory and thread information.

```
C:\Users\garci\Desktop\SysinternalsSuite>pslist -x

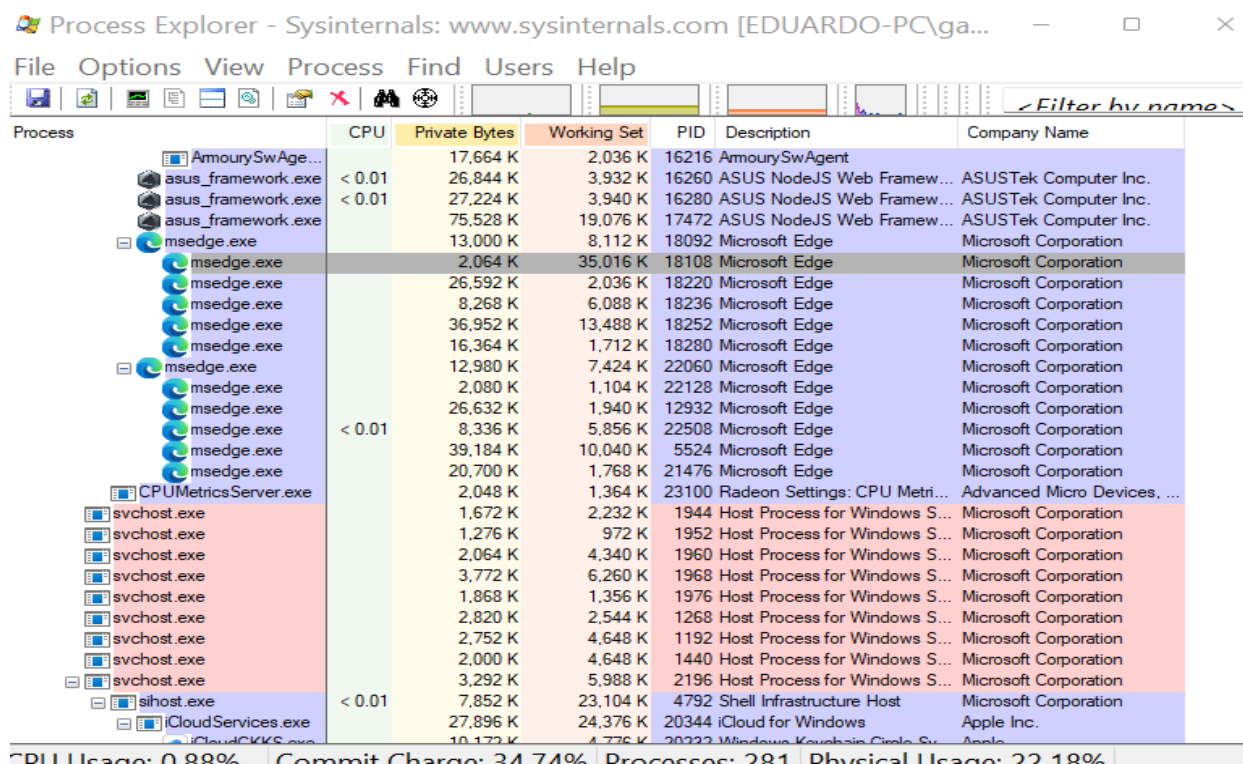
PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process and thread information for EDUARDO-PC:

Name                               Pid      VM      WS      Priv Priv Pk      Faults      NonP Page
Idle                               0         8       8       60    60    60      9         0      0

Tid Pri      Cswtch      State      User Time      Kernel Time      Elapsed Time
0  0  53285434      Running  0:00:00.000  13:06:13.000  0:00:00.000
0  0  47002688      Running  0:00:00.000  13:12:50.921  0:00:00.000
0  0  39902171      Running  0:00:00.000  13:53:26.937  0:00:00.000
0  0  34613532      Running  0:00:00.000  13:49:49.156  0:00:00.000
0  0  54725460      Running  0:00:00.000  13:22:23.343  0:00:00.000
0  0  48035495      Running  0:00:00.000  13:24:17.015  0:00:00.000
0  0  7929835       Running  0:00:00.000  14:04:07.781  0:00:00.000
```

Another way to view processes by utilizing the **procexp** application. You can create dumps of a given process and analyzing the bits of that process. You can also perform malware analysis on any given processes.



