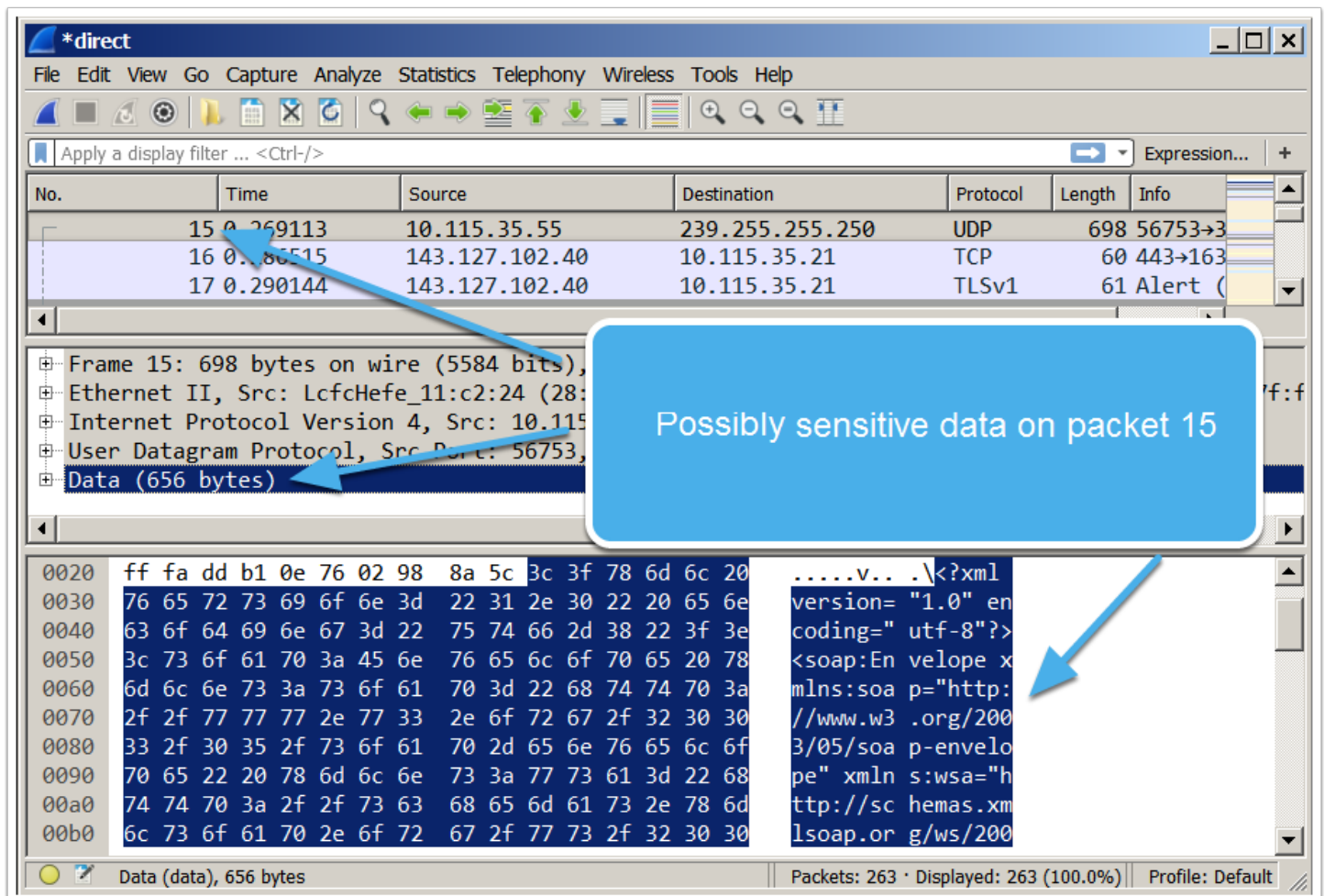


Prepare the Tool Bittwist

Download the tool bittwist from <http://bittwist.sourceforge.net/>

1. bittwist-win-2.0.zip (MD5 = 038a9994ec8248649904d9736509a108)
 - Take the file `bittwist-win-2.0\src\bittwiste.exe` and copy it into `C:\bittwist\bittwiste.exe`
2. cygwin1.zip
 - Take the file `cygwin1\cygwin1.dll` and copy it into `C:\bittwist\cygwin1.dll`

Capture your Traffic in Wireshark



The screenshot shows the Wireshark interface with a packet list table and a detailed view of packet 15. A blue callout box highlights the data field of packet 15, indicating it contains sensitive information.

