

fs2007

V Foro de  
Seguridad RedIRIS



# Detección de intrusos en la red: más allá del NIDS

David Pérez  
(Consultor independiente)

Puerto de la Cruz, 12-13 Abril 2007



Red IRIS

# Ponente

- David Pérez Conde
- Consultor independiente de seguridad
- Instructor de The SANS Institute
- GSE (<http://www.giac.org/certifications/gse.php>)
- [david.perez.conde@gmail.com](mailto:david.perez.conde@gmail.com)
- <http://www.radajo.com>

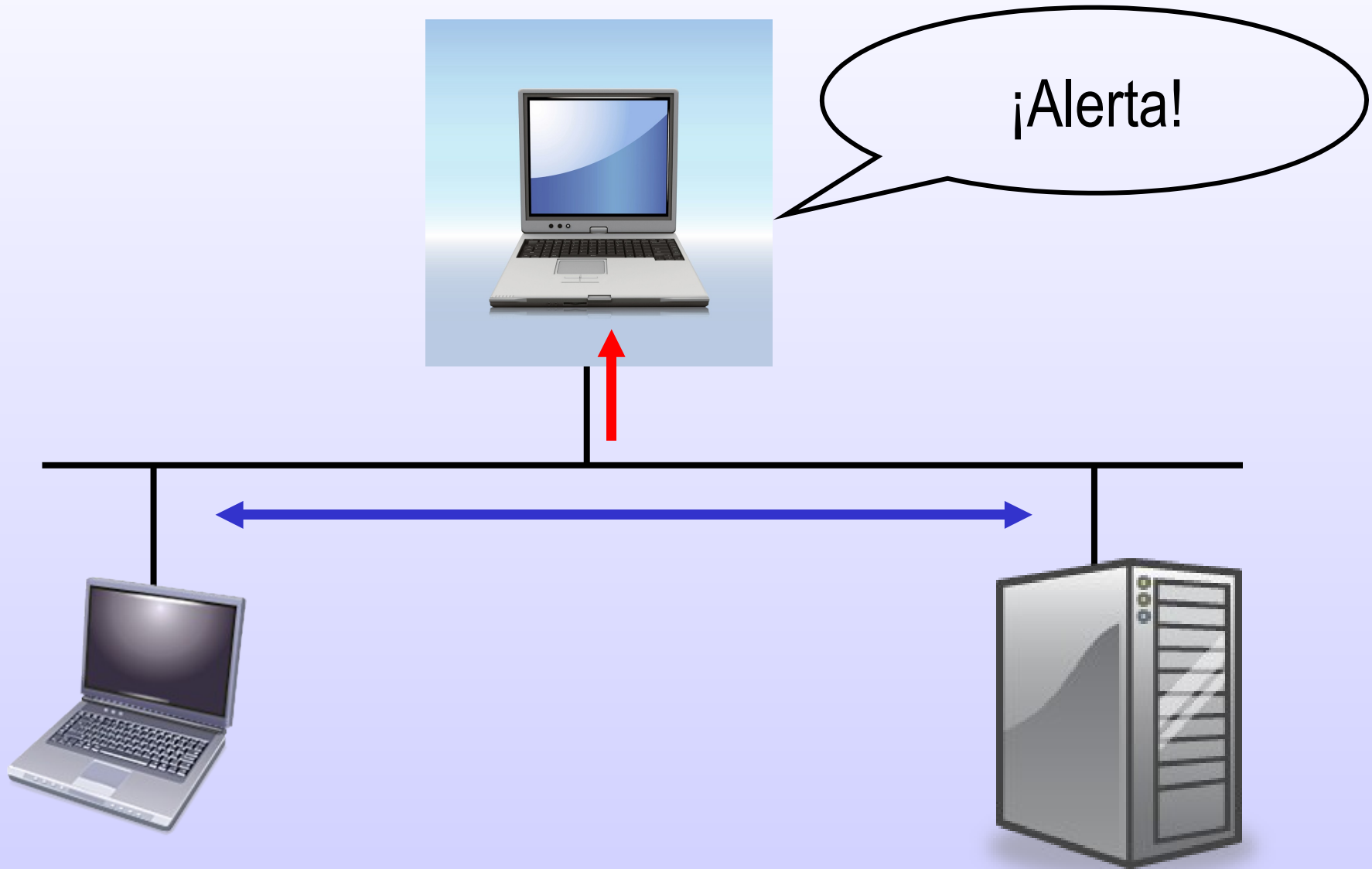
# Agenda

- Introducción
- Limitaciones del NIDS/NIPS
- Más allá del NIDS:
  - Análisis de trazas de red
  - Análisis de logs de sistema
  - Automatización

