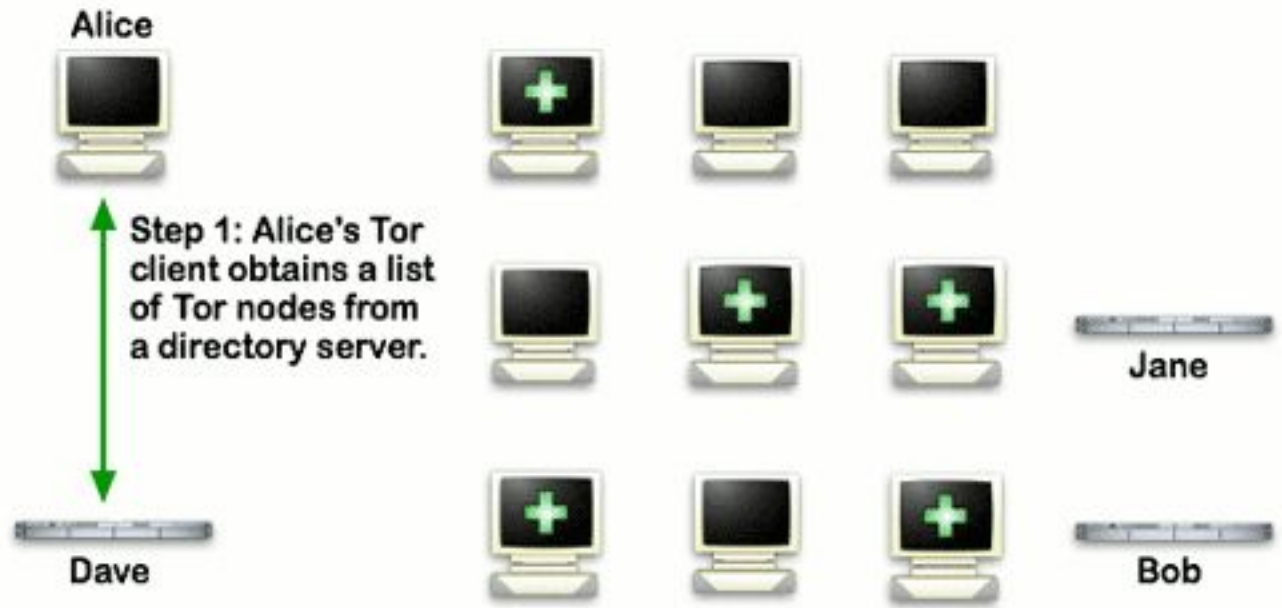


# Анонимная сеть TOR

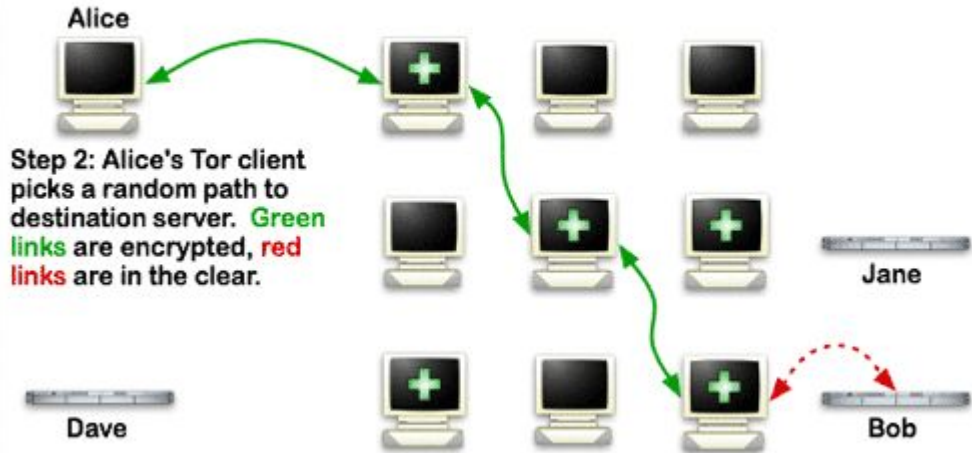
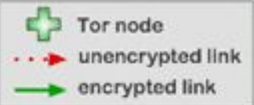
Выполнил студент группы

Принцип работы Tor основан на идее так называемой "Луковой Маршрутизации" (Onion Routing), которая была предложена еще в середине 90-х годов и запатентована Военно-морскими силами США. Весь смысл в том, что если клиент будет общаться с сервером не напрямую, а через цепочку посредников, каждому из которых известны только следующее и предыдущее звенья цепочки - отследить истинный источник и приемник данных (одновременно) будет невозможно в любом звене цепи.

