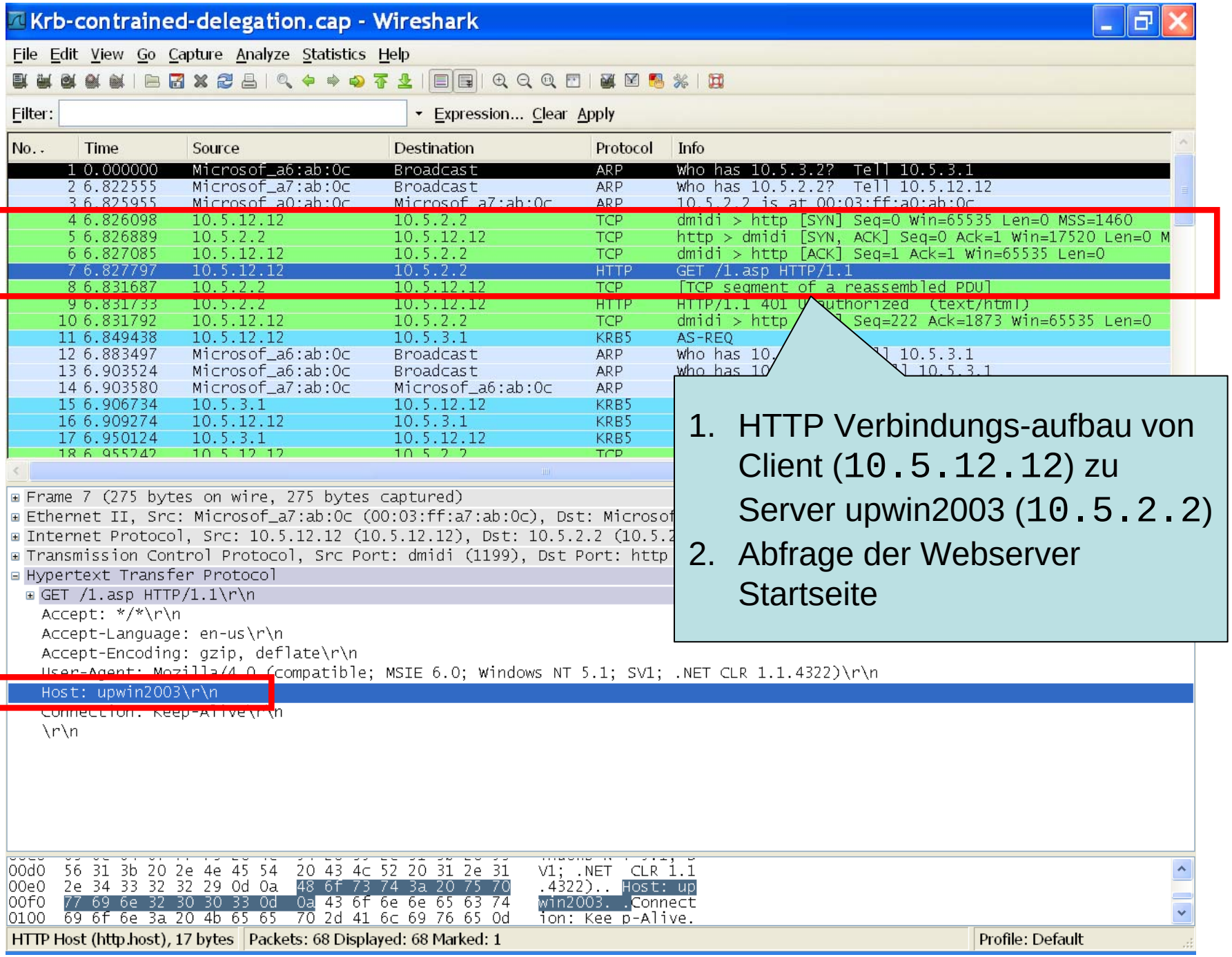
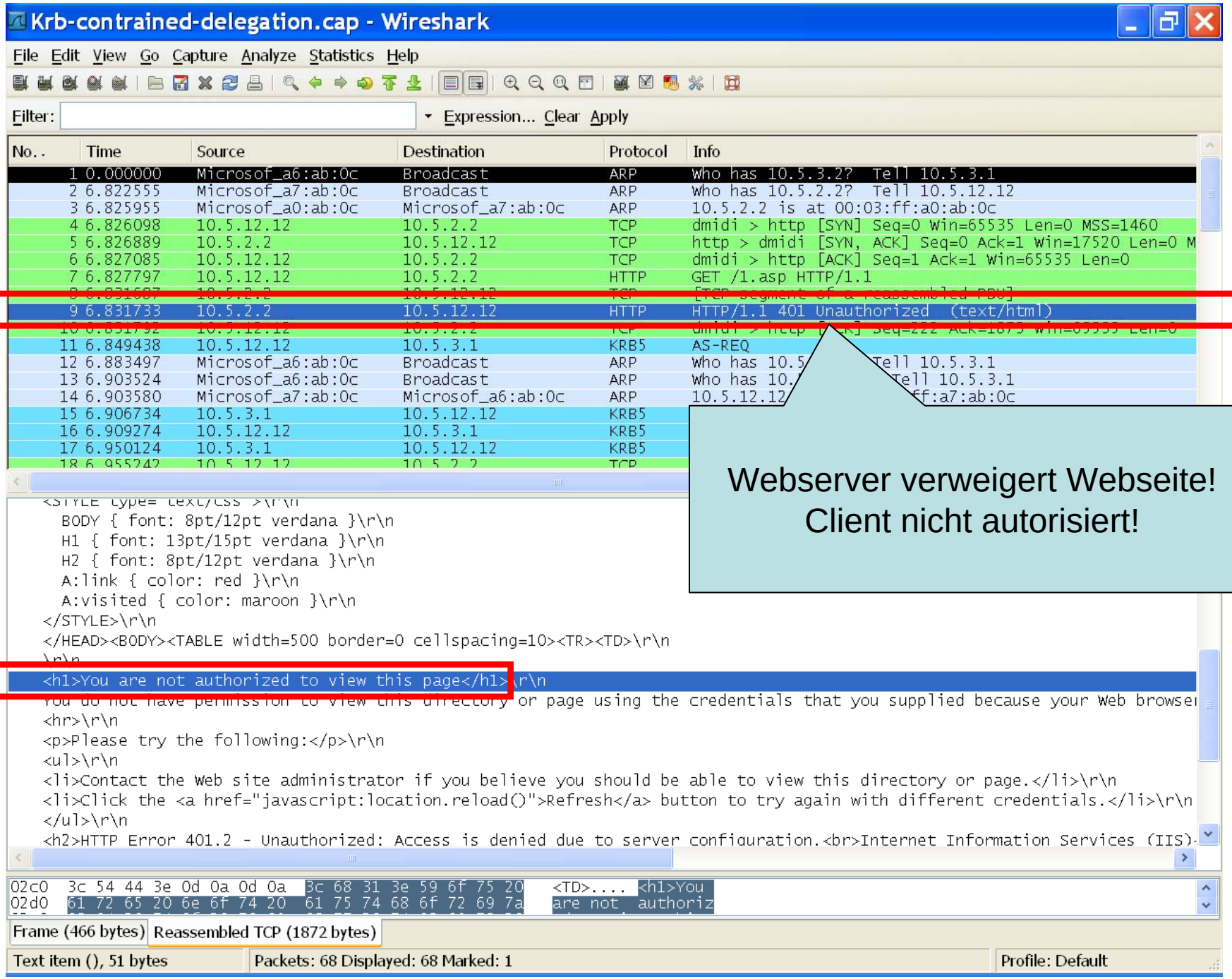
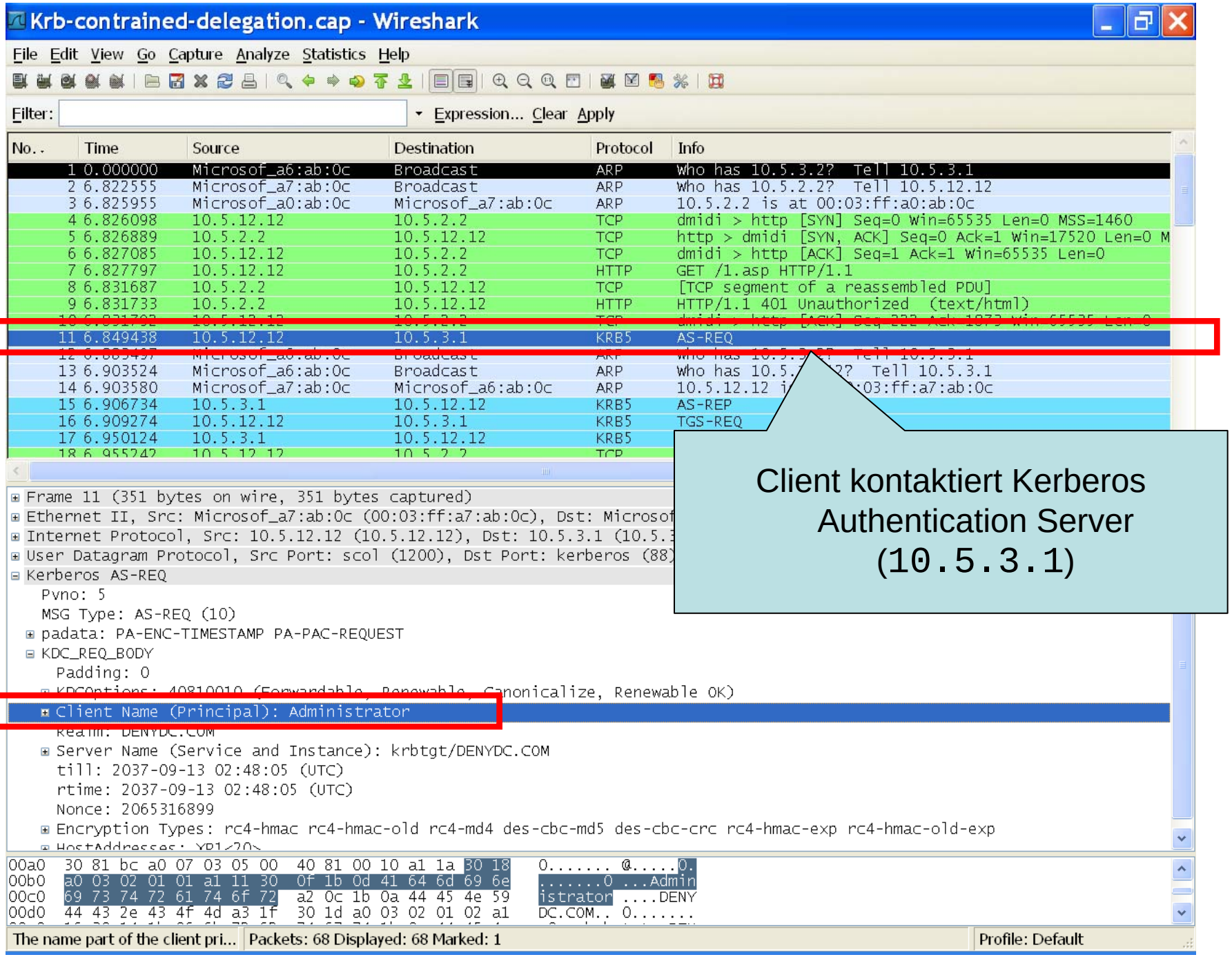
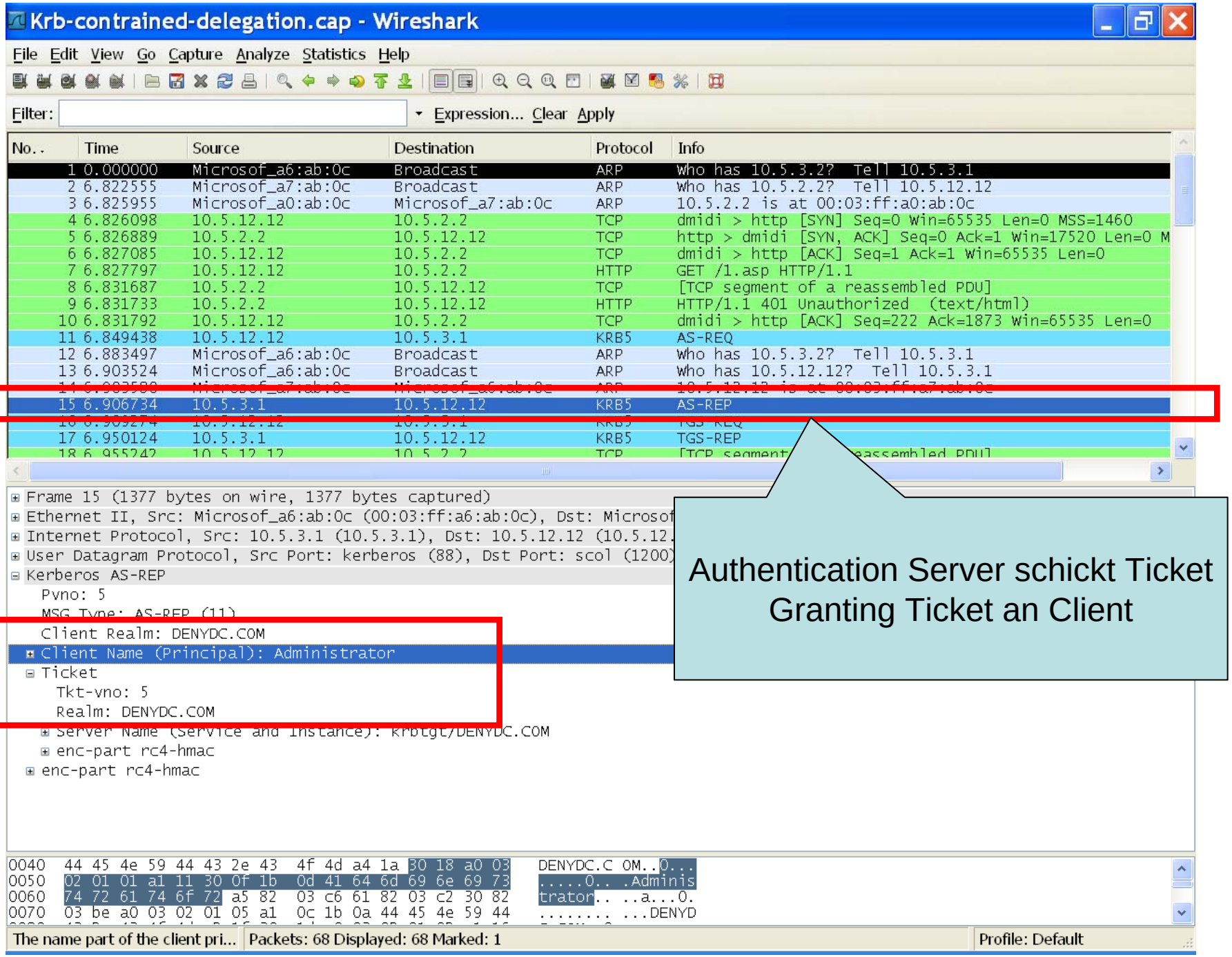
Kerberos Netzverkehr

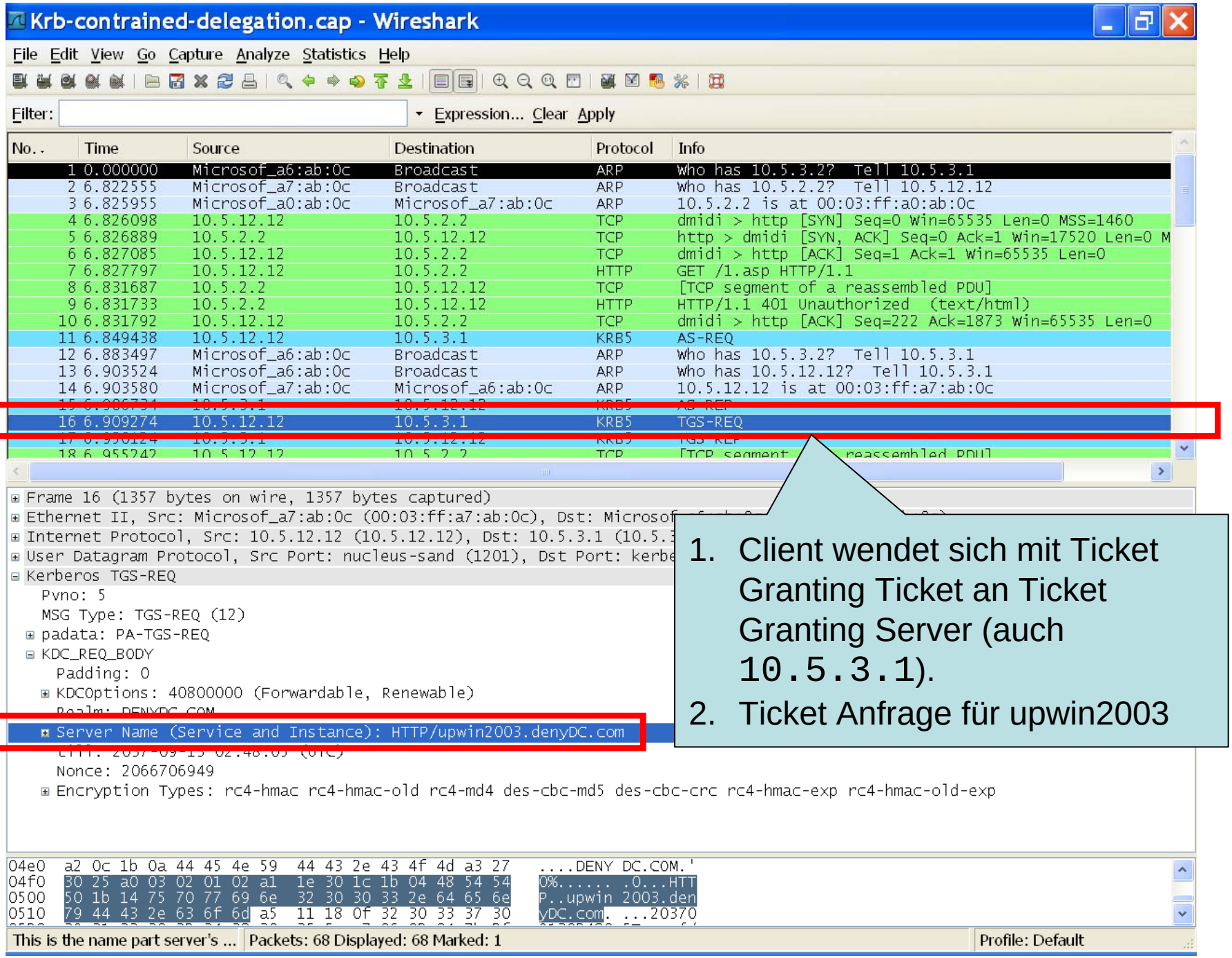
- Client `10.5.12.12`
- Kerberos `10.5.3.1`
- Webserver `10.5.2.2`

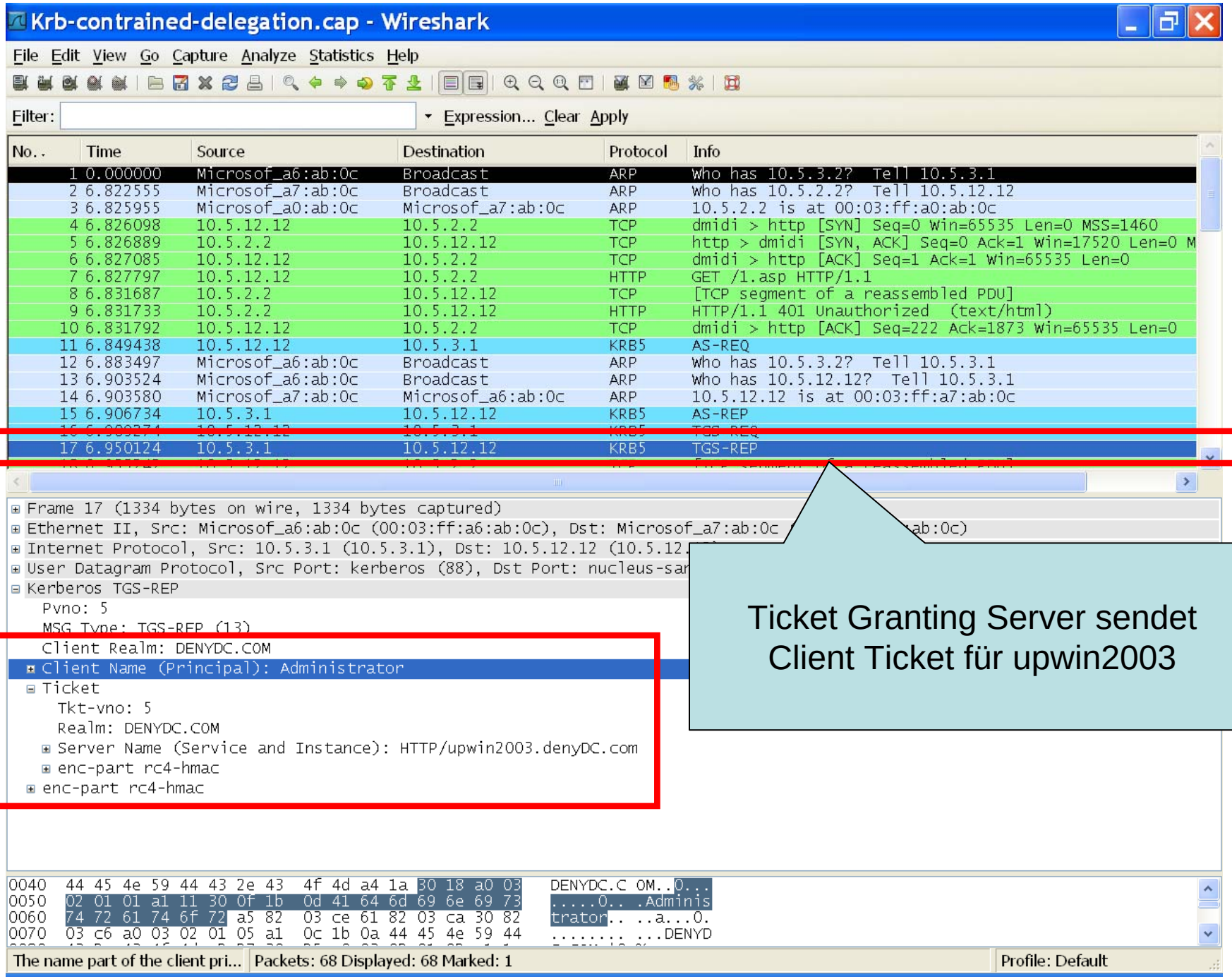

Krb-contrained-delegation.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
2 6.822555 Microsof_a7:ab:0c Broadcast ARP Who has 10.5.2.2? Tell 10.5.12.12