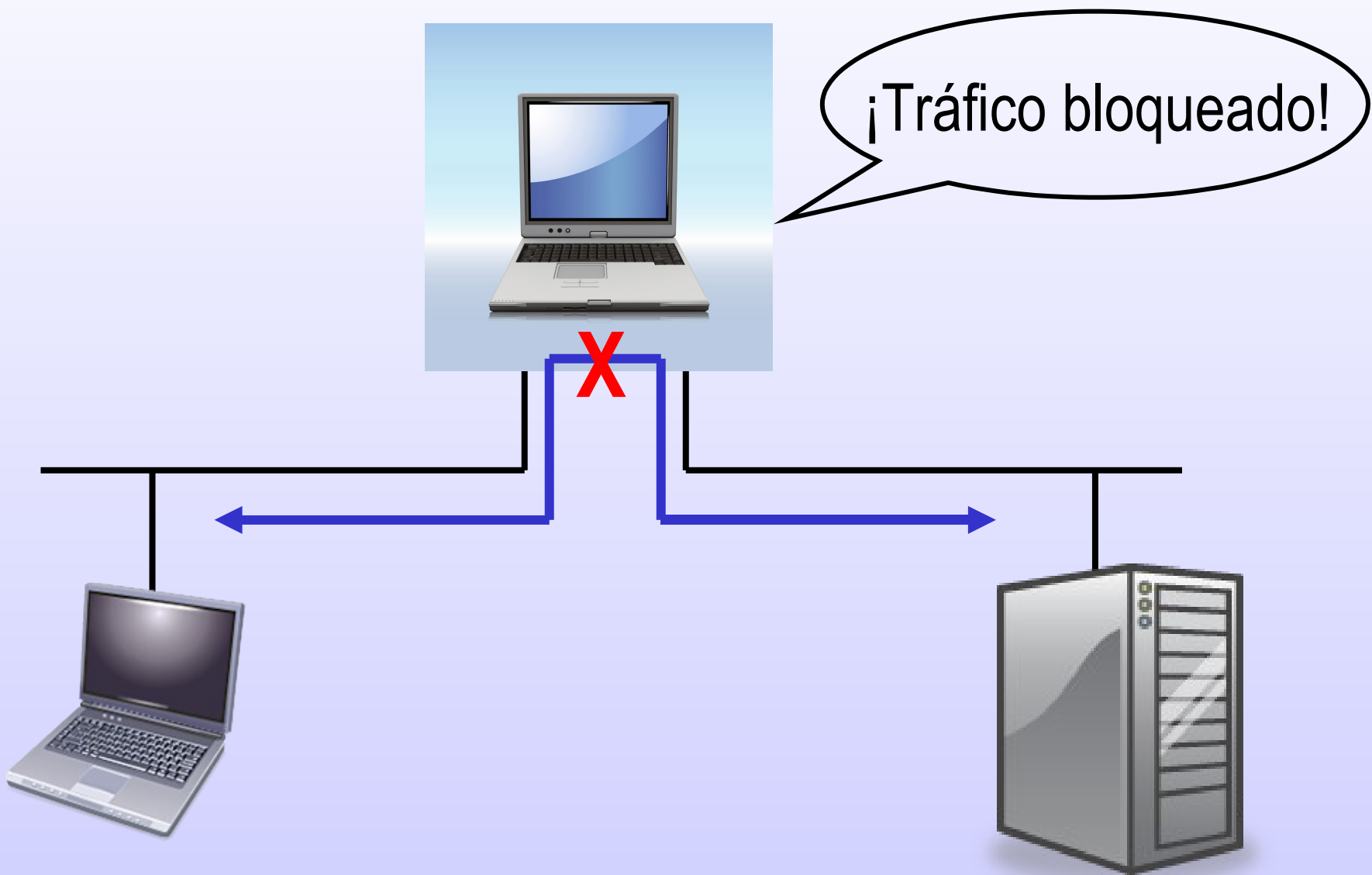
# Definiciones

- **IDS:** Sistema de detección de intrusiones
  - HIDS:** IDS de host
  - NIDS:** IDS de red
- **IPS:** Sist. de prevención contra intrusiones
  - HIPS:** IPS de host
  - NIPS:** IPS de red

# NIDS



# NIPS





```
alert tcp 10.10.10.10 !80 -> any any \  
  (msg: "Tráfico sospechoso")
```

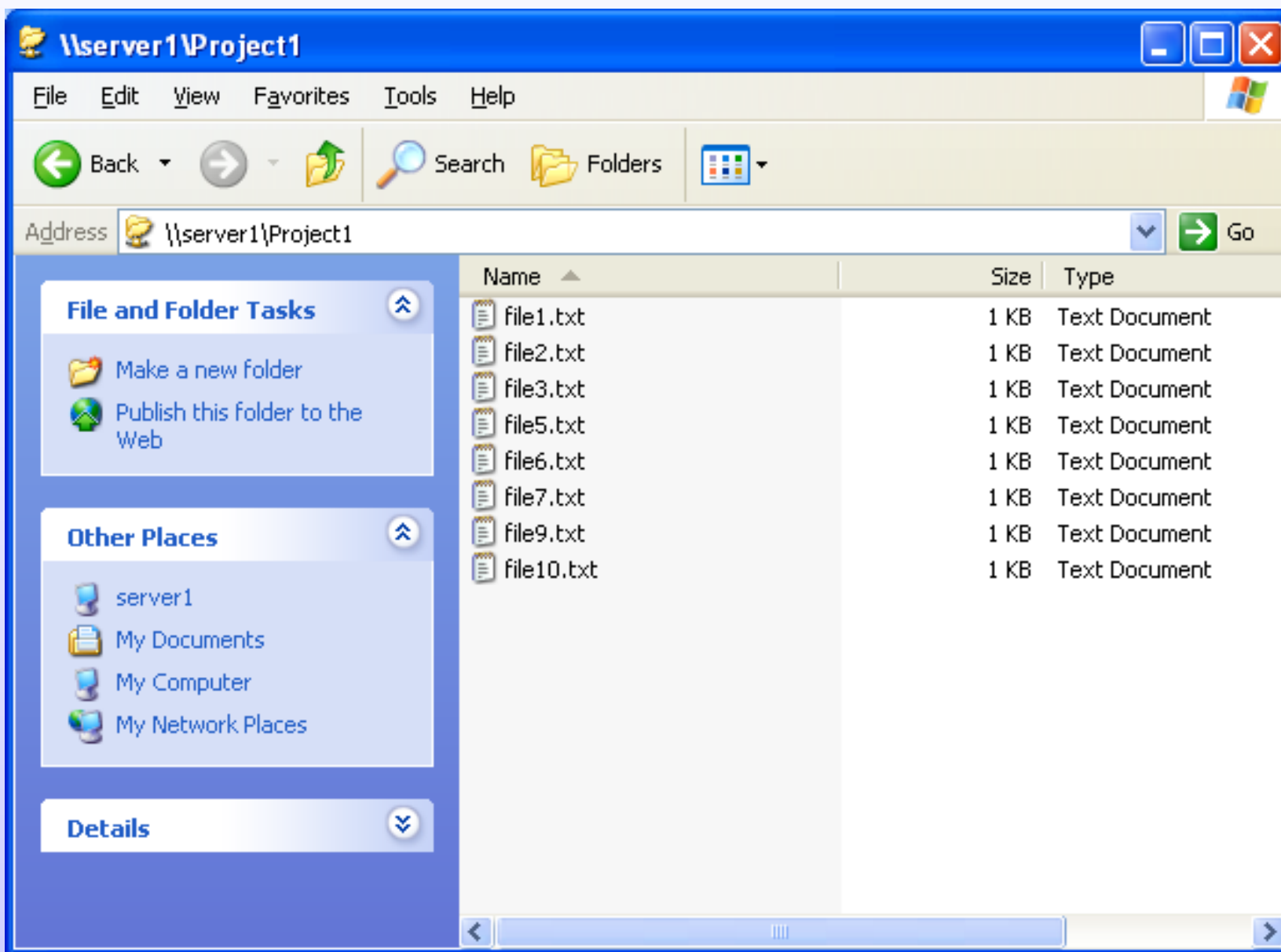
```
drop tcp 10.10.10.10 !80 -> any any \  
  (msg: "Tráfico sospechoso eliminado")
```