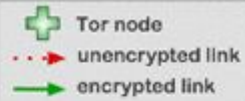
# How Tor Works: 1



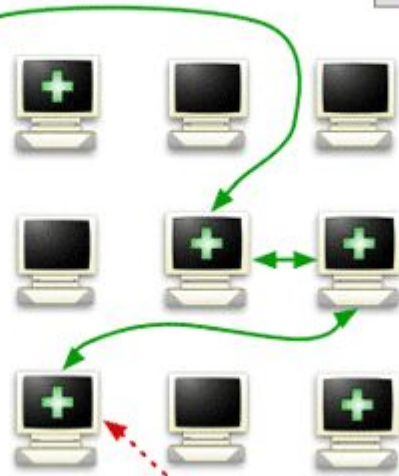
# How Tor Works: 2



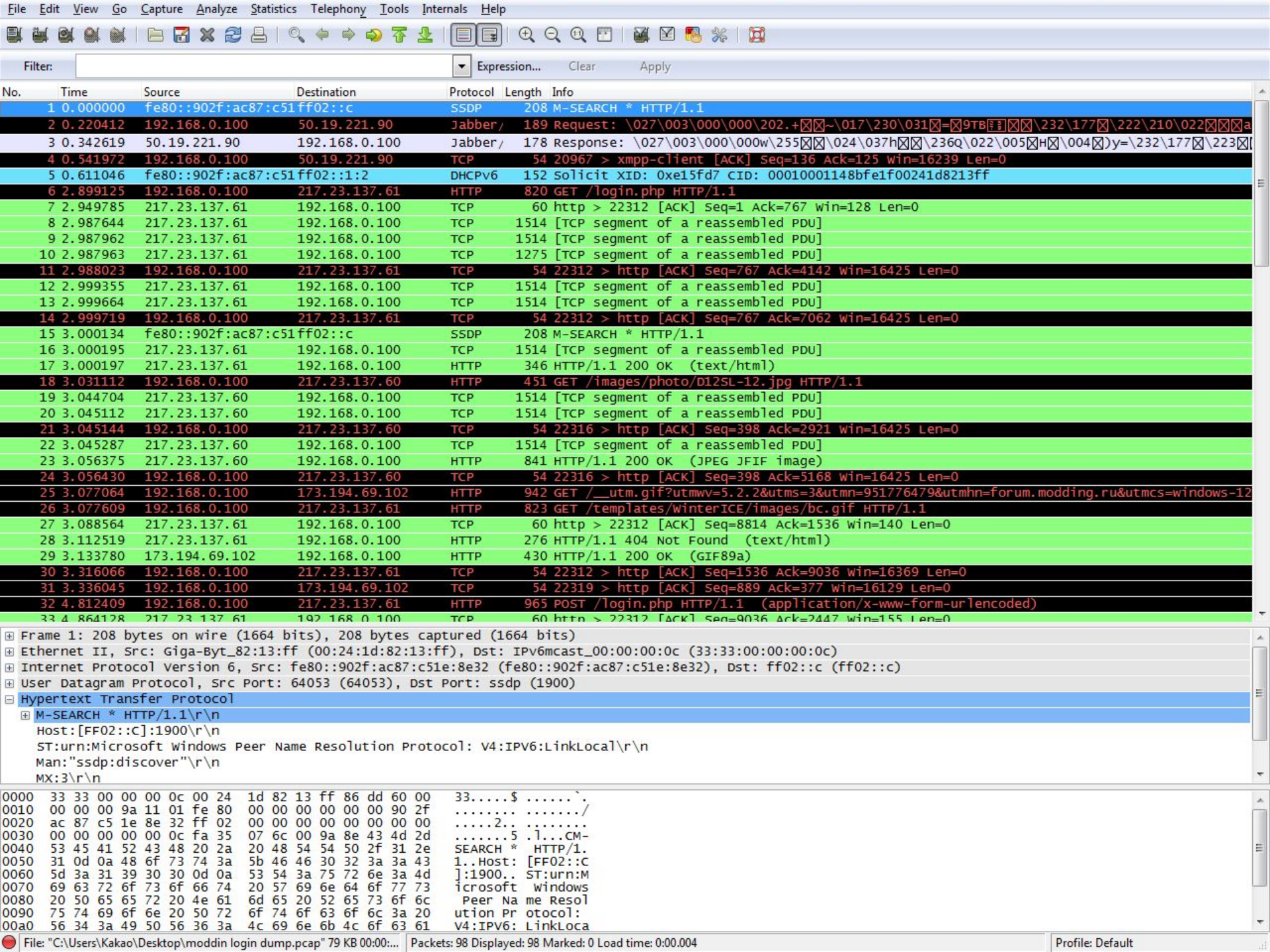
## How Tor Works: 3



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Перехват трафика



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::902f:ac87:c51ff02::c	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
2	0.220412	192.168.0.100	50.19.221.90	Jabber/	189	Request: \027\003\000\000\202.+ [unprintable] \017\230\031 [unprintable] \09T [unprintable] \232\177 [unprintable] \222\210\022 [unprintable] \a
3	0.342619	50.19.221.90	192.168.0.100	Jabber/	178	Response: \027\003\000\000w\255 [unprintable] \024\037h [unprintable] \236q\022\005 [unprintable] H [unprintable] \004 [unprintable] y=\232\177 [unprintable] \223 [unprintable]
4	0.541972	192.168.0.100	50.19.221.90	TCP	54	20967 > xmpp-client [ACK] Seq=136 Ack=125 win=16239 Len=0
5	0.611046	fe80::902f:ac87:c51ff02::1:2	ff02::1:2	DHCPv6	152	solicit XID: 0xe15fd7 CID: 00010001148bfe1f00241d8213ff
6	2.899125	192.168.0.100	217.23.137.61	HTTP	820	GET /login.php HTTP/1.1
7	2.949785	217.23.137.61	192.168.0.100	TCP	60	http > 22312 [ACK] Seq=1 Ack=767 win=128 Len=0
8	2.987644	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
9	2.987962	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
10	2.987963	217.23.137.61	192.168.0.100	TCP	1275	[TCP segment of a reassembled PDU]
11	2.988023	192.168.0.100	217.23.137.61	TCP	54	22312 > http [ACK] Seq=767 Ack=4142 win=16425 Len=0
12	2.999355	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
13	2.999664	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
14	2.999719	192.168.0.100	217.23.137.61	TCP	54	22312 > http [ACK] Seq=767 Ack=7062 win=16425 Len=0
15	3.000134	fe80::902f:ac87:c51ff02::c	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
16	3.000195	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
17	3.000197	217.23.137.61	192.168.0.100	HTTP	346	HTTP/1.1 200 OK (text/html)
18	3.031112	192.168.0.100	217.23.137.60	HTTP	451	GET /images/photo/DI2SL-12.jpg HTTP/1.1
19	3.044704	217.23.137.60	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
20	3.045112	217.23.137.60	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
21	3.045144	192.168.0.100	217.23.137.60	TCP	54	22316 > http [ACK] Seq=398 Ack=2921 win=16425 Len=0
22	3.045287	217.23.137.60	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
23	3.056375	217.23.137.60	192.168.0.100	HTTP	841	HTTP/1.1 200 OK (JPEG JFIF image)
24	3.056430	192.168.0.100	217.23.137.60	TCP	54	22316 > http [ACK] Seq=398 Ack=5168 win=16425 Len=0
25	3.077064	192.168.0.100	173.194.69.102	HTTP	942	GET /__utm.gif?utmwv=5.2.2&utms=3&utm=951776479&utmhn=forum.modding.ru&utmc=windows-12
26	3.077609	192.168.0.100	217.23.137.61	HTTP	823	GET /templates/winterICE/images/bc.gif HTTP/1.1
27	3.088564	217.23.137.61	192.168.0.100	TCP	60	http > 22312 [ACK] Seq=8814 Ack=1536 win=140 Len=0
28	3.112519	217.23.137.61	192.168.0.100	HTTP	276	HTTP/1.1 404 Not Found (text/html)
29	3.133780	173.194.69.102	192.168.0.100	HTTP	430	HTTP/1.1 200 OK (GIF89a)
30	3.316066	192.168.0.100	217.23.137.61	TCP	54	22312 > http [ACK] Seq=1536 Ack=9036 win=16369 Len=0
31	3.336045	192.168.0.100	173.194.69.102	TCP	54	22319 > http [ACK] Seq=889 Ack=377 win=16129 Len=0
32	4.812409	192.168.0.100	217.23.137.61	HTTP	965	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
33	4.864128	217.23.137.61	192.168.0.100	TCP	60	http > 22312 [ACK] Seq=9036 Ack=2447 win=155 Len=0