The last task was to examine the print spool files that are located in the **c:\windows\system32\spool\PRINTERS** folder. Here below are the files

Name	Date modified	Type	Size
00002.SHD	10/6/2022 3:5...	SHD File	6 KB
00002.SPL	10/6/2022 3:5...	SPL File	670 KB

Below are the binary values for the SHD and SPL files.

HxD - [C:\Windows\System32\spool\PRINTERS\00002.SHD]

16Windows (ANSI)hex

File Edit Search View Analysis Tools Window Help

00002.SHD00002.SPL

Offset(h)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Decoded text
00000000	23	51	00	00	E0	00	00	00	00	28	00	02	00	00	00	00	#Q...ä.....(.....
00000010	01	00	00	00	00	00	00	00	00	70	16	00	00	00	00	00p.....
00000020	7C	16	00	00	00	00	00	00	88	16	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	A0	16	00	00	00	00	00	00	00	ü.....ë.....
00000040	DC	16	00	00	00	00	00	00	02	00	00	00	00	00	00	008.....
00000050	28	17	00	00	00	00	00	00	40	17	00	00	00	00	00	008.....
00000060	00	00	00	00	00	00	00	E6	07	0A	00	04	00	06	00	008.....
00000070	08	00	36	00	2B	0A	03	00	00	00	00	00	00	00	00	00	..6.+.....
00000080	B7	77	0A	00	03	00	00	18	01	00	00	00	00	00	00	00	'w.....
00000090	58	15	00	00	00	00	00	00	00	00	00	04	00	00	00	00	X.....
000000A0	00	00	00	00	00	00	00	48	17	00	00	00	00	00	00	008.....
000000B0	00	00	00	00	00	00	00	62	17	00	00	00	00	00	00	008.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	008.....
000000D0	9A	01	00	00	00	00	00	E0	00	00	00	00	00	00	00	00	š.....ä.....
000000E0	89	50	53	46	0D	0A	1A	0A	00	00	22	49	48	44	52	00	tsPSF....."IHDR
000000F0	50	72	69	6E	74	65	72	50	63	65	72	69	61	6C	69	7A	Printer Serializ
00000100	61	74	69	6F	6E	20	46	6F	72	6D	61	74	20	76	31	2E	ation Format vl.
00000110	30	00	A9	EA	06	16	00	00	01	58	6A	64	73	31	01	01	0.0ë.....Xjds1.
00000120	CC	0C	04	5D	88	0A	EB	1C	C9	11	9F	E8	08	00	2B	10	ii.)Šë.f.Yë..+
00000130	48	60	02	00	00	00	2F	EB	91	94	EF	EE	0E	48	86	36	H...../e""ii.Krë
00000140	00	76	9A	9A	9C	9E	01	00	00	00	00	00	00	00	00	01	Ëvššëz.....
00000150	00	00	20	01	00	00	02	00	00	00	00	00	02	02	00	00
00000160	00	00	00	00	00	00	04	00	02	00	00	00	00	00	00	01
00000170	01	00	08	00	02	00	0C	00	02	00	00	00	00	00	00	01
00000180	01	00	10	00	02	00	1D	00	00	00	00	00	00	00	00	1D
00000190	00	00	53	00	70	00	6F	00	6C	00	20	00	46	00	00	00	..S.p.o.o.l. .F.
000001A0	69	00	6C	00	65	00	20	49	00	6E	00	74	00	65	00	00	i.l.e. .l.n.t.e.
000001B0	72	00	6C	00	65	00	61	00	76	00	69	00	6E	00	67	00	r.l.e.a.v.i.n.g.
000001C0	20	00	4D	00	6F	00	64	00	65	00	00	00	00	00	20	00	.M.o.d.e.....
000001D0	00	00	00	00	00	00	20	00	00	53	00	50	00	4C	00	00S.P.L.
000001E0	46	00	49	00	4C	00	45	00	5F	00	43	00	4F	00	4E	00	F.I.L.E.....C.O.N.
000001F0	54	00	45	00	4E	00	54	00	5F	00	49	00	4E	00	54	00	T.E.N.T.....I.N.T.
00000200	45	00	52	00	4C	00	45	00	41	00	56	00	49	00	4E	00	E.R.L.E.A.V.I.N.
00000210	47	00	5F	00	4F	00	4E	00	00	14	00	00	00	00	00	00	G....._O.N.....
00000220	00	00	14	00	00	53	00	70	00	6F	00	6F	00	6C	00	00S.p.o.o.l.
00000230	20	00	46	00	69	00	6C	00	65	00	20	00	43	00	6F	00	.F.i.l.e. .C.o.
00000240	6E	00	74	00	65	00	6E	00	74	00	73	00	00	00	0C	00	n.t.e.n.t.s.....
00000250	00	00	00	00	00	00	00	00	54	00	59	00	50	00	00	00T.Y.P.
00000260	45	00	5F	00	58	00	50	00	53	00	5F	00	4D	00	53	00	E.....X.P.S.....M.S.
00000270	00	00	00	00	00	00	6A	00	69	00	6A	00	00	00	00	00S.p.j.....
00000280	4E	00	50	00	49	00	43	00	36	00	33	00	46	00	32	00	N.P.I.C.6.3.F.2.
00000290	35	00	20	00	28	00	48	00	50	00	20	00	4C	00	61	00	5.....(H.P. .L.a.
000002A0	73	00	65	00	72	00	4A	00	65	00	74	00	20	00	4D	00	s.e.r.J.e.t. .M.
000002B0	34	00	30	00	32	00	6E	00	29	00	00	00	00	00	00	00	4.0.2.n.)......
000002C0	01	04	1A	0D	DC	00	F9	11	0F	FF	00	02	01	00	01	00Ü.ä.ÿ.....