# Limitaciones de NIDS/NIPS

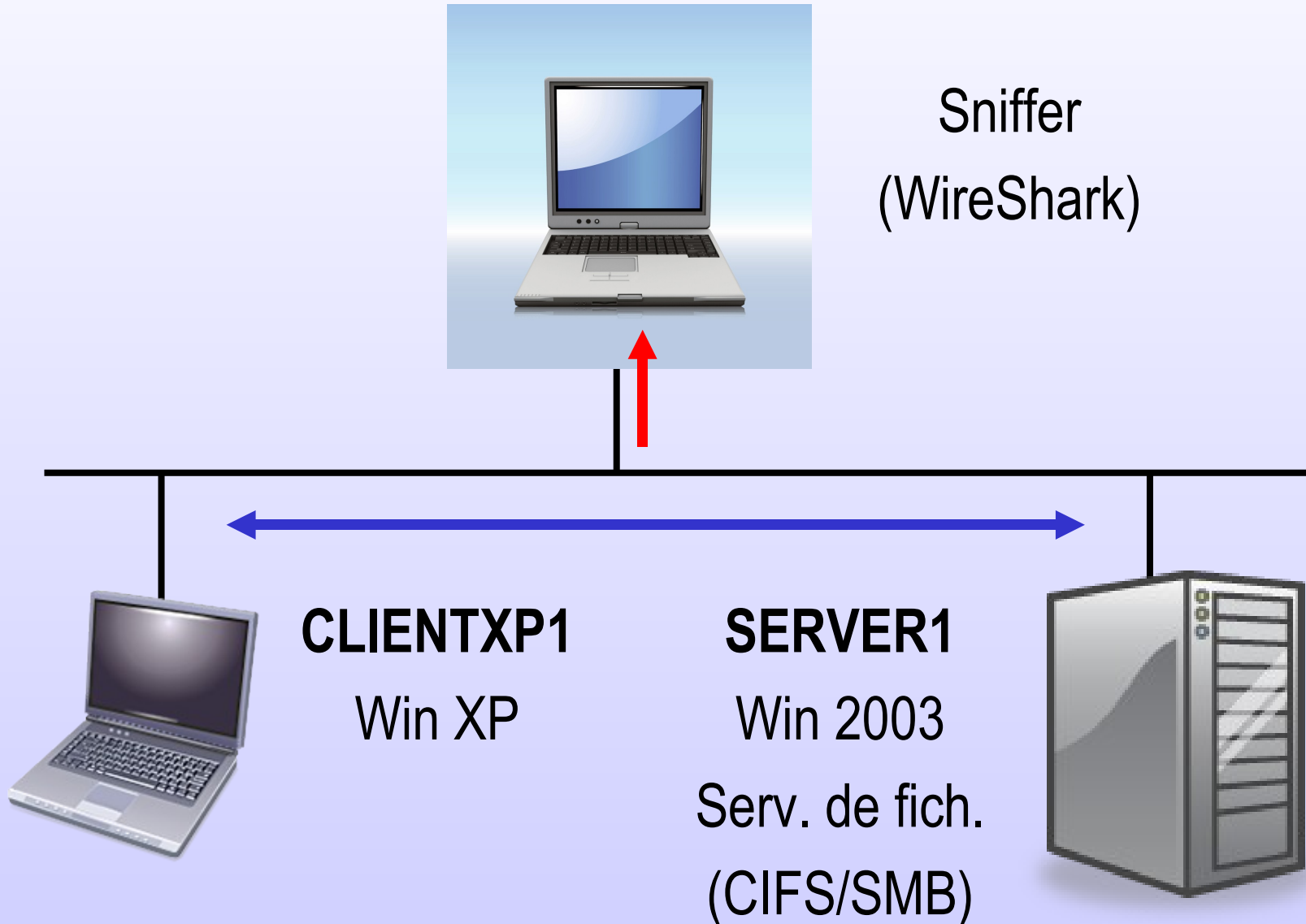
- Ancho de banda
- Firmas / anomalías
- Falsos positivos
- Gestión de las alertas
- ***Visión limitada***



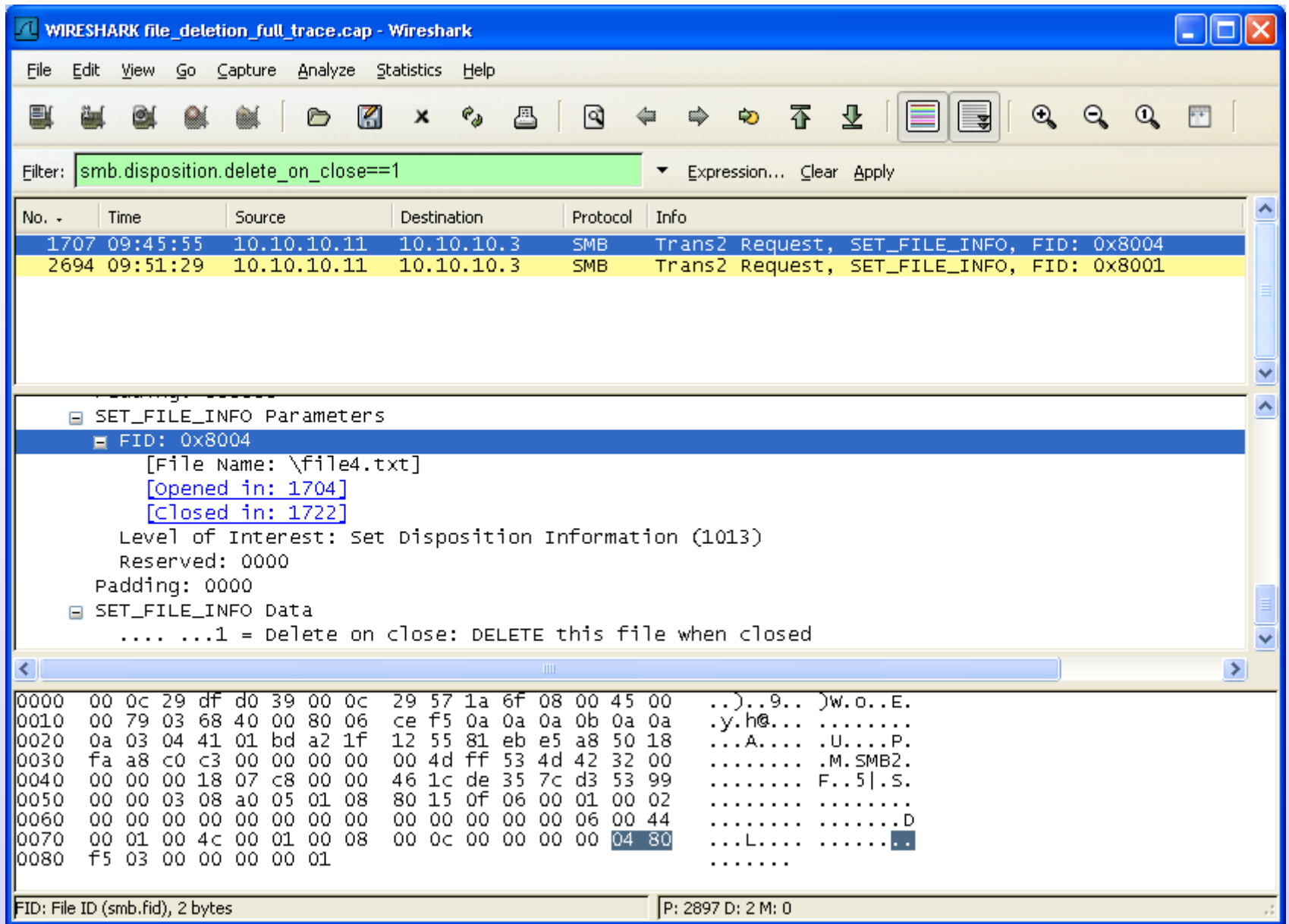
# Incidente: Ficheros borrados



# Incidente: Ficheros borrados



# Análisis de la traza de red



`smb.disposition.delete_on_close`: el cliente marca un fichero (smb.fid) para ser borrado