[E] Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)  
 [E] Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: IPv6mcast\_00:00:00:0c (33:33:00:00:00:0c)  
 [E] Internet Protocol Version 6, Src: fe80::902f:ac87:c51e:8e32 (fe80::902f:ac87:c51e:8e32), Dst: ff02::c (ff02::c)  
 [E] User Datagram Protocol, Src Port: 64053 (64053), Dst Port: sssdp (1900)  
 [E] Hypertext Transfer Protocol  
 [E] M-SEARCH \* HTTP/1.1\r\n
 Host: [FF02::C]:1900\r\n
 ST:urn:microsoft-windows:peer-name-resolution-protocol-v4:ipv6:link-local\r\n
 Man: "ssdp:discover"\r\n
 MX:3\r\n

```

0000 33 33 00 00 00 0c 00 24 1d 82 13 ff 86 dd 60 00 33.....$ .....
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 90 2f ...../
0020 ac 87 c5 1e 8e 32 ff 02 00 00 00 00 00 00 00 00 .....2..
0030 00 00 00 00 00 0c fa 35 07 6c 00 9a 8e 43 4d 2d .....5 .l...CM-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1..Host: [FF02::C
0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 72 6e 3a 4d ]:1900.. ST:urn:M
0070 69 63 72 6f 73 6f 6e 74 20 57 69 6e 64 6f 77 73 icrosoft win
0080 20 50 65 65 72 20 4e 61 6d 65 20 52 65 73 6f 6c Peer Na me Resol
0090 75 74 69 6f 6e 20 50 72 6f 74 6f 63 6f 6c 3a 20 ution Pr otocol:
00a0 56 34 3a 49 50 56 36 3a 4c 69 6e 6b 4c 6f 63 61 v4:IPV6: LinkLoca
  
```





No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::902f:ac87:c51ff02::c	50.19.221.90	SSDP	208	M-SEARCH * HTTP/1.1
2	0.220412	192.168.0.100	50.19.221.90	Jabber/	189	Request: \027\003\000\000\202.+~\017\230\031=9T\232\177\222\210\022
3	0.342619	50.19.221.90	192.168.0.100	Jabber/	178	Response: \027\003\000\000w\255\024\037h\236Q\022\005H\004)y=\232\177\223
4	0.541972	192.168.0.100	50.19.221.90	TCP	54	20967 > xmpp-client [ACK] Seq=136 Ack=125 win=16239 Len=0
5	0.611046	fe80::902f:ac87:c51ff02::1:2	217.23.137.61	DHCPv6	152	solicit XID: 0xe15fd7 CID: 00010001148bfe1f00241d8213ff
6	2.899125	192.168.0.100	217.23.137.61	HTTP	820	GET /login.php HTTP/1.1
7	2.949785	217.23.137.61	192.168.0.100	TCP	60	http > 22312 [ACK] Seq=1 Ack=767 win=128 Len=0
8	2.987644	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
9	2.987962	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
10	2.987963	217.23.137.61	192.168.0.100	TCP	1275	[TCP segment of a reassembled PDU]
11	2.988023	192.168.0.100	217.23.137.61	TCP	54	22312 > http [ACK] Seq=767 Ack=4142 win=16425 Len=0
12	2.999355	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
13	2.999664	217.23.137.61	192.168.0.100	TCP	1514	[TCP segment of a reassembled PDU]
14	2.999719	192.168.0.100	217.23.137.61	TCP	54	22312 > http [ACK] Seq=767 Ack=7062 win=16425 Len=0
15	3.000134	fe80::902f:ac87:c51ff02::c	50.19.221.90	SSDP	208	M-SEARCH * HTTP/1.1

Frame 6: 820 bytes on wire (6560 bits), 820 bytes captured (6560 bits) on Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)

Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 217.23.137.61 (217.23.137.61)

Transmission Control Protocol, Src Port: 22312 (22312), Dst Port: http (80), Seq: 1, Ack: 1, Len: 766

Hypertext Transfer Protocol

GET /login.php HTTP/1.1\r\n

Host: forum.modding.ru\r\n

User-Agent: Mozilla/5.0 (windows NT 6.1; WOW64; rv:7.0.1) Gecko/20100101 Firefox/7.0.1\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

Accept-Language: ru,en;q=0.7,en-us;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Charset: windows-1251,utf-8;q=0.7,\*;q=0.7\r\n

DNT: 1\r\n

Connection: keep-alive\r\n

Referer: http://forum.modding.ru/\r\n

[truncated] cookie: nbnhh2mvsol data=a%3d%78%3d11%3d%22autoLoginid%22%38%3d0%3d%22%22%38%3d6%3d%22userid%22%38%3d-1%38%7D: nbnhh2mvsol sid=r096h

```

0000 1c af f7 49 94 c2 00 24 1d 82 13 ff 08 00 45 00 ...I...$ .....E.
0010 03 26 34 14 40 00 80 06 00 00 c0 a8 00 64 d9 17 .&4.@... ..d..
0020 89 3d 57 28 00 50 c4 aa 68 6f bb 33 50 49 50 18 .=w(.P.. ho.3PIP.
0030 3f a7 26 7a 00 00 47 45 54 20 2f 6c 6f 67 69 6e ?.&z..GE T /login
0040 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 .php HTT P/1.1..H
0050 6f 73 74 3a 20 66 6f 72 75 6d 2e 6d 6f 64 64 69 ost: for um.moddi
0060 6e 67 2e 72 75 0d 0a 55 73 65 72 2d 41 67 65 6e ng.ru..U ser-Agen
0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0080 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 windows NT 6.1;
0090 57 4f 57 36 34 3b 20 72 76 3a 37 2e 30 2e 31 29 wOw64; r v:7.0.1)
00a0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 gecko/2 0100101
00b0 46 69 72 65 66 6f 78 2f 37 2e 30 2e 31 0d 0a 41 Firefox/ 7.0.1..A
00c0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html
00d0 2c 61 70 70 7c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht
00e0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml,a pplicati
00f0 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a on/xml;q =0.9,*/*
0100 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c ;q=0.8.. Accept-L
0110 61 6e 67 75 61 67 65 3a 20 72 75 2c 65 6e 3b 71 anguage: ru,en;q
0120 3d 30 2e 37 2c 65 6e 2d 75 73 3b 71 3d 30 2e 33 =0.7,en- us;q=0.3
0130 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e ..Accept -Encodin
0140 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 g: gzip, deflate
0150 0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73 65 74 ..Accept -Charset
0160 3a 20 77 69 6e 64 6f 77 73 2d 31 32 35 31 2c 75 ; window s-1251,u

```

Wireshark interface showing a network capture. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A 'Find Packet' dialog box is open, with the search filter set to 'a' and 'String' selected. The 'Packet details' pane shows the structure of a selected packet, including headers like User-Agent, Accept, and Content-Type, and a 'Line-based text data' section containing a form submission. The 'Packet bytes' pane shows the raw hex and ASCII data of the selected packet. Red arrows point to the search filter, the 'Line-based text data' section, and the form data in the hex pane.