Special editors

Data inspector

Binary (8 bit)00100011

Int8go to:35

UInt8go to:35

Int16go to:20771

UInt16go to:20771

Int24go to:20771

UInt24go to:20771

Int32go to:20771

UInt32go to:20771

Int64go to:962072695075

UInt64go to:962072695075

LEB128go to:35

ULEB128go to:35

AnsiChar / char8_t#

WideChar / char16_t儸

UTF-8 code point# (U+0023)

Single (float32)2.91063704024908E

Double (float64)4.75327067438459E

OLETIME12/30/1899

FILETIME1/2/1601 2:43:27 AM

DOS date9/3/2020

Byte orderLittle endianRin endian

Hexadecimal basis (for integral numbers)

Offset(h): 0

Overwrite

HxD - [C:\Windows\System32\spool\PRINTERS\00002.SPL]

16Windows (ANSI)hex

File Edit Search View Analysis Tools Window Help

00002.SHD00002.SPL

Offset(h)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Decoded text
00000000	50	4B	03	04	14	00	08	00	08	00	D6	1E	46	55	00	00	EK.....ö.FU..
00000010	00	00	00	00	00	00	00	00	00	00	1D	00	00	00	5B	43[C
00000020	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	content_Types}.xm
00000030	6C	2F	5B	30	5D	2E	70	69	65	63	65	15	8C	01	0D	C2	1/[0].piece.0A.Ä
00000040	30	0C	00	57	8F	FC	6F	1D	78	20	84	1A	FA	EB	04	65	0..Whüo.x ..üë.e
00000050	80	28	98	B4	82	D8	51	6C	21	D8	9E	F0	3C	DD	E9	A6	E(,"",0011020zCfë;
00000060	F9	53	5E	EE	4D	4D	77	E1	00	87	D1	83	23	42	7E	DF	üS"üWüä..üfFüNüB
00000070	39	07	B8	AD	CB	70	86	F9	3A	AD	DF	4A	EA	7A	CA	1A	9...Eprtu.ÄJëzE.
00000080	60	33	AB	17	44	4D	1B	95	A8	A3	54	E2	6E	1E	D2	4A	'3w.DM..''ëTän.Ü
00000090	B4	8E	2D	63	8D	E9	19	33	E1	D1	F1	B3	26	61	23	B6	'Z-c-ë.3aüü.ëa#g
000000A0	C1	FE	0F	F8	01	50	4B	07	08	E9	EA	58	9A	00	00	00	Äp.ø.PK..ëëXp.j..
000000B0	00	71	00	00	00	50	4B	03	04	14	00	08	00	00	00	D6	.q...PK.....ö