WIRESHARK file\_deletion\_full\_trace.cap - Wireshark

Filter: `smb.fid==0x8004`

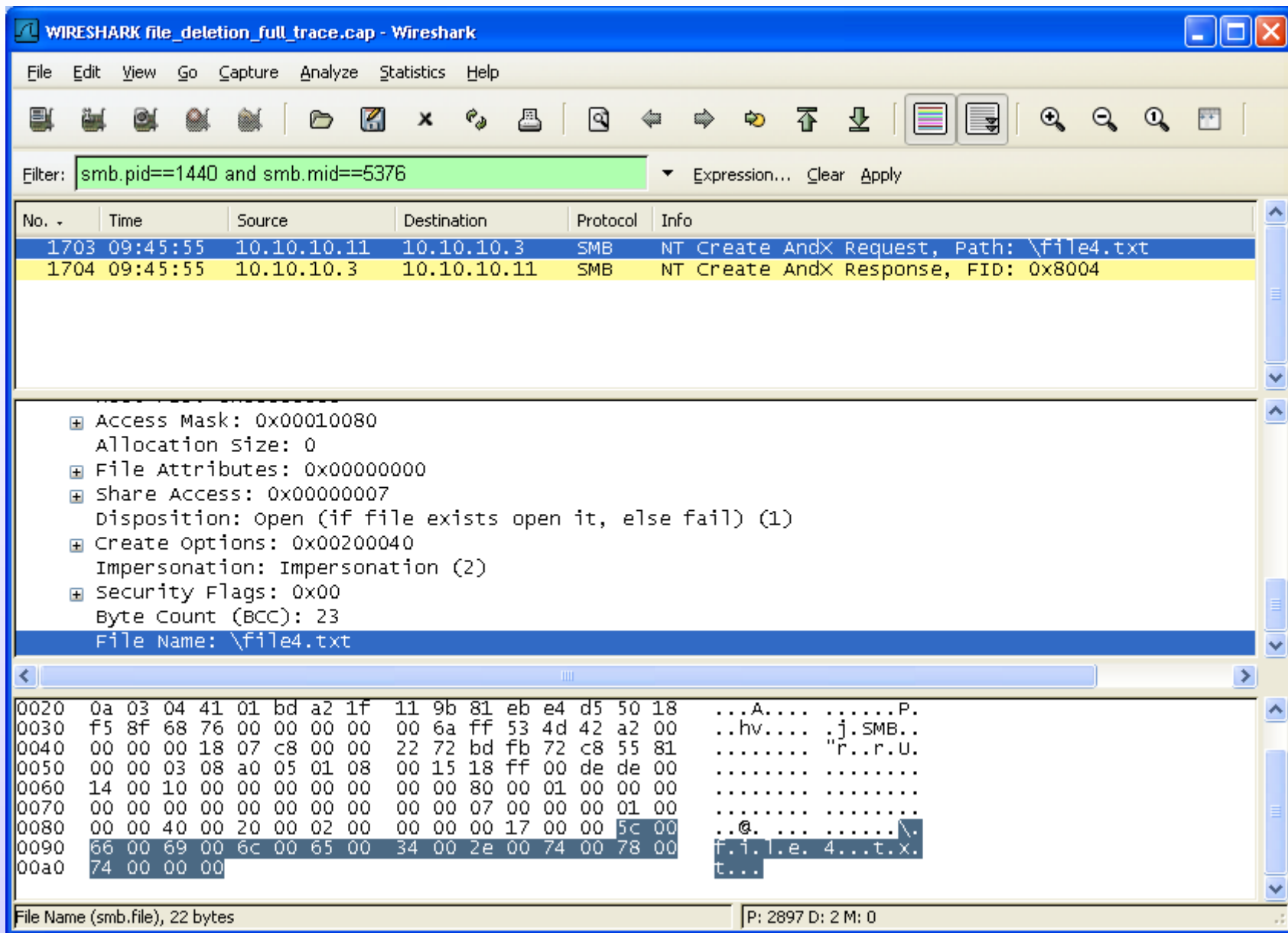
No. -	Time	Source	Destination	Protocol	Info
1704	09:45:55	10.10.10.3	10.10.10.11	SMB	NT Create AndX Response, FID: 0x8004
1705	09:45:55	10.10.10.11	10.10.10.3	SMB	Trans2 Request, QUERY_FILE_INFO, FID: 0x8004, Qu
1707	09:45:55	10.10.10.11	10.10.10.3	SMB	Trans2 Request, SET_FILE_INFO, FID: 0x8004
1709	09:45:55	10.10.10.11	10.10.10.3	SMB	Close Request, FID: 0x8004

Flags: 0x98  
Flags2: 0xc807  
Process ID High: 0  
Signature: 12B85609CB7FEBE2  
Reserved: 0000  
Tree ID: 2051  
Process ID: 1440  
User ID: 2049  
Multiplex ID: 5376  
NT Create AndX Response (0xa2)

```
0040 00 00 00 98 07 c8 00 00 12 b8 56 09 cb 7f eb e2 .....V.....
0050 00 00 03 08 a0 05 01 08 00 15 2a ff 00 87 00 00 .....*.....
0060 04 80 01 00 00 00 4a aa 0e 41 6a 6a c7 01 12 70 .....J..Ajj...p
0070 03 73 6a 6a c7 01 12 70 03 73 6a 6a c7 01 2a 05 .sjj...p .sjj...*
0080 21 e8 ab 6b c7 01 20 00 00 00 18 00 00 00 00 00 !..k..
0090 00 00 12 00 00 00 00 00 00 00 00 00 07 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 ff 01 1f 00 00 00 00 00 00 .....
00c0 00
```

Multiplex ID (smb.mid), 2 bytes | P: 2897 D: 4 M: 0

smb.fid: Identificador de fichero, asignado por el servidor  
al abrir un fichero



smb.pid: Identificador de proceso, asignado por cliente.

smb.mid: Identificador de petición/resp., asignado por cliente.

