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

RedIRIS

# Ponente

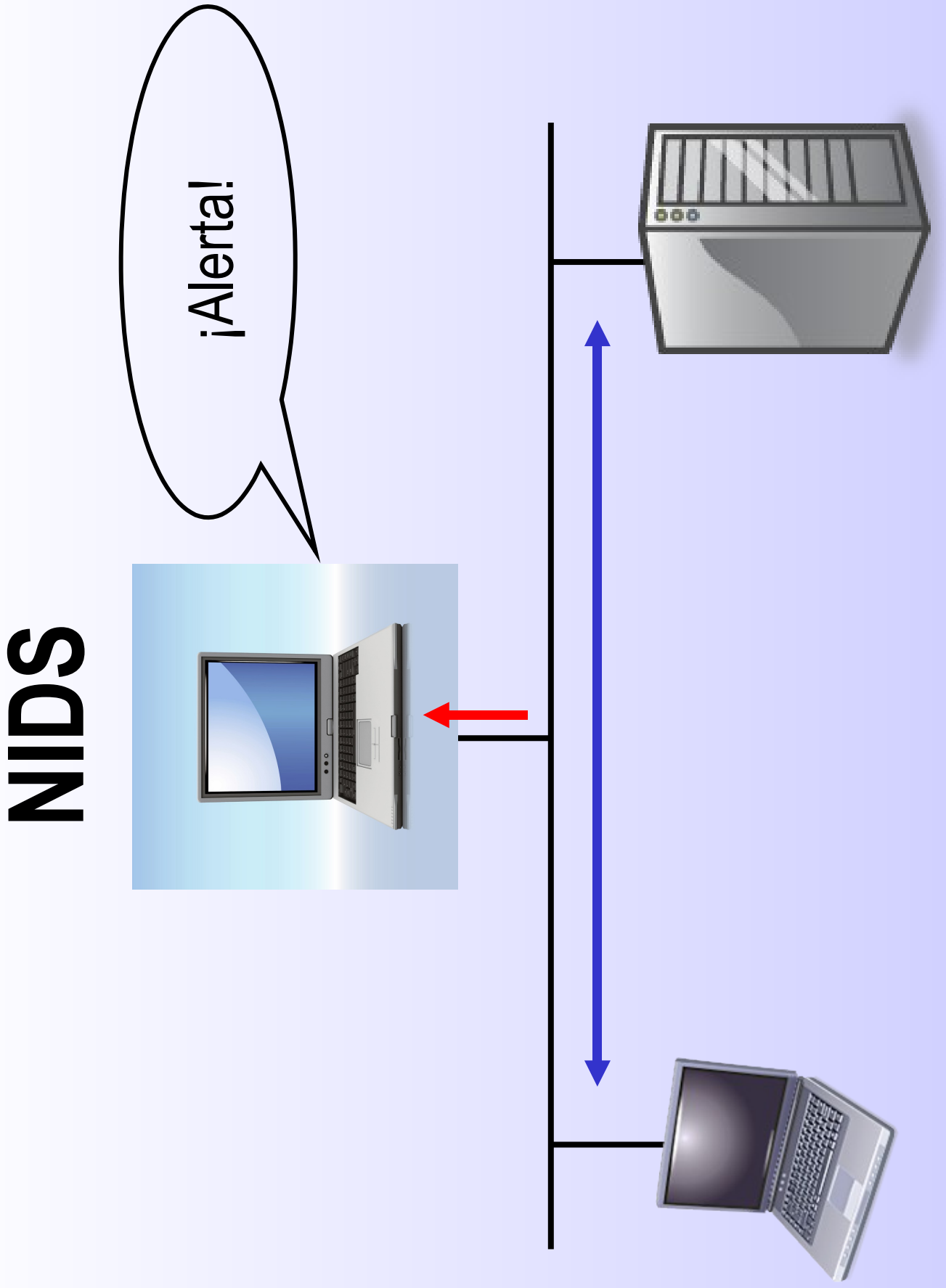
- David Pérez Conde
- Consultor independiente de seguridad
- Instructor de The SANS Institute
- GSE (http://www.giac.org/certifications/gse.php)
- david.perez.conde@gmail.com
- http://www.radajo.com

# Agenda

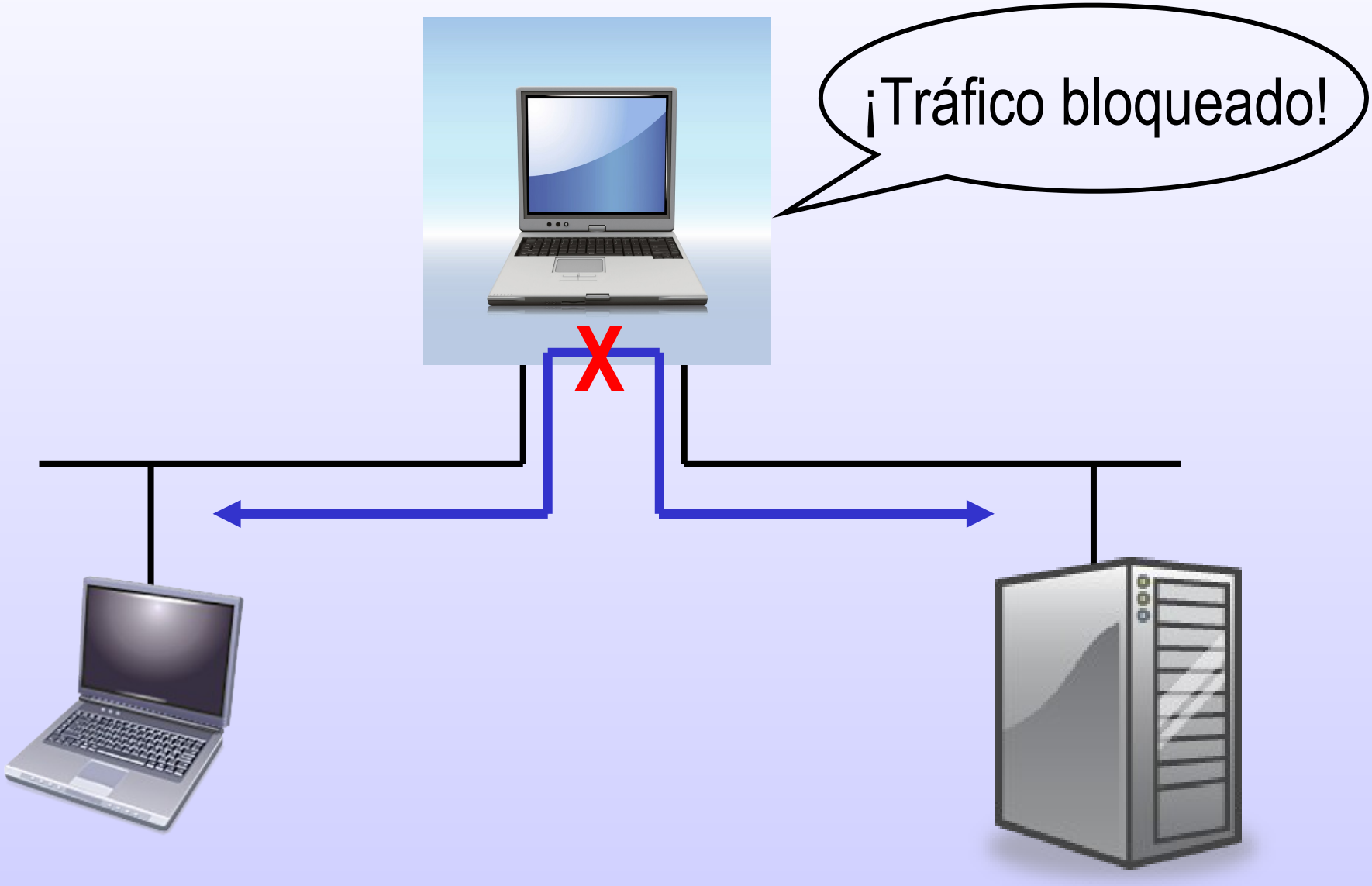
- Introducción
- Limitaciones del NIDS/NIPS
- Más allá del NIDS:
  - Análisis de trazas de red
  - Análisis de logs de sistema
  - Automatización

# 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


¡Alerta!