4 6.826098 10.5.12.12 10.5.2.2 TCP dmidi > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5 6.826889 10.5.2.2 10.5.12.12 TCP http > dmidi [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 M
6 6.827085 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 6.827797 10.5.12.12 10.5.2.2 HTTP GET /1.asp HTTP/1.1
8 6.831687 10.5.2.2 10.5.12.12 TCP [TCP segment of a reassembled PDU]
11 6.849438 10.5.12.12 10.5.3.1 KRB5 AS-REQ
12 6.883497 Microsof_a6:ab:0c Broadcast ARP
13 6.903524 Microsof_a6:ab:0c Broadcast ARP
14 6.903580 Microsof_a7:ab:0c Microsof_a6:ab:0c ARP
15 6.906734 10.5.3.1 10.5.12.12 KRB5
16 6.909274 10.5.12.12 10.5.3.1 KRB5
17 6.950124 10.5.3.1 10.5.12.12 KRB5
Frame 7 (275 bytes on wire, 275 bytes captured)
Ethernet II, Src: Microsof_a7:ab:0c (00:03:ff:a7:ab:0c), Dst: Microsof
Internet Protocol, Src: 10.5.12.12 (10.5.12.12), Dst: 10.5.2.2 (10.5.2
Transmission Control Protocol, Src Port: dmidi (1199), Dst Port: http
Hypertext Transfer Protocol
GET /1.asp HTTP/1.1\r\n
Accept: */*\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)\r\n
Host: upwin2003\r\n
Connection: Keep-Alive\r\n
\r\n
00d0 56 31 3b 20 2e 4e 45 54 20 43 4c 52 20 31 2e 31 V1; .NET CLR 1.1
00e0 2e 34 33 32 32 29 0d 0a 48 6f 73 74 3a 20 75 70 .4322).. Host: up
00f0 77 69 6e 32 30 30 33 0d 0a 43 6f 6e 6e 65 63 74 win2003. .Connect
0100 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Kee p-Alive.