WIRESHARK file\_deletion\_full\_trace.cap - Wireshark

Filter: `smb.tid==2051`

No. -	Time	Source	Destination	Protocol	Info
1659	09:45:42	10.10.10.3	10.10.10.11	SMB	Tree Connect AndX Response
1660	09:45:42	10.10.10.11	10.10.10.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Basi
1661	09:45:42	10.10.10.3	10.10.10.11	SMB	Trans2 Response, QUERY_PATH_INFO
1662	09:45:42	10.10.10.11	10.10.10.3	SMB	Trans2 Request, FIND_FIRST2, Pattern: \*
1663	09:45:42	10.10.10.3	10.10.10.11	SMB	Trans2 Response, FIND_FIRST2, Files: . . . file1.
1665	09:45:42	10.10.10.11	10.10.10.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Basi
1666	09:45:42	10.10.10.3	10.10.10.11	SMB	Trans2 Response, QUERY_PATH_INFO, Error: STATUS_

Signature: 0110C03654F8F557  
Reserved: 0000  
Tree ID: 2051  
[Path: \\SERVER1\PROJECT1]  
[Mapped in: 1659]  
Process ID: 65279  
User ID: 2049  
Multiplex ID: 4097  
Tree Connect AndX Response (0x75)  
Word Count (WCT): 7  
AndXCommand: No further commands (0xff)

```
0000 00 0c 29 57 1a 6f 00 0c 29 df d0 39 08 00 45 00  ..)w.o.. )..9..E.
0010 00 6a 1a 6b 40 00 80 06 b8 01 0a 0a 0a 03 0a 0a  .j.k@... ..
0020 0a 0b 01 bd 04 41 81 eb d9 52 a2 1f 0b 75 50 18  ....A.. .R...UP.
0030 f9 d2 24 7b 00 00 00 00 00 3e ff 53 4d 42 75 00  ..${.... .>.SMBu.
0040 00 00 00 98 07 c8 00 00 01 10 c0 36 54 f8 f5 57  .... ..6T..W
0050 00 00 03 08 ff fe 01 08 01 10 07 ff 00 3e 00 01  .... ..>..
0060 00 bf 01 13 00 00 00 00 00 0d 00 41 3a 00 4e 00  .... ..A:.N.
0070 54 00 46 00 53 00 00 00  T.F.S...
```

Multiplex ID (smb.mid), 2 bytes | P: 2897 D: 59 M: 0

smb.tid: (Tree ID) Identificador de directorio compartido,  
asignado por el servidor

The image shows a Wireshark capture of network traffic. The filter is set to `smb.mid==4097`. Two packets are highlighted: packet 1658 (SMB Tree Connect AndX Request) and packet 1659 (SMB Tree Connect AndX Response). The packet details pane shows the following information:

- Word Count (WCT): 4
- AndxCommand: No further commands (0xff)
- Reserved: 00
- Andxoffset: 88
- Flags: 0x0008
- Password Length: 1
- Byte Count (BCC): 45
- Password: 00
- Path: `\\SERVER1\PROJECT1`
- Service: `?????`

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion of the packet data is as follows:

```
0010 00 84 03 4d 40 00 80 06 cf 05 0a 0a 0a 0b 0a 0a ...M@... .....
```

```
0020 0a 03 04 41 01 bd a2 1f 0b 19 81 eb d9 52 50 18 ...A....RP.
```

```
0030 fa c9 91 18 00 00 00 00 00 58 ff 53 4d 42 75 00 .....X.SMBU.
```

```
0040 00 00 00 18 07 c8 00 00 67 fd 93 90 c6 6d 38 05 .....g....m8.
```

```
0050 00 00 00 00 ff fe 01 08 01 10 04 ff 00 58 00 08 .....X..
```

```
0060 00 01 00 2d 00 00 5c 00 5c 00 53 00 45 00 52 00 ...-.\. \.S.E.R.
```

```
0070 56 00 45 00 52 00 31 00 5c 00 50 00 52 00 4f 00 V.E.R.1. \.P.R.O.
```

```
0080 4a 00 45 00 43 00 54 00 31 00 00 00 3f 3f 3f 3f J.E.C.T. 1...????
```

```
0090 3f 00 ?.
```

The status bar at the bottom indicates: Path. Server name and share name (smb.path), 38 bytes | P: 2897 D: 2 M: 0

Fichero borrado: `\\SERVER1\PROJECT1\file4.txt`



The image shows a Wireshark capture window titled "WIRESHARK file\_deletion\_full\_trace.cap - Wireshark". The filter is set to "smb.uid==2049 and smb.cmd==0x73". The packet list shows four SMB Session Setup AndX Response packets (No. 598, 828, 1527, 2815) from 10.10.10.3 to 10.10.10.11. The packet details pane shows the structure of the response, including Flags, Process ID, Signature, Reserved, Tree ID, Process ID (65279), User ID (2049), Multiplex ID (64), and Session Setup AndX Response (0x73) with a Word Count (WCT) of 4. The packet bytes pane shows the raw data, with the User ID field (01 08) highlighted in blue. The status bar at the bottom indicates "User ID (smb.uid), 2 bytes" and "P: 2897 D: 4 M: 0".

No.	Time	Source	Destination	Protocol	Info
598	09:40:19	10.10.10.3	10.10.10.11	SMB	Session Setup AndX Response
828	09:40:20	10.10.10.3	10.10.10.11	SMB	Session Setup AndX Response
1527	09:45:35	10.10.10.3	10.10.10.11	SMB	Session Setup AndX Response
2815	09:55:28	10.10.10.3	10.10.10.11	SMB	Session Setup AndX Response

Flags: 0x98  
Flags2: 0xc807  
Process ID High: 0  
Signature: 83FEC98E4D771DC6  
Reserved: 0000  
Tree ID: 0  
Process ID: 65279  
User ID: 2049  
Multiplex ID: 64  
Session Setup AndX Response (0x73)  
Word Count (WCT): 4

0050 00 00 00 00 ff fe 01 08 40 00 04 ff 00 59 01 00 ..... @....Y..  
0060 00 a2 00 2e 01 a1 81 9f 30 81 9c a0 03 0a 01 00 ..... 0.....  
0070 a1 0b 06 09 2a 86 48 82 f7 12 01 02 02 a2 81 87 ..... \*.H. ....  
0080 04 81 84 60 81 81 06 09 2a 86 48 86 f7 12 01 02 ..... \*.H.....  
0090 02 02 00 6f 72 30 70 a0 03 02 01 05 a1 03 02 01 ...or0p. ....  
00a0 0f a2 64 30 62 a0 03 02 01 17 a2 5b 04 59 88 90 ..d0b... ..[.Y..  
00b0 d3 8f c1 23 be a9 13 16 e0 40 5a da 68 4b 29 3f ...#. .... .@Z.hk)?  
00c0 9c 86 b4 12 b5 8c 11 f0 ac 9c 0f 86 63 34 f2 20 ..... ....c4..  
00d0 bc 55 b4 15 03 c0 7f 75 dd 08 8d 68 29 cf a4 98 .U.....u ...h)...  
00e0 c3 67 56 d6 2f 2b 8a 07 39 c3 2b cb bc 8d 8c bb .gv./+.. 9.+.....

