

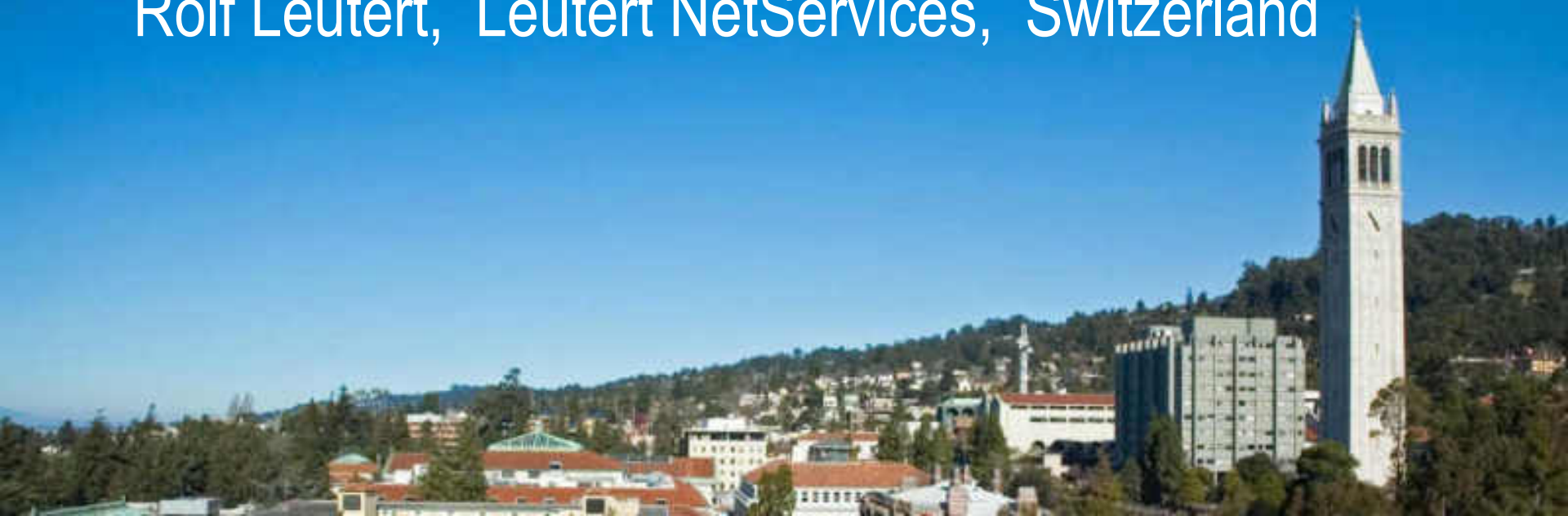


# SHARKFEST '13

Wireshark Developer and User Conference

**NAP-3 Microsoft SMB Troubleshooting**

Rolf Leutert, Leutert NetServices, Switzerland



# Server Message Block (SMB) Protokoll

## SMB History

---

Server Message Block (SMB) is **Microsoft's client-server protocol** and is most commonly used in networked environments where Windows® operating systems are in place.

Invented by **IBM** in 1983, SMB has become Microsoft's core protocol for **shared services** like files, printers etc.

Initially SMB was running on top of non routable **NetBIOS/NetBEUI API** and was designed to work in **small to medium size** workgroups.

1996 Microsoft renamed SMB to **Common Internet File System (CIFS)** and added more features like larger file sizes, Windows RPC, the NT domain service and many more.

**Samba** is the open source SMB/CIFS implementation for Unix and Linux systems



# Server Message Block (SMB) Protokoll

## SMB over TCP/UDP/IP

SMB / NetBIOS was made routable by running over TCP/IP (**NBT**) using encapsulation over TCP/UDP-Ports 137–139

Port 137 = NetBIOS Name Service (NS)

Port 138 = NetBIOS Datagram Service (DGM)

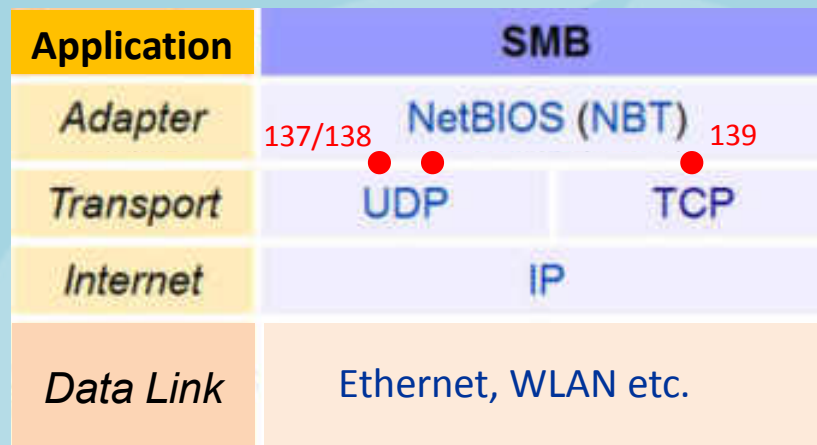
Port 139 = NetBIOS Session Service (SS)

Since Windows 2000, SMB runs, by default, with a thin layer, the NBT's Session Service, on top of **TCP-Port 445**.

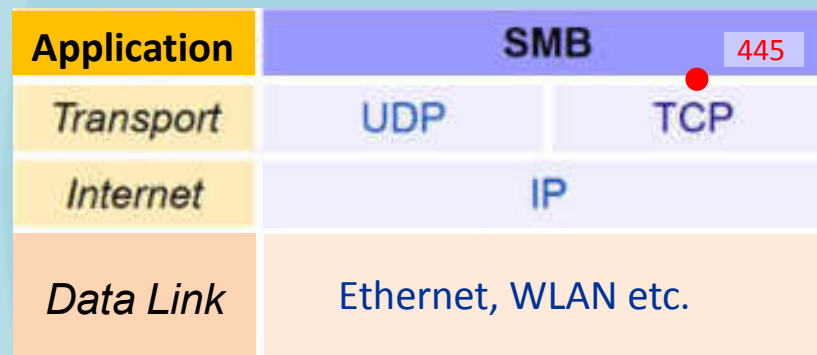
**DNS** and **LLMNR** (Link Local Multicast Name Resolution) is used for name resolution.

Port 445 = Microsoft Directory Services (DS)  
SMB File Sharing, Windows Shares,  
Printer Sharing, Active Directory

### SMB over NetBIOS over UDP/TCP



### SMB “naked” over TCP



# Server Message Block (SMB) Protokoll

## NetBIOS / SMB History

### NetBIOS Name Service (UDP Port 137)

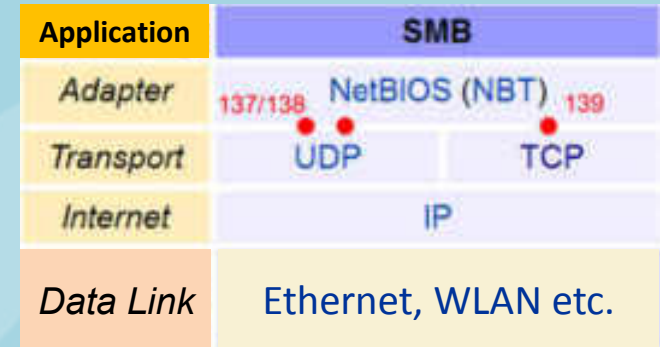
- Using **NetBIOS names** for clients and services.
- NetBIOS names where **not routable**
- Initially, **name to IP resolution** using **broadcast** (B-Node)
- Later, name directory **WINS-Server** was introduced
- Client was configured with **WINS IP-Adresse** (P-Node)
- With W2K, **DNS** name structure was introduced

### NetBIOS Datagram Service (UDP Port 138)

- Datagram mode is connectionless
- The application is responsible for error detection and recovery
- Receiver are single stations (**Unicast**), groups (**Multicast**) or all stations (**Broadcast**)
- Multicast und Broadcast Datagram beyond local subnet was not implemented
- Datagram for **Browser Election** and announcements in the local subnet