NIDS

# NIPS



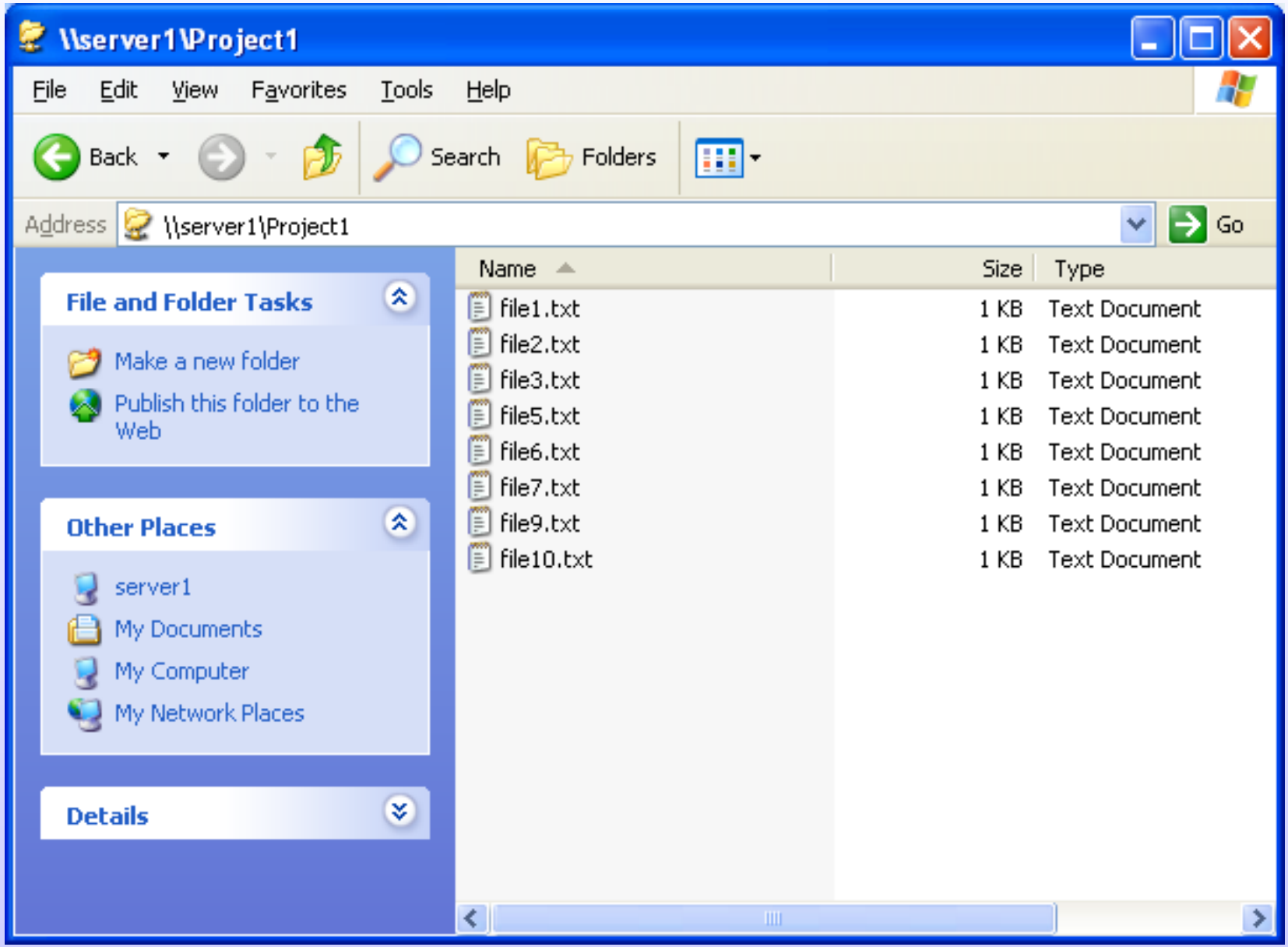

```
alert tcp 10.10.10.10 !80 -> any any \
(msg: "Trafico sospechoso")

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

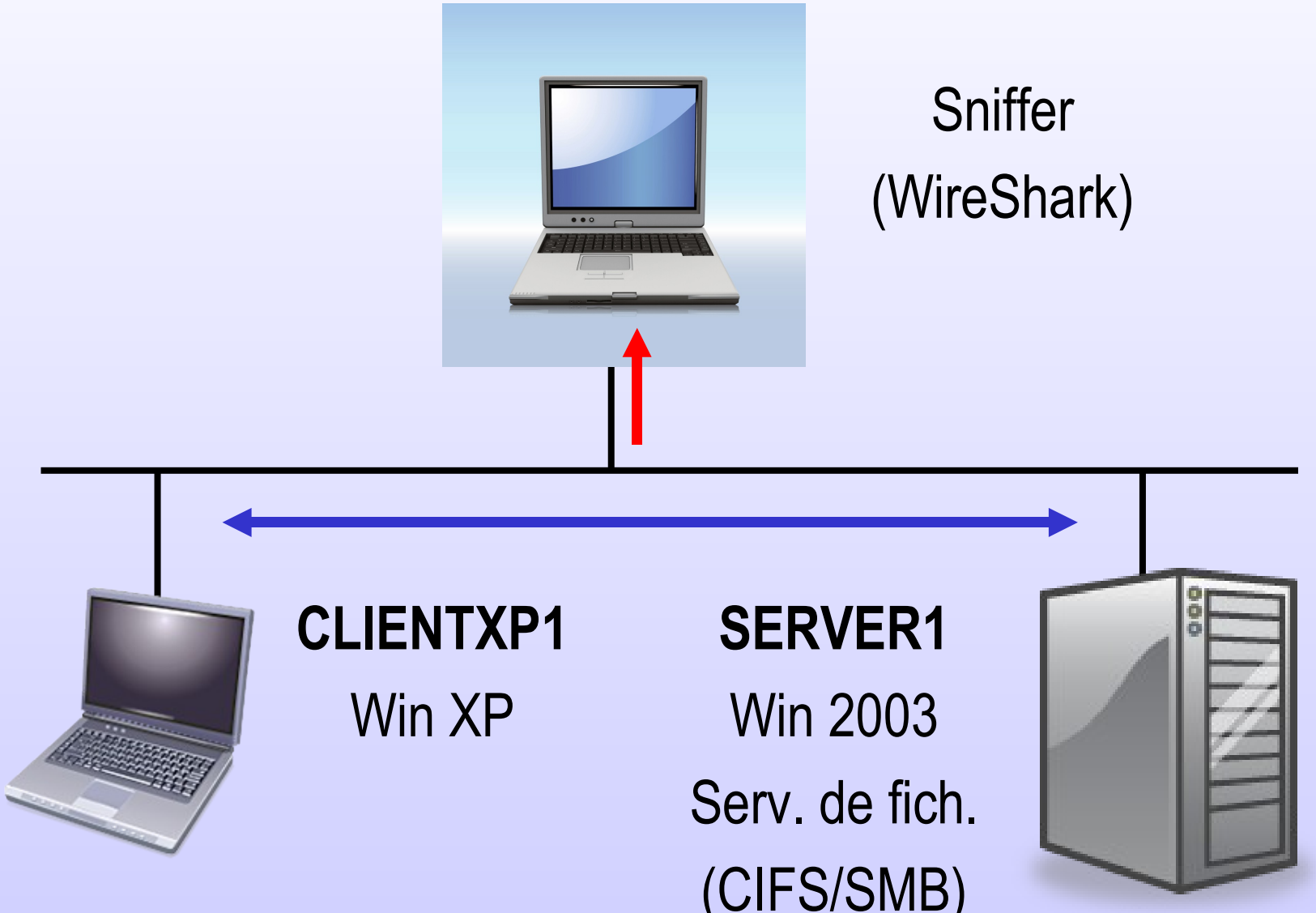
# Limitaciones de NIDS/NIPS

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

