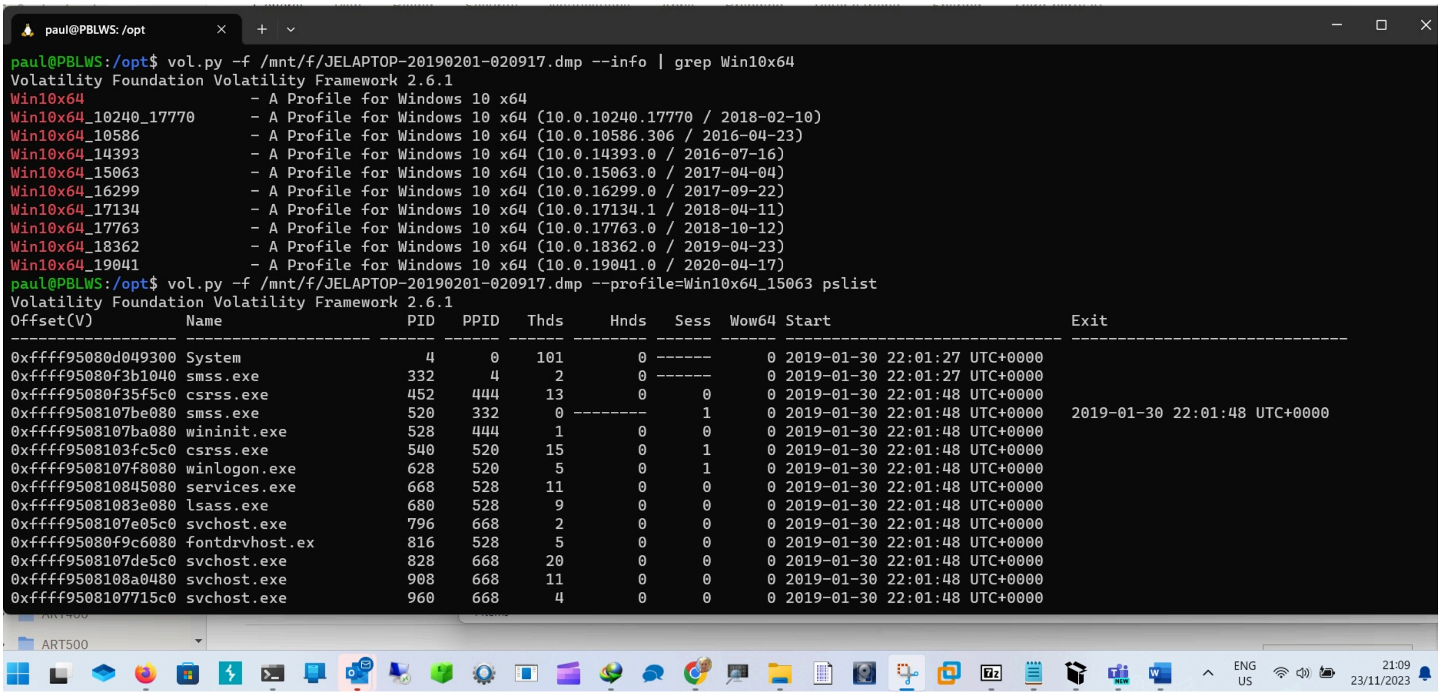
2019 Narcos



```
paul@PBLWS:/opt$ vol.py -f /mnt/f/JELAPTOP-20190201-020917.dmp --info | grep Win10x64
Volatility Foundation Volatility Framework 2.6.1
Win10x64                  - A Profile for Windows 10 x64
Win10x64_10240_17770      - A Profile for Windows 10 x64 (10.0.10240.17770 / 2018-02-10)
Win10x64_10586            - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393            - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x64_15063            - A Profile for Windows 10 x64 (10.0.15063.0 / 2017-04-04)
Win10x64_16299            - A Profile for Windows 10 x64 (10.0.16299.0 / 2017-09-22)
Win10x64_17134            - A Profile for Windows 10 x64 (10.0.17134.1 / 2018-04-11)
Win10x64_17763            - A Profile for Windows 10 x64 (10.0.17763.0 / 2018-10-12)
Win10x64_18362            - A Profile for Windows 10 x64 (10.0.18362.0 / 2019-04-23)
Win10x64_19041            - A Profile for Windows 10 x64 (10.0.19041.0 / 2020-04-17)
paul@PBLWS:/opt$ vol.py -f /mnt/f/JELAPTOP-20190201-020917.dmp --profile=Win10x64_15063 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffff95080d049300 System                    4      0    101        0 ------      0 2019-01-30 22:01:27 UTC+0000
0xffff95080f3b1040 smss.exe                332      4      2        0 ------      0 2019-01-30 22:01:27 UTC+0000
0xffff95080f35f5c0 csrss.exe               452    444     13        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107be080 smss.exe                520    332      0 --------      1      0 2019-01-30 22:01:48 UTC+0000   2019-01-30 22:01:48 UTC+0000
0xffff9508107ba080 wininit.exe             528    444      1        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508103fc5c0 csrss.exe               540    520     15        0      1      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107f8080 winlogon.exe            628    520      5        0      1      0 2019-01-30 22:01:48 UTC+0000
0xffff950810845080 services.exe            668    528     11        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff95081083e080 lsass.exe               680    528      9        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107e05c0 svchost.exe             796    668      2        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff95080f9c6080 fontdrvhost.ex          816    528      5        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107de5c0 svchost.exe             828    668     20        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508108a0480 svchost.exe             908    668     11        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107715c0 svchost.exe             960    668      4        0      0      0 2019-01-30 22:01:48 UTC+0000
```