User ID (smb.uid), 2 bytes | P: 2897 D: 4 M: 0

smb.uid: Identificador de usuario, asignado por el servidor al establecer la sesión (Session Setup AndX Req/Resp)

The image shows a Wireshark capture window titled "WIRESHARK file\_deletion\_full\_trace.cap - Wireshark". The filter is set to "smb.cmd==0x73 and smb.pid==65279 and smb.mid==64". The packet list shows several SMB "Session Setup AndX Request" packets. The selected packet (No. 1751) is expanded to show its structure:

- MSG Type: AP-REQ (14)
- Padding: 0
- APOptions: 20000000 (Mutual required)
- Ticket
  - Tkt-vno: 5
  - Realm: SANS.ORG
  - Server Name (Service and Instance): cifs/server1.sans.org
    - Name-type: Service and Instance (2)
    - Name: cifs
    - Name: server1.sans.org
  - enc-part rc4-hmac
    - Encryption type: rc4-hmac (23)
    - Kvno: 5
    - enc-part: C26F4754CD8AEC79F9A8C095147CC075F6038D85074CC0E3...
  - Authenticator rc4-hmac

The bottom of the window shows the raw data of the selected packet, including a hex dump and its ASCII representation. The ASCII part shows the beginning of the Kerberos ticket data: "...Z... v.OGT... y...|. u...L. ....Z.. .X...dv. %.j..... f..G....".

La petición de establecimiento de sesión incluye un ticket de kerberos que identifica al usuario, aunque el nombre...

The image shows a Wireshark capture window titled "WIRESHARK file\_deletion\_full\_trace.cap - Wireshark". The filter is set to "kerberos.ticket.data[0:4]==C2:6F:47:54". The packet list shows four packets, with the third packet (No. 1525) selected. The details pane shows the expanded structure of the TGS-REP packet:

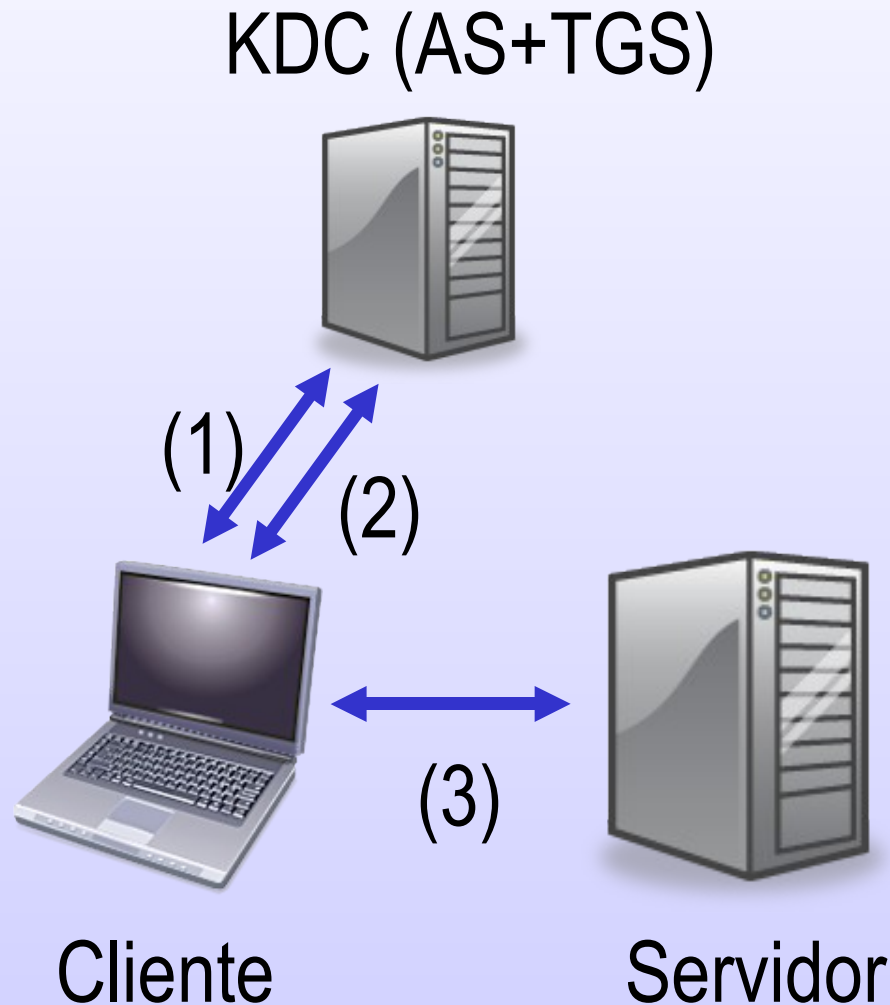
- Client Name (Principal): david
  - Name-type: Principal (1)
  - Name: david
- Ticket
  - Tkt-vno: 5
  - Realm: SANS.ORG
  - Server Name (Service and Instance): cifs/server1.sans.org
    - Name-type: Service and Instance (2)
    - Name: cifs
    - Name: server1.sans.org
  - enc-part rc4-hmac
    - Encryption type: rc4-hmac (23)
    - Kvno: 5
    - enc-part: C26F4754CD8AEC79F9A8C095147CC075F6038D85074CC0E3...
  - enc-part rc4-hmac

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion includes "SANS.ORG" and "david".

File: "C:\davidhome\datos\SMB Forensics\070323\file\_deletion\_full\_trace.cap" 814 KB 00:35:01 | P: 2897 D: 4 M: 0

... sólo aparece en claro en la respuesta del servidor KDC que proporcionó el ticket. **Principal: david. Realm: SANS.ORG**

# Inciso: KERBEROS



**KDC:** Kerberos Distribution Center

**AS:** Authentication Service

**TGS:** Ticket Granting Service

**Tickets:**

- Ticket Granting Ticket (TGT)
- Service Ticket (ST)

(1) Obtener TGT

(2) Obtener ST

(3) Presentar ST

WIRESHARK file\_deletion\_full\_trace.cap - Wireshark

Filter: `beros.ticket.data[0:4]==C2:6F:47:54 or kerberos.msg.type==12` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
823	09:40:20	10.10.10.11	10.10.10.3	KRB5	TGS-REQ
824	09:40:20	10.10.10.3	10.10.10.11	KRB5	TGS-REP
826	09:40:20	10.10.10.11	10.10.10.3	SMB	Session Setup AndX Request
1525	09:45:35	10.10.10.11	10.10.10.3	SMB	Session Setup AndX Request
1758	09:51:07	10.10.10.11	10.10.10.3	KRB5	TGS-REQ