HTTP Host (http.host), 17 bytes
Packets: 68 Displayed: 68 Marked: 1
Profile: Default
1. HTTP Verbindungs-aufbau von Client (10.5.12.12) zu Server upwin2003 (10.5.2.2)
2. Abfrage der Webserver Startseite

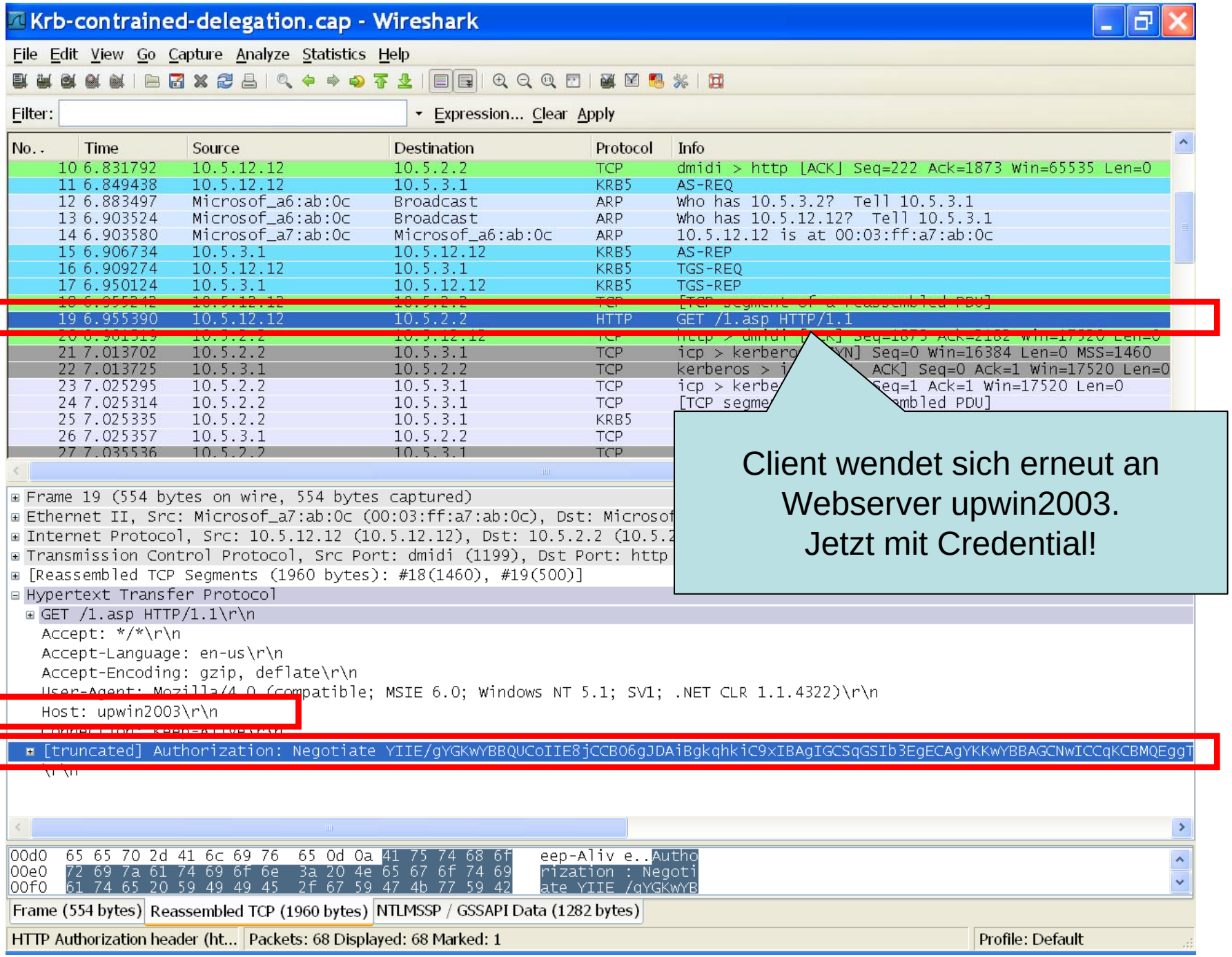

Krb-contrained-delegation.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
2 6.822555 Microsof_a7:ab:0c Broadcast ARP Who has 10.5.2.2? Tell 10.5.12.12
3 6.825955 Microsof_a0:ab:0c Microsof_a7:ab:0c ARP 10.5.2.2 is at 00:03:ff:a0:ab:0c
4 6.826098 10.5.12.12 10.5.2.2 TCP dmidi > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5 6.826889 10.5.2.2 10.5.12.12 TCP http > dmidi [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 M
6 6.827085 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 6.827797 10.5.12.12 10.5.2.2 HTTP GET /1.asp HTTP/1.1
9 6.831733 10.5.2.2 10.5.12.12 HTTP HTTP/1.1 401 Unauthorized (text/html)
11 6.849438 10.5.12.12 10.5.3.1 KRB5 AS-REQ
12 6.883497 Microsof_a6:ab:0c Broadcast ARP
13 6.903524 Microsof_a6:ab:0c Broadcast ARP
14 6.903580 Microsof_a7:ab:0c Microsof_a6:ab:0c ARP
15 6.906734 10.5.3.1 10.5.12.12 KRB5
16 6.909274 10.5.12.12 10.5.3.1 KRB5
17 6.950124 10.5.3.1 10.5.12.12 KRB5
BODY { font: 8pt/12pt verdana }\r\n
H1 { font: 13pt/15pt verdana }\r\n
H2 { font: 8pt/12pt verdana }\r\n
A:link { color: red }\r\n
A:visited { color: maroon }\r\n
</STYLE>\r\n
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>\r\n
<h1>You are not authorized to view this page</h1>\r\n
<hr>\r\n
Please try the following: \r\n
\r\n
Contact the Web site administrator if you believe you should be able to view this directory or page.
\r\n
Click the Refresh button to try again with different credentials.
\r\n
\r\n
02c0 3c 54 44 3e 0d 0a 0d 0a 3c 68 31 3e 59 6f 75 20 <TD>.... <h1>You
02d0 61 72 65 20 6e 6f 74 20 61 75 74 68 6f 72 69 7a are not authoriz
Frame (466 bytes) Reassembled TCP (1872 bytes)
Text item (), 51 bytes
Packets: 68 Displayed: 68 Marked: 1
Profile: Default
Webserver verweigert Webseite!
Client nicht autorisiert!

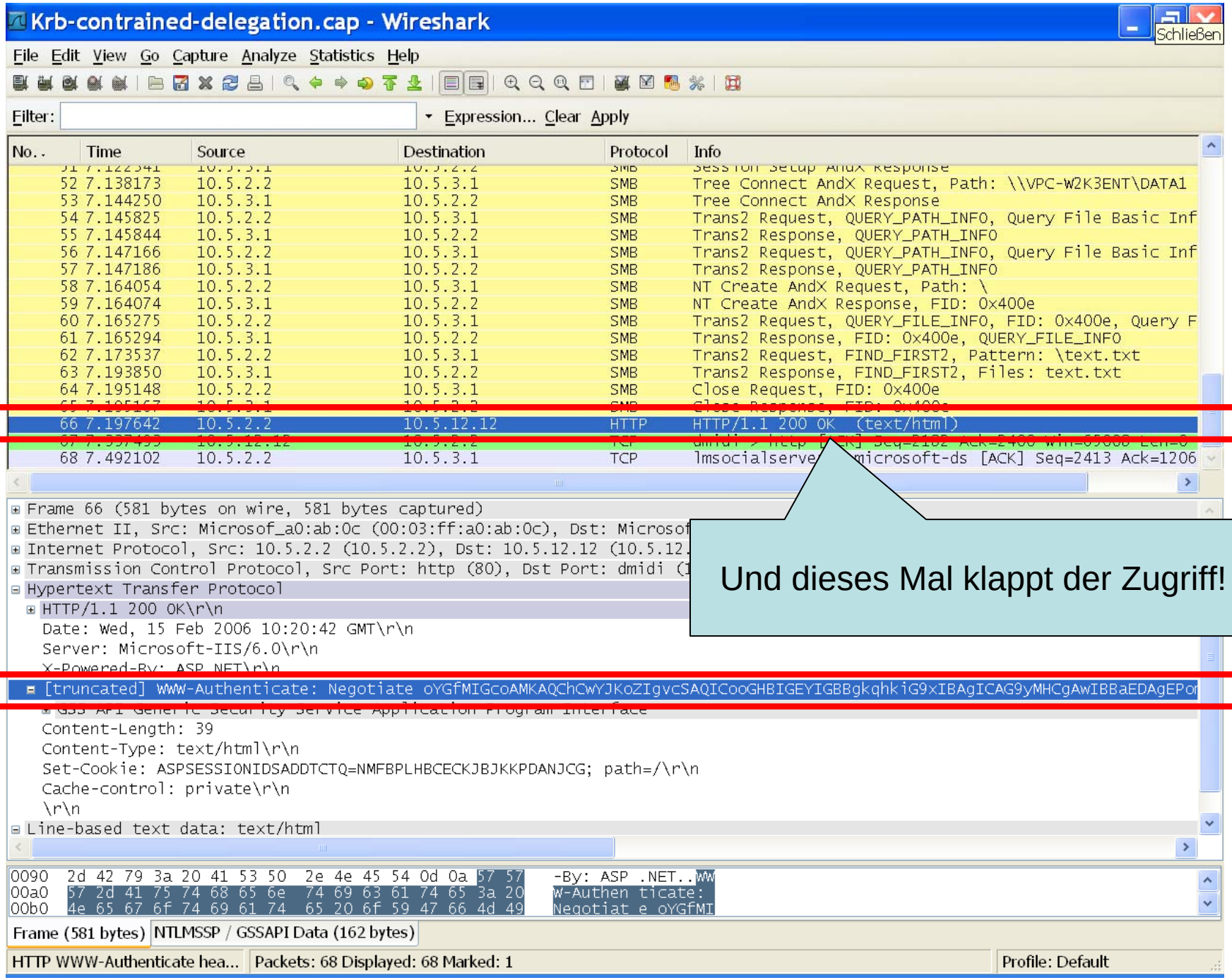

Krb-contrained-delegation.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
2 6.822555 Microsof_a7:ab:0c Broadcast ARP Who has 10.5.2.2? Tell 10.5.12.12
3 6.825955 Microsof_a0:ab:0c Microsof_a7:ab:0c ARP 10.5.2.2 is at 00:03:ff:a0:ab:0c
4 6.826098 10.5.12.12 10.5.2.2 TCP dmidi > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5 6.826889 10.5.2.2 10.5.12.12 TCP http > dmidi [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 M
6 6.827085 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 6.827797 10.5.12.12 10.5.2.2 HTTP GET /1.asp HTTP/1.1
8 6.831687 10.5.2.2 10.5.12.12 TCP [TCP segment of a reassembled PDU]
9 6.831733 10.5.2.2 10.5.12.12 HTTP HTTP/1.1 401 Unauthorized (text/html)
11 6.849438 10.5.12.12 10.5.3.1 KRB5 AS-REQ
13 6.903524 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.