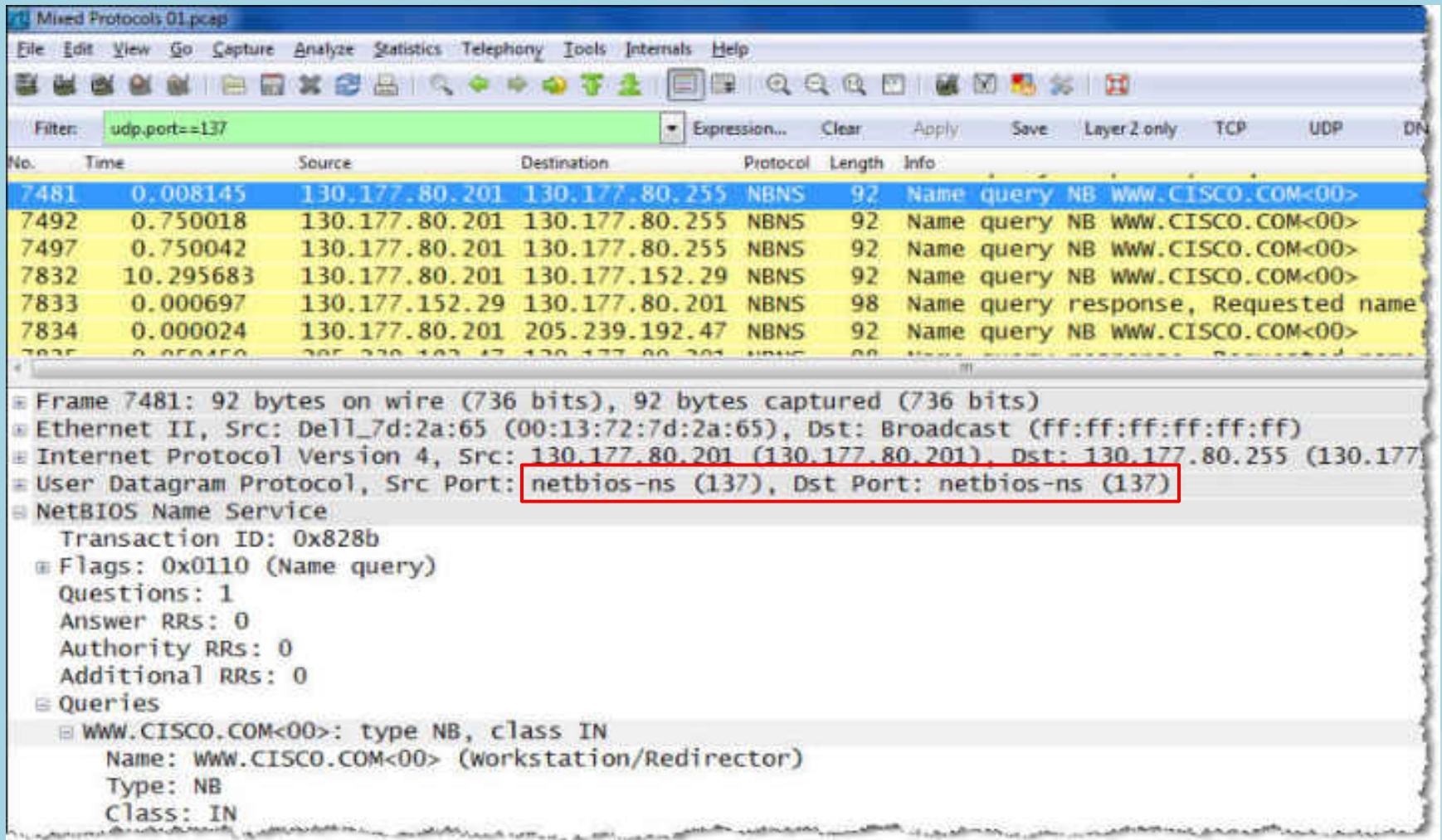
### NetBIOS Session Service (TCP Port 139)

- Reliable, connection oriented service to access **Shared Resources**



# Server Message Block (SMB) Protokoll

NetBIOS Name Service (UDP Port 137)



The image shows a Wireshark capture of NetBIOS Name Service (NBNS) traffic. The filter is set to 'udp.port==137'. The packet list shows several name queries and one response. The details pane for packet 7481 shows the NetBIOS Name Service structure, including a name query for 'WWW.CISCO.COM'.

No.	Time	Source	Destination	Protocol	Length	Info
7481	0.008145	130.177.80.201	130.177.80.255	NBNS	92	Name query NB WWW.CISCO.COM<00>
7492	0.750018	130.177.80.201	130.177.80.255	NBNS	92	Name query NB WWW.CISCO.COM<00>
7497	0.750042	130.177.80.201	130.177.80.255	NBNS	92	Name query NB WWW.CISCO.COM<00>
7832	10.295683	130.177.80.201	130.177.152.29	NBNS	92	Name query NB WWW.CISCO.COM<00>
7833	0.000697	130.177.152.29	130.177.80.201	NBNS	98	Name query response, Requested name
7834	0.000024	130.177.80.201	205.239.192.47	NBNS	92	Name query NB WWW.CISCO.COM<00>

Frame 7481: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)  
Ethernet II, Src: Dell\_7d:2a:65 (00:13:72:7d:2a:65), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: 130.177.80.201 (130.177.80.201), Dst: 130.177.80.255 (130.177.80.255)  
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)  
NetBIOS Name Service  
Transaction ID: 0x828b  
Flags: 0x0110 (Name query)  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
WWW.CISCO.COM<00>: type NB, class IN  
Name: WWW.CISCO.COM<00> (workstation/Redirector)  
Type: NB  
Class: IN

# Server Message Block (SMB) Protokoll

NetBIOS Datagram Service (UDP Port 138)

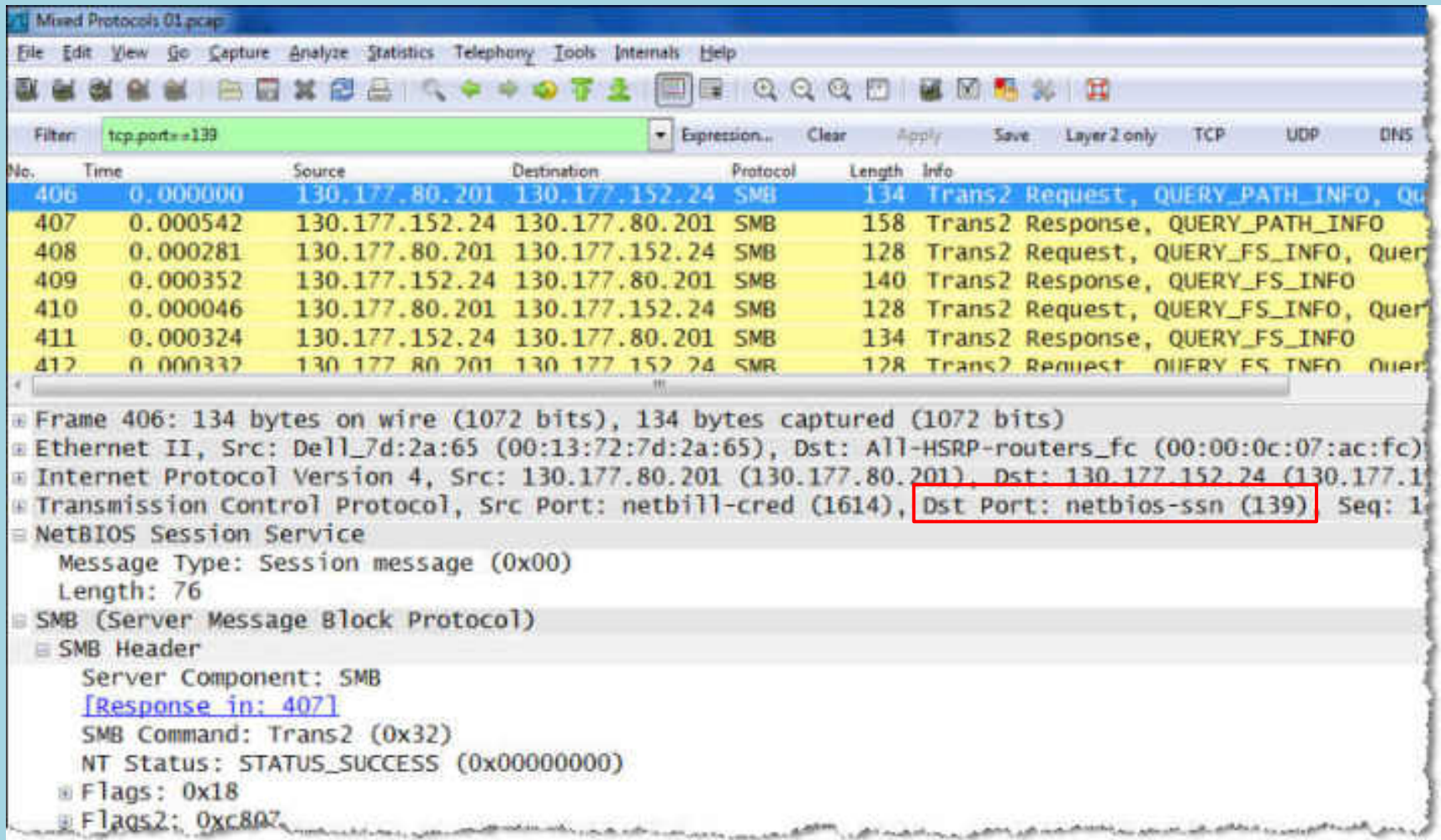
The image shows a Wireshark capture of network traffic. The filter is set to 'udp.port==138'. The packet list shows several entries, with packet 14 selected. The packet details pane shows the following layers:

- Frame 14: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
- Ethernet II, Src: WWPcBaTe\_a8:45:fe (00:0f:1f:a8:45:fe), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 130.177.80.69 (130.177.80.69), Dst: 130.177.80.255 (130.177.80.255)
- User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
- NetBIOS Datagram Service
- SMB (Server Message Block Protocol)
- SMB Mailslot Protocol
- Microsoft Windows Browser Protocol