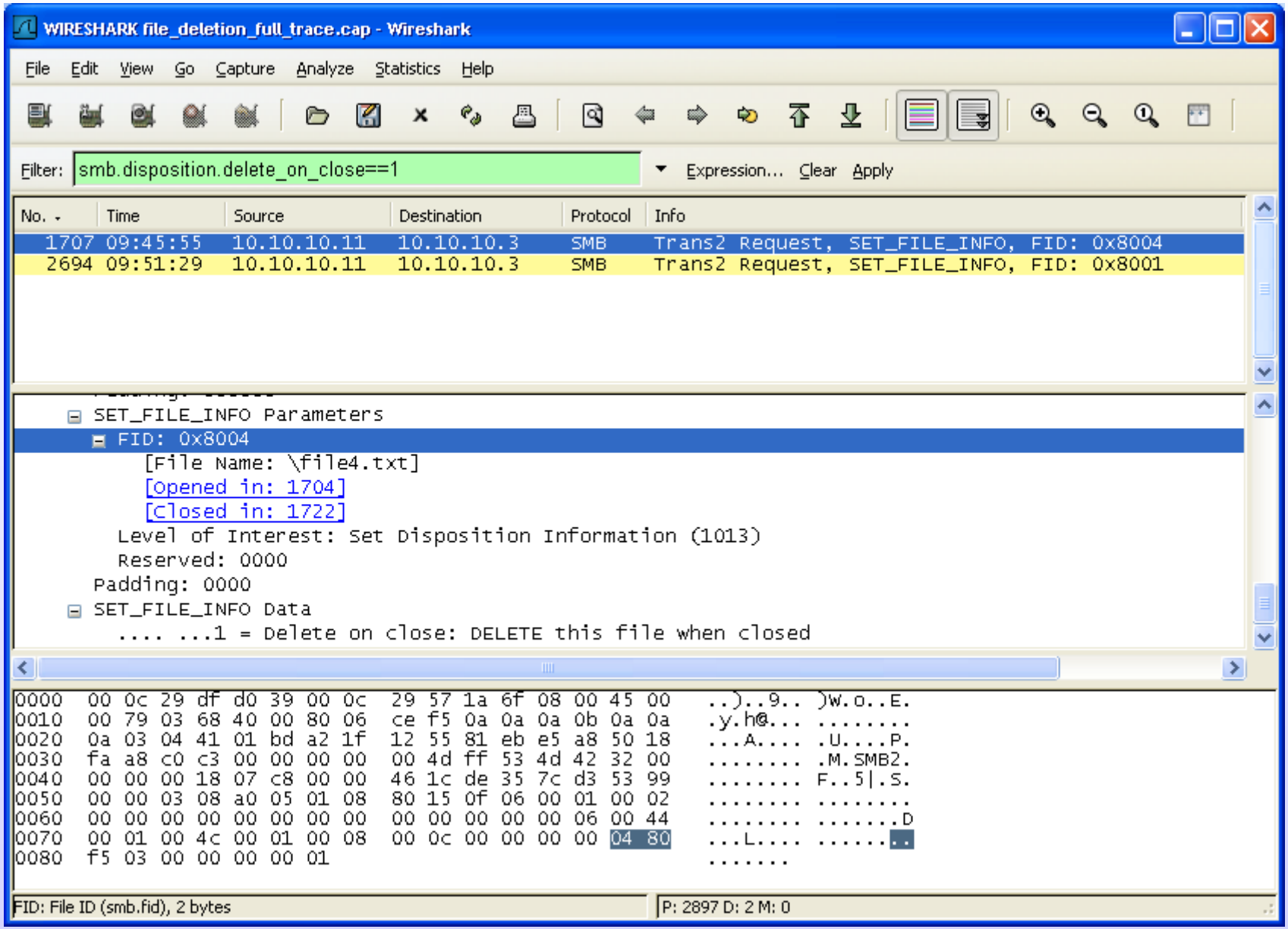
# Incidente: Ficheros borrados



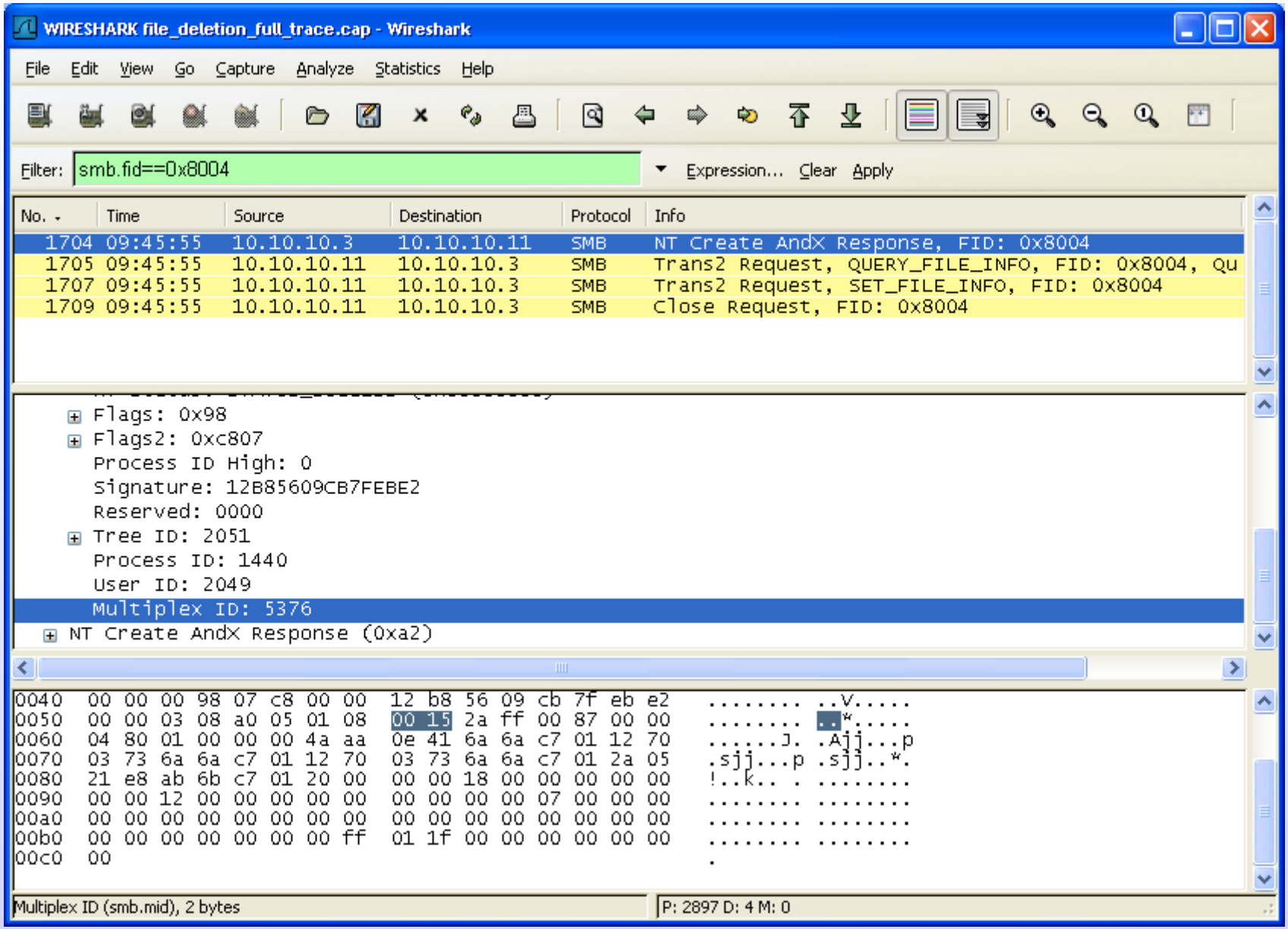
# Incidente: Ficheros borrados



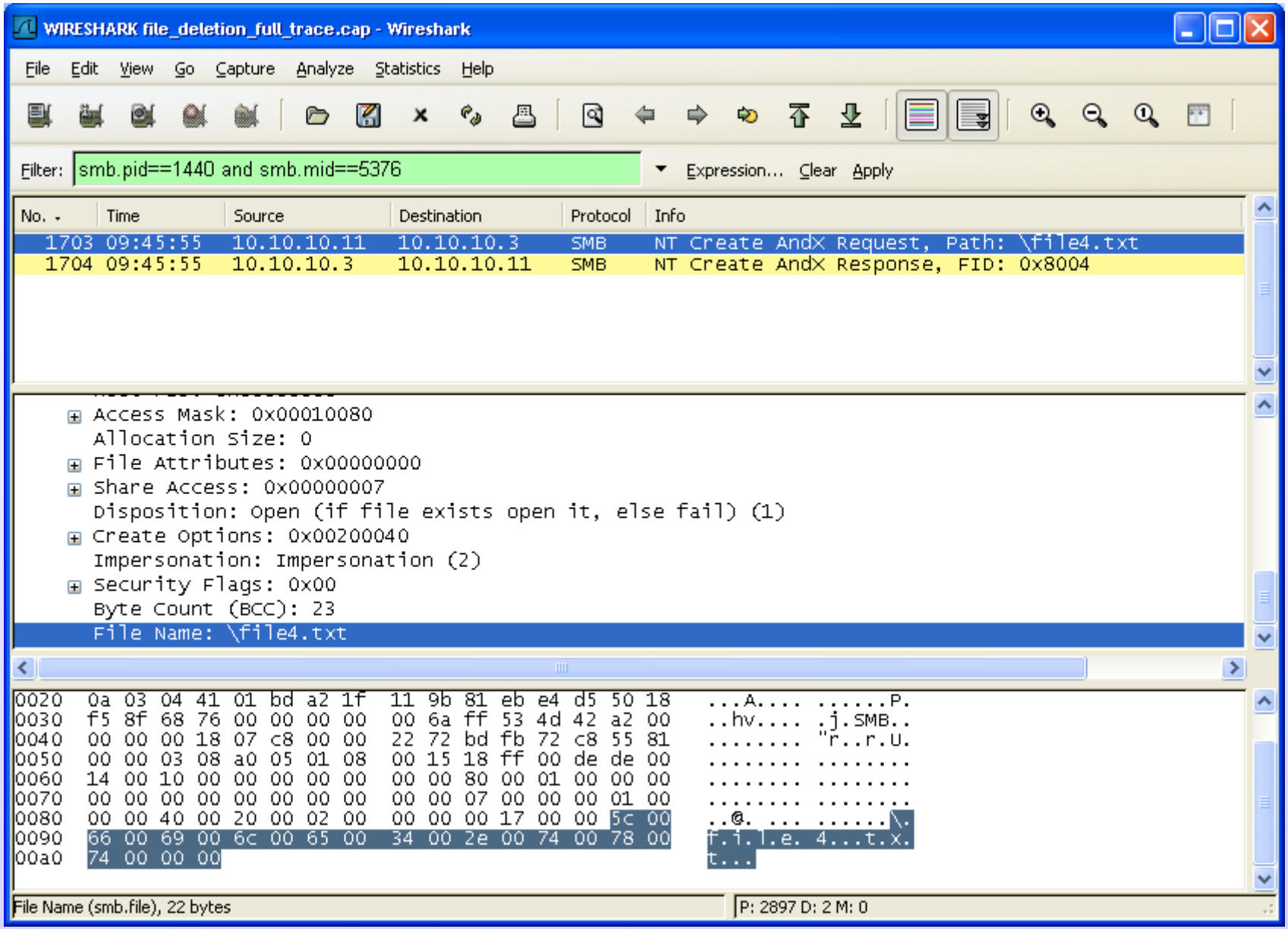
# Análisis de la traza de red