No.	Time	Source	Destination	Protocol	Length	Info
25	3.077064	192.168.0.100	173.194.69.102	HTTP	942	GET /__utm.gif?utmwv=5.2.2&utms=3&utm=951776479&utmhn=forum.modding.ru&utmcs=windows-12
26	3.077609	192.168.0.100	217.23.137.61	HTTP	823	GET /templates/winterICE/images/bc.gif HTTP/1.1
27	3			HTTP	60	http > 22312 [ACK] Seq=8814 Ack=1536 win=140 Len=0
28	3			HTTP	276	HTTP/1.1 404 Not Found (text/html)
29	3			HTTP	430	HTTP/1.1 200 OK (GIF89a)
30	3			HTTP	54	22312 > http [ACK] Seq=1536 Ack=9036 win=16369 Len=0
31	3			HTTP	54	22319 > http [ACK] Seq=889 Ack=377 win=16129 Len=0
32	4			HTTP	585	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
33	4			HTTP	60	http > 22312 [ACK] Seq=9036 Ack=2447 win=155 Len=0
34	4			HTTP	588	HTTP/1.1 302 Moved Temporarily
35	4			HTTP	879	GET /index.php?sid=c607df0afb897deaaae14fb2816fb959 HTTP/1.1
36	4			HTTP	60	http > 22312 [ACK] Seq=9570 Ack=3272 win=169 Len=0
37	5			TCP	1514	[TCP segment of a reassembled PDU]
38	5			TCP	1514	[TCP segment of a reassembled PDU]
39	5			TCP	1275	[TCP segment of a reassembled PDU]

Find Packet dialog box:  
Find: a  
By:  Display filter  Hex value  String  
Search In:  Packet list  Packet details  Packet bytes  
String Options:  Case sensitive  
Character set: ASCII Unicode & Non-Unicode  
Direction:  Up  Down

Packet details:  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:7.0.1) Gecko/20100101 Firefox/7.0.1\r\n  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n  
Accept-Language: ru,en;q=0.7,en-us;q=0.3\r\n  
Accept-Encoding: gzip, deflate\r\n  
Accept-Charset: windows-1251,utf-8;q=0.7,\*;q=0.7\r\n  
DNT: 1\r\n  
Connection: keep-alive\r\n  
Referer: http://forum.modding.ru/login.php\r\n  
[truncated] cookie: phpbb2mysql\_data=a%3A2%3A%7B%3A1%3A%22auto\_loginid%22%3B%3A0%3A%22%22%3B%3A6%3A%22userid%22%3B%3A-1%3B%7D; phpbb2mysql\_sid=c096be  
Content-Type: application/x-www-form-urlencoded\r\n  
Content-Length: 66\r\n  
Full request URI: http://forum.modding.ru/login.php

Line-based text data: application/x-www-form-urlencoded  
username=A...

Packet bytes:  
0270 38 38 38 34 63 66 33 63 3b 20 5f 5f 75 74 6d 61 8884cf3c ; \_\_utma  
0280 3d 32 33 32 38 30 39 39 32 31 2e 36 30 31 37 32 =2328099 21.60172  
0290 39 37 39 34 2e 31 33 32 34 38 30 34 32 37 30 2e 9794.132 4804270.  
02a0 31 33 32 34 38 30 34 32 37 30 2e 31 33 32 34 38 13248042 70.13248  
02b0 30 34 32 37 30 2e 31 3b 20 5f 5f 75 74 6d 62 3d 04270.1; \_\_utmb=  
02c0 32 33 32 38 30 39 39 32 31 2e 33 2e 31 30 2e 31 23280992 1.3.10.1  
02d0 33 32 34 38 30 34 32 37 30 3b 20 5f 5f 75 74 6d 32480427 0; \_\_utm  
02e0 63 3d 32 33 32 38 30 39 39 32 31 3b 20 5f 5f 75 c=232809 921; \_\_u  
02f0 74 6d 7a 3d 32 33 32 38 30 39 39 32 31 2e 31 33 tmz=2328 09921.13  
0300 32 34 38 30 34 32 37 30 2e 31 2e 31 2e 75 74 6d 24804270 .1.1.utm  
0310 63 73 72 3d 28 64 69 72 65 63 74 29 7c 75 74 6d csr=(dir ect)|utm  
0320 63 63 6e 3d 28 64 69 72 65 63 74 29 7c 75 74 6d ccn=(dir ect)|utm  
0330 63 6d 64 3d 28 6e 6f 6e 65 29 0d 0a 43 6f 6e 74 cmd=(non e)..Cont  
0340 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic  
0350 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d ation/x-ww-form  
0360 2d 75 72 6c 65 6c 63 6f 64 65 64 0d 0a 43 6f 6e -urlenco ded..Con  
0370 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 36 0d tent-Len gth: 66.  
0380 0a 0d 0a 75 73 65 72 6e 61 6d 65 3d 41 70 6f 66 ...usern ame=A  
0390 69 67 65 6e 26 70 61 73 73 77 6f 72 64 3d 34 38 = &pas sword=4  
03a0 &redirec  
03b0 t=&login =%C2%F5%  
03c0 EE%E4

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
25	3.077064	192.168.0.100	173.194.69.102	HTTP	942	GET /__utm.gif?utmwv=5.2.2&utms=3&utm=951776479&utmhn=forum.modding.ru&utms=windows-12

```
32 4.812409 192.168.0.100 217.23.137.61 HTTP 965 POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)

Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.7\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Referer: http://forum.modding.ru/login.php\r\n
[truncated] Cookie: phpb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22auto_login_id%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22user_id%22%
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 66\r\n
\r\n
[Full request URI: http://forum.modding.ru/login.php]
Line-based text data: application/x-www-form-urlencoded
username=A
```

User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0.1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: ru,en;q=0.7,en-us;q=0.3  
Accept-Charset: windows-1251,utf-8;q=0.7,\*;q=0.7  
DNT: 1  
Connection: keep-alive  
Referer: http://forum.modding.ru/login.php  
[truncated] Cookie: phpb2mysql\_data=a%3A2%3A%7Bs%3A11%3A%22auto\_login\_id%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22user\_id%22%  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 66  
[Full request URI: http://forum.modding.ru/login.php]  
Line-based text data: application/x-www-form-urlencoded  
username=A