No.	Time	Source	Destination	Protocol	Length	Info
14	0.000000	130.177.80.69	130.177.80.255	BROWSER	243	Host Announcement W2JZLCHM09, workstation
385	22.686378	130.177.80.48	130.177.80.255	BROWSER	243	Host Announcement W2HZQN1802, workstation
2912	28.002125	130.177.80.200	130.177.80.255	BROWSER	243	Host Announcement W2JZD6CQ01, workstation
6274	27.827270	130.177.80.208	130.177.80.255	BROWSER	289	Local Master Announcement STORAGE, Workst
6275	0.000094	130.177.80.208	130.177.80.255	BROWSER	250	Domain/Workgroup Announcement WORKGROUP,
9112	112.542460	130.177.80.15	130.177.80.255	BROWSER	243	Host Announcement W2PZ4PP859, workstation
9444	48.659752	130.177.80.20	130.177.80.255	BROWSER	243	Local Master Announcement W2G2RTR902, Wor

# Server Message Block (SMB) Protokoll

NetBIOS Session Service (TCP Port 139)



Mixed Protocols 01.pcap

Filter: tcp.port==139

No.	Time	Source	Destination	Protocol	Length	Info
406	0.000000	130.177.80.201	130.177.152.24	SMB	134	Trans2 Request, QUERY_PATH_INFO, Qu
407	0.000542	130.177.152.24	130.177.80.201	SMB	158	Trans2 Response, QUERY_PATH_INFO
408	0.000281	130.177.80.201	130.177.152.24	SMB	128	Trans2 Request, QUERY_FS_INFO, Quer
409	0.000352	130.177.152.24	130.177.80.201	SMB	140	Trans2 Response, QUERY_FS_INFO
410	0.000046	130.177.80.201	130.177.152.24	SMB	128	Trans2 Request, QUERY_FS_INFO, Quer
411	0.000324	130.177.152.24	130.177.80.201	SMB	134	Trans2 Response, QUERY_FS_INFO
412	0.000332	130.177.80.201	130.177.152.24	SMB	128	Trans2 Request, QUERY_FS_INFO, Quer

Frame 406: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)

Ethernet II, Src: Dell\_7d:2a:65 (00:13:72:7d:2a:65), Dst: All-MSRP-routers\_fc (00:00:0c:07:ac:fc)

Internet Protocol Version 4, Src: 130.177.80.201 (130.177.80.201), Dst: 130.177.152.24 (130.177.152.24)

Transmission Control Protocol, Src Port: netbill-cred (1614), Dst Port: netbios-ssn (139) Seq: 1

NetBIOS Session Service

Message Type: Session message (0x00)

Length: 76

SMB (Server Message Block Protocol)

SMB Header

Server Component: SMB

[\[Response in: 407\]](#)

SMB Command: Trans2 (0x32)

NT Status: STATUS\_SUCCESS (0x00000000)

Flags: 0x18

Flags2: 0xc807

# Server Message Block (SMB) Protokoll

NetBIOS / SMB present implementation

## SMB „naked“ over TCP (Port 445)

- NetBIOS Names are replaced by **DNS Names**
- Name resolution by **DNS Resolver**
- Name registration by **Dynamic DNS**
- **Thin** NetBIOS layer **leftover**, Type **Session Message**
- Underlying **TCP layer** handles connection reliability
- Implemented since Microsoft **Windows 2000 / XP** and **Samba** (SMB for Unix and Linux)

Application	SMB 445	
Transport	UDP	TCP
Internet	IP	
Data Link	Ethernet, WLAN etc.	



# Server Message Block (SMB) Protokoll

SMB „naked“ over TCP (Port 445)

The image shows a Wireshark capture of network traffic. The top pane displays a list of packets filtered by 'tcp.port==445'. The bottom pane shows the detailed view of frame 414, which is an SMB response. A red box highlights the destination port '445' in the TCP layer details.

No.	Time	Source	Destination	Protocol	Length	Info
414	3.530612	130.177.80.201	130.177.152.23	SMB	128	Trans2 Request, QUERY_FS_INFO, Que
415	0.000410	130.177.152.23	130.177.80.201	SMB	140	Trans2 Response, QUERY_FS_INFO
416	0.000063	130.177.80.201	130.177.152.23	SMB	128	Trans2 Request, QUERY_FS_INFO, Que
417	0.000326	130.177.152.23	130.177.80.201	SMB	134	Trans2 Response, QUERY_FS_INFO
418	0.000288	130.177.80.201	130.177.152.23	SMB	128	Trans2 Request, QUERY_FS_INFO, Que
419	0.000328	130.177.152.23	130.177.80.201	SMB	134	Trans2 Response, QUERY_FS_INFO

Frame 414: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)  
Ethernet II, Src: Dell\_7d:2a:65 (00:13:72:7d:2a:65), Dst: All-MSRP-routers\_fc (00:00:0c:07:ac:fc)  
Internet Protocol Version 4, Src: 130.177.80.201 (130.177.80.201), Dst: 130.177.152.23 (130.177.152.23)  
Transmission Control Protocol, Src Port: 4592 (4592), Dst Port: microsoft-ds (445), Seq: 673, Ack: 673, Win: 0, Len: 0  
NetBIOS Session Service  
Message Type: Session message (0x00)  
Length: 70  
SMB (Server Message Block Protocol)  
SMB Header  
Server Component: SMB  
[Response in: 415]  
SMB Command: Trans2 (0x32)  
NT Status: STATUS\_SUCCESS (0x00000000)  
Flags: 0x18

# Server Message Block (SMB) Protokoll

## SMB Versions and Dialects

---

Over the last 30 years, SMB has been consciously improved and extended. There are different **Versions** and **Dialects**.

**CIFS** Old version implemented in Windows NT 4.0 in 1996

**SMB 1** More than 10 Dialects, latest Version is **NT LM 0.12**  
<http://msdn.microsoft.com/en-us/library/cc246231.aspx> (782 pages)

SMB 2 & 3 are completely new Versions including **new Commands and Headers**

**SMB 2** **2.0** with Windows Vista / Windows Server 2008  
(Performance improvements, Reconnection after network outages)

**2.1** with Windows 7 / Windows Server 2008 R2  
(Improved latency, Large MTU support)

**SMB 3** **3.0** with Windows 8 / Windows Server 2012 (renamed from version **2.2**)  
(Support of parallel TCP Sessions, Server Cluster support)  
<http://msdn.microsoft.com/en-us/library/cc246482.aspx> (424 pages)

# Server Message Block (SMB) Protokoll

## SMB Versions and Dialects

---

**SMB2** reduces the 'chattiness' of the SMB 1.0 protocol by reducing the number of commands and subcommands from over a **hundred to just nineteen**.

**SMB2** introduces the notion of **durable file handles**: these allow a connection to an SMB server to survive brief network outages, as are typical in a wireless network, without having to incur the overhead of re-negotiating a new session.

**SMB3** is not a new protocol, but a superset of SMB2 and contains performance improvements for **Virtual Server environments**.

**SMB 3.0 Support is announced or available by the following vendors:**

- Windows 8, Windows server 2012
- NetApp
- EMC Computer Systems AG
- Samba Team (open source SMB for Unix, Linux, Mac OS etc.)
- QNAP Systems, Inc. (NAS Storage systems)

# Server Message Block (SMB) Protokoll

## SMB Versions and Dialects

---

### From SMB 1.0 to SMB 2.0 - First major redesign of SMB

- Increased file sharing scalability
- Improved performance
  - Request compounding
  - Asynchronous operations
  - Larger reads/writes
- More secure and robust
  - Small command set
  - Signing now uses HMAC SHA-256 instead of MD5
  - Durable file handles

### From SMB 2.0 to SMB 2.1

- File leasing improvements
- Large MTU support
- BranchCache

### From SMB 2.1 to SMB 3.0

- Availability
  - SMB Transparent Failover
  - SMB Witness
  - SMB Multichannel
- Performance
  - SMB Scale-Out
  - SMB Direct (SMB 3.0 over RDMA)
  - SMB Multichannel
  - Directory Leasing
  - BranchCache V2
- Backup
  - VSS for Remote File Shares
- Security
  - SMB Encryption using AES-CCM
  - Signing now uses AES-CMAC
- Management
  - SMB PowerShell
  - Improved Performance Counters
  - Improved Eventing