Tell 10.5.3.1
14 6.903580 Microsof_a7:ab:0c Microsof_a6:ab:0c ARP 10.5.12.12 i
:03:ff:a7:ab:0c
15 6.906734 10.5.3.1 10.5.12.12 KRB5 AS-REP
16 6.909274 10.5.12.12 10.5.3.1 KRB5 TGS-REQ
17 6.950124 10.5.3.1 10.5.12.12 KRB5
Frame 11 (351 bytes on wire, 351 bytes captured)
Ethernet II, Src: Microsof_a7:ab:0c (00:03:ff:a7:ab:0c), Dst: Microsof
Internet Protocol, Src: 10.5.12.12 (10.5.12.12), Dst: 10.5.3.1 (10.5.
User Datagram Protocol, Src Port: scol (1200), Dst Port: kerberos (88)
Kerberos AS-REQ
Pvno: 5
MSG Type: AS-REQ (10)
padata: PA-ENC-TIMESTAMP PA-PAC-REQUEST
KDC_REQ_BODY
Padding: 0
Client Name (Principal): Administrator
Server Name (Service and Instance): krbtgt/DENYDC.COM
till: 2037-09-13 02:48:05 (UTC)
rtime: 2037-09-13 02:48:05 (UTC)
Nonce: 2065316899
Encryption Types: rc4-hmac rc4-hmac-old rc4-md4 des-cbc-md5 des-cbc-crc rc4-hmac-exp rc4-hmac-old-exp
00a0 30 81 bc a0 07 03 05 00 40 81 00 10 a1 1a 30 18 0....... @.....0.
00b0 a0 03 02 01 01 a1 11 30 0f 1b 0d 41 64 6d 69 6e ....0 ...Admin
00c0 69 73 74 72 61 74 6f 72 a2 0c 1b 0a 44 45 4e 59 istrator ....DENY
00d0 44 43 2e 43 4f 4d a3 1f 30 1d a0 03 02 01 02 a1 DC.COM.. 0.......
The name part of the client pri...
Packets: 68 Displayed: 68 Marked: 1
Profile: Default
Client kontaktiert Kerberos Authentication Server (10.5.3.1)


Krb-contrained-delegation.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
2 6.822555 Microsof_a7:ab:0c Broadcast ARP Who has 10.5.2.2? Tell 10.5.12.12
3 6.825955 Microsof_a0:ab:0c Microsof_a7:ab:0c ARP 10.5.2.2 is at 00:03:ff:a0:ab:0c
4 6.826098 10.5.12.12 10.5.2.2 TCP dmidi > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5 6.826889 10.5.2.2 10.5.12.12 TCP http > dmidi [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 M
6 6.827085 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 6.827797 10.5.12.12 10.5.2.2 HTTP GET /1.asp HTTP/1.1
8 6.831687 10.5.2.2 10.5.12.12 TCP [TCP segment of a reassembled PDU]
9 6.831733 10.5.2.2 10.5.12.12 HTTP HTTP/1.1 401 Unauthorized (text/html)
10 6.831792 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=222 Ack=1873 Win=65535 Len=0
11 6.849438 10.5.12.12 10.5.3.1 KRB5 AS-REQ
12 6.883497 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
13 6.903524 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.12.12? Tell 10.5.3.1
15 6.906734 10.5.3.1 10.5.12.12 KRB5 AS-REP
17 6.950124 10.5.3.1 10.5.12.12 KRB5 TGS-REP
Frame 15 (1377 bytes on wire, 1377 bytes captured)
Ethernet II, Src: Microsof_a6:ab:0c (00:03:ff:a6:ab:0c), Dst: Microsof
Internet Protocol, Src: 10.5.3.1 (10.5.3.1), Dst: 10.5.12.12 (10.5.12.
User Datagram Protocol, Src Port: kerberos (88), Dst Port: scol (1200)
Kerberos AS-REP
Pvno: 5
Client Realm: DENYDC.COM
Client Name (Principal): Administrator
Ticket
Tkt-vno: 5
Realm: DENYDC.COM
enc-part rc4-hmac
enc-part rc4-hmac
0040 44 45 4e 59 44 43 2e 43 4f 4d a4 1a 30 18 a0 03 DENYDC.C OM..0...