000000C0	1E	46	55	00	00	00	00	00	00	00	00	00	00	00	00	1D	..FU.....
000000D0	00	00	00	5B	43	6F	6E	74	65	6E	74	5F	54	79	70	65	...[Content_Type
000000E0	73	5D	2E	78	6D	6C	2F	5B	31	5D	2E	70	69	65	63	65	s}.xml/[1].piece
000000F0	1D	8B	31	0E	83	30	0C	00	BF	12	65	45	24	1F	00	96	.çl.fö...ç.eEö...-
00000100	EE	85	1A	7B	65	05	43	A3	26	8E	E5	58	11	FC	BE	00	l...;e.C6zZÄX.üWü
00000110	E5	96	BB	9B	86	B9	A1	48	5C	D1	2C	20	FA	84	8C	A3	Ä-»+";H\ü.ü.üE
00000120	F5	6F	C1	54	BD	BB	69	CD	A3	90	22	E9	E9	EB	48	01	öoÄTüwifä."ëëëK.
00000130	73	8A	01	34	16	F2	8D	56	57	18	E9	C8	69	2B	92	41	së.4.ö.VW.ëEü+*A
00000140	68	CF	10	BE	B0	E3	70	FE	9B	7A	89	5C	BB	2B	B0	C6	Kf."q"Ä)püWü+*E
00000150	4F	3F	50	4B	07	08	4B	14	88	6A	62	00	00	00	00	00	0?PK..K..jü...l.
00000160	00	00	50	4B	03	04	14	00	08	00	08	00	D6	1E	46	55	..EK.....ö.FU
00000170	00	00	00	00	00	00	00	00	00	00	00	00	15	00	00	00
00000180	5F	72	65	6C	73	2F	2E	72	65	6C	73	2F	5B	30	5D	2E	..rels/.rels/[0].
00000190	70	69	65	63	65	4D	8C	41	0E	02	21	0C	45	AF	42	BA	pieceMöA...l.E"ö
000001A0	77	8A	2E	8C	31	83	B3	F3	00	C6	39	40	83	15	88	43	wS.Üfö*.E9öf..C
000001B0	21	94	18	8F	3F	2C	5D	FE	BC	F7	FE	BC	FC	F2	66	BE	!"...;jü+*üüöfN
000001C0	DC	34	15	71	70	9C	20	16	5F	5E	49	82	83	F5	79	00	Ü4.que... 'I.föy
000001D0	3F	5C	60	B9	CD	0F	DE	A8	0F	43	63	AA	6A	46	22	EA	?\i.f..Cç+jFmë
000001E0	20	F6	5E	AF	88	EA	23	67	D2	A9	54	96	41	DE	A5	65	ö""ëgöüT-Äfëë
000001F0	EA	63	B6	80	95	FC	87	02	E3	C9	DA	33	B6	FF	0F	D8	ëçëë+ü+..äEÜ3gü.0
00000200	01	50	4B	07	08	EB	42	70	4A	6C	00	00	00	00	79	00	..PK..ëBpü1...y...
00000210	00	50	4B	03	04	14	00	08	00	08	00	D6	1E	46	55	00	..EK.....ö.FU.
00000220	00	00	00	00	00	00	00	00	00	00	15	00	00	00	00	5F
00000230	72	65	6C	73	2F	2E	72	65	6C	73	2F	5B	31	5D	2E		