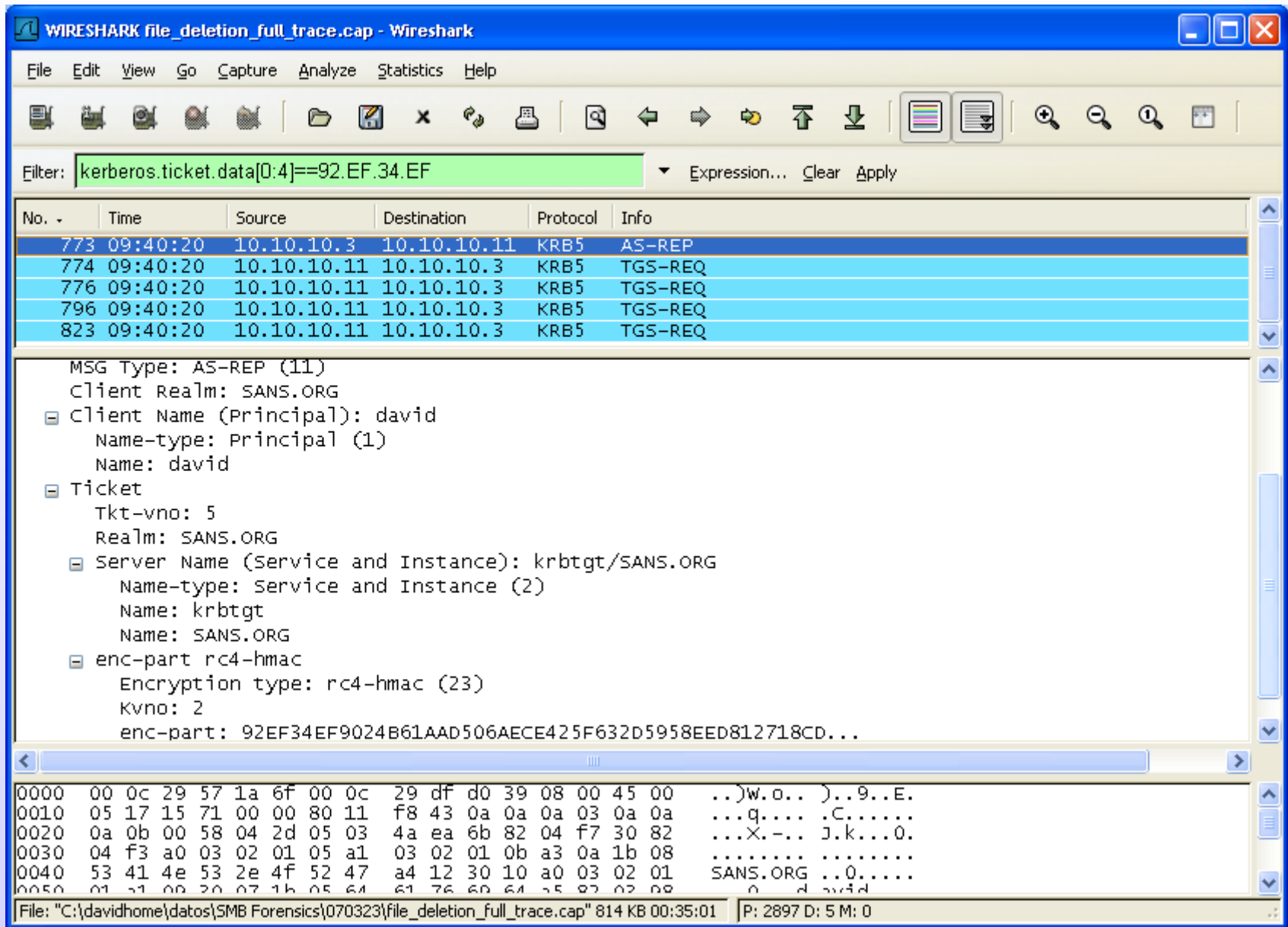
Type: PA-TGS-REQ (1)

- Value: 6E8204413082043DA003020105A10302010EA20703050000... AP-REQ
  - Pvno: 5
  - MSG Type: AP-REQ (14)
  - Padding: 0
  - APOptions: 00000000
  - Ticket
    - Tkt-vno: 5
    - Realm: SANS.ORG
    - Server Name (Service and Instance): krbtgt/SANS.ORG
    - enc-part rc4-hmac
      - Encryption type: rc4-hmac (23)
      - Kvno: 2
      - enc-part: 92EF34EF9024B61AAD506AECE425F632D5958EED812718CD...
  - Authenticator rc4-hmac

00c0 03 4a 04 82 03 46 92 ef 34 ef 90 24 b6 1a ad 50 .J...F.. 4..\$....P  
00d0 6a ec e4 25 f6 32 d5 95 8e ed 81 27 18 cd ce d2 j..%.2.. ..'....  
00e0 6f 59 57 d3 8b 06 9c 17 09 3c c6 c0 37 8c f4 03 DYw.... .<.7...  
00f0 57 f5 54 fb 7e fa 81 52 2b 15 4c d6 f2 20 ae b7 w.T.~..R+.L...  
0100 d1 bd bd df c2 51 de b2 64 54 0e 8b 2f d6 e9 c3 .....Q..dT../...  
0110 ae 5a 6b 01 a1 07 24 9a de 2f 73 1c 47 7c 84 cf .Zk...\$. ./s.G|..

The encrypted part of a ticket (kerberos.ticket.data), 838 bytes | P: 2897 D: 16 M: 0

La petición correspondiente contiene el TGT del usuario...



...que fue obtenido en un mensaje AS-REP, como respuesta a una petición AS-REQ...

WIRESHARK file\_deletion\_full\_trace.cap - Wireshark

Filter: `beros.ticket.data[0:4]==92.EF.34.EF or kerberos.msg.type==10`

No.	Time	Source	Destination	Protocol	Info
586	09:40:19	10.10.10.11	10.10.10.3	KRB5	AS-REQ
772	09:40:20	10.10.10.11	10.10.10.3	KRB5	AS-REQ
773	09:40:20	10.10.10.3	10.10.10.11	KRB5	AS-REP
774	09:40:20	10.10.10.11	10.10.10.3	KRB5	TGS-REQ
776	09:40:20	10.10.10.11	10.10.10.3	KRB5	TGS-REQ

**KDC\_REQ\_BODY**

- Padding: 0
- KDCOptions: 40810010 (Forwardable, Renewable, Canonicalize, Renewable OK)
- Client Name (Enterprise Name): david@sans.org
  - Name-type: Enterprise Name (10)
  - Name: david@sans.org
  - Realm: SANS.ORG
- Server Name (Service and Instance): krbtgt/SANS.ORG
  - Name-type: Service and Instance (2)
  - Name: krbtgt
  - Name: SANS.ORG
- till: 2037-09-13 02:48:05 (Z)
- rtime: 2037-09-13 02:48:05 (Z)
- Nonce: 1650559562
- Encryption Types: rc4-hmac rc4-hmac-old rc4-md4 des-cbc-md5 des-cbc-crc rc4-hmac-exp rc4-hmac-c
- HostAddresses: CLIENTXP1<20>

This is a list of Kerberos HostAddress sequences (kerberos.hostaddresses), 27 bytes

P: 2897 D: 9 M: 0

...y esa petición AS-REQ contiene el nombre NETBIOS del equipo cliente desde el que se realizó la petición: **CLIENTXP1**