0050 02 01 01 a1 11 30 0f 1b 0d 41 64 6d 69 6e 69 73 .....0.. .Adminis
0060 74 72 61 74 6f 72 a5 82 03 c6 61 82 03 c2 30 82 trator.. ..a...0.
0070 03 be a0 03 02 01 05 a1 0c 1b 0a 44 45 4e 59 44 ....DENYD
The name part of the client pri...
Packets: 68 Displayed: 68 Marked: 1
Profile: Default
Authentication Server schickt Ticket Granting Ticket an Client


Krb-contrained-delegation.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
2 6.822555 Microsof_a7:ab:0c Broadcast ARP Who has 10.5.2.2? Tell 10.5.12.12
3 6.825955 Microsof_a0:ab:0c Microsof_a7:ab:0c ARP 10.5.2.2 is at 00:03:ff:a0:ab:0c
4 6.826098 10.5.12.12 10.5.2.2 TCP dmidi > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5 6.826889 10.5.2.2 10.5.12.12 TCP http > dmidi [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 M
6 6.827085 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 6.827797 10.5.12.12 10.5.2.2 HTTP GET /1.asp HTTP/1.1
8 6.831687 10.5.2.2 10.5.12.12 TCP [TCP segment of a reassembled PDU]
9 6.831733 10.5.2.2 10.5.12.12 HTTP HTTP/1.1 401 Unauthorized (text/html)
10 6.831792 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=222 Ack=1873 Win=65535 Len=0
11 6.849438 10.5.12.12 10.5.3.1 KRB5 AS-REQ
12 6.883497 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
13 6.903524 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.12.12? Tell 10.5.3.1
14 6.903580 Microsof_a7:ab:0c Microsof_a6:ab:0c ARP 10.5.12.12 is at 00:03:ff:a7:ab:0c
16 6.909274 10.5.12.12 10.5.3.1 KRB5 TGS-REQ
Frame 16 (1357 bytes on wire, 1357 bytes captured)
Ethernet II, Src: Microsof_a7:ab:0c (00:03:ff:a7:ab:0c), Dst: Microsof
Internet Protocol, Src: 10.5.12.12 (10.5.12.12), Dst: 10.5.3.1 (10.5.3
User Datagram Protocol, Src Port: nucleus-sand (1201), Dst Port: kerbe
Kerberos TGS-REQ
Pvno: 5
MSG Type: TGS-REQ (12)
padata: PA-TGS-REQ
KDC_REQ_BODY
Padding: 0
KDCOptions: 40800000 (Forwardable, Renewable)
Server Name (Service and Instance): HTTP/upwin2003.denyDC.com
Nonce: 2066706949
Encryption Types: rc4-hmac rc4-hmac-old rc4-md4 des-cbc-md5 des-cbc-crc rc4-hmac-exp rc4-hmac-old-exp
04e0 a2 0c 1b 0a 44 45 4e 59 44 43 2e 43 4f 4d a3 27 ....DENY DC.COM.'
04f0 30 25 a0 03 02 01 02 a1 1e 30 1c 1b 04 48 54 54 0%..... .0...HTT
0500 50 1b 14 75 70 77 69 6e 32 30 30 33 2e 64 65 6e P..upwin 2003.den
0510 79 44 43 2e 63 6f 6d a5 11 18 0f 32 30 33 37 30 yDC.com. ...20370
This is the name part server's ...
Packets: 68 Displayed: 68 Marked: 1
Profile: Default
1. Client wendet sich mit Ticket Granting Ticket an Ticket Granting Server (auch 10.5.3.1).
2. Ticket Anfrage für upwin2003


Krb-contrained-delegation.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
2 6.822555 Microsof_a7:ab:0c Broadcast ARP Who has 10.5.2.2? Tell 10.5.12.12
3 6.825955 Microsof_a0:ab:0c Microsof_a7:ab:0c ARP 10.5.2.2 is at 00:03:ff:a0:ab:0c
4 6.826098 10.5.12.12 10.5.2.2 TCP dmidi > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5 6.826889 10.5.2.2 10.5.12.12 TCP http > dmidi [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 M
6 6.827085 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 6.827797 10.5.12.12 10.5.2.2 HTTP GET /1.asp HTTP/1.1
8 6.831687 10.5.2.2 10.5.12.12 TCP [TCP segment of a reassembled PDU]
9 6.831733 10.5.2.2 10.5.12.12 HTTP HTTP/1.1 401 Unauthorized (text/html)
10 6.831792 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=222 Ack=1873 Win=65535 Len=0
11 6.849438 10.5.12.12 10.5.3.1 KRB5 AS-REQ
12 6.883497 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
13 6.903524 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.12.12? Tell 10.5.3.1
14 6.903580 Microsof_a7:ab:0c Microsof_a6:ab:0c ARP 10.5.12.12 is at 00:03:ff:a7:ab:0c
15 6.906734 10.5.3.1 10.5.12.12 KRB5 AS-REP
17 6.950124 10.5.3.1 10.5.12.12 KRB5 TGS-REP
Frame 17 (1334 bytes on wire, 1334 bytes captured)
Ethernet II, Src: Microsof_a6:ab:0c (00:03:ff:a6:ab:0c), Dst: Microsof_a7:ab:0c
Internet Protocol, Src: 10.5.3.1 (10.5.3.1), Dst: 10.5.12.12
User Datagram Protocol, Src Port: kerberos (88), Dst Port: nucleus-sar
Kerberos TGS-REP
Pvno: 5
MSG Type: TGS-REP (13)
Client Realm: DENYDC.COM
Client Name (Principal): Administrator
Ticket
Tkt-vno: 5
Realm: DENYDC.COM
Server Name (Service and Instance): HTTP/upwin2003.denyDC.com
enc-part rc4-hmac
enc-part rc4-hmac
0040 44 45 4e 59 44 43 2e 43 4f 4d a4 1a 30 18 a0 03 DENYDC.C OM..0...
0050 02 01 01 a1 11 30 0f 1b 0d 41 64 6d 69 6e 69 73 .....0.. .Adminis
0060 74 72 61 74 6f 72 a5 82 03 ce 61 82 03 ca 30 82 trator.. ..a...0.
0070 03 c6 a0 03 02 01 05 a1 0c 1b 0a 44 45 4e 59 44 ....DENYD
The name part of the client pri...