01b0	74	70	3a	2f	2f	66	6f	72	75	6d	2e	6d	6f	64	64	69	tp://for	um.moddi
01c0	6e	67	2e	72	75	2f	6c	6f	67	69	6e	2e	70	68	70	0d	ng.ru/lo	gin.php.
01d0	0a	43	6f	6f	6b	69	65	3a	20	70	68	70	62	62	32	6d	.Cookie:	phpbb2m
01e0	79	73	71	6c	5f	64	61	74	61	3d	61	25	33	41	32	25	ysql_dat	a=a%3A2%
01f0	33	41	25	37	42	73	25	33	41	31	31	25	33	41	25	32	3A%7Bs%3	A11%3A%2
0200	32	61	75	74	6f	6c	6f	6f	69	6e	69	64	25	32	32	25	2autolog	inid%22%
0210	33	42	73	25	33	41	30	25	33	41	25	32	32	25	32	32	3Bs%3A0%	3A%22%22
0220	25	33	42	73	25	33	41	36	25	33	41	25	32	32	75	73	%3Bs%3A6%	%3A%22us
0230	65	72	69	64	25	32	32	25	33	42	69	25	33	41	2d	31	erid%22%	3Bi%3A-1
0240	25	33	42	25	37	44	3b	20	70	68	70	62	62	32	6d	79	%3B%7D;	phpbb2my
0250	73	71	6c	5f	73	69	64	3d	63	30	39	36	62	65	32	36	sql_sid=	c096be26
0260	35	65	37	30	62	30	31	63	62	38	35	30	64	66	33	39	5e70b01c	b850df39
0270	38	38	38	34	63	66	33	63	3b	20	5f	5f	75	74	6d	61	8884cf3c	;_utma
0280	3d	32	33	32	38	30	39	39	32	31	2e	36	30	31	37	32	=2328099	21.60172
0290	39	37	39	34	2e	31	33	32	34	38	30	34	32	37	30	2e	9794.132	4804270.
02a0	31	33	32	34	38	30	34	32	37	30	2e	31	33	32	34	38	13248042	70.13248
02b0	30	34	32	37	30	2e	31	3b	20	5f	5f	75	74	6d	62	3d	04270.1;	_utmb=
02c0	32	33	32	38	30	39	39	32	31	2e	33	2e	31	30	2e	31	23280992	1.3.10.1
02d0	33	32	34	38	30	34	32	37	30	3b	20	5f	5f	75	74	6d	32480427	0;_utm
02e0	63	3d	32	33	32	38	30	39	39	32	31	3b	20	5f	5f	75	c=232809	921;_u
02f0	74	6d	7a	3d	32	33	32	38	30	39	39	32	31	2e	31	33	tmz=2328	09921.13
0300	32	34	38	30	34	32	37	30	2e	31	2e	31	2e	75	74	6d	24804270	.1.1.utm
0310	63	73	72	3d	28	64	69	72	65	63	74	29	7c	75	74	6d	csr=(dir	ect) utm
0320	63	63	6e	3d	28	64	69	72	65	63	74	29	7c	75	74	6d	ccn=(dir	ect) utm
0330	63	6d	64	3d	28	6e	6f	6e	65	29	0d	0a	43	6f	6e	74	cmd=(non	e)..Cont
0340	65	6e	74	2d	54	79	70	65	3a	20	61	70	70	6c	69	63	ent-Type	:applic
0350	61	74	69	6f	6e	2f	78	2d	77	77	77	2d	66	6f	72	6d	ation/x-	www-Form
0360	2d	75	72	6c	65	6e	63	6f	64	65	64	0d	0a	43	6f	6e	-urlenco	ded..Con
0370	74	65	6e	74	2d	4c	65	6e	67	74	68	3a	20	36	36	0d	tent-Len	gth: 66.
0380	0a	0d	0a	75	73	65	72	6e	61	6d	65	3d	41	70	6f	66	...usern	ame=A
0390	69	67	65	6e	26	70	61	73	77	6f	72	64	3d	34	38		&pas	word=4
03a0	31	35	31	36	32	33	34	32	26	72	65	64	69	72	65	63	&redire	c
03b0	74	3d	26	6c	6f	67	69	6e	3d	25	43	32	25	46	35	25	t=&login	=%C2%F5%
03c0	45	45	25	45	34												EE%E4	



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	146.66.152.14	UDP	126	Source port: 56506 Destination port: 27017
2	0.068733	192.168.0.100	173.194.69.125	Jabber/	55	Request: \000
3	0.124843	173.194.69.125	192.168.0.100	TCP	66	xmpp-client > 20976 [ACK] Seq=1 Ack=2 win=778 Len=0 SLE=1 SRE=2
4	0.626064	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
5	0.626185	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
6	0.626260	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
7	0.626334	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
8	0.626415	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
9	0.626488	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
10	0.626558	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
11	0.626631	192.168.0.100	173.194.69.125	HTTP	126	> http [RST, ACK] Seq=1 Ack=1 win=0 Len=0
12	0.626632	192.168.0.100	173.194.69.125	HTTP	126	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
13	0.629025	87.240.184.95	192.168.0.100	HTTP	126	> 22283 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
14	0.629197	87.240.184.95	192.168.0.100	HTTP	126	> http [ACK] Seq=2 Ack=2 win=16425 Len=0
15	0.629359	87.240.184.95	192.168.0.100	HTTP	126	> 22284 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
16	0.629508	192.168.0.100	87.240.184.95	HTTP	126	> http [ACK] Seq=2 Ack=2 win=16425 Len=0
17	0.629887	87.240.184.95	192.168.0.100	HTTP	126	> 22282 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
18	0.629980	192.168.0.100	87.240.184.95	HTTP	126	> http [ACK] Seq=2 Ack=2 win=16425 Len=0
19	0.630480	87.240.180.126	192.168.0.100	TCP	60	http > 22280 [FIN, ACK] Seq=1 Ack=2 win=31 Len=0
20	0.630637	192.168.0.100	87.240.180.126	TCP	54	22280 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
21	0.630796	87.240.184.95	192.168.0.100	TCP	60	http > 22279 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
22	0.630887	192.168.0.100	87.240.184.95	TCP	54	22279 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
23	0.631330	87.240.129.75	192.168.0.100	TCP	60	http > 22277 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
24	0.631426	192.168.0.100	87.240.129.75	TCP	54	22277 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
25	0.631615	93.186.225.15	192.168.0.100	TCP	60	http > 22278 [FIN, ACK] Seq=1 Ack=2 win=16 Len=0
26	0.631717	192.168.0.100	93.186.225.15	TCP	54	22278 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
27	0.632240	87.240.180.134	192.168.0.100	TCP	60	http > 22281 [FIN, ACK] Seq=1 Ack=2 win=31 Len=0
28	0.632363	192.168.0.100	87.240.180.134	TCP	54	22281 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
29	1.663985	fe80::902f:ac87:c51ff02::c	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
30	2.376870	146.66.152.14	192.168.0.100	UDP	254	Source port: 27017 Destination port: 56506
31	2.599853	192.168.0.100	146.66.152.14	UDP	78	Source port: 56506 Destination port: 27017
32	3.067318	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
33	3.285040	173.254.216.67	192.168.0.100	TCP	60	https > 22436 [ACK] Seq=1 Ack=587 win=501 Len=0
34	3.285089	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
35	3.503084	173.254.216.67	192.168.0.100	TCP	60	https > 22436 [ACK] Seq=1 Ack=1173 win=501 Len=0
36	3.556888	192.168.0.100	93.186.230.82	HTTP	55	Continuation or non-HTTP traffic [Malformed Packet]

Wireshark: Find Packet

Find

By:  Display filter  Hex value  String

Filter: login

Search In:  Packet list  Packet details  Packet bytes

String Options:  Case sensitive

Character set: ASCII Unicode & Non-Unicode

Direction:  Up  Down

Buttons: Help Find Cancel

Frame 12: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)

Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 93.186.225.15 (93.186.225.15)

Transmission Control Protocol, Src Port: 22278 (22278), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

```

0000 1c af f7 49 94 c2 00 24 1d 82 13 ff 08 00 45 00  ...I...$ .....E.
0010 00 28 3d 79 40 00 80 06 00 00 c0 a8 00 64 5d ba  .(=y@... ..d].
0020 e1 0f 57 06 00 50 df e2 10 a5 2e c0 56 ff 50 11  ..W..P. ....V.P.
0030 40 29 ff f0 00 00  @.....
    
```