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

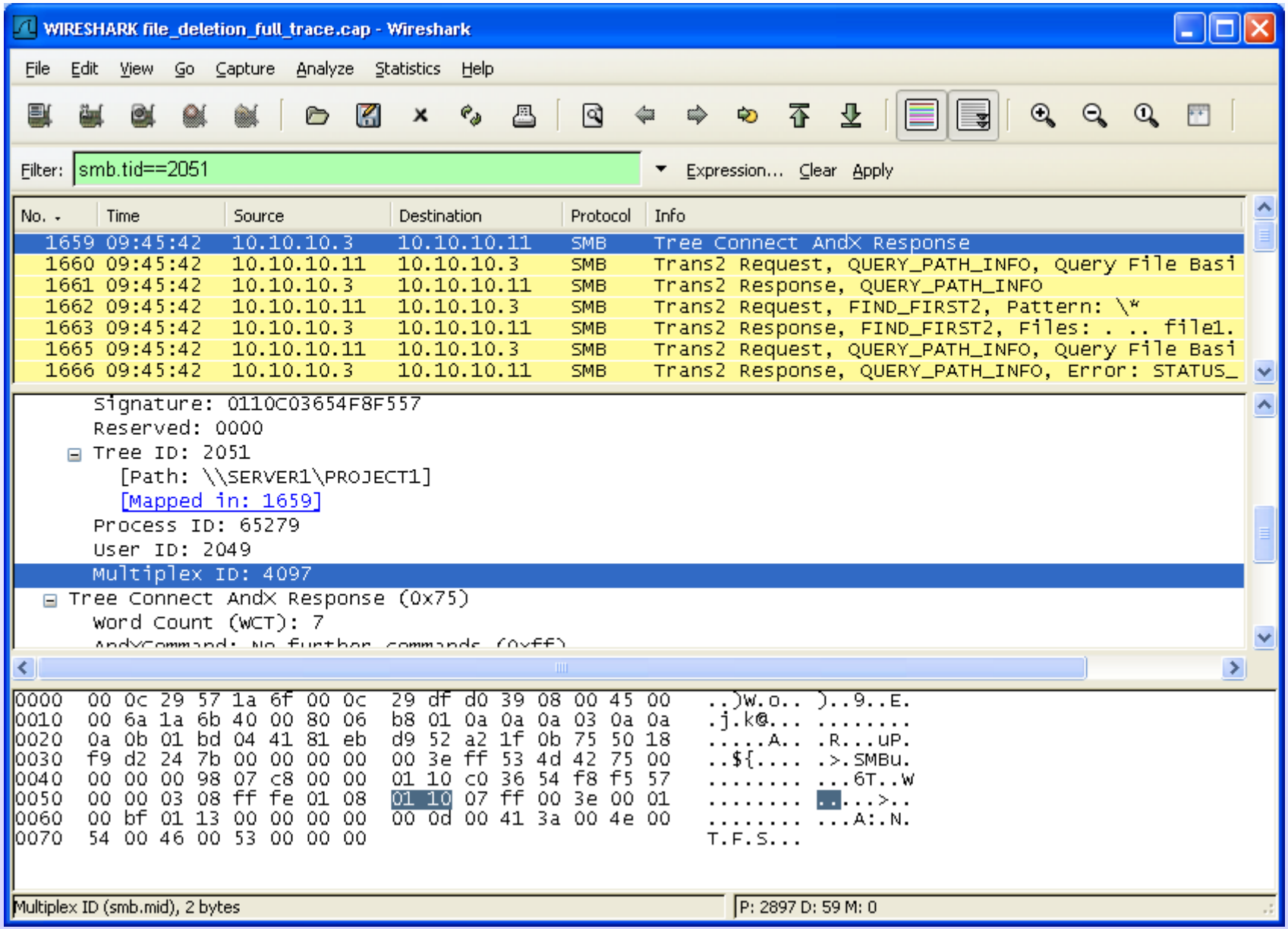



smb.fid: Identificador de fichero, asignado por el servidor al abrir un fichero

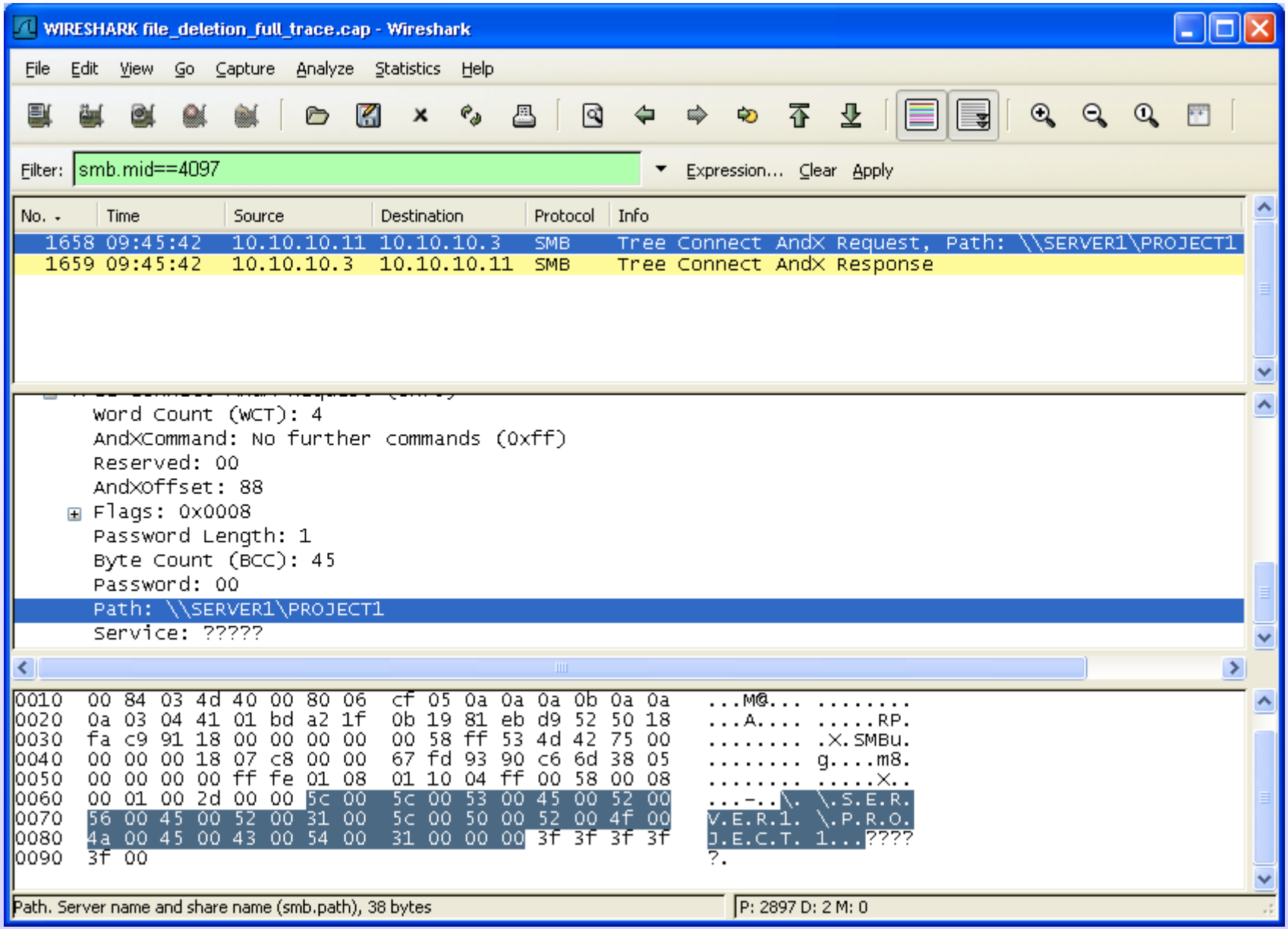



smb.pid: Identificador de proceso, asignado por cliente.