Packets: 68 Displayed: 68 Marked: 1
Profile: Default
Ticket Granting Server sendet
Client Ticket für upwin2003


Krb-contrained-delegation.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
10 6.831792 10.5.12.12 10.5.2.2 TCP dmidi > http [ACK] Seq=222 Ack=1873 Win=65535 Len=0
11 6.849438 10.5.12.12 10.5.3.1 KRB5 AS-REQ
12 6.883497 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.3.2? Tell 10.5.3.1
13 6.903524 Microsof_a6:ab:0c Broadcast ARP Who has 10.5.12.12? Tell 10.5.3.1
14 6.903580 Microsof_a7:ab:0c Microsof_a6:ab:0c ARP 10.5.12.12 is at 00:03:ff:a7:ab:0c
15 6.906734 10.5.3.1 10.5.12.12 KRB5 AS-REP
16 6.909274 10.5.12.12 10.5.3.1 KRB5 TGS-REQ
17 6.950124 10.5.3.1 10.5.12.12 KRB5 TGS-REP
19 6.955390 10.5.12.12 10.5.2.2 HTTP GET /1.asp HTTP/1.1
21 7.013702 10.5.2.2 10.5.3.1 TCP
22 7.013725 10.5.3.1 10.5.2.2 TCP
23 7.025295 10.5.2.2 10.5.3.1 TCP
24 7.025314 10.5.2.2 10.5.3.1 TCP
25 7.025335 10.5.2.2 10.5.3.1 KRB5
26 7.025357 10.5.3.1 10.5.2.2 TCP
Frame 19 (554 bytes on wire, 554 bytes captured)
Ethernet II, Src: Microsof_a7:ab:0c (00:03:ff:a7:ab:0c), Dst: Microsof
Internet Protocol, Src: 10.5.12.12 (10.5.12.12), Dst: 10.5.2.2 (10.5.2
Transmission Control Protocol, Src Port: dmidi (1199), Dst Port: http
[Reassembled TCP Segments (1960 bytes): #18(1460), #19(500)]
Hypertext Transfer Protocol
GET /1.asp HTTP/1.1\r\n
Accept: */*\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)\r\n
Host: upwin2003\r\n
[truncated] Authorization: Negotiate YIIE/gYGKwYBBQUCoIIE8jCCB06gJDAiBgkqhkiC9xIBAgIGCSqGSIb3EgECAgYKKwYBBAGCNwICCqKCBMQEggT
\r\n
00d0 65 65 70 2d 41 6c 69 76 65 0d 0a 41 75 74 68 6f eep-Aliv e..Autho
00e0 72 69 7a 61 74 69 6f 6e 3a 20 4e 65 67 6f 74 69 rization : Negoti
00f0 61 74 65 20 59 49 49 45 2f 67 59 47 4b 77 59 42 ate YIIE /gYGKwYB
Frame (554 bytes) Reassembled TCP (1960 bytes) NTLMSSP / GSSAPI Data (1282 bytes)
HTTP Authorization header (ht... Packets: 68 Displayed: 68 Marked: 1 Profile: Default
Client wendet sich erneut an Webserver upwin2003. Jetzt mit Credential!


Krb-contrained-delegation.cap - Wireshark
Schließen
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
52 7.138173 10.5.2.2 10.5.3.1 SMB Tree Connect AndX Request, Path: \\VPC-W2K3ENT\DATA1
53 7.144250 10.5.3.1 10.5.2.2 SMB Tree Connect AndX Response
54 7.145825 10.5.2.2 10.5.3.1 SMB Trans2 Request, QUERY_PATH_INFO, Query File Basic Inf
55 7.145844 10.5.3.1 10.5.2.2 SMB Trans2 Response, QUERY_PATH_INFO
56 7.147166 10.5.2.2 10.5.3.1 SMB Trans2 Request, QUERY_PATH_INFO, Query File Basic Inf
57 7.147186 10.5.3.1 10.5.2.2 SMB Trans2 Response, QUERY_PATH_INFO
58 7.164054 10.5.2.2 10.5.3.1 SMB NT Create AndX Request, Path: \
59 7.164074 10.5.3.1 10.5.2.2 SMB NT Create AndX Response, FID: 0x400e
60 7.165275 10.5.2.2 10.5.3.1 SMB Trans2 Request, QUERY_FILE_INFO, FID: 0x400e, Query F
61 7.165294 10.5.3.1 10.5.2.2 SMB Trans2 Response, FID: 0x400e, QUERY_FILE_INFO
62 7.173537 10.5.2.2 10.5.3.1 SMB Trans2 Request, FIND_FIRST2, Pattern: \text.txt
63 7.193850 10.5.3.1 10.5.2.2 SMB Trans2 Response, FIND_FIRST2, Files: text.txt
64 7.195148 10.5.2.2 10.5.3.1 SMB Close Request, FID: 0x400e
66 7.197642 10.5.2.2 10.5.12.12 HTTP HTTP/1.1 200 OK (text/html)
68 7.492102 10.5.2.2 10.5.3.1 TCP
Frame 66 (581 bytes on wire, 581 bytes captured)
Ethernet II, Src: Microsof_a0:ab:0c (00:03:ff:a0:ab:0c), Dst: Microsof
Internet Protocol, Src: 10.5.2.2 (10.5.2.2), Dst: 10.5.12.12 (10.5.12.
Transmission Control Protocol, Src Port: http (80), Dst Port: dmidi (1
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Wed, 15 Feb 2006 10:20:42 GMT\r\n
Server: Microsoft-IIS/6.0\r\n
X-Powered-By: ASP.NET\r\n
[truncated] WWW-Authenticate: Negotiate oYGfMIGcoAMKAQChCwYJKoZIgvcSAQICooGHBIGEYIGBBgkqhkiG9xIBAgICAG9yMHCgAwIBBaEDAgEPor
Content-Length: 39
Content-Type: text/html\r\n
Set-Cookie: ASPSESSIONIDSADDTCTQ=NMFBPLHBCECKJBJKKPDANJCG; path=/\r\n
Cache-control: private\r\n
\r\n
Line-based text data: text/html
0090 2d 42 79 3a 20 41 53 50 2e 4e 45 54 0d 0a 57 57 -By: ASP .NET..WW
00a0 57 2d 41 75 74 68 65 6e 74 69 63 61 74 65 3a 20 W-Authen ticate:
00b0 4e 65 67 6f 74 69 61 74 65 20 6f 59 47 66 4d 49 Negotiat e oYGfMI
Frame (581 bytes)
NTLMSSP / GSSAPI Data (162 bytes)
HTTP WWW-Authenticate hea...
Packets: 68 Displayed: 68 Marked: 1
Profile: Default
Und dieses Mal klappt der Zugriff!

Mal selber reinschauen?

- Wireshark installieren
  - http://www.wireshark.org/download.html
- Sample Trace runterladen
  - http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=view&target=constained-delegation.zip
  - jede Menge mehr Sample Traces auf http://wiki.wireshark.org/SampleCaptures