# Server Message Block (SMB) Protokoll

## SMB Versions and Dialects

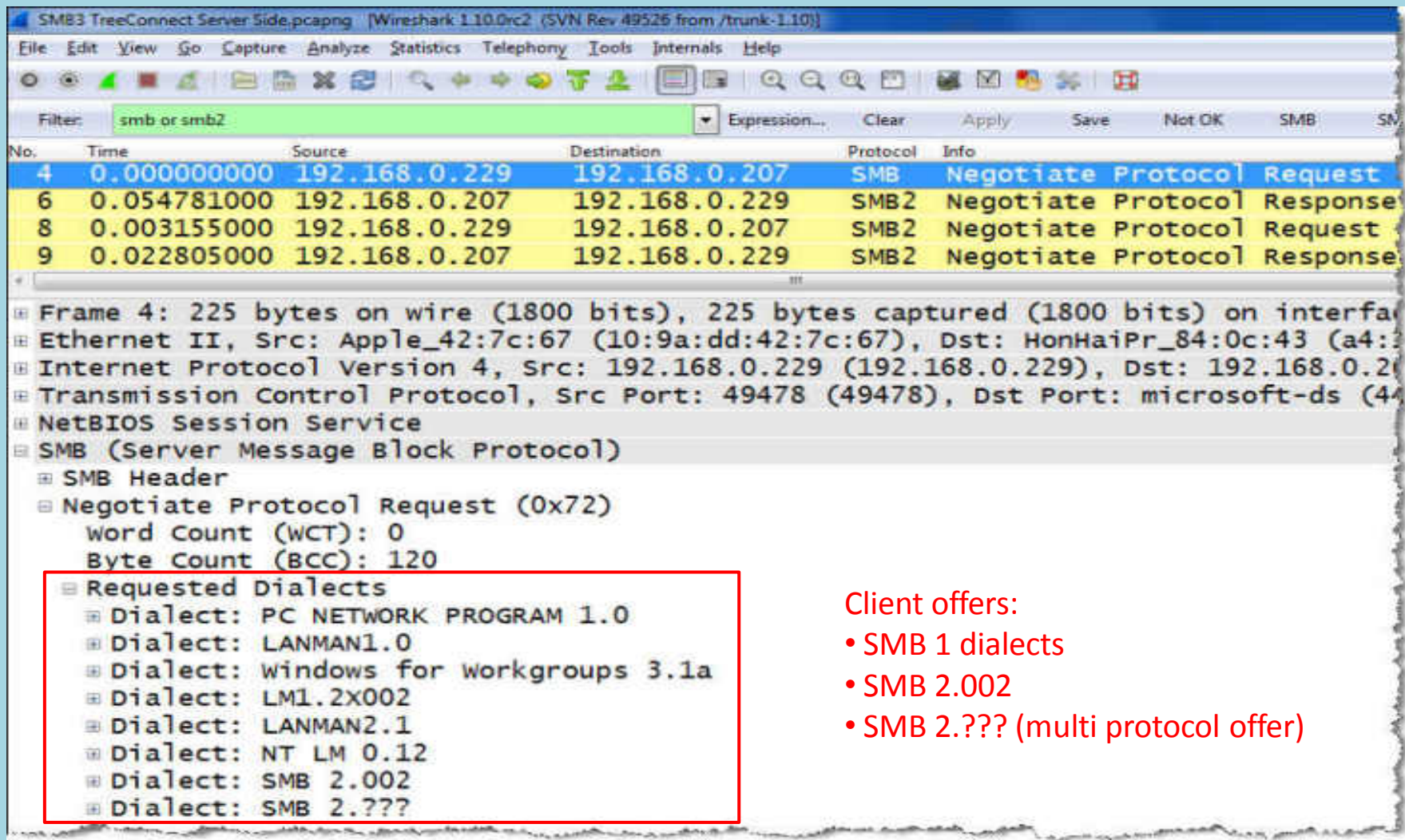
- At session setup the highest supported version / dialect is negotiated between client and server

Client / Server OS	Windows 8 Windows Server 2012	Windows 7 Windows Server 2008 R2	Windows Vista Windows Server 2008	Previous versions of Windows
Windows 8 Windows Server 2012	<b>SMB 3.0</b>	SMB 2.1	SMB 2.0	SMB 1.0
Windows 7 Windows Server 2008 R2	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
Windows Vista Windows Server 2008	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
Previous versions of Windows	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0

Source: <http://blogs.technet.com/b/josebda/>

# Server Message Block (SMB) Protokoll

## SMB Version/Dialect Negotiation Request



The image shows a Wireshark capture of an SMB negotiation process. The packet list pane shows four packets: a Negotiate Protocol Request (SMB), a Negotiate Protocol Response (SMB2), another Negotiate Protocol Request (SMB2), and another Negotiate Protocol Response (SMB2). The details pane for the first packet (Frame 4) is expanded to show the SMB Header and Negotiate Protocol Request (0x72) structure. The 'Requested Dialects' section is highlighted with a red box and lists the following dialects: PC NETWORK PROGRAM 1.0, LANMAN1.0, windows for workgroups 3.1a, LM1.2X002, LANMAN2.1, NT LM 0.12, SMB 2.002, and SMB 2.???. To the right of the red box, a list of client offers is provided in red text.

No.	Time	Source	Destination	Protocol	Info
4	0.000000000	192.168.0.229	192.168.0.207	SMB	Negotiate Protocol Request
6	0.054781000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response
8	0.003155000	192.168.0.229	192.168.0.207	SMB2	Negotiate Protocol Request
9	0.022805000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response

```
Frame 4: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface Ethernet II, Src: Apple_42:7c:67 (10:9a:dd:42:7c:67), Dst: HonHaiPr_84:0c:43 (a4:8c:39:84:0c:43)
Internet Protocol Version 4, Src: 192.168.0.229 (192.168.0.229), Dst: 192.168.0.207 (192.168.0.207)
Transmission Control Protocol, Src Port: 49478 (49478), Dst Port: microsoft-ds (445)
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
  Negotiate Protocol Request (0x72)
    Word Count (WCT): 0
    Byte Count (BCC): 120
    Requested Dialects
      Dialect: PC NETWORK PROGRAM 1.0
      Dialect: LANMAN1.0
      Dialect: windows for workgroups 3.1a
      Dialect: LM1.2X002
      Dialect: LANMAN2.1
      Dialect: NT LM 0.12
      Dialect: SMB 2.002
      Dialect: SMB 2.???
```

Client offers:

- SMB 1 dialects
- SMB 2.002
- SMB 2.???. (multi protocol offer)

# Server Message Block (SMB) Protokoll

## SMB Version/Dialect Negotiation Request

The image shows a Wireshark capture of SMB traffic. The filter is set to 'smb or smb2'. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Info
4	0.000000000	192.168.0.229	192.168.0.207	SMB	Negotiate Protocol Request
6	0.054781000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response
8	0.003155000	192.168.0.229	192.168.0.207	SMB2	Negotiate Protocol Request
9	0.022805000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response

The details pane for packet 6 is expanded to show the SMB2 header and negotiate response structure:

- SMB2 Header
- Negotiate Protocol Response (0x00)
  - StructureSize: 0x0041
  - Security mode: 0x01
  - Dialect: 0x02ff
  - Server Guid: 6f2922b3-bb37-430d-8df7-ca6c31f5dbd8
  - Capabilities: 0x00000007
  - Max Transaction Size: 1048576
  - Max Read Size: 1048576
  - Max Write Size: 1048576

Server response:

- SMB2 0x02ff (wildcard revision number)

# Server Message Block (SMB) Protokoll

## SMB Version/Dialect Negotiation Request

The image shows a Wireshark capture of an SMB2 Negotiate Protocol Request and Response. The packet list pane shows four packets:

No.	Time	Source	Destination	Protocol	Info
4	0.000000000	192.168.0.229	192.168.0.207	SMB	Negotiate Protocol Request
6	0.054781000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response
8	0.003155000	192.168.0.229	192.168.0.207	SMB2	Negotiate Protocol Request
9	0.022805000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response

The packet details pane for Frame 8 shows the following structure:

- Frame 8: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) on interface
- Ethernet II, Src: Apple\_42:7c:67 (10:9a:dd:42:7c:67), Dst: HonHaiPr\_84:0c:43 (a4:11:00:00:84:0c:43)
- Internet Protocol Version 4, Src: 192.168.0.229 (192.168.0.229), Dst: 192.168.0.207 (192.168.0.207)
- Transmission Control Protocol, Src Port: 49478 (49478), Dst Port: microsoft-ds (445)
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
  - Negotiate Protocol Request (0x00)
    - StructureSize: 0x0024
    - Dialect count: 3
    - Security mode: 0x01
    - Capabilities: 0x0000007f
    - Client Guid: 491caeb4-ca9c-11e2-afb3-001c4221644f
    - Boot Time: No time specified (0)
    - Dialect: 0x0202
    - Dialect: 0x0210
    - Dialect: 0x0300