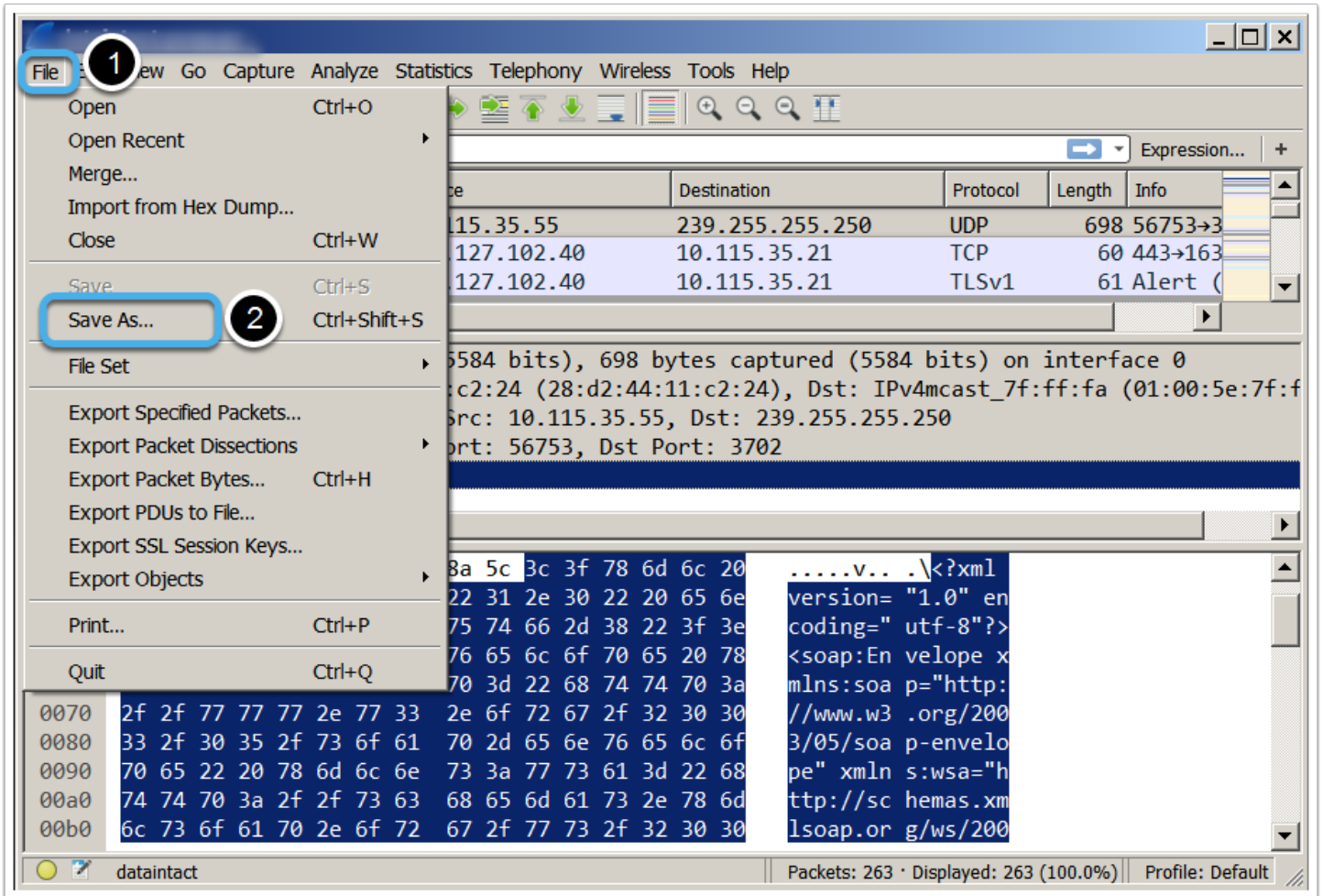
No.	Time	Source	Destination	Protocol	Length	Info
15	0.269113	10.115.35.55	239.255.255.250	UDP	698	56753→3
16	0.286515	143.127.102.40	10.115.35.21	TCP	60	443→163
17	0.290144	143.127.102.40	10.115.35.21	TLSv1	61	Alert (

