Con uno programa snifer se capturan tramas ethernet que provienen de una PC que se está analizando. Lo capturado en Formato Hexadecimal es lo siguiente:

a) ff ff ff ff ff ff 00 0b 6a 39 7e 79 08 06 00 01
08 00 06 04 00 01 00 0b 6a 39 7e 79 a3 0a 0a 0e
00 00 00 00 00 00 a3 0a 0a 02

b) 00 0b 6a 39 7e 79 00 a0 24 a0 4f ad 08 06 00 01
08 00 06 04 00 02 00 a0 24 a0 4f ad a3 0a 0a 02
00 0b 6a 39 7e 79 a3 0a 0a 0e 0e 0e 0e 0e 0e 0e
0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e

c) 00 a0 24 a0 4f ad 00 0b 6a 39 7e 79 08 00 45 00
00 3b 9e 16 00 00 80 11 42 77 a3 0a 0a 0e a3 0a
0a 02 04 36 00 35 00 27 dd 53 00 b7 01 00 00 01
00 00 00 00 00 00 03 77 77 77 05 63 69 73 63 6f
03 63 6f 6d 00 00 01 00 01

d) 00 0b 6a 39 7e 79 00 a0 24 a0 4f ad 08 00 45 00
00 6f 00 00 40 00 40 11 e0 59 a3 0a 0a 02 a3 0a
0a 0e 00 35 04 36 00 5b 91 24 00 b7 81 80 00 01
00 01 00 02 00 00 03 77 77 77 05 63 69 73 63 6f
03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00
01 51 80 00 04 c6 85 db 19 c0 10 00 02 00 01 00
01 51 80 00 06 03 6e 73 31 c0 10 c0 10 00 02 00
01 00 01 51 80 00 06 03 6e 73 32 c0 10

e) 00 e0 7d 84 12 8b 00 0b 6a 39 7e 79 08 00 45 00
00 30 9e 17 40 00 80 06 0d f9 a3 0a 0a 0e c6 85
db 19 09 8e 00 50 21 c5 5d 99 00 00 00 00 70 02
fa f0 b0 3a 00 00 02 04 05 b4 01 01 04 02

f) 00 0b 6a 39 7e 79 00 e0 7d 84 12 8b 08 00 45 04
00 2c 63 f7 00 00 2d 06 db 19 c6 85 db 19 a3 0a
0a 0e 00 50 09 8e e5 5a fd bd 21 c5 5d 9a 60 12
40 00 9d 24 00 00 02 04 05 98 05 63

g) 00 e0 7d 84 12 8b 00 0b 6a 39 7e 79 08 00 45 00
00 28 9e 19 40 00 80 06 0d ff a3 0a 0a 0e c6 85
db 19 09 8e 00 50 21 c5 5d 9a e5 5a fd be 50 10
fb b8 f9 0c 00 00

h) 00 e0 7d 84 12 8b 00 0b 6a 39 7e 79 08 00 45 00
01 8d 9e 1a 40 00 80 06 0c 99 a3 0a 0a 0e c6 85
db 19 09 8e 00 50 21 c5 5d 9a e5 5a fd be 50 18
fb b8 b3 c9 00 00 47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d
61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78
2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f
6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65
67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78

2d 73 68 6f 63 6b 77 61 76 65 2d 66 6c 61 73 68
2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e
64 2e 6d 73 2d 65 78 63 65 6c 2c 20 61 70 70 6c
69 63 61 74 69 6f 6e 2f 76 6e 64 2e 6d 73 2d 70
6f 77 65 72 70 6f 69 6e 74 2c 20 61 70 70 6c 69
63 61 74 69 6f 6e 2f 6d 73 77 6f 72 64 2c 20 2a
2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75
61 67 65 3a 20 65 73 2d 61 72 0d 0a 41 63 63 65
70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69
70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72
2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f
34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b
20 4d 53 49 45 20 36 2e 30 3b 20 57 69 6e 64 6f
77 73 20 4e 54 20 35 2e 31 29 0d 0a 48 6f 73 74
3a 20 77 77 77 2e 63 69 73 63 6f 2e 63 6f 6d 0d
0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65
70 2d 41 6c 69 76 65 0d 0a 0d 0a

Buscaremos determinar que eventos generaron este trafico. Para ello interpretaremos de a una las tramas capturadas.

a)
ff ff ff ff ff ff 00 0b 6a 39 7e 79 08 06 00 01
08 00 06 04 00 01 00 0b 6a 39 7e 79 a3 0a 0a 0e
00 00 00 00 00 00 a3 0a 0a 02

Header del Frame Ethernet
ff ff ff ff ff ff ->6 Bytes , Dirección MAC de Destino - > Broadcasting
00 0b 6a 39 7e 79 -> 6 Bytes , Dirección MAC Origen
08 06 ->Tipo de Frame ARP