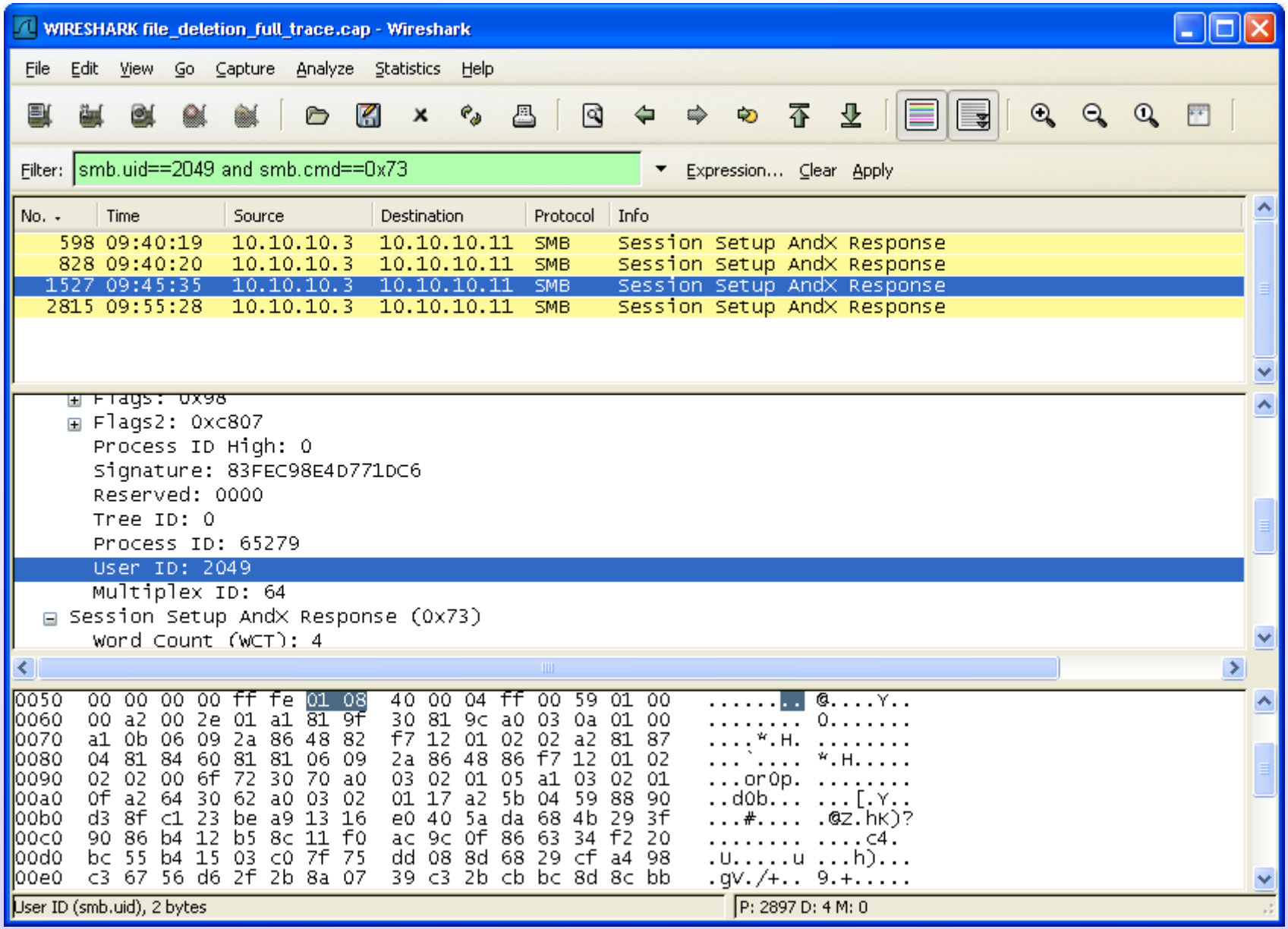
smb.mid: Identificador de petición/resp., asignado por cliente.



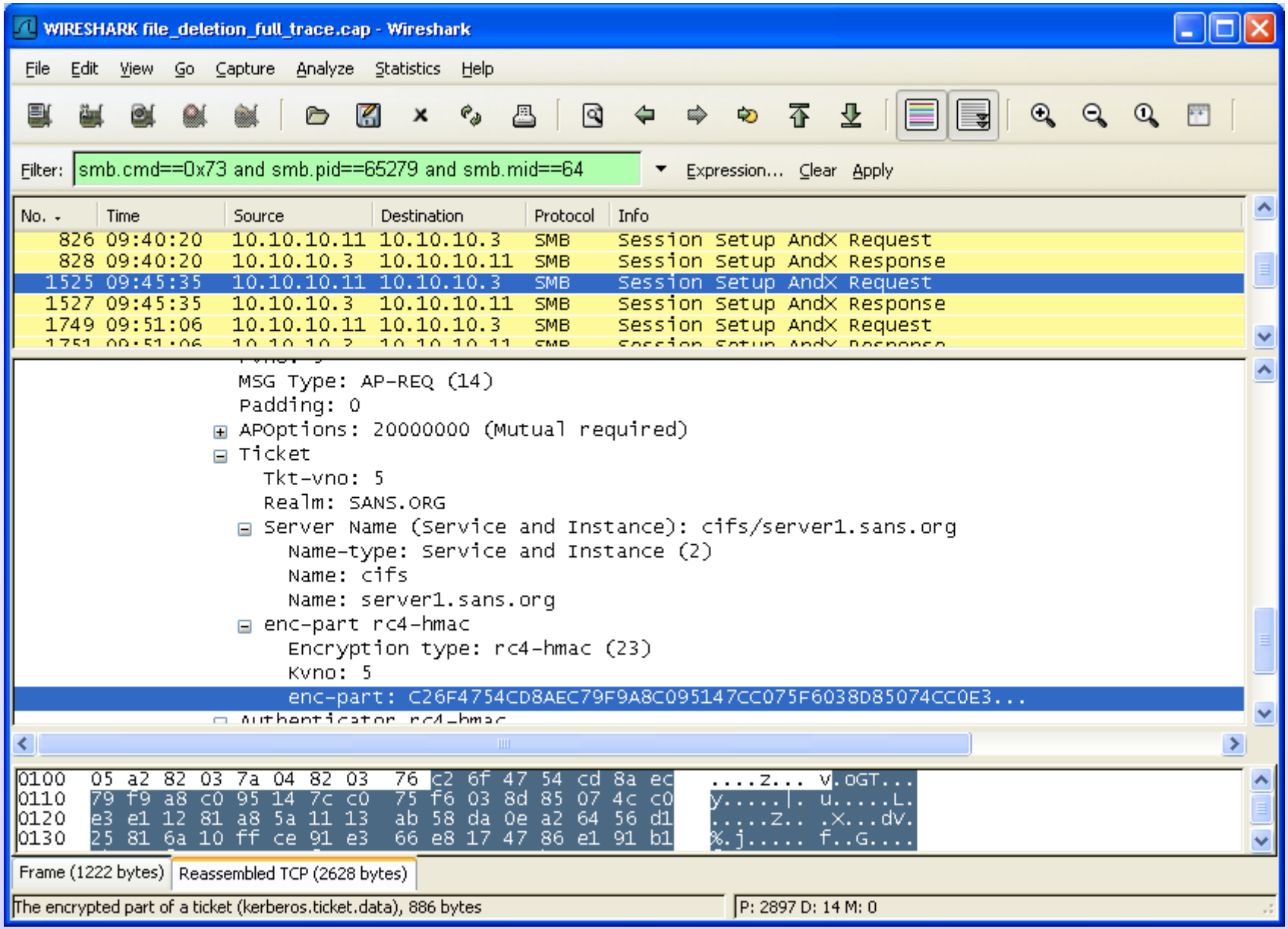

smb.tid: (Tree ID) Identificador de directorio compartido, asignado por el servidor



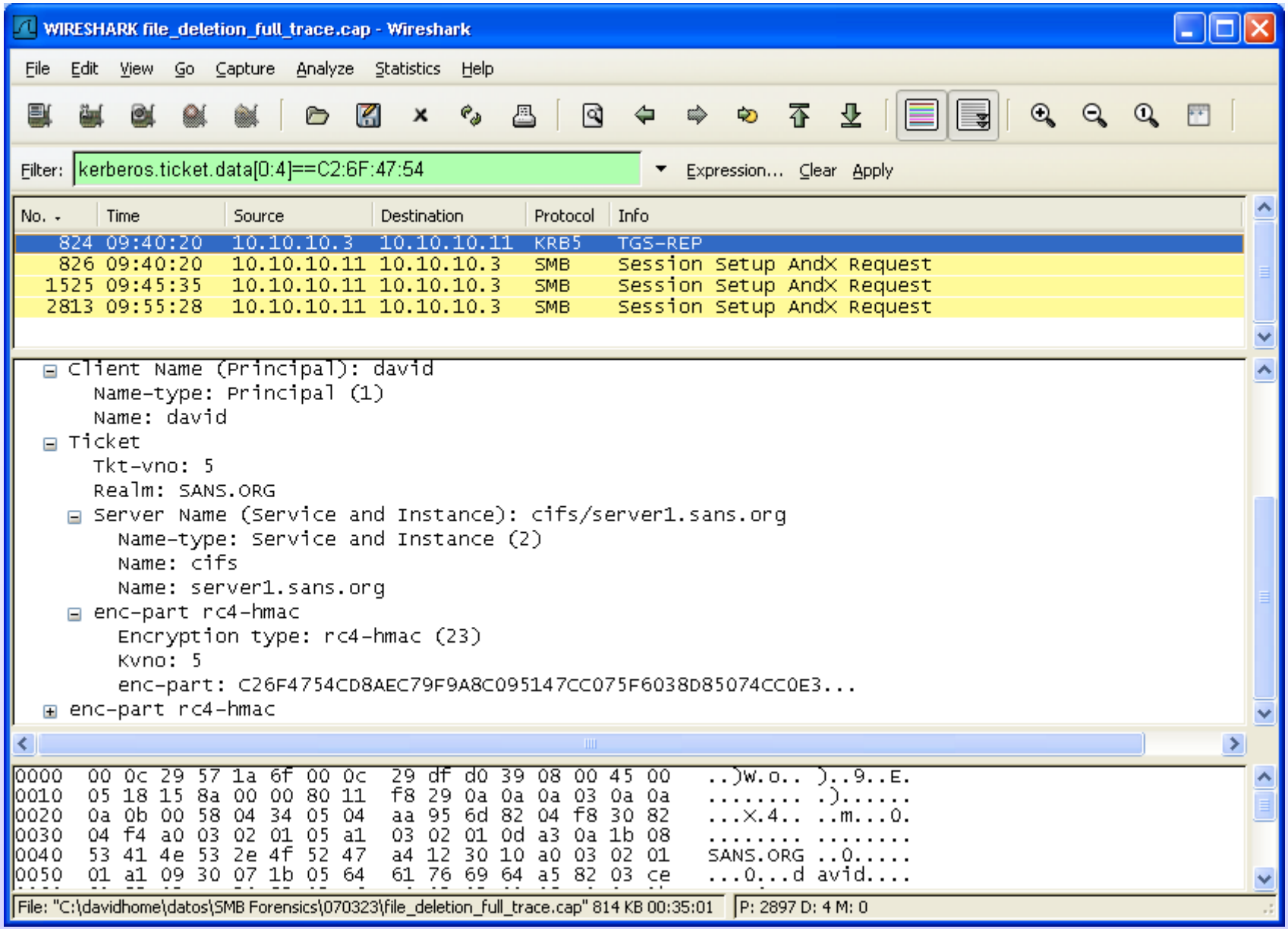