Frame 15: 698 bytes on wire (5584 bits),
 Ethernet II, Src: LcfcHefe_11:c2:24 (28:
 Internet Protocol Version 4, Src: 10.115
 User Datagram Protocol, Src Port: 56753,
 Data (656 bytes)

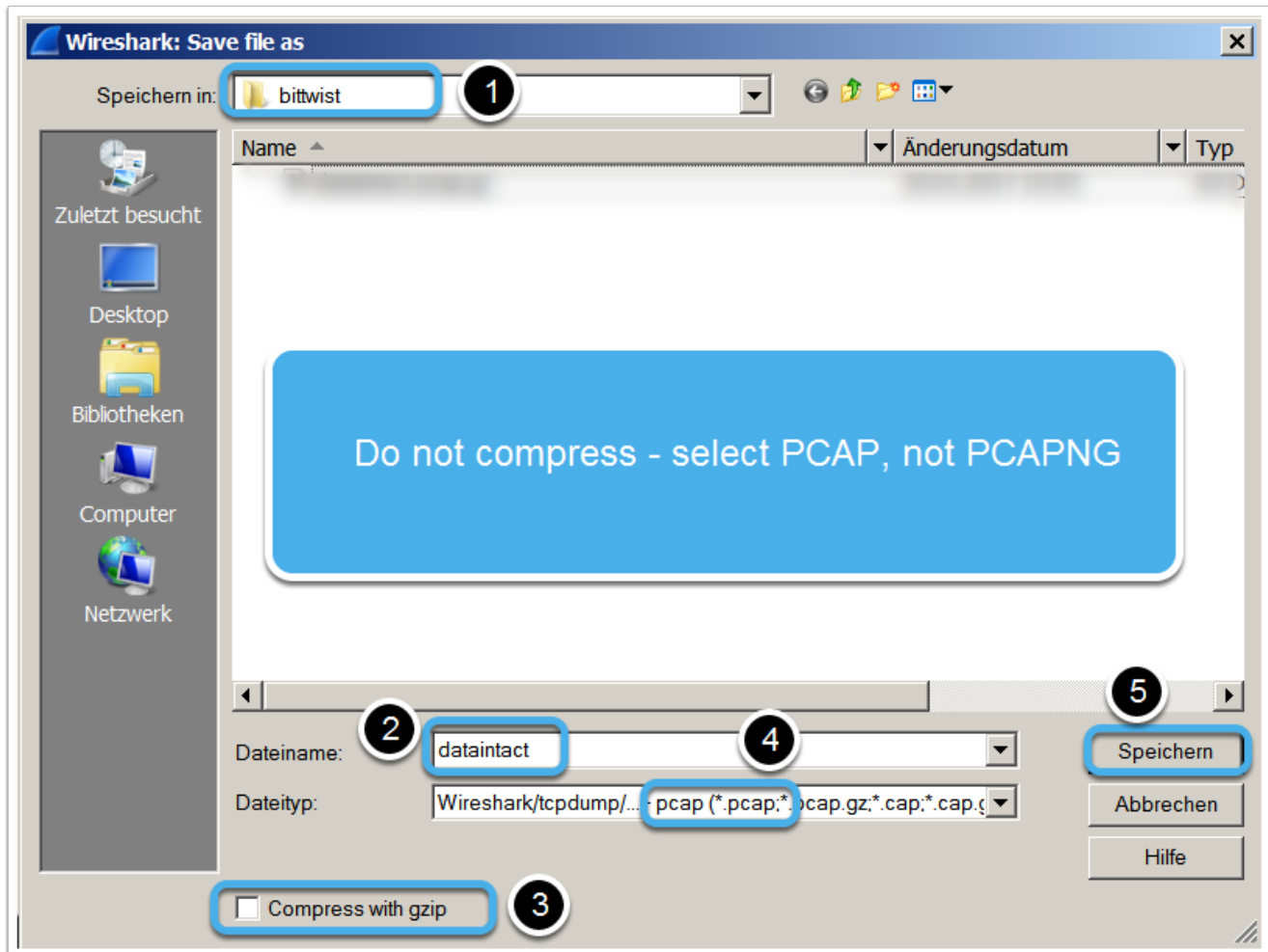
```

.....v... \<?xml
version= "1.0" en
coding=" utf-8"?>
<soap:Envelope x
xmlns:soap="http:
//www.w3 .org/200
3/05/soap-envelope
pe" xmlns:wsa="h
ttp://schemas.xml
soap.org/ws/200
  