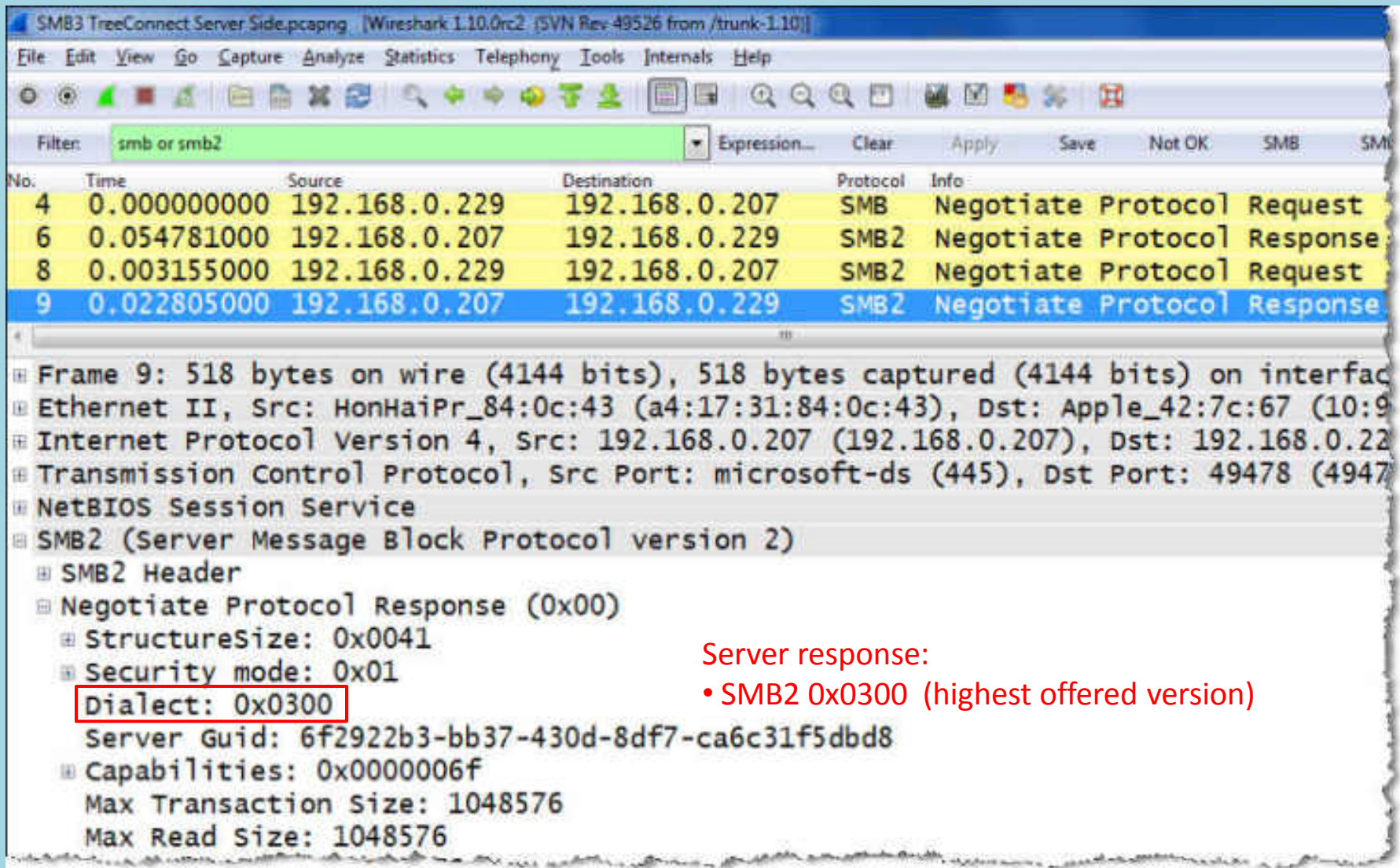
Client renegotiates with SMB2 and offers:

- SMB 2 dialect 0x0202
- SMB 2 dialect 0x0210
- SMB 2 dialect 0x0300 (SMB3)



# Server Message Block (SMB) Protokoll

## SMB Version/Dialect Negotiation Request



The image shows a Wireshark capture of an SMB2 Negotiate Protocol Response. The packet list pane shows four packets: a request (No. 4), a response (No. 6), another request (No. 8), and another response (No. 9). Packet 9 is selected, and its details pane is expanded to show the SMB2 header and Negotiate Protocol Response (0x00) structure. The 'Dialect' field is highlighted with a red box and labeled as the server response.

No.	Time	Source	Destination	Protocol	Info
4	0.000000000	192.168.0.229	192.168.0.207	SMB	Negotiate Protocol Request
6	0.054781000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response
8	0.003155000	192.168.0.229	192.168.0.207	SMB2	Negotiate Protocol Request
9	0.022805000	192.168.0.207	192.168.0.229	SMB2	Negotiate Protocol Response

Frame 9: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface Ethernet II, Src: HonHaiPr\_84:0c:43 (a4:17:31:84:0c:43), Dst: Apple\_42:7c:67 (10:9 Internet Protocol Version 4, Src: 192.168.0.207 (192.168.0.207), Dst: 192.168.0.22 Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: 49478 (4947 NetBIOS Session Service

SMB2 (Server Message Block Protocol version 2)

- SMB2 Header
- Negotiate Protocol Response (0x00)
  - StructureSize: 0x0041
  - Security mode: 0x01
  - Dialect: 0x0300**
  - Server Guid: 6f2922b3-bb37-430d-8df7-ca6c31f5dbd8
  - Capabilities: 0x0000006f
  - Max Transaction Size: 1048576
  - Max Read Size: 1048576

Server response:

- SMB2 0x0300 (highest offered version)

# Server Message Block (SMB) Protokoll

## SMB 1 Versions & Dialects

Source: <http://msdn.microsoft.com/en-us/library/cc246231.aspx>

Dialect name	Dialect Identifier String	Comments
Manager 1.0		system functions and file system features. It is documented in <a href="#">[SMB-LM1X]</a> and [XOPEN-SMB].
DOS LAN Manager 1.0	MICROSOFT NETWORKS 3.0	This is the DOS LAN Manager 1.0 extended protocol. It is identical to "LANMAN1.0", except that OS/2 error codes are translated to DOS error codes before being transmitted to the client.
LAN Manager 1.2	LANMAN1.2	The LAN Manager 1.2 extended protocol adds support for additional OS/2 commands and features to "LANMAN1.0". LAN Manager 1.2 is documented in <a href="#">[SMB-LM12]</a> and [XOPEN-SMB].
LAN Manager 2.0	LM1.2X002	This represents the LAN Manager 2.0 extended protocol for OS/2. It is documented in <a href="#">[SMB-LM20]</a> and [XOPEN-SMB]. Also known as the LANMAN2.0 dialect.
DOS LAN Manager 2.0	DOS LM1.2X002	This is the DOS version of LAN Manager 2.0. It is also documented in <a href="#">[SMB-LM20]</a> and [XOPEN-SMB]. When this dialect is selected, OS/2 error codes are translated to DOS error codes by the server before transmission to the client. Also known as the DOS LANMAN2.0 dialect.
LAN Manager 2.1	LANMAN2.1	LAN Manager 2.1 extended protocol. The additions and changes with respect to LAN Manager 2.0 are documented in <a href="#">[SMB-LM21]</a> .
DOS LAN Manager 2.1	DOS LANMAN2.1	DOS LAN Manager 2.1 extended protocol. This is, once again, identical to the OS/2 version of the dialect except that error codes are translated. See <a href="#">[SMB-LM21]</a> .
NT LAN Manager	NT LM 0.12	NT LAN Manager extended protocol. This set of extensions was created to support Windows NT. OS/2 LAN Manager 2.1 features are also supported. This dialect was originally documented in <a href="#">[CIFS]</a> . Also known as the NT LANMAN dialect.

# Server Message Block (SMB) Protokoll

SMB 2 / 3 Versions & Dialects

Source: <http://msdn.microsoft.com/en-us/library/cc246482.aspx>

Value	Meaning
0x0202	SMB 2.002 dialect revision number.
0x0210	SMB 2.1 dialect revision number.
0x0300	SMB 3.0 dialect revision number.

Windows Vista / 7 / 8; Server 2008 / 2008-R2 / 2012

Windows 7 / 8; Server 2008-R2 / 2012

Windows 8; Server 2012

In order to provide backwards compatibility, during the negotiation process the latest SMB version and dialect supported by both, client and server is negotiated using the following commands:

SMB Negotiate Protocol Request  
SMB Negotiate Protocol Response

SMB2 Negotiate Protocol Request  
SMB2 Negotiate Protocol Response

Remark: For the rest of this following presentation only SMB2 sessions are analyzed.

# Server Message Block (SMB) Protokoll

## SMB Request / Response Dialog

- SMB is based on a **Request /Response** dialog using **Sequence Numbers as reference**
- SMB Responses contain a **NT Status messages** useful for troubleshooting
- Adding specific **Wireshark columns** facilitates the interpretation of the SMB dialog

The screenshot shows a Wireshark capture of SMB3 traffic. The filter is set to 'smb or smb2'. The packet list pane shows 14 packets, with the first 7 highlighted in yellow. A red box highlights the first 7 rows of the packet list, which correspond to the data in the table below.

Protocol	Seq. No.	NT Status	Info
SMB2	1		Negotiate Protocol Request
SMB2	1	STATUS_SUCCESS	Negotiate Protocol Response, ACCEPTOR_NEGO, ACCE
SMB2	2		Session Setup Request, NTLMSSP_NEGOTIATE
SMB2	2	STATUS_MORE_PROCESSING_REQUIRED	Session Setup Response, Error: STATUS_MORE_PROCE
SMB2	3		Session Setup Request, NTLMSSP_AUTH, User: \John
SMB2	3	STATUS_SUCCESS	Session Setup Response, Unknown NTLMSSP message
SMB2	4		Tree Connect Request Tree: \\192.168.0.207\IPCS
SMB2	4	STATUS_SUCCESS	Tree Connect Response
SMB2	5		Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2	5	STATUS_SUCCESS	Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2	6		Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2	7		Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \19
SMB2	6	STATUS_SUCCESS	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INF
SMB2	7	STATUS_FS_DRIVER_REQUIRED	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED

# Server Message Block (SMB) Protokoll

## SMB Request / Response Dialog

- You may create a **Quick Filter Button** on responses **other** than STATUS\_SUCCESS
- Display Filter string: `smb2.nt_status > 0xc0000000`

The screenshot shows the Wireshark interface with the following details:

- Filter:** `smb2.nt_status > 0xc0000000`
- Table of captured packets:**

Protocol	Seq. No	NT Status	Info
SMB2	2	STATUS_MORE_PROCESSING_REQUIRED	Session Setup Response, Error: STATUS_MOR
SMB2	7	STATUS_FS_DRIVER_REQUIRED	Ioctl Response, Error: STATUS_FS_DRIVER_R
SMB2	10	STATUS_OBJECT_NAME_NOT_FOUND	Create Response, Error: STATUS_OBJECT_NAM
SMB2	11	STATUS_OBJECT_NAME_NOT_FOUND	Create Response, Error: STATUS_OBJECT_NAM

The detailed view of the selected packet (SMB2) shows the following fields:

- SMB2 (Server Message Block Protocol version 2)
- SMB2 Header
  - Server Component: SMB2
  - Header Length: 64
  - Credit Charge: 1
  - NT Status: STATUS\_MORE\_PROCESSING\_REQUIRED (0xc0000016)**
  - Command: Session Setup (1)
  - Credits granted: 1
  - Flags: 0x00000001
  - Chain offset: 0x00000000

# Server Message Block (SMB) Protokoll

## SMB Request / Response messages

---

- SMB 2/3 comprises **19 different Requests/Responses** for the Client-Server dialog
- Main purpose is **File I/O** but also Printing, Desktop.ini, Policies, Certificates etc.
- SMB also provides an authenticated **inter-process communication mechanism**.