Fichero borrado: \\SERVER1\PROJECT1\file4.txt




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

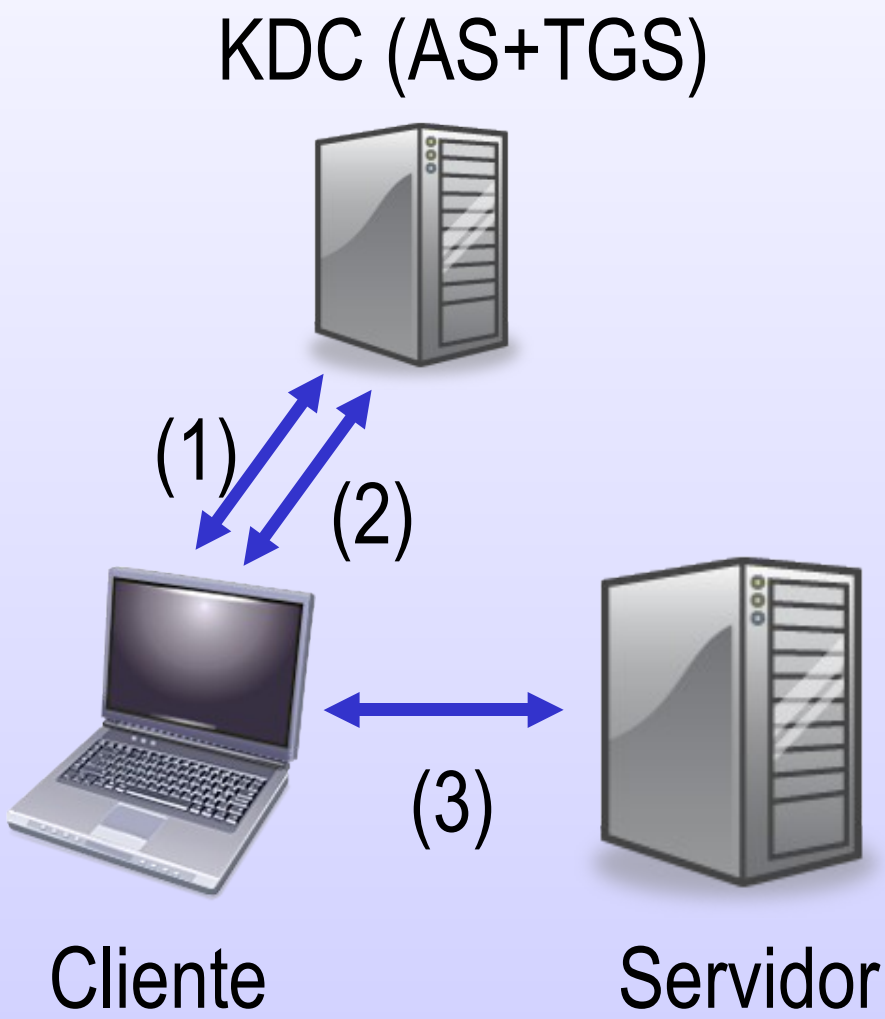



La petición de establecimiento de sesión incluye un ticket de kerberos que identifica al usuario, aunque el nombre...