```

Save

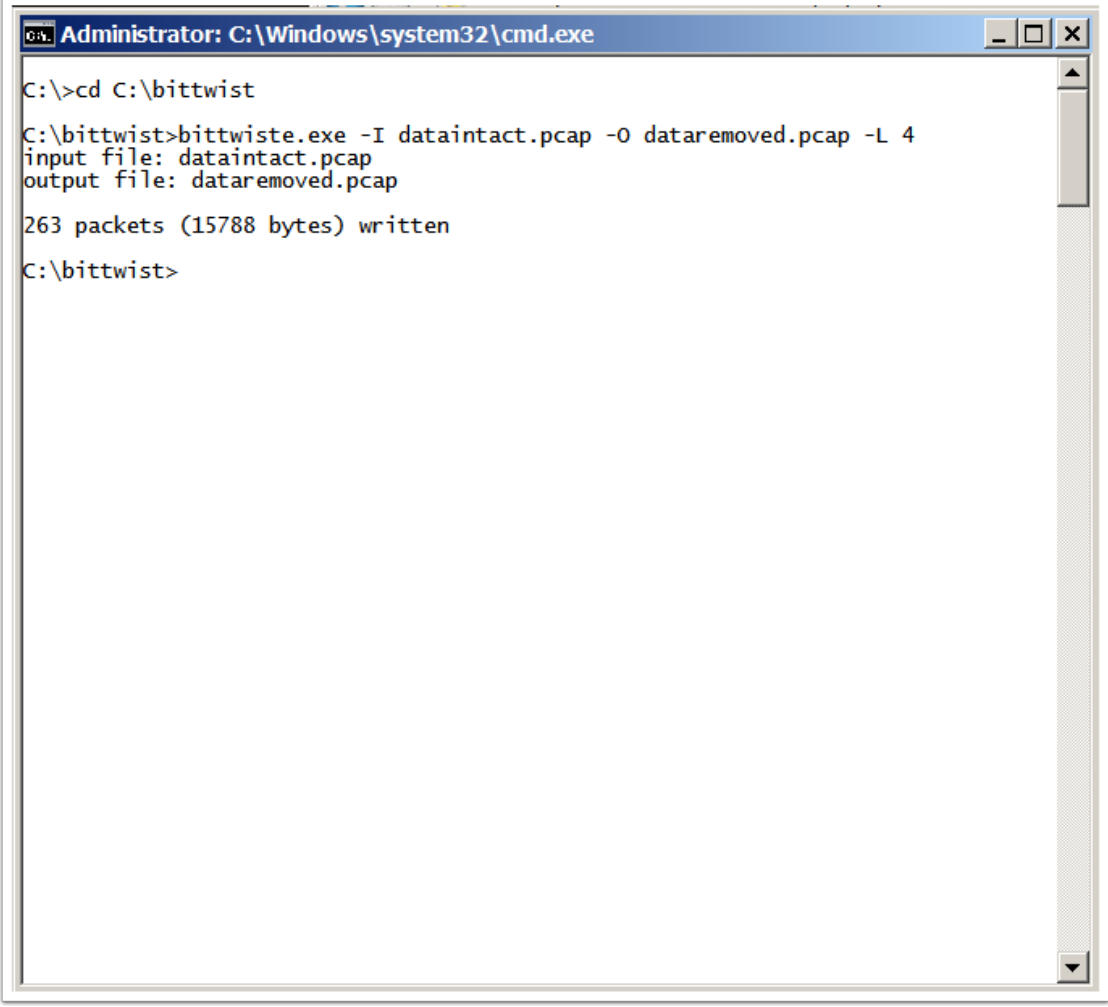


Uncompressed PCAP



Strip Data