Campos del ARP Request
00 01-> Tipo de Hard
08 00-> Tipo de Protocolo -> IP
06 04 -> hard y type size
00 01 - > Especifica que es un Request ARP
00 0b 6a 39 7e 79-> MAC del Sender
a3 0a 0a 0e -> Ip del Sender 163.10.10.14
00 00 00 00 00 00->Ethernet target. -> todas
a3 0a 0a 02 -> IP del Target 163.10.10.2

Conclusión: Un Host de IP 163.10.10.14 manda un ARP para poder determinar la MAC de la máquina con IP 163.10.10.2

b)
00 0b 6a 39 7e 79 00 a0 24 a0 4f ad 08 06 00 01
08 00 06 04 00 02 00 a0 24 a0 4f ad a3 0a 0a 02

00 0b 6a 39 7e 79 a3 0a 0a 0e 0e 0e 0e 0e 0e 0e
0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e

Header del Frame Ethernet

00 0b 6a 39 7e 79 -> 6 Bytes , Mac de Destino
00 a0 24 a0 4f ad -> 6 Bytes , Mac de Origen
08 06 ->Tipo de Frame ARP

Campos del ARP Reply

00 01 -> Tipo de Hard
08 00 ->Tipo de Protocolo IP
06 04 -> hard y type size
00 02 - > Especifica que es un Reply ARP
00 a0 24 a0 4f ad > MAC del Sender
a3 0a 0a 02-> Ip del Sender 163.10.10.2
00 0b 6a 39 7e 79> MAC Ethernet target.
a3 0a 0a 0e -> IP del Target 163.10.10.14
0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e 0e -> Relleno

Conclusión: El Host de IP 163.10.10.2 responde el ARP indicando su MAC

c)
00 a0 24 a0 4f ad 00 0b 6a 39 7e 79 08 00 45 00
00 3b 9e 16 00 00 80 11 42 77 a3 0a 0a 0e a3 0a
0a 02 04 36 00 35 00 27 dd 53 00 b7 01 00 00 01
00 00 00 00 00 00 03 77 77 77 05 63 69 73 63 6f
03 63 6f 6d 00 00 01 00 01

Header del Frame

00 a0 24 a0 4f ad -> 6 Bytes MAC de Destino
00 0b 6a 39 7e 79-> 6 Bytes , Mac de Origen
08 00 -> Tipo Datagrama IP

Header Datagrama IP

45 ->Versión (0100) y long. del Header en palabras de 32 bits (01010 =5) , 00 -> TOS ,
00 3b -> Largo en Bytes 59 ,
9e 16 -> ID 40470
00 00 ->-> 000= Flag DF=0, MF=0 , 0 0000 0000 0000(13)= Offset
80 -> TTL, 11-> Protocol UDP
42 77 -> Header Checksum ,
a3 0a 0a 0e -> IP Source , 163.10.10.14
a3 0a 0a 02 ->IP Dest. 163.10.10.2

Header del UDP (8 bytes)

04 36 Source Port Number 1078
00 35 Dest. Port Number 53
00 27 UDP Length 39 (datos 31 +header 8 =>ok)
dd 53 UDP CRC

Datos de UDP (31 bytes)
00 b7 01 00 00 01 00 00 00 00 00 00 03 77 77 77 05 63 69 73 63 6f 03 63 6f 6d 00 00 01 00 01

Conclusión: El host de IP 163.10.10.14 , manda al Host 163.10.10.2 una consulta DNS sobre "www. cisco.com" (77 77 77 05 63 69 73 63 6f 03 63 6f 6d)

d)
00 0b 6a 39 7e 79 00 a0 24 a0 4f ad 08 00 45 00
00 6f 00 00 40 00 40 11 e0 59 a3 0a 0a 02 a3 0a
0a 0e 00 35 04 36 00 5b 91 24 00 b7 81 80 00 01
00 01 00 02 00 00 03 77 77 77 05 63 69 73 63 6f
03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00
01 51 80 00 04 c6 85 db 19 c0 10 00 02 00 01 00
01 51 80 00 06 03 6e 73 31 c0 10 c0 10 00 02 00
01 00 01 51 80 00 06 03 6e 73 32 c0 10