Simplified Scenario

Due to intelligence provided by the Australian government, two passengers were intercepted by Customs upon arriving at Wellington, New Zealand from Brisbane. The Intel provided stated that Jane Esteban and John Fredricksen may be involved in illegal activity.

The suspects were searched by a customs officer. John Fredricksen's baggage consisted of clothing, toiletries and a Windows laptop. Jane Esteban's baggage also consisted of clothing, toiletries and a small windows laptop.

Upon further search of the lining of John Fredricksen's suitcase, one kilogram of Methamphetamine was located. Both suspects were taken into separate interview rooms where they were interrogated. John Fredricksen refused to answer any questions.

Jane Esteban stated all she knew and that she had to deliver the suitcase to the *Eastbourne library* but if all else failed then they were to deliver it to 666 Rewera Avenue, Petone as told by John Fredricksen.

Customs and police subsequently raided that address. There was nobody present at the address. Customs did, however, find drugs, guns and a desktop computer in the living room of the suspect's house.

You are a Customs forensics investigator. Customs officers have delivered a forensic image and memory dump of the suspect's desktop computer to you. Your task is to determine the relationship between John Fredrickson and the suspect, their future intentions and any other supporting evidence that pertains to the case.

Complex Scenario

Due to intelligence provided by the Australian government, two passengers were intercepted by Customs upon arriving in Wellington, New Zealand from Brisbane. The Intel stated that Jane Esteban and John Fredricksen may be involved in illegal activity.

The suspects were each searched by a customs officer. John Fredricksen's baggage consisted of clothing, toiletries and a Windows laptop. Jane Esteban's baggage also consisted of clothing, toiletries and a small windows laptop.

Upon further search of the lining of the suitcase, one kilogram of Methamphetamine was located. Both suspects were taken into separate interview rooms where they were interrogated. John Fredricksen refused to answer any questions.

Jane Esteban stated all she knew was that she had to deliver the suitcase to the â€œEastbourne libraryâ€⍰ but if all else failed then they were to deliver it to 666 Rewera Avenue, Petone as told by John.

Customs and police subsequently raided that address. There was nobody present at the address. Customs did, however, find drugs, guns and a desktop computer in the living room of the suspect's house.