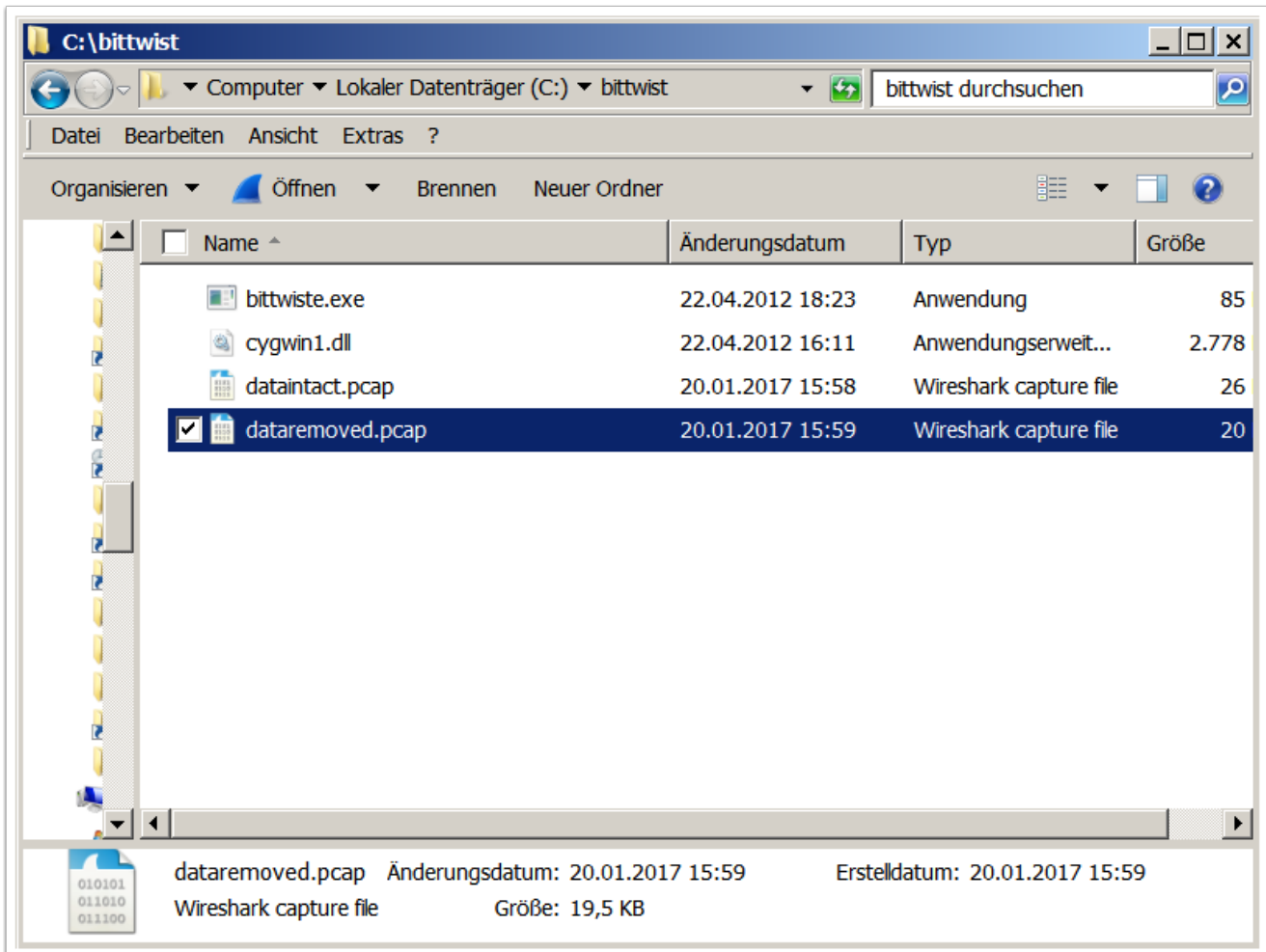
```
cd C:\bittwist  
bittwiste.exe -I dataintact.pcap -O dataremoved.pcap -L 4
```