The most frequently used Request/ Response messages are:

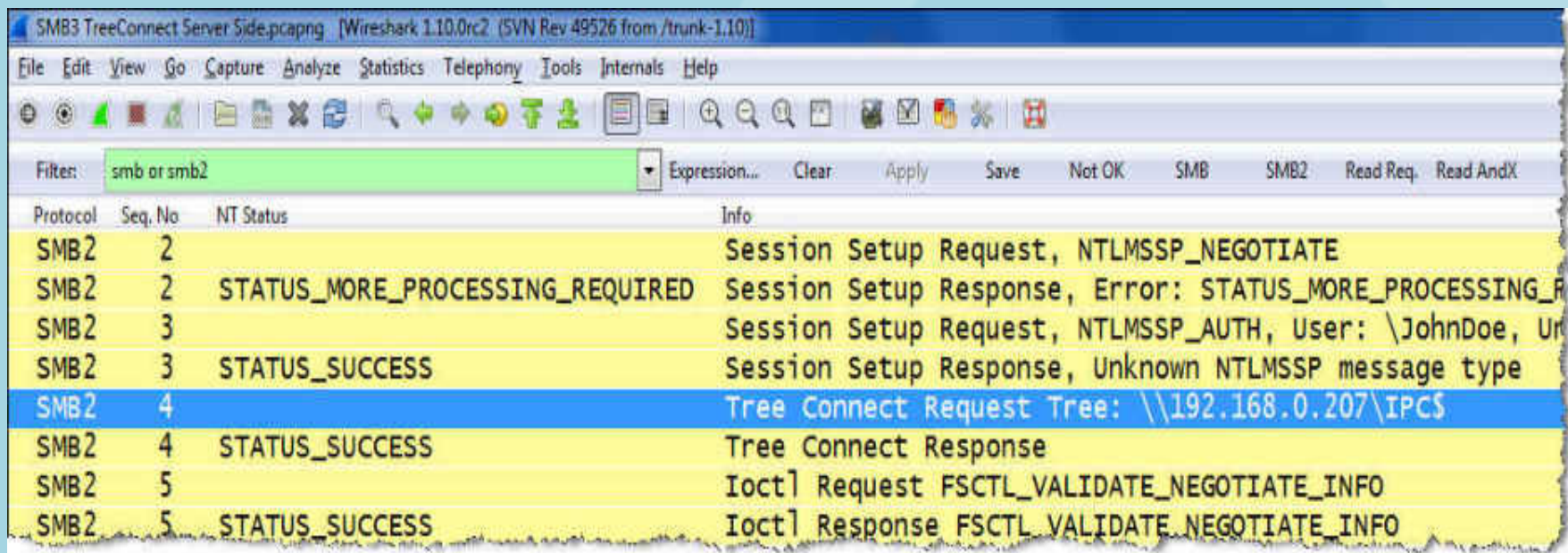
- Negotiate Protocol
- Setup Account
- Tree Connect
- Create
- Ioctl
- Read
- Write
- Close
- Tree Disconnect
- Logoff

# Server Message Block (SMB) Protokoll

## SMB Request / Response messages

- CIFS Server resources are called **Shares** , shares may be files, directories, printers etc.
- First connection is made to the **Inter-Process Communication share IPC\$**
- **IPC\$ is a virtual share** used to facilitate communication between processes, authentication, fetch a list of shared resources from a server etc.
- The **Tree Connect Request** message is used to connect a share

```
C:\> net use X: \\192.168.0.207\public /USER:JohnDoe Wireshark.ch
```



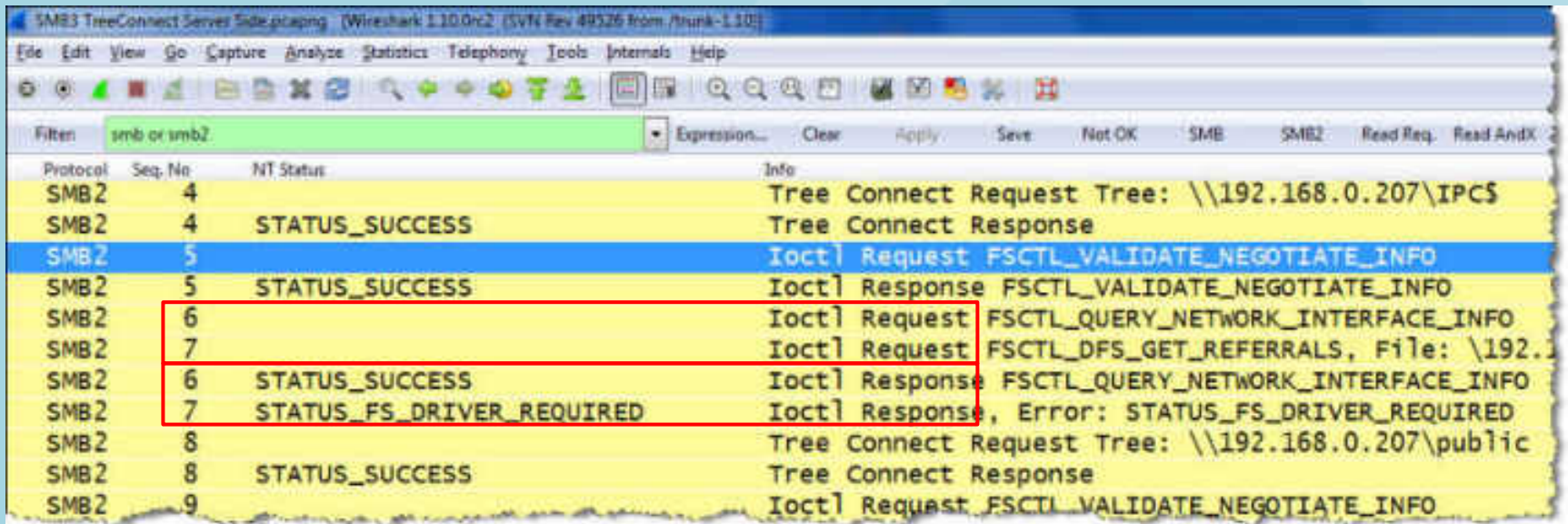
The image shows a Wireshark capture of SMB traffic. The filter is set to 'smb or smb2'. The capture shows a sequence of messages between a client and a server. The messages are as follows:

Protocol	Seq. No	NT Status	Info
SMB2	2		Session Setup Request, NTLMSSP_NEGOTIATE
SMB2	2	STATUS_MORE_PROCESSING_REQUIRED	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
SMB2	3		Session Setup Request, NTLMSSP_AUTH, User: \JohnDoe, UR
SMB2	3	STATUS_SUCCESS	Session Setup Response, Unknown NTLMSSP message type
SMB2	4		Tree Connect Request Tree: \\192.168.0.207\IPC\$
SMB2	4	STATUS_SUCCESS	Tree Connect Response
SMB2	5		Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2	5	STATUS_SUCCESS	Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO

# Server Message Block (SMB) Protokoll

## SMB Request / Response messages

- The **IOCTL/FSCTL** (I/O control & File System control) messages are very versatile in use
- This **IOCTL/FSCTL** delivers a device- or file-specific request to a server
- There are **dozens of options** for these commands, refer to the Internet for more information
- Note: **Multiple Requests** can be sent out as a burst, use the Sequence No to find the Responses



The image shows a Wireshark capture of SMB traffic. The filter is set to 'smb or smb2'. The table below represents the data shown in the packet list pane:

Protocol	Seq. No.	NT Status	Info
SMB2	4		Tree Connect Request Tree: \\192.168.0.207\IPC\$
SMB2	4	STATUS_SUCCESS	Tree Connect Response
SMB2	5		Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2	5	STATUS_SUCCESS	Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2	6		Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2	7		Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \\192.
SMB2	6	STATUS_SUCCESS	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2	7	STATUS_FS_DRIVER_REQUIRED	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
SMB2	8		Tree Connect Request Tree: \\192.168.0.207\public
SMB2	8	STATUS_SUCCESS	Tree Connect Response
SMB2	9		Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO



# Server Message Block (SMB) Protokoll

## SMB Request / Response messages

- **Multiple** SMB2 Requests/Response can be chained in **Compounded Requests/Responses**
- The SMB2 **Chain Offset** field contains the **Byte offset value** of the next Request
- If the SMB2 **Chain Offset** field contains the value **0x00000000** no more requests will follow

The screenshot displays a Wireshark capture of SMB2 traffic. The packet list pane shows the following messages:

Protocol	Seq. No	NT Status	Info
SMB2	16		Create Request File:
SMB2	16	STATUS_SUCCESS	Create Response File:
SMB2	17,18		GetInfo Request FS_INFO/SMB2_FS_INFO_01 File
SMB2	17,18	STATUS_SUCCESS, STATUS_SUCCESS	GetInfo Response; GetInfo Response
SMB2	19		Close Request File:
SMB2	19	STATUS_SUCCESS	Close Response
SMB2	20,21		Find Request SMB2_FIND_ID_BOTH_DIRECTORY_INF

The packet details pane for frame 3 shows the following structure:

- Frame 3: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits) on interface 0
- Ethernet II, Src: QuantaCo\_6d:6c:e0 (00:23:8b:6d:6c:e0), Dst: Hewlett-\_b1:eb:0b (1c:c1:de:11:11:11)
- Internet Protocol Version 4, Src: 192.168.0.201 (192.168.0.201), Dst: 192.168.0.197 (192.168.0.197)
- Transmission Control Protocol, Src Port: 53813 (53813), Dst Port: microsoft-ds (445), Seq: 300000000
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
  - GetInfo Request (0x10)
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
  - GetInfo Request (0x10)

# Server Message Block (SMB) Protokoll

## SMB Request / Response messages

- There seems to be two kinds of **Compounded Requests/Responses** implementation ?

```
72326 0.000496000 192.168.50.251 192.168.51.250 SMB2 10880 GetInfo Request FILE_INFO/SMB2_FI
72328 0.000719000 192.168.50.251 192.168.51.250 SMB2 10881,10882 GetInfo Request FS_INFO/SMB2_FS_I
72330 0.000788000 192.168.50.251 192.168.51.250 SMB2 10883 GetInfo Request FS_INFO/SMB2_FS_I

Internet Protocol Version 4, Src: 192.168.50.251 (192.168.50.251), Dst: 192.168.51.250 (192.168.51.250)
Transmission Control Protocol, Src Port: 49176 (49176), Dst Port: microsoft-ds (445), Seq: 3734317142, Ack:
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  GetInfo Request (0x10)
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  GetInfo Request (0x10)
```

Compounded Request with ONE NetBIOS header  
(works as defined in Microsoft specifications)

```
72336 0.000001000 192.168.50.251 192.168.51.250 SMB2 10888 read request Len:65536 Off:26214
72338 0.002252000 192.168.50.251 192.168.51.250 SMB2 10889,10890 Read Request Len:65536 Off:393216
72421 0.383451000 192.168.50.251 192.168.51.250 SMB2 10891 Read Request Len:65536 Off:458752
72423 0.000000000 192.168.50.251 192.168.51.250 SMB2 10892 Read Request Len:65536 Off:521288

Internet Protocol Version 4, Src: 192.168.50.251 (192.168.50.251), Dst: 192.168.51.250 (192.168.51.250)
Transmission Control Protocol, Src Port: 49176 (49176), Dst Port: microsoft-ds (445), Seq: 3734318056, Ack:
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  Read Request (0x08)
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  Read Request (0x08)
```

Compounded Request with TWO NetBIOS header  
(recognized in retransmissions)

# Server Message Block (SMB) Protokoll

## SMB Request / Response messages

- The **Read Request** specifies **read block length** and **file offset** in bytes
- **Multiple Read Requests** can be issued by client and **may not** be delivered **in order** by the server

The screenshot shows a Wireshark capture of SMB2 traffic. The filter is '(smb2.cmd == 8)'. The table below summarizes the captured packets:

Protocol	Seq. No.	NT Status	Info
SMB2	1059		Read Request Len:65536 off:0 File: Documents\wireshark.jpg
SMB2	1060		Read Request Len:65536 off:65536 File: Documents\wireshark.jpg
SMB2	1059	STATUS_SUCCESS	Read Response
SMB2	1060	STATUS_SUCCESS	Read Response
SMB2	1061		Read Request Len:65536 off:131072 File: Documents\wireshark.jpg
SMB2	1062		Read Request Len:38431 off:196608 File: Documents\wireshark.jpg
SMB2	1061	STATUS_SUCCESS	Read Response
SMB2	1062	STATUS_SUCCESS	Read Response

The screenshot shows the reassembly of TCP segments for Read Responses. The table below summarizes the captured packets:

Protocol	Seq. No.	NT Status	Info
SMB2	1059	STATUS_SUCCESS	Read Response
SMB2	1060	STATUS_SUCCESS	Read Response

Internet Protocol Version 4, Src: 192.168.0.197 (192.168.0.197), Dst: 192.168.0.201 (192.168.0.201)  
Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: 53859 (53859), Seq: 35905563  
[45 Reassembled TCP Segments (65620 bytes): #45(1460), #46(1460), #47(1460), #48(1460), #49(1460),  
[Frame: 45, payload: 0-1459 (1460 bytes)]  
[Frame: 46, payload: 1460-2919 (1460 bytes)]  
[Frame: 47, payload: 2920-4379 (1460 bytes)]  
[Frame: 48, payload: 4380-5839 (1460 bytes)]

Wireshark will reassemble TCP segments of Read Responses (if configured to do so)

# Server Message Block (SMB) Protokoll

## SMB2 Durable File Handle feature

- The **Durable File Handles** allow a connection to an SMB server to survive brief network outages

The initial Read request at Offset 5570560

```
Filter: smb2
Protocol  Seq. No.  Info
SMB2     13908    Read Request Len:65536 off:5505024 File: iltis\iadmin\xcopy\iltis_012.000000000_000000023.bdg
SMB2     13909    Read Request Len:65536 Off:5570560 File: iltis\iadmin\xcopy\iltis_012.000000000_000000023.bdg
SMB2     13910    Read Request Len:65536 Off:5636096 File: iltis\iadmin\xcopy\iltis_012.000000000_000000023.bdg
SMB2     13911    Read Request Len:65536 off:5701632 File: iltis\iadmin\xcopy\iltis_012.000000000_000000023.bdg
```

The TCP session is broken by a network outage

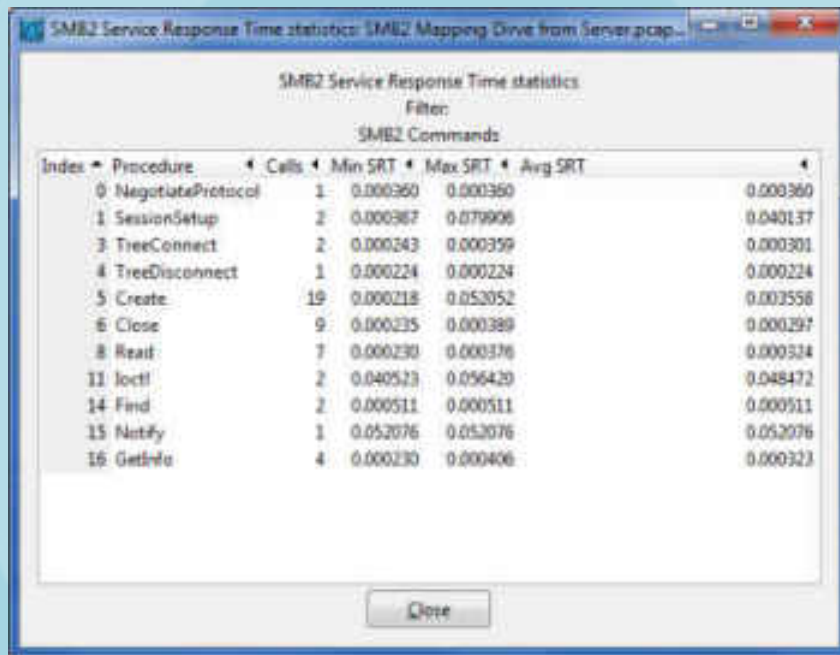
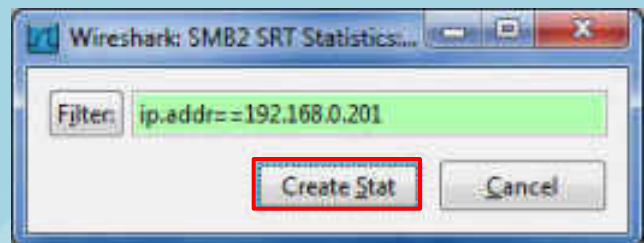
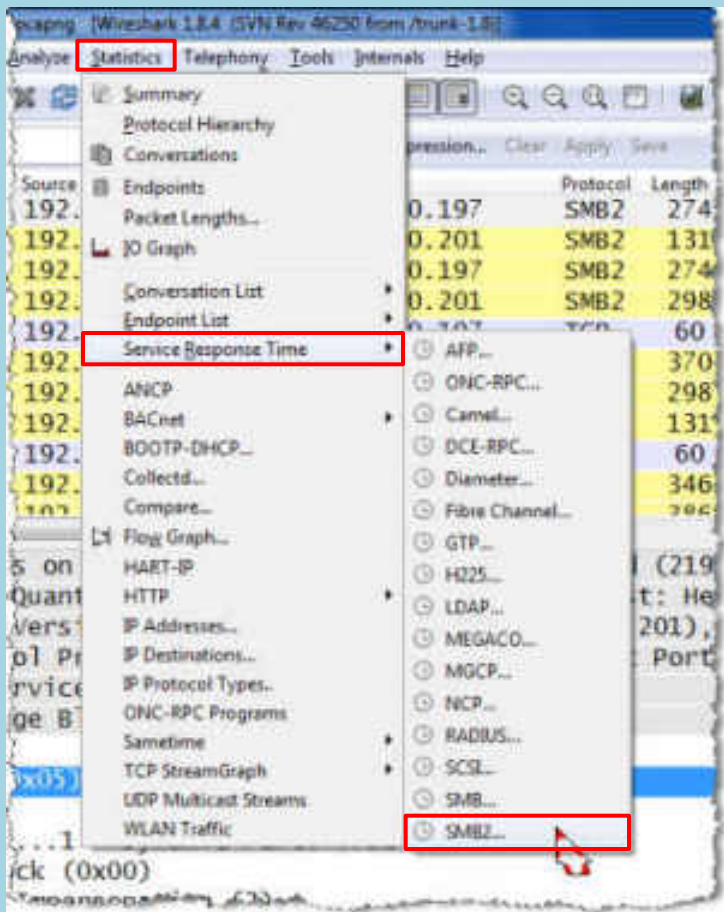
```
TCP      microsoft-ds > 49176 [ACK] Seq=3923545567 Ack=3734680075 win=62953 Len=0 SLE=3734680074 SRE=3734680075
TCP      49176 > microsoft-ds [RST, ACK] Seq=3734680075 Ack=3923544107 win=0 Len=0
TCP      49178 > microsoft-ds [SYN] Seq=4126720917 win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP      microsoft-ds > 49178 [SYN, ACK] Seq=3831215352 Ack=4126720918 win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP      49178 > microsoft-ds [ACK] Seq=4126720918 Ack=3831215353 win=64240 Len=0
SMB2     0       Negotiate Protocol Request
SMB2     0       Negotiate Protocol Response
SMB2     1       Session Setup Request NTLMSSP_NEGOTIATE
```