You are a Customs forensics investigator. Customs officers have delivered images and memory dumps of the 2 laptops and 1 desktop computer to you. Your task is to carry out a forensic examination of John Fredricksen, Jane Esteban and the unknown suspect's laptops and desktop computers to further understand their motives, goals and objectives. It should be noted that all three devices contain different Windows 10 builds and resulting artefacts may not be located in the same location or even be present.

Personas:

John Fredricksen

John has been communicating with Steve Kowhai (NZ dealer) via with what he believes is a secure and private chat room (Discord) to discuss his new consignment. Their chat contains information on where they are going and what he wants John Fredricksen to deliver. Furthermore, Steve shares some documents via (email, cloud, etc) that will assist with his job.

John Fredricksen now has enough information to concoct his plan of smuggling the 1kg of methamphetamine into New Zealand but he needs to find some cover that can take the heat off of himself if any surprises were to happen. John identifies Jane Esteban a regular user of his businesses product (meth) and thinks she will make a great mule for smuggling the drugs.

Jane Esteban

Jane is an undercover Australian Federal Police (AFP) officer tasked with gathering evidence about a drug ring involving John Fredricksen and his associate Steve Kowhai in New Zealand.

Jane will be using the following persona while working undercover. She has a terrible addiction and has been visiting John to feed her addiction, which has lead to a transactional friendship with him as a result. John approaches Jane soon after his discussion with Steve to try and convince her to assist with his job.

Steve Kowhai

Steve is a big player drug distributor/dealer in the lower north island of New Zealand and is wanting to find some quality product to expand his growing empire even more. Steve has contacted a source (John) in the US to smuggle in a taster of the product he plans to buy in larger quantities later. Steve has provided John with information about New Zealand and points on how best to smuggle the product into Wellington without raising any alarms at customs. Steve knows a thing or two about digital forensics and decided to use steganography to hide the document within a picture.

The root directory for this scenario is here.

The evidence for this scenario includes:

Steve Kowhai drive image: here

Jane Esteban drive image: here

John Fredricksen drive image: here

Steve Kowhai memory image: here

Jane Esteban memory image: here

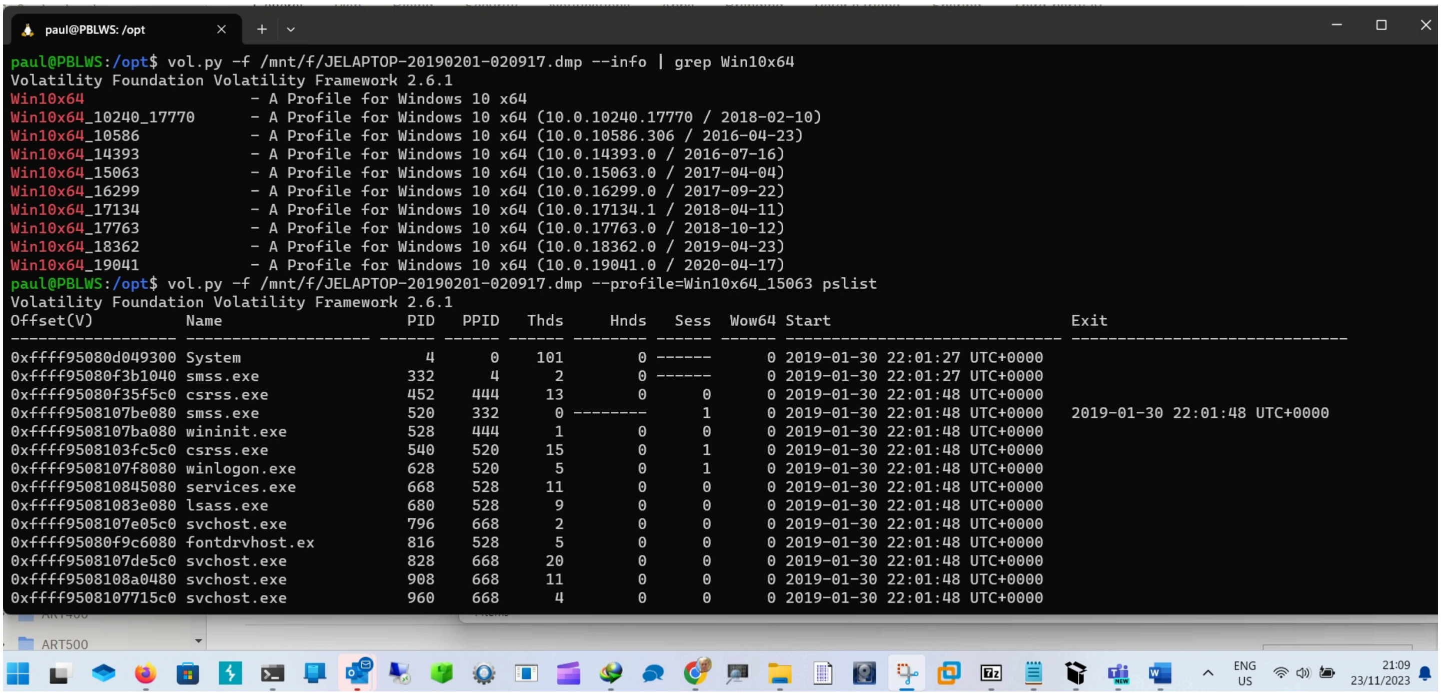
John Fredricksen memory image: here

As a reminder, this scenario is imaginary, and as such, should only be used for teaching purposes. Any likeness to any real life person or persons is purely coincidental.

Solving the Case

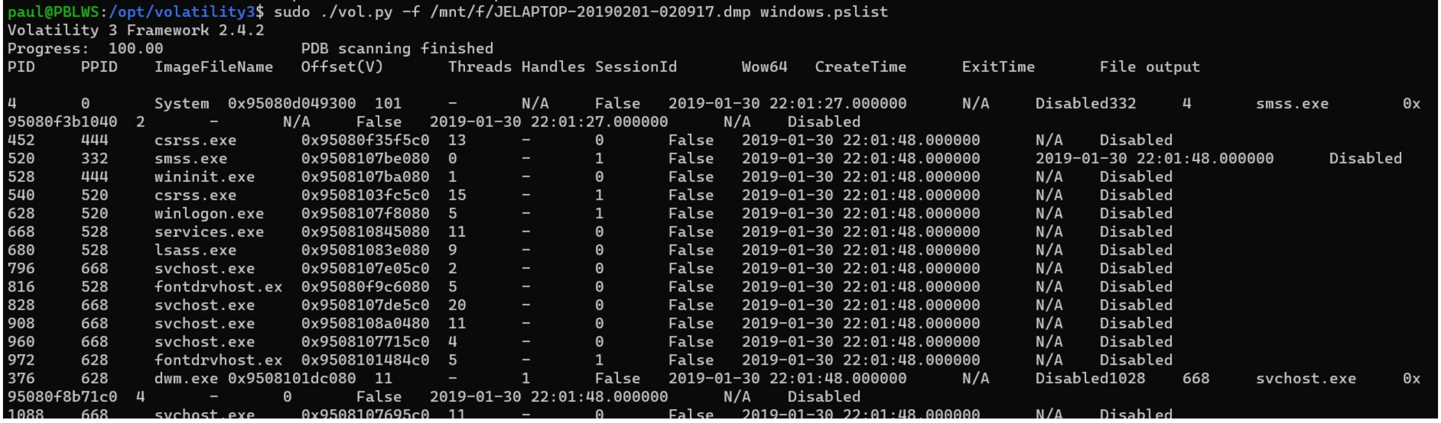
The memory dumps can be analyzed with Volatility 2.6.1 , Volatility3 and MemProcFS.