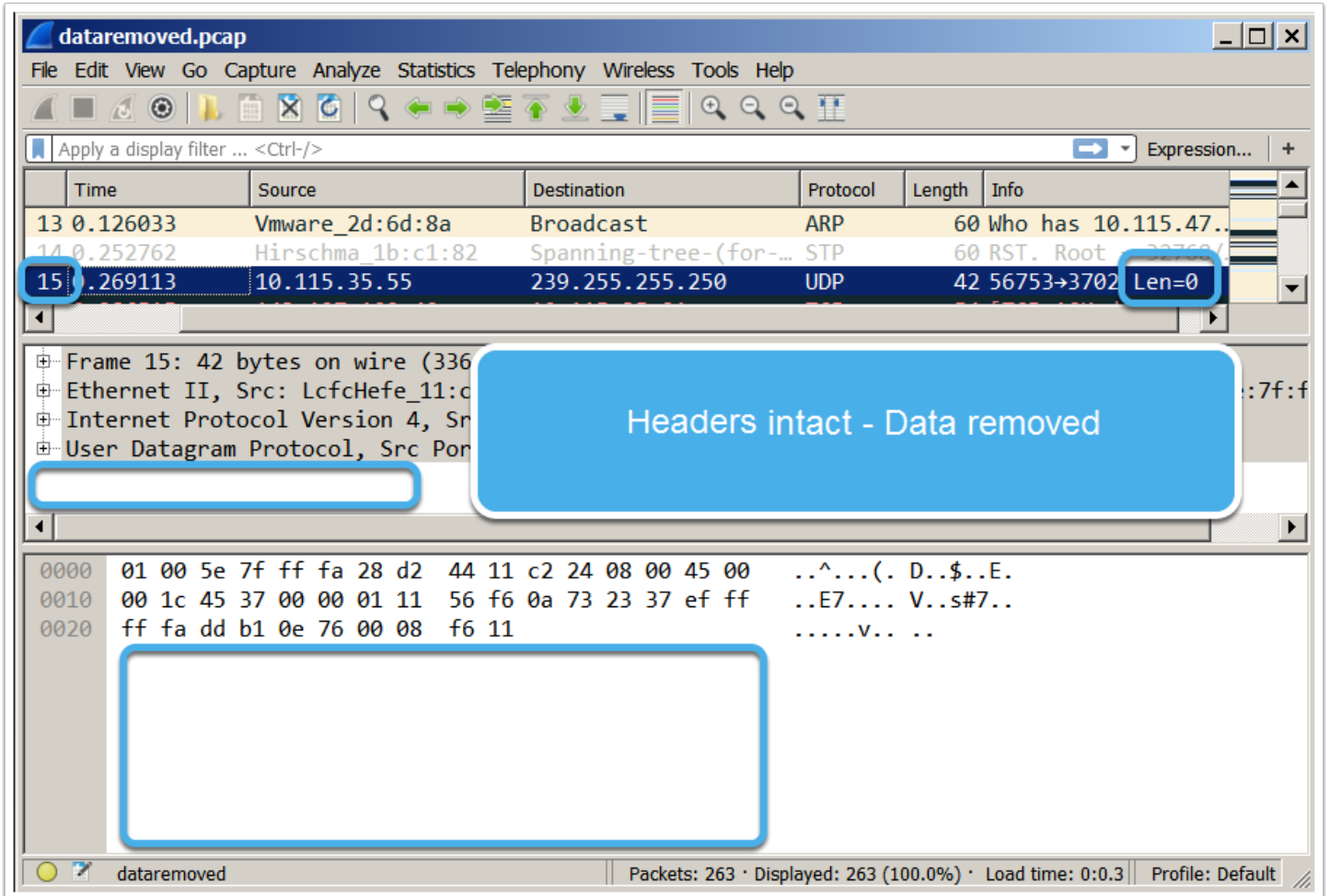
The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window content is as follows:

```
C:\>cd C:\bittwist  
C:\bittwist>bittwiste.exe -I dataintact.pcap -O dataremoved.pcap -L 4  
input file: dataintact.pcap  
output file: dataremoved.pcap  
263 packets (15788 bytes) written  
C:\bittwist>
```

Open the New File



Verify Data is Removed



The image shows a Wireshark window titled "dataremoved.pcap". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a display filter field. A table of captured packets is visible, with packet 15 selected. The packet details pane shows the structure of the frame: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. A blue callout box with the text "Headers intact - Data removed" is overlaid on the packet details pane. The packet bytes pane shows the raw data in hexadecimal and ASCII, with a large white rectangular redaction box covering the data portion of the packet.

Time	Source	Destination	Protocol	Length	Info
13 0.126033	Vmware_2d:6d:8a	Broadcast	ARP	60	Who has 10.115.47..
14 0.252762	Hirschma_1b:c1:82	Spanning-tree-(for-...	STP	60	RST. Root 22769/
15 0.269113	10.115.35.55	239.255.255.250	UDP	42	56753→3702 Len=0