... 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

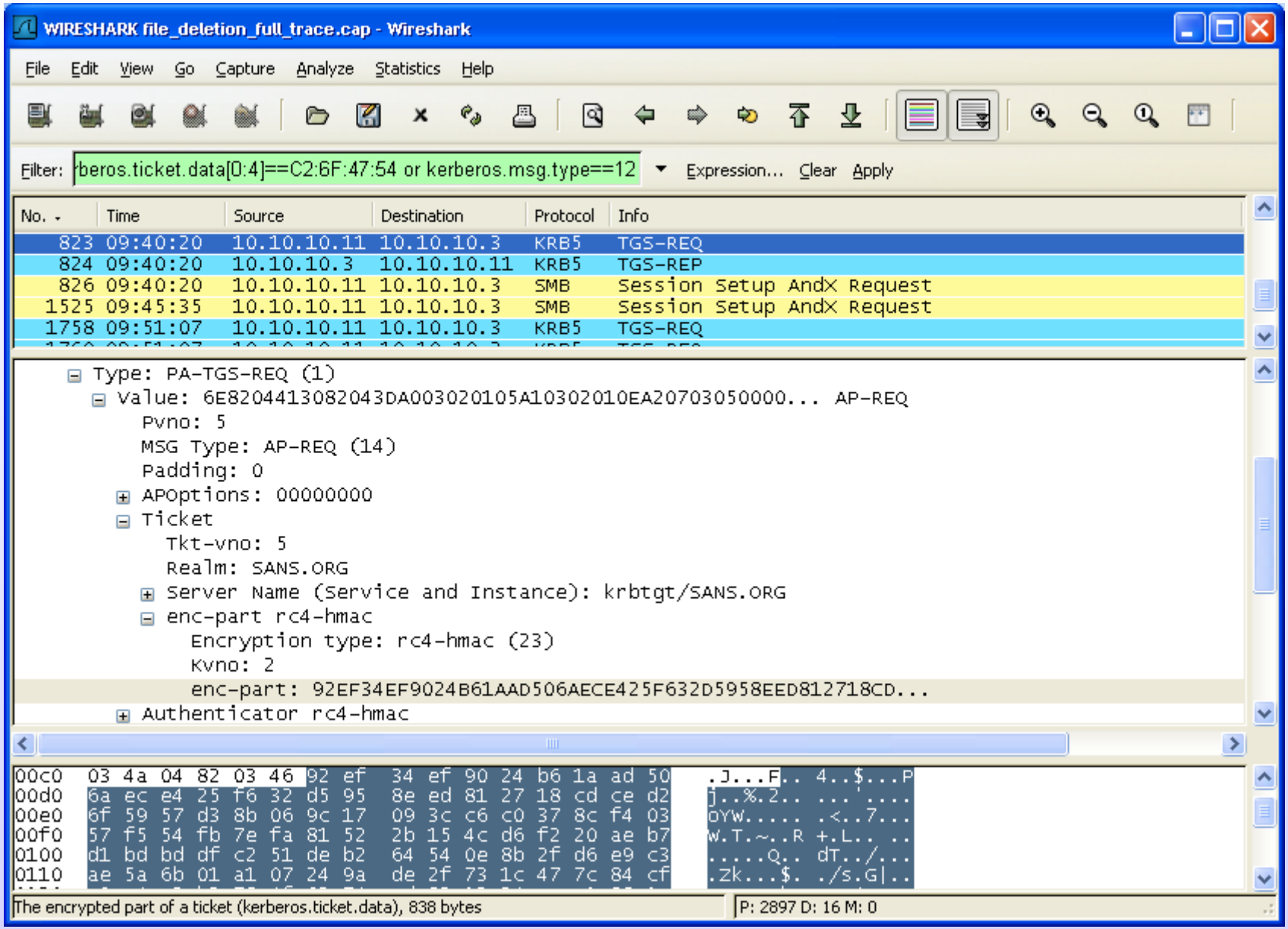
**Tickets:**

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

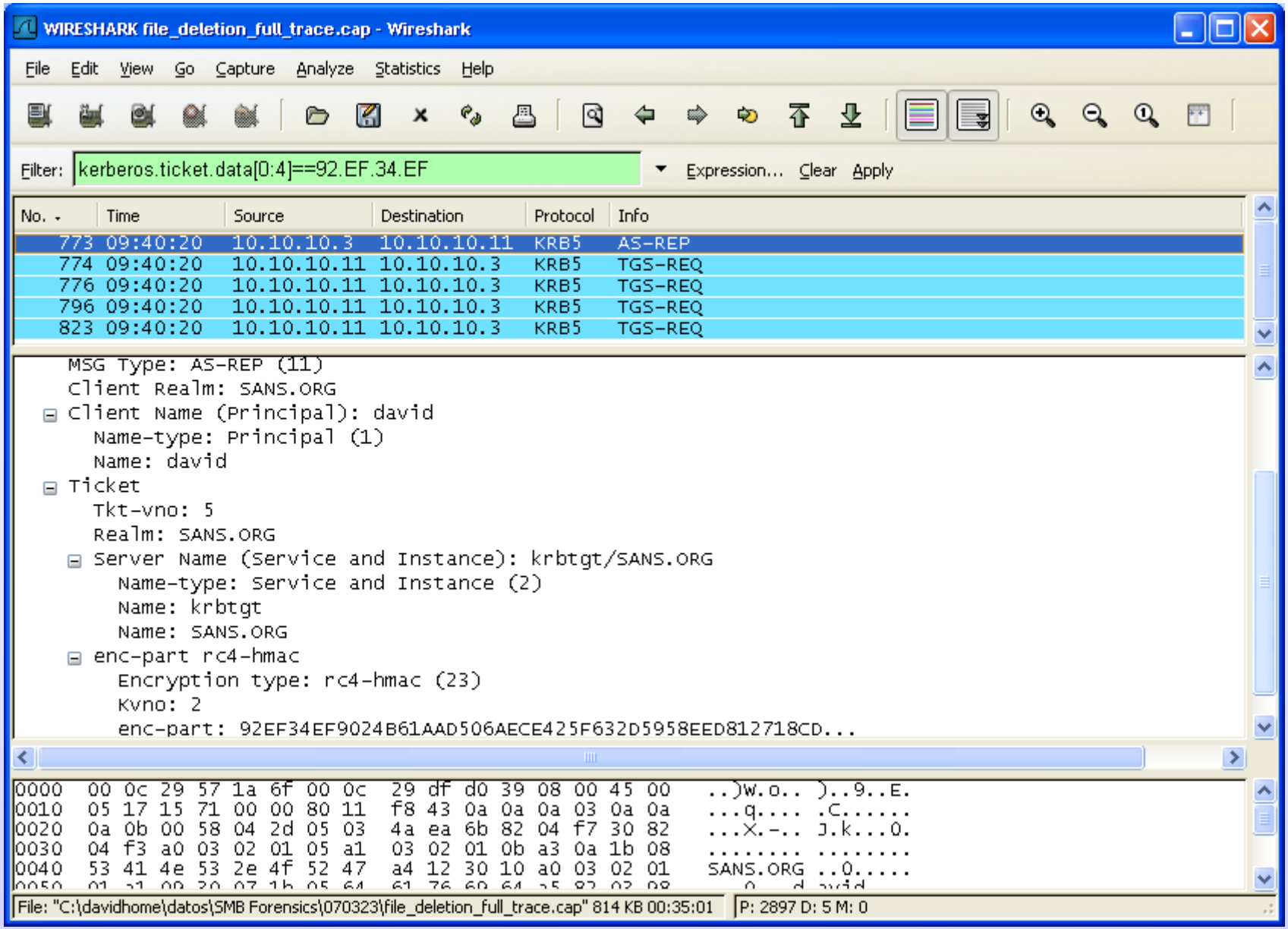
(1) Obtener TGT

(2) Obtener ST

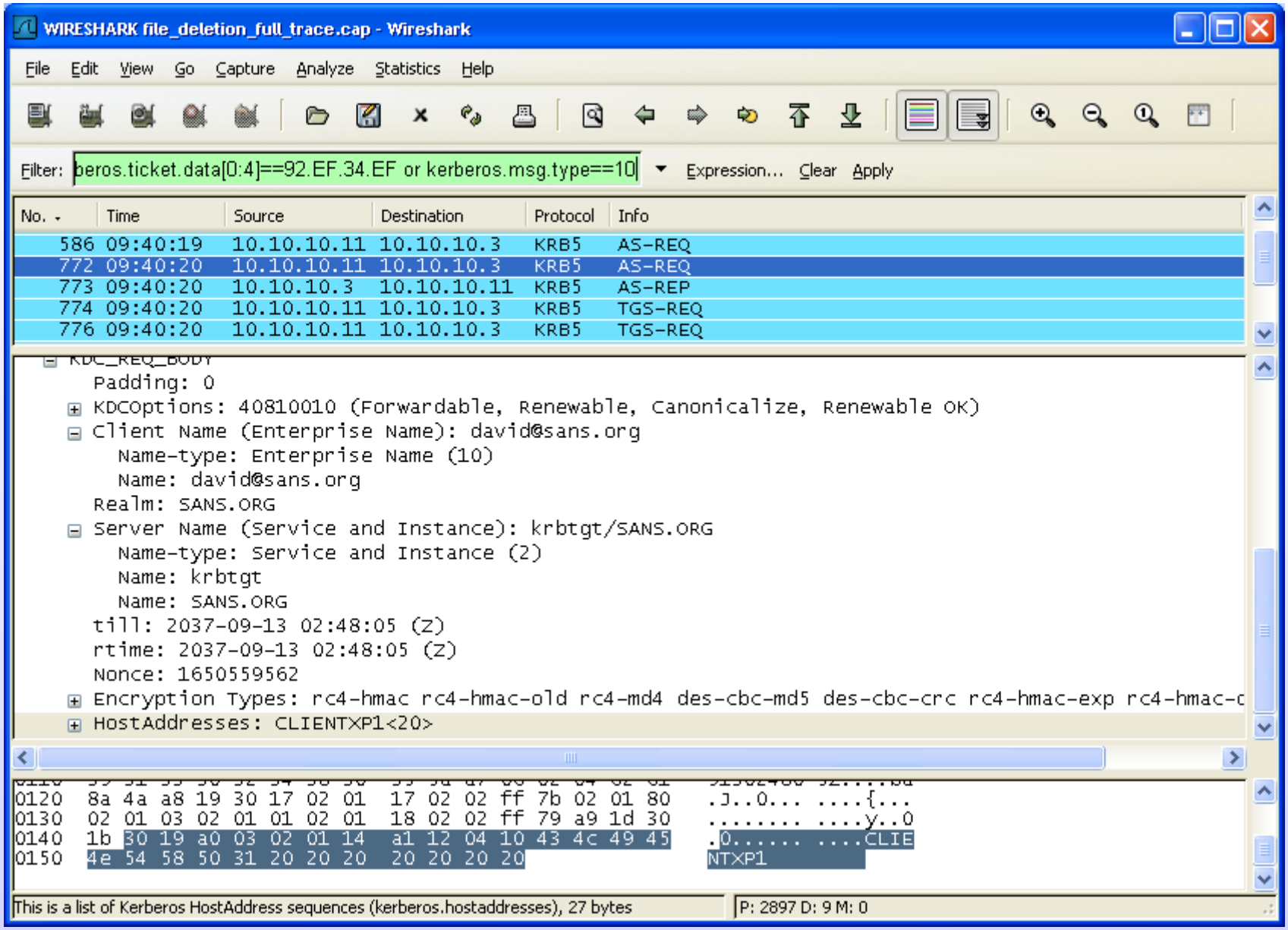
(3) Presentar ST




La petición correspondiente contiene el TGT del usuario...