File Edit View Go Capture Analyze Statistics Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	146.66.152.14	UDP	126	Source port: 56506 Destination port: 27017
2	0.068733	192.168.0.100	173.194.69.125	Jabber/	55	Request: \000
3	0.124843	173.194.69.125	192.168.0.100	TCP	66	xmpp-client > 20976 [ACK] Seq=1 Ack=2 win=778 Len=0 SLE=1 SRE=2
4	0.626064	192.168.0.100	192.168.0.100	HTTP	0	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
5	0.626185	192.168.0.100	192.168.0.100	HTTP	0	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
6	0.626260	192.168.0.100	192.168.0.100	HTTP	0	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
7	0.626334	192.168.0.100	192.168.0.100	HTTP	0	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
8	0.626415	192.168.0.100	192.168.0.100	HTTP	0	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
9	0.626488	192.168.0.100	192.168.0.100	HTTP	0	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
10	0.626558	192.168.0.100	192.168.0.100	HTTP	0	> http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
11	0.626631	192.168.0.100	192.168.0.100	HTTP	0	> http [RST, ACK] Seq=1 Ack=1 win=0 Len=0
12	0.626632	192.168.0.100	192.168.0.100	HTTP	0	> 22283 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
13	0.629025	87.240.184.95	192.168.0.100	HTTP	0	> http [ACK] Seq=2 Ack=2 win=16425 Len=0
14	0.629197	192.168.0.100	192.168.0.100	HTTP	0	> 22284 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
15	0.629359	87.240.184.95	192.168.0.100	HTTP	0	> http [ACK] Seq=2 Ack=2 win=16425 Len=0
16	0.629508	192.168.0.100	192.168.0.100	HTTP	0	> 22282 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
17	0.629887	87.240.184.95	192.168.0.100	HTTP	0	> http [ACK] Seq=2 Ack=2 win=16425 Len=0
18	0.629980	192.168.0.100	192.168.0.100	HTTP	0	> 22280 [FIN, ACK] Seq=1 Ack=2 win=31 Len=0
19	0.630480	87.240.180.126	192.168.0.100	TCP	60	http > 22280 [ACK] Seq=2 Ack=2 win=16425 Len=0
20	0.630637	192.168.0.100	87.240.180.126	TCP	54	22280 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
21	0.630796	87.240.184.95	192.168.0.100	TCP	60	http > 22279 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
22	0.630887	192.168.0.100	87.240.184.95	TCP	54	22279 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
23	0.631330	87.240.129.75	192.168.0.100	TCP	60	http > 22277 [FIN, ACK] Seq=1 Ack=2 win=14 Len=0
24	0.631426	192.168.0.100	87.240.129.75	TCP	54	22277 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
25	0.631615	93.186.225.15	192.168.0.100	TCP	60	http > 22278 [FIN, ACK] Seq=1 Ack=2 win=16 Len=0
26	0.631717	192.168.0.100	93.186.225.15	TCP	54	22278 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
27	0.632240	87.240.180.134	192.168.0.100	TCP	60	http > 22281 [FIN, ACK] Seq=1 Ack=2 win=31 Len=0
28	0.632363	192.168.0.100	87.240.180.134	TCP	54	22281 > http [ACK] Seq=2 Ack=2 win=16425 Len=0
29	1.663985	fe80::902f:ac87:c51ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
30	2.376870	146.66.152.14	192.168.0.100	UDP	254	Source port: 27017 Destination port: 56506
31	2.599853	192.168.0.100	146.66.152.14	UDP	78	Source port: 56506 Destination port: 27017
32	3.067318	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
33	3.285040	173.254.216.67	192.168.0.100	TCP	60	https > 22436 [ACK] Seq=1 Ack=587 win=501 Len=0
34	3.285089	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
35	3.503084	173.254.216.67	192.168.0.100	TCP	60	https > 22436 [ACK] Seq=1 Ack=1173 win=501 Len=0
36	3.556888	192.168.0.100	93.186.230.82	HTTP	55	Continuation or non-HTTP traffic (Malformed Packet)

Wireshark: Find Packet

Find

By:  Display filter  Hex value  String

Filter: a

Search In:  Packet list  Packet details  Packet bytes

String Options:  Case sensitive Character set: ASCII Unicode & Non-Unicode

Direction:  Up  Down

Buttons: Help Find Cancel

Frame 12: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)


Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 93.186.225.15 (93.186.225.15)

Transmission Control Protocol, Src Port: 22278 (22278), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

```

0000 1c af f7 49 94 c2 00 24 1d 82 13 ff 08 00 45 00  ...I...$ .....E.
0010 00 28 3d 79 40 00 80 06 00 00 c0 a8 00 64 5d ba  .(=y@... .....d|.
0020 e1 0f 57 06 00 50 df e2 10 a5 2e c0 56 ff 50 11  ..W..P.. ....V.P.
0030 40 29 ff f0 00 00                                @).....

```

No packet contained that string in its dissected display. 

Packets: 150 Displayed: 150 Marked: 0 Load time: 0:00.003 Profile: Default

Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
29	1.663985	fe80::902f:ac87:c51ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
36	3.556888	192.168.0.100	93.186.230.82	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
45	4.664086	fe80::902f:ac87:c51ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
47	5.285944	192.168.0.100	87.240.143.244	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
54	5.943966	192.168.0.100	87.242.112.250	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
55	5.953958	192.168.0.100	87.242.112.250	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
56	5.954001	192.168.0.100	87.242.112.250	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
60	5.963939	192.168.0.100	87.242.112.250	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
61	5.963978	192.168.0.100	87.242.112.250	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
65	6.333989	192.168.0.100	87.242.112.250	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
113	7.664111					

65 6.333989 192.168.0.100 87.242.112.250 HTTP 55 Continuation or non-HTTP traffic[Malformed Packet]

Frame 65: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

- Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)
- Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 87.242.112.250 (87.242.112.250)
- Transmission Control Protocol, Src Port: 22404 (22404), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1
- Hypertext Transfer Protocol
- [Malformed Packet: GIF image]

```

0000 1c af f7 49 94 c2 00 24 1d 82 13 ff 08 00 45 00  ...I...$ .....E.
0010 00 29 3d 92 40 00 80 06 00 00 c0 a8 00 64 57 f2  .)=.@... ..dw.
0020 70 fa 57 84 00 50 e1 ca f0 67 42 8f 8c 46 50 10  p.w..P.. .gB..FP.
0030 40 29 8a 14 00 00 00  @).....
    
```

Frame 65: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

- Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)
- Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 87.242.112.250 (87.242.112.250)
- Transmission Control Protocol, Src Port: 22404 (22404), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1
- Hypertext Transfer Protocol
- [Malformed Packet: GIF image]

```

0000 1c af f7 49 94 c2 00 24 1d 82 13 ff 08 00 45 00  ...I...$ .....E.
0010 00 29 3d 92 40 00 80 06 00 00 c0 a8 00 64 57 f2  .)=.@... ..dw.
0020 70 fa 57 84 00 50 e1 ca f0 67 42 8f 8c 46 50 10  p.w..P.. .gB..FP.
0030 40 29 8a 14 00 00 00  @).....
    
```

Wireshark interface showing a network capture. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 1013 is highlighted in red, indicating it is selected. A search filter '4' is applied to the packet list, highlighted by a red arrow.