Header del Frame
00 0b 6a 39 7e 79-> 6 Bytes MAC de Destino
00 a0 24 a0 4f ad -> 6 Bytes , Mac de Origen
08 00 -> Tipo Datagrama IP
Header del Datagrama IP
45 ->Versión (0100) y long. del Header en palabras de 32 bits (01010 =5) , 00 -> TOS
00 6f -> Largo en Bytes 111. (20 Header IP+ 8 Header UDP+83 =>OK)
00 00 -> ID 0
40 00 -> -> 010= Flag DF=1,MF=0 , 0 0000 0000 0000(13)= Offset
40 ->TTL , 11-> Protocol UDP
e0 59 ->Header Checksum,
a3 0a 0a 02 ->IP Source 163.10.10.2
a3 0a 0a 0e -> IP Dest. 163.10.10.1
Header de UDP (8 bytes)
00 35 Source Port Number 53 (DNS)
04 36 Dest. Port Number 1078
00 5b UDP Length 91 bytes (datos 83+ Header 8 => ok)
91 24 UDP CRC
Datos de UPD del DNS (total 83 bytes)
00 b7 81 80 00 01 00 01 00 02 00 00 DNS ->Header 12 Bytes
03 77 77 77 05 63 69 73 63 6f 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 -> Question 25 bytes
00 01 51 80 00 04 c6 85 db 19 c0 10 00 02 00 01-> IP Address 16 bytes de cisco 198.133.219.25
00 01 51 80 00 06 03 6e 73 31 c0 10 c0 10 00 02 IP Address 16 bytes
00 01 00 01 51 80 00 06 03 6e 73 32 c0 10

Conclusión : el Host 163.10.10.2 responde la consulta DNS sobre la IP de www.cisco.com que es : c6 85 db 19 =198.133.219.25

e)
00 e0 7d 84 12 8b 00 0b 6a 39 7e 79 08 00 45 00

00 30 9e 17 40 00 80 06 0d f9 a3 0a 0a 0e c6 85
db 19 09 8e 00 50 21 c5 5d 99 00 00 00 00 70 02
fa f0 b0 3a 00 00 02 04 05 b4 01 01 04 02

Header del Frame
00 e0 7d 84 12 8b -> 6 Bytes MAC de Destino
00 0b 6a 39 7e 79 -> 6 Bytes , Mac de Origen
08 00 -> Tipo Datagrama IP
Header del Datagrama
45 ->Versión (0100) y long. del Header en palabras de 32 bits (01010 =5), 00 -> TOS
00 30 -> Largo en Bytes 48 (20 Header IP + 20 Header TCP + 8 =>OK)
9e 17 -> ID
40 00 -> -> 010= Flag DF=1,MF=0 , 0 0000 0000 0000(13)= Offset
80 ->TTL , 06-> Protocol TCP
0d f9->Header Checksum,
a3 0a 0a 0e ->IP Source 163.10.10.14
c6 85 db 19 -> IP Dest. 198.133.219.25
Datos de Datagrama proveniente de Capa de Transporte (Total 28 bytes)
Header Segmento TCP
09 8e Source Port 2446
00 50 Dest. Port 80 (Web Service)
21 c5 5d 99 Sec. Nro. 566582681
00 00 00 00 ACK.
70 02= 0111 (-> Header Lengh 7=28 Bytes) 000000 (Reserva) 000010 (Bits Flags =SYN)
fa f0 windows Size
b0 3a TCP CRC
00 00 URG Poniter
02 04 05 b4 01 01 04 02 -> Options

Conclusión : Este es el primer envío al Servidor web de cisco del three handshake, comienza el establecimiento de la conexión, este sería el lado Active Open

f)
00 0b 6a 39 7e 79 00 e0 7d 84 12 8b 08 00 45 04
00 2c 63 f7 00 00 2d 06 db 19 c6 85 db 19 a3 0a
0a 0e 00 50 09 8e e5 5a fd bd 21 c5 5d 9a 60 12
40 00 9d 24 00 00 02 04 05 98 05 63

Header del Frame
00 0b 6a 39 7e 79-> 6 Bytes MAC de Destino
00 e0 7d 84 12 8b-> 6 Bytes MAC de Origen
08 00-> Tipo Datagrama IP
Header del Datagrama IP
45 ->Versión (0100) y long. del Header en palabras de 32 bits (01010 =5) , 04 -> TOS
00 2c -> Largo en Bytes 44
63 f7 -> ID,
00 00 -> -> 000 (3)= Flag DF=0,MF=0 , 0 0000 0000 0000(13)= Offset

2d ->TTL , 06-> Protocol TCP
db 19 ->Header Checksum,
c6 85 db 19 ->IP Source 198 198.133.219.25
a3 0a 0a 0e -> IP Dest. 163.10.10.14

Header del Segmento TCP

00 50 -> Source Port 80 (Web Service)
09 8e -> 2446
e5 5a fd bd -> Sec. Number 3847945661
21 c5 5d 9a -> ACK Number 566582682
60 12 ->0110 (Header Lengh 6 =24 bytes) 000000 (Reserverd) 010010 (Flags ACK y SYN)
40 00 -> Windows Size
9d 24 -> TC CRC
00 00 -> Urgent Point
02 04 05 98 -> Options