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



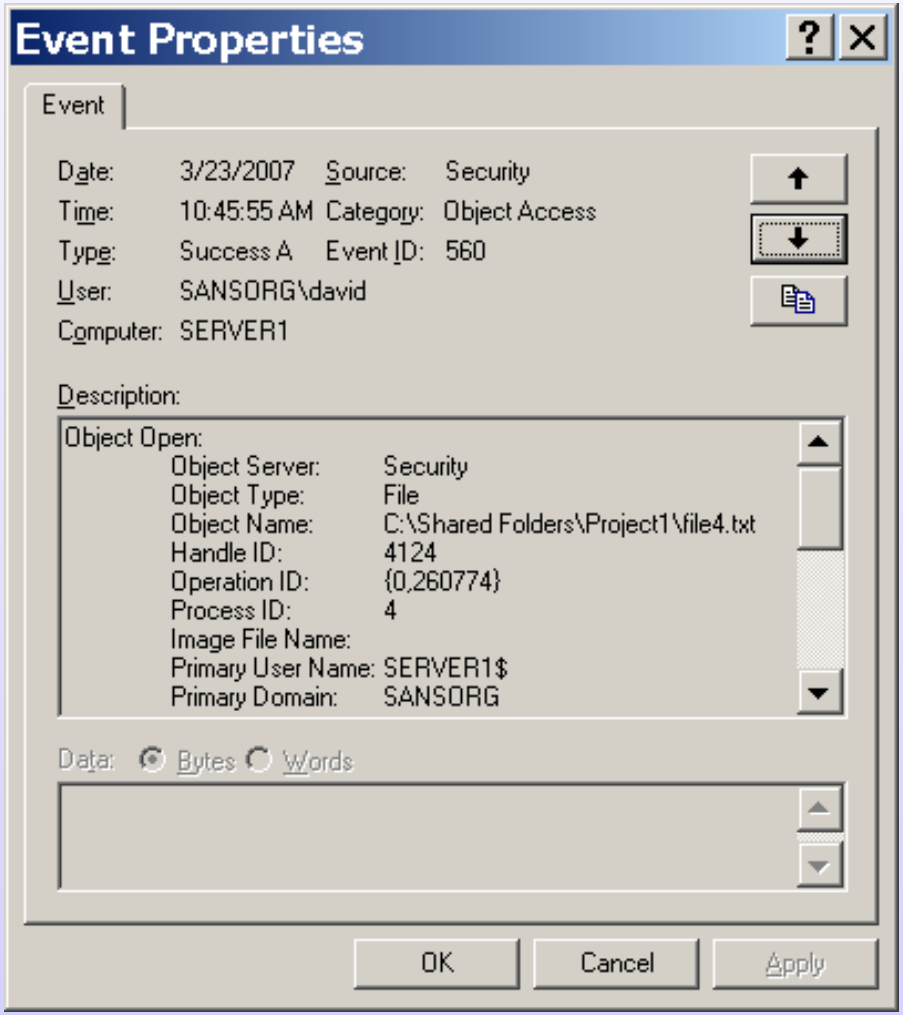

...y esa petición AS-REQ contiene el nombre NETBIOS del equipo cliente desde el que se realizó la petición: **CLIENTXP1**

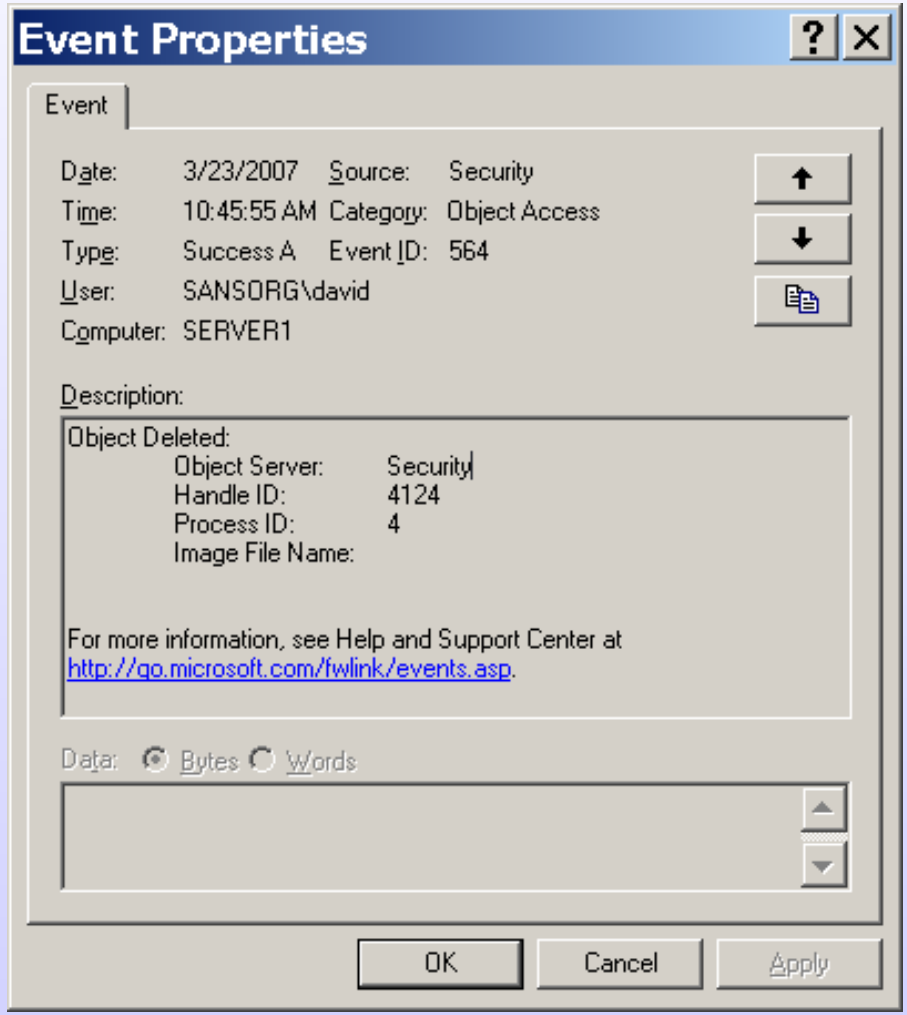
# Ya sabemos:

- 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**