The packet details pane for the selected packet (Frame 9) shows the following structure:

- Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)
- Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 84.47.169.155 (84.47.169.155)
- Transmission Control Protocol, Src Port: 23448 (23448), Dst Port: http (80), Seq: 1, Ack: 1, Len: 959
- Hypertext Transfer Protocol
- Line-based text data: application/x-www-form-urlencoded
  - username=
  - password=4
  - &login=%D0%92%D1%85%D0%BE%D0%B4

The hex dump pane shows the raw data of the selected packet, with the text data portion highlighted in blue. A red arrow points to the hex value '34' (0x24) corresponding to the character '4' in the password field.

At the bottom, the status bar indicates: Text item (text), 133 bytes. Packets: 117 Displayed: 117 Marked: 0 Dropped: 0. Profile: Default.

9 2.253813 192.168.0.100 84.47.169.155 HTTP 1013 POST /ucp.php?mode=login HTTP/1.1 (application/x-www-form-urlencoded)

- Frame 9: 1013 bytes on wire (8104 bits), 1013 bytes captured (8104 bits)
- Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)
- Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 84.47.169.155 (84.47.169.155)
- Transmission Control Protocol, Src Port: 23448 (23448), Dst Port: http (80), Seq: 1, Ack: 1, Len: 959
- Hypertext Transfer Protocol
  - POST /ucp.php?mode=login HTTP/1.1\r\n
  - Host: forums.overclockers.ru\r\n

00e0	2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74	, applica
00f0	6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69	tion/xht
0100	6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a	ml+xml, a
0110	3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c	pplicati
0120	61 6e 67 75 61 67 65 3a 2d 72 75 2c 65 6e 3b 71	on/xml;q
0130	3d 30 2e 37 2c 65 6e 20 75 73 3b 71 3d 30 2e 33	=0.9, */*
0140	0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e	;q=0.8..
0150	67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65	Accept-L
0160	0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73 65 74	anguage: r
0170	3a 20 77 69 6e 64 6f 77 73 2d 31 32 35 31 2c 75	ru,en;q
0180	74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 3d 30	=0.7,en-
0190	2e 37 0d 0a 44 4e 54 3a 20 31 0d 0a 43 6f 6e 6e	us;q=0.3
01a0	65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69	..Accept
01b0	76 65 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74	-Encodin
01c0	70 3a 2f 2f 66 6f 72 75 6d 73 2e 6f 76 65 72 63	g: gzip,
01d0	6c 6f 63 6b 65 72 73 2e 72 75 2f 69 6e 64 65 78	deflate
01e0	2e 70 68 70 3f 73 69 64 3d 66 62 65 37 39 31 37	..Accept
01f0	37 31 65 30 37 63 36 33 33 30 39 35 61 62 32 32	-Charset
0200	31 66 65 36 31 34 63 62 34 0d 0a 43 6f 6f 6b 69	: window
0210	65 3a 20 6f 76 65 72 5f 66 6f 72 75 6d 73 5f 75	s-1251,u
0220	3d 31 3b 20 6f 76 65 72 5f 66 6f 72 75 6d 73 5f	tf-8;q=0
0230	6b 3d 3b 20 6f 76 65 72 5f 66 6f 72 75 6d 73 5f	.7,*;q=0
0240	73 69 64 3d 66 62 65 37 39 31 37 37 31 65 30 37	..DNT: 1
0250	63 36 33 33 30 39 35 61 62 32 32 31 66 65 36 31	.Conn
0260	34 63 62 34 3b 20 5f 5f 75 74 6d 61 3d 31 36 34	ection: kee
0270	33 36 39 34 34 38 2e 37 37 34 34 30 35 37 35 32	ep: htt
0280	2e 31 33 32 34 38 30 36 37 30 31 2e 31 33 32 34	p://foru
0290	38 30 36 37 30 31 2e 31 33 32 34 38 30 36 37 30	ms.overc
02a0	31 2e 31 3b 20 5f 5f 75 74 6d 62 3d 31 36 34 33	lockers.
02b0	36 39 34 34 38 2e 32 2e 31 30 2e 31 33 32 34 38	ru/index
02c0	30 36 37 30 31 3b 20 5f 5f 75 74 6d 63 3d 31 36	.php?sid
02d0	34 33 36 39 34 34 38 3b 20 5f 5f 75 74 6d 7a 3d	=fbe7917
02e0	31 36 34 33 36 39 34 34 38 2e 31 33 32 34 38 30	71e07c63
02f0	36 37 30 31 2e 31 2e 31 2e 75 74 6d 63 73 72 3d	3095ab22
0300	28 64 69 72 65 63 74 29 7c 75 74 6d 63 63 6e 3d	1fe614cb
0310	28 64 69 72 65 63 74 29 7c 75 74 6d 63 6d 64 3d	4..cooki
0320	28 6e 6f 6e 65 29 0d 0a 43 6f 6e 74 65 6e 74 2d	e: over_
0330	54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f	forums_u
0340	6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c	=1; over
0350	65 6e 63 6f 67 65 64 0d 0a 43 6f 6e 74 65 6e 74	_forums_
0360	2d 4c 65 6e 67 74 68 3a 2d 31 33 33 0d 0a 0d 0a	k; over
0370	75 73 65 72 6e 61 6d 65 3d 25 44 30 25 39 41 25	_forums_
0380	44 30 25 42 30 25 44 30 25 42 46 25 44 30 25 42	sid=fbe7
0390	38 25 44 31 25 38 32 25 44 30 25 42 30 25 44 30	91771e07
03a0	25 42 44 2b 25 44 30 25 39 41 25 44 30 25 42 30	c633095a
03b0	25 44 30 25 42 41 25 44 30 25 42 30 25 44 30 25	b221fe61
03c0	42 45 26 70 61 73 73 77 6f 72 64 3d 34 38 31 35	utma=164
03d0	31 36 32 33 34 32 26 6c 6f 67 69 6e 3d 25 44 30	369448.7
03e0	25 39 32 25 44 31 25 38 35 25 44 30 25 42 45 25	744405752
03f0	44 30 25 42 34	.1324806

0000 1c af  
0010 03 e7  
0020 a9 9b  
0030 40 29  
0040 70 68  
0050 54 54  
0060 6f 72  
0070 72 73  
0080 74 3a  
0090 57 69  
00a0 57 4f  
00b0 20 47  
00c0 46 69  
00d0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html