With Volatility 2.6.1:



```
paul@PBLWS:/opt$ vol.py -f /mnt/f/JELAPTOP-20190201-020917.dmp --info | grep Win10x64
Volatility Foundation Volatility Framework 2.6.1
Win10x64                  - A Profile for Windows 10 x64
Win10x64_10240_17770      - A Profile for Windows 10 x64 (10.0.10240.17770 / 2018-02-10)
Win10x64_10586            - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393            - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x64_15063            - A Profile for Windows 10 x64 (10.0.15063.0 / 2017-04-04)
Win10x64_16299            - A Profile for Windows 10 x64 (10.0.16299.0 / 2017-09-22)
Win10x64_17134            - A Profile for Windows 10 x64 (10.0.17134.1 / 2018-04-11)
Win10x64_17763            - A Profile for Windows 10 x64 (10.0.17763.0 / 2018-10-12)
Win10x64_18362            - A Profile for Windows 10 x64 (10.0.18362.0 / 2019-04-23)
Win10x64_19041            - A Profile for Windows 10 x64 (10.0.19041.0 / 2020-04-17)
paul@PBLWS:/opt$ vol.py -f /mnt/f/JELAPTOP-20190201-020917.dmp --profile=Win10x64_15063 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffff95080d049300 System                    4      0    101        0 ------      0 2019-01-30 22:01:27 UTC+0000
0xffff95080f3b1040 smss.exe                332      4      2        0 ------      0 2019-01-30 22:01:27 UTC+0000
0xffff95080f35f5c0 csrss.exe               452    444     13        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107be080 smss.exe                520    332      0 --------      1      0 2019-01-30 22:01:48 UTC+0000   2019-01-30 22:01:48 UTC+0000
0xffff9508107ba080 wininit.exe             528    444      1        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508103fc5c0 csrss.exe               540    520     15        0      1      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107f8080 winlogon.exe            628    520      5        0      1      0 2019-01-30 22:01:48 UTC+0000
0xffff950810845080 services.exe            668    528     11        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff95081083e080 lsass.exe               680    528      9        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107e05c0 svchost.exe             796    668      2        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff95080f9c6080 fontdrvhost.ex          816    528      5        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107de5c0 svchost.exe             828    668     20        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508108a0480 svchost.exe             908    668     11        0      0      0 2019-01-30 22:01:48 UTC+0000
0xffff9508107715c0 svchost.exe             960    668      4        0      0      0 2019-01-30 22:01:48 UTC+0000
```

With Volatility 3:



```
paul@PBLWS:/opt/volatility3$ sudo ./vol.py -f /mnt/f/JELAPTOP-20190201-020917.dmp windows.pslist
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x95080d049300  101     -       N/A     False   2019-01-30 22:01:27.000000      N/A     Disabled332     4       smss.exe        0x
95080f3b1040  2       -       N/A     False   2019-01-30 22:01:27.000000      N/A     Disabled
452     444     csrss.exe       0x95080f35f5c0  13      -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
520     332     smss.exe        0x9508107be080  0       -       1       False   2019-01-30 22:01:48.000000      2019-01-30 22:01:48.000000      Disabled
528     444     wininit.exe     0x9508107ba080  1       -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
540     520     csrss.exe       0x9508103fc5c0  15      -       1       False   2019-01-30 22:01:48.000000      N/A     Disabled
628     520     winlogon.exe    0x9508107f8080  5       -       1       False   2019-01-30 22:01:48.000000      N/A     Disabled
668     528     services.exe    0x950810845080  11      -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
680     528     lsass.exe       0x95081083e080  9       -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
796     668     svchost.exe     0x9508107e05c0  2       -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
816     528     fontdrvhost.ex  0x95080f9c6080  5       -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
828     668     svchost.exe     0x9508107de5c0  20      -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
908     668     svchost.exe     0x9508108a0480  11      -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
960     668     svchost.exe     0x9508107715c0  4       -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
972     628     fontdrvhost.ex  0x9508101484c0  5       -       1       False   2019-01-30 22:01:48.000000      N/A     Disabled
376     628     dwm.exe 0x9508101dc080  11      -       1       False   2019-01-30 22:01:48.000000      N/A     Disabled1028    668     svchost.exe     0x
95080f8b71c0  4       -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
1088    668     svchost.exe     0x9508107695c0  11      -       0       False   2019-01-30 22:01:48.000000      N/A     Disabled
```