The TCP/SMB session is recovered and the Read Request reissued

```
SMB2     15      Read Response
SMB2     21      Read Request Len:65536 Off:5570560 File: iltis\iadmin\xcopy\iltis_012.000000000_000000023.bdg
SMB2     22      Read Request Len:65536 Off:5636096 File: iltis\iadmin\xcopy\iltis_012.000000000_000000023.bdg
SMB2     16      Read Response
SMB2     23      Read Request Len:65536 off:5701632 File: iltis\iadmin\xcopy\iltis_012.000000000_000000023.bdg
```

# Server Message Block (SMB) Protokoll

## SMB2 Service Response Time statistics with Wireshark



# Server Message Block (SMB) Protokoll

## SMB2 Service Response Time statistics with Wireshark

SMB2 Service Response Time statistics

Filter: ip.addr==192.168.0.201

SMB2 Commands

Index	Procedure	Calls	Min SRT	Max SRT	Avg SRT
0	NegotiateProtocol	1	0.000360	0.000360	0.000360
1	SessionSetup	2	0.000367	0.079906	0.040137
3	TreeConnect	2	0.000243	0.000359	0.000301
4	TreeDisconnect	1	0.000224	0.000224	0.000224
5	Create	18	0.000218	0.052052	0.000218
6	Close	9	0.000235	0.000389	0.000235
8	Read	7	0.000230	0.000376	0.000230
11	Ioctl	2	0.040523	0.056420	0.040523
14	Find	2	0.000511	0.000511	0.000511
15	Notify	1	0.052076	0.052076	0.052076
16	GetInfo	4	0.000230	0.000406	0.000230

Apply as Filter  
Prepare a Filter  
Find Frame  
Colorize Procedure

Selected  
... not Selected  
... and Selected  
... or Selected  
... and not Selected  
... or not Selected

Length Seq. No. Info

274 7 Create Request File:

131 7 Create Response, Error: STAT

274 8 Create Request File:

298 8 Create Response File:

50 53365 > microsoft-ds [ACK] S

Create Request File: ;Notify

Create Response File:

Notify Response, Error: STAT

53365 > microsoft-ds [ACK] S

Create Request File: desktop

Create Response File: deskto

(2192 bits) on interface 0

Host: Hewlett-\_b1:eb:0b (1c:c1:de:b1:eb:0b)

(.201), Dst: 192.168.0.197 (192.168.0.197)

Port: microsoft-ds (445), Seq: 1525, Ack: 1

- Right mouse click on specific command opens filter selections
- Wireshark filters on Requests AND Responses of the selected command

# Server Message Block (SMB) Protokoll

## SMB2 Request / Response messages

---

- **SMB2 NEGOTIATE** Negotiation of SMB2 dialects between client and server
- **SMB2 SESSION\_SETUP** Sent by a client to request a new authenticated session
- **SMB2 LOGOFF** Sent by a client to request termination of a particular session
- **SMB2 TREE\_CONNECT** Sent by a client to request access to a particular share on the server
- **SMB2 TREE\_DISCONNECT** Sent by a client to request that the specified tree is disconnected
- **SMB2 CREATE** Sent by a client to request either creation of or access to a file
- **SMB2 CLOSE** Sent by a client to close an instance of a file previously opened
- **SMB2 FLUSH** Sent by a client to request that a server flush cached file information
- **SMB2 READ** Sent by a client to request a read operation on a specified file
- **SMB2 WRITE** Sent by a client to write data to the file or named pipe
- **SMB2 LOCK** Sent by a client to either lock or unlock portions of a file
- **SMB2 IOCTL** Sent by a client to issue an implementation-specific I/O Control
- **SMB2 CANCEL** Sent by a client to cancel a previously sent message
- **SMB2 ECHO** Sent by a client to determine whether a server is processing requests
- **SMB2 QUERY\_DIRECTORY** Sent by a client to obtain a directory enumeration on a directory
- **SMB2 CHANGE\_NOTIFY** Sent by a client to request change notifications on a directory
- **SMB2 QUERY\_INFO** Sent by a client to request information on a file, named pipe, volume
- **SMB2 SET\_INFO** Sent by a client to set information on a file or underlying object store
- **SMB2 OPLOCK\_BREAK** Sent by a server to indicate that an opportunistic lock is being broken

# Server Message Block (SMB) Protokoll

## SMB2 Response NT Status messages

---

- NT Status: **STATUS\_SUCCESS (0x00000000)**
- NT Status: STATUS\_NO\_MORE\_FILES
- NT Status: STATUS\_INVALID\_HANDLE
- NT Status: STATUS\_INVALID\_PARAMETER
- NT Status: STATUS\_NO\_SUCH\_FILE
- NT Status: STATUS\_MORE\_PROCESSING\_REQUIRED
- NT Status: STATUS\_INVALID\_SYSTEM\_SERVICE
- NT Status: STATUS\_ACCESS\_DENIED
- NT Status: STATUS\_OBJECT\_NAME\_INVALID
- NT Status: STATUS\_OBJECT\_NAME\_NOT\_FOUND
- NT Status: STATUS\_OBJECT\_NAME\_COLLISION
- NT Status: STATUS\_OBJECT\_PATH\_NOT\_FOUND
- NT Status: STATUS\_OBJECT\_PATH\_SYNTAX\_BAD
- NT Status: STATUS\_SHARING\_VIOLATION
- NT Status: STATUS\_EA\_TOO\_LARGE
- NT Status: STATUS\_FILE\_LOCK\_CONFLICT
- NT Status: STATUS\_LOCK\_NOT\_GRANTED
- NT Status: STATUS\_LOGON\_FAILURE
- NT Status: STATUS\_RANGE\_NOT\_LOCKED
- NT Status: STATUS\_FILE\_IS\_A\_DIRECTORY
- NT Status: STATUS\_NOT\_SUPPORTED
- NT Status: STATUS\_BAD\_DEVICE\_TYPE
- NT Status: STATUS\_REQUEST\_NOT\_ACCEPTED
- NT Status: STATUS\_DIRECTORY\_NOT\_EMPTY
- NT Status: STATUS\_NOT\_A\_DIRECTORY
- NT Status: STATUS\_CANCELLED



# Server Message Block (SMB) Protokoll

SMB useful links and references

---



Despite the widespread and successful use of the SMB protocol, there are almost no books available, covering the topic in a easy readable but still detailed manner.

Microsoft [MS-SMB2]: Server Message Block Protocol Versions 2 and 3

<http://msdn.microsoft.com/en-us/library/cc246482.aspx>

Blog by Jose Barreto, a member of the File Server team at Microsoft.

<http://blogs.technet.com/b/josebda/>

Ronnie Sahlberg: Using Wireshark for Analyzing CIFS Traffic

[http://www.snia.org/sites/default/files2/sdc\\_archives/2008\\_presentations/monday/RonnieSahlberg\\_UsingWireshark.pdf](http://www.snia.org/sites/default/files2/sdc_archives/2008_presentations/monday/RonnieSahlberg_UsingWireshark.pdf)

**Book:** Implementing CIFS: The Common Internet File System, Christopher Hertel Publication  
Date: August 21, 2003 (very detailed, but not covering SMB 2/3)

<http://www.amazon.com/Implementing-CIFS-Common-Internet-System/dp/013047116X>

# Thank you for your attention

---



Rolf Leutert, Leutert NetServices,  
leutert@wireshark.ch / [www.wireshark.ch](http://www.wireshark.ch)