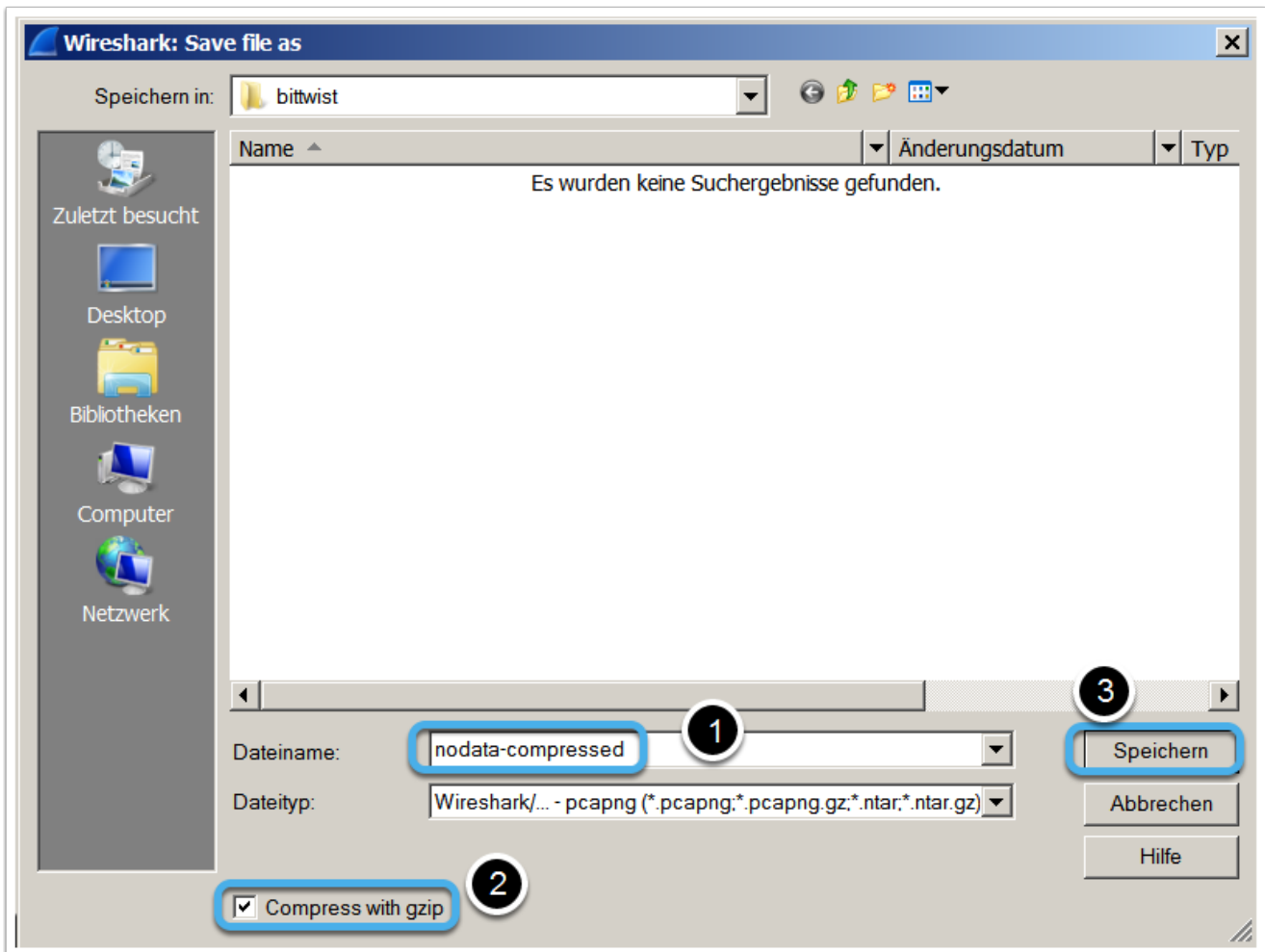
Frame 15: 42 bytes on wire (336 bytes captured) on interface 0:00:00:00:00:00

- Ethernet II, Src: LcfcHefe_11:c1:82, Dst: 01:00:5e:7f:ff:fa
- Internet Protocol Version 4, Src: 10.115.35.55, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 56753, Dst Port: 3702

0000 01 00 5e 7f ff fa 28 d2 44 11 c2 24 08 00 45 00 ..^...(. D..\$.E.
0010 00 1c 45 37 00 00 01 11 56 f6 0a 73 23 37 ef ff ..E7.... V..s#7..
0020 ff fa dd b1 0e 76 00 08 f6 11V... ..

dataremoved | Packets: 263 · Displayed: 263 (100.0%) · Load time: 0:0.3 | Profile: Default

Save Compressed Data for Easier Transfer to Support Portals



Upload to the Hirschmann Support

<https://hirschmann-support.belden.eu.com/>