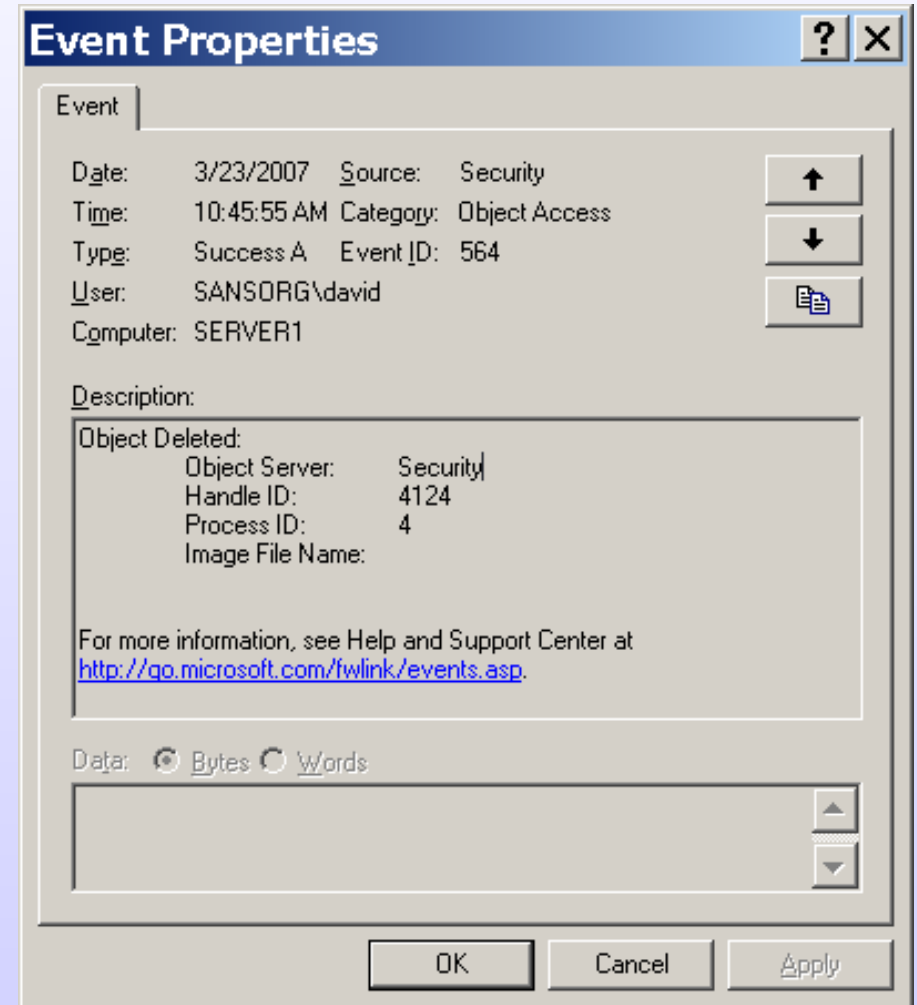
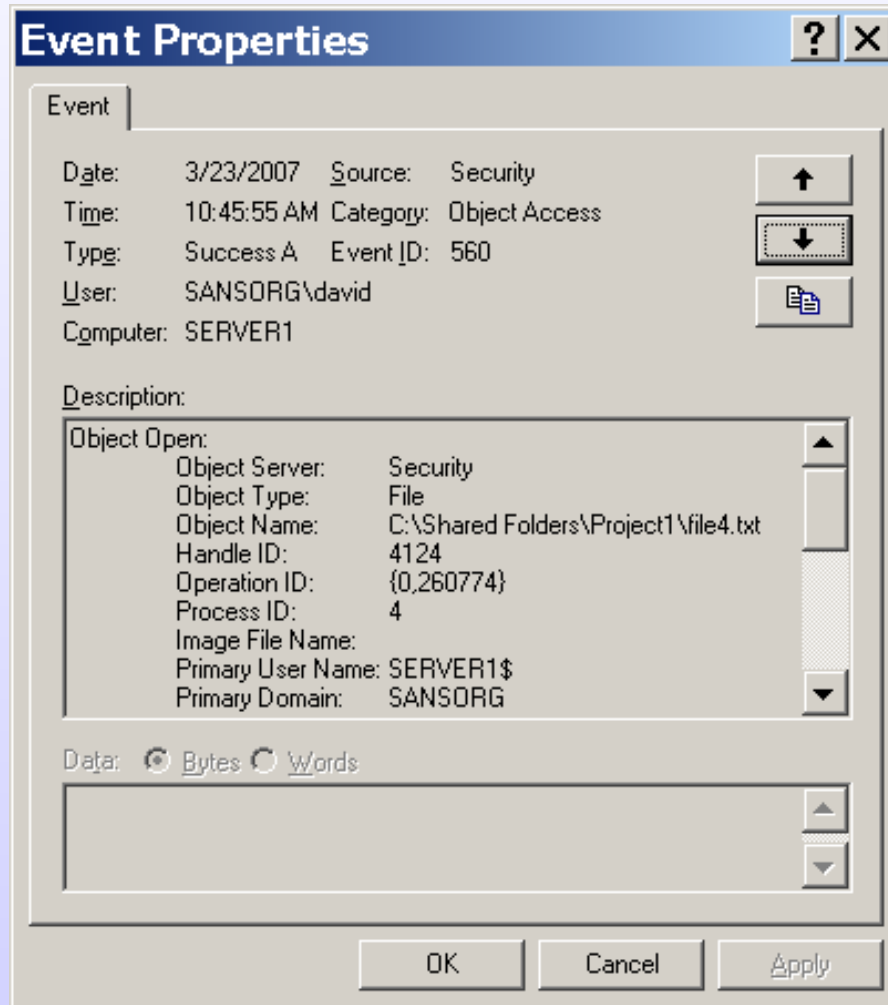
# Ya sabemos:

- El fichero `\\server1\Project1\file04.txt` fue borrado a las **09:45:55** a través de una sesión **SMB** establecida como usuario  **david@sans.org**  desde el equipo **CLIENTXP1** (**10.10.10.11** en aquel momento).



# Análisis de logs de sistema

# Object Access: 560 y 564



Nota: Reloj desplazado 1h por el cambio horario (de invierno a verano) del 25-mar-2007

# Nos confirma:

- El fichero `\\server1\Project1\file04.txt` fue borrado a las **09:45:55** a través de una sesión remota (¿**SMB**?) como usuario **david@sans.org** desde el equipo **CLIENTXP1 (10.10.10.11** en aquel momento).
- Otros eventos confirman (¿o sólo indican?) que era SMB

# Eventos interesantes (1/2)

- Account Logon
  - 672 : Auth. Ticket Request
  - 673 : Service Ticket Request
- Logon/Logoff
  - 540 : Successful Network Logon
  - 576 : Special priv. Assigned to New Logon
  - 538 : User Logoff

# Eventos interesantes (2/2)

- Object Access
  - 560 : Object Open
  - 564 : Object Deleted
  - 567 : Object Access Attempt
  - 562 : Handle Closed
- Process Tracking
  - 592 : A new process was created
  - 593 : A process exited

# Automatización

# Automatización

- tshark
- Scripts (Perl, Visual Basic Script, PowerShell, etc.)
- Programas en otros lenguajes
- Productos comerciales

# Referencias

- <http://www.radajo.com>
- <http://www.sans.org>
- <http://www.snort.org>
- <http://www.wireshark.org>
- <http://www.isascripts.org>
- <http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx>
- <http://www.microsoft.com/technet/scriptcenter/default.mspx>
- <http://www.niksun.com>