Datos del Segmento

05 63

Conclusión: Reconoce el Segmento 566582681 diciendo que espera 566582682; 2do segmento de los tres que corresponden al Establecimiento de la coneción TCP, El servidor Web de Cisco sería el Pasive Open.

g)
00 e0 7d 84 12 8b 00 0b 6a 39 7e 79 08 00 45 00
00 28 9e 19 40 00 80 06 0d ff a3 0a 0a 0e c6 85
db 19 09 8e 00 50 21 c5 5d 9a e5 5a fd be 50 10
fb b8 f9 0c 00 00

Header del Frame

00 e0 7d 84 12 8b-> 6 Bytes MAC de Destino
00 0b 6a 39 7e 79-> 6 Bytes MAC de Origen
08 00-> Tipo Datagrama IP

Header del Datagrama IP

45 ->Versión (0100) y long. del Header en palabras de 32 bits (01010 =5) , 00 -> TOS
00 28-> Largo en Bytes 40 (20 Datagrama+ 20 Segmento)
9e 19 -> ID 40473
40 00-> 010= Flag DF=1,MF=0 , 0 0000 0000 0000= Offset
80-> TTL , 06 -> Protocolo TCP
0d ff ->Header Checksum,
a3 0a 0a 0e -> IP Source 163.10.10.14
c6 85 db 19 -> IP Destino 198.133.219.25

Header del Segmento TCP

09 8e -> Source Port 2446
00 50 -> Dest. Port 80 (Web Service)
21 c5 5d 9a ->Sec. Number 566582682
e5 5a fd be ->ACK Number 3847945662
50 10 ->101 (->Header Length 5= 20 Bytes) 000000 (Reserverd) 010000 (Flags) ACK

fb b8 ->Windows Size
f9 0c -> TCR CRC
00 00 -> Urgent Point
Datos del Segmento -> No hay

Conclusión: Es el tercer y último Segmento del establecimoento de la conexión de TCP del host 163.10.10.14 con el Servidor Web de Cisco , contesta con un ACK 3847945662, o sea que valida el segmento 3847945661 que había sido enviado en f.

h)
00 e0 7d 84 12 8b 00 0b 6a 39 7e 79 08 00 45 00
01 8d 9e 1a 40 00 80 06 0c 99 a3 0a 0a 0e c6 85
db 19 09 8e 00 50 21 c5 5d 9a e5 5a fd be 50 18
fb b8 b3 c9 00 00 47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d
61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78
2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f
6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65
67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78
2d 73 68 6f 63 6b 77 61 76 65 2d 66 6c 61 73 68
2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e
64 2e 6d 73 2d 65 78 63 65 6c 2c 20 61 70 70 6c
69 63 61 74 69 6f 6e 2f 76 6e 64 2e 6d 73 2d 70
6f 77 65 72 70 6f 69 6e 74 2c 20 61 70 70 6c 69
63 61 74 69 6f 6e 2f 6d 73 77 6f 72 64 2c 20 2a

Header del Frame
00 e0 7d 84 12 8b-> 6 Bytes MAC de Destino
00 0b 6a 39 7e 79-> 6 Bytes MAC de Origen
08 00 -> Tipo Datagrama IP
Header del Datagrama
45 ->Versión (0100) y long. del Header en palabras de 32 bits (01010 =5) , 00 -> TOS
01 8d -> Largo en Bytes 397 (20 header IP+ 20 header TCP + datos del 357)
9e 1a->ID
40 00> 010= Flag DF=1,MF=0 , 0 0000 0000 0000= Offset
80 > TTL , 06 -> Protocolo TCP
0c 99 ->Header Checksum,
a3 0a 0a 0e->IP Source 163.10.10.14
c6 85 db 19> IP Dest. 198.133.219.25
Header del Segmento TCP
09 8e -> Source Port 2446
00 50 -> Dest. Port 80 Web Service
21 c5 5d 9a ->Sec. Number 566582682
e5 5a fd be -> Ack Number 240844222
50 18 -> 0101 (-> Header Lengh 5= 20 bytes) 000000 (Reserva) 011 000 (Flags => ACK ,

PUSH)
fb b8 > Windows size
b3 c9 –> TCP CRC
00 00 -> Urgent Point

Datos del Segmento

47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78 2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f 6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65 67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 73 68 6f 63 6b 77 61 76 65 2d 66 6c 61 73 68 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e 64 2e 6d 73 2d 65 78 63 65 6c 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e 64 2e 6d 73 2d 70 6f 77 65 72 70 6f 69 6e 74 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6d 73 77 6f 72 64 2c 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 73 2d 61 72 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 36 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 29 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 63 69 73 63 6f 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a

Conclusión: este último segmento es el que envía el host 163.10.10.14 al servidor Web de cisco supongo que solicitando la pagina 77 77 77 05 63 69 73 63 6f 03 63 6f 6d no creo que sea relevante el analisis del contenido