1 WS=128

PERM=1

1 WS=128

1 WS=128





Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	50.16.189.191	192.168.0.100	TCP	60	http > 24612 [ACK] Seq=1 Ack=1 win=27 Len=0
2	0.000340	50.16.189.191	192.168.0.100	TCP	60	HTTP/1.1 200 OK
3	0.134466	178.254.216.67	192.168.0.100	TCP	60	Continuation or non-HTTP traffic[Malformed Packet]
4	0.152218	fe80::902f:ac87:c51ff02::c	192.168.0.100	SSDP	208	M-SEARCH * HTTP/1.1
5	0.206039	192.168.0.100	192.168.0.100	TCP	60	http [ACK] Seq=1 Ack=147 win=16388 Len=0
6	0.310502	146.67.240.188	192.168.0.100	TCP	60	port: 27017 Destination port: 56506
7	0.334029	192.168.0.100	192.168.0.100	TCP	60	http [ACK] Seq=1 Ack=4 win=16402 Len=0
8	0.336912	178.254.216.67	192.168.0.100	TCP	60	Continuation or non-HTTP traffic
9	0.337330	192.168.0.100	192.168.0.100	TCP	60	Continuation or non-HTTP traffic[Malformed Packet]
10	0.343071	192.168.0.100	192.168.0.100	TCP	60	> 27292 [PSH, ACK] Seq=1 Ack=1 win=63419 Len=71
11	0.359507	178.254.216.67	192.168.0.100	TCP	60	> 20954 [PSH, ACK] Seq=1 Ack=72 win=64169 Len=4
12	0.471165	178.254.216.67	192.168.0.100	TCP	60	24609 [ACK] Seq=16 Ack=5 win=65476 Len=0
13	0.519156	192.168.0.100	192.168.0.100	TCP	60	port: 56506 Destination port: 27017
14	0.559026	192.168.0.100	192.168.0.100	TCP	60	> 27292 [ACK] Seq=72 Ack=5 win=63415 Len=0
15	2.384385	192.168.0.100	192.168.0.100	TCP	60	port: 56506 Destination port: 27017
16	2.804731	146.67.240.188	192.168.0.100	TCP	60	port: 27017 Destination port: 56506
17	3.152420	fe80::902f:ac87:c51ff02::c	192.168.0.100	SSDP	208	M-SEARCH * HTTP/1.1
18	3.235735	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
19	3.448741	173.254.216.67	192.168.0.100	TCP	60	https > 23599 [ACK] seq=1 Ack=587 win=501 Len=0
20	3.967227	173.254.216.67	192.168.0.100	TLSv1	640	Application Data, Application Data
21	3.968610	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
22	4.181357	173.254.216.67	192.168.0.100	TCP	60	https > 23599 [ACK] Seq=587 Ack=1173 win=501 Len=0
23	4.181430	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
24	4.394273	173.254.216.67	192.168.0.100	TCP	60	https > 23599 [ACK] Seq=587 Ack=1759 win=501 Len=0
25	5.366243	192.168.0.100	87.240.188.249	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
26	5.369257	87.240.188.249	192.168.0.100	TCP	66	http > 24590 [ACK] Seq=1 Ack=2 win=1803 Len=0 SLE=1 SRE=2
27	5.448474	fe80::902f:ac87:c51ff02::1:2	192.168.0.100	DHCPv6	152	solicit xID: 0xee5e03 CID: 00010001148bfe1f00241d8213ff
28	5.470323	173.254.216.67	192.168.0.100	TLSv1	640	Application Data, Application Data
29	5.670258	192.168.0.100	173.254.216.67	TCP	54	23599 > https [ACK] Seq=1759 Ack=1173 win=16278 Len=0

Wireshark: Find Packet

Find

By:  Display filter  Hex value  String

Filter: 4

Search In:  Packet list  Packet details  Packet bytes

String Options:  Case sensitive  
Character set: ASCII Unicode & Non-Unicode

Direction:  Up  Down

Buttons: Help Find Cancel

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
 Ethernet II, Src: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2), Dst: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff)  
 Internet Protocol Version 4, Src: 50.16.189.191 (50.16.189.191), Dst: 192.168.0.100 (192.168.0.100)  
 Transmission Control Protocol, Src Port: http (80), Dst Port: 24612 (24612), Seq: 1, Ack: 1, Len: 0

```

0000  00 24 1d 82 13 ff 1c af f7 49 94 c2 08 00 45 80  .$. . . . . .I. . . .E.
0010  00 28 6e e4 40 00 2c 06 2e 90 32 10 bd bf c0 a8  .(n.@. . .2. . . . .
0020  00 64 00 50 60 24 32 b5 54 44 c8 14 06 62 50 10  .d.P`$2. TD. . .bP.
0030  00 1b 48 f9 00 00 00 00 00 00 00 00 00 00 00  ..H. . . . .
    
```



Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	50.16.189.191	192.168.0.100	TCP	60	http > 24612 [ACK] Seq=1 Ack=1 win=27 Len=0
2	0.000340	50.16.189.191	192.168.0.100	HTTP	200	HTTP/1.1 200 OK
3	0.134466	178.252.102.18	192.168.0.100	HTTP	60	Continuation or non-HTTP traffic[Malformed Packet]
4	0.152218	fe80::902f:ac87:c51ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
5	0.206039	192.168.0.100	50.16.189.191	TCP	54	24612 > http [ACK] Seq=1 Ack=147 win=16388 Len=0
6	0.310502	146.66.152.14	192.168.0.100	UDP	302	Source port: 27017 Destination port: 56506
7	0.310502	146.66.152.14	192.168.0.100	CP	54	24609 > http [ACK] Seq=1 Ack=4 win=16402 Len=0
8	0.310502	146.66.152.14	192.168.0.100	ITP	66	Continuation or non-HTTP traffic
9	0.310502	146.66.152.14	192.168.0.100	ITP	58	Continuation or non-HTTP traffic[Malformed Packet]
10	0.310502	146.66.152.14	192.168.0.100	CP	125	20954 > 27292 [PSH, ACK] Seq=1 Ack=1 win=63419 Len=71
11	0.310502	146.66.152.14	192.168.0.100	CP	60	27292 > 20954 [PSH, ACK] Seq=1 Ack=72 win=64169 Len=4
12	0.310502	146.66.152.14	192.168.0.100	CP	60	http > 24609 [ACK] Seq=16 Ack=5 win=65476 Len=0
13	0.310502	146.66.152.14	192.168.0.100	DP	78	Source port: 56506 Destination port: 27017
14	0.310502	146.66.152.14	192.168.0.100	CP	54	20954 > 27292 [ACK] Seq=72 Ack=5 win=63415 Len=0
15	0.310502	146.66.152.14	192.168.0.100	DP	126	Source port: 56506 Destination port: 27017
16	0.310502	146.66.152.14	192.168.0.100	DP	78	Source port: 27017 Destination port: 56506
17	0.310502	146.66.152.14	192.168.0.100	SDP	208	M-SEARCH * HTTP/1.1
18	0.310502	146.66.152.14	192.168.0.100	LSv1	640	Application Data, Application Data
19	0.310502	146.66.152.14	192.168.0.100	CP	60	https > 23599 [ACK] Seq=1 Ack=587 win=501 Len=0
20	0.310502	146.66.152.14	192.168.0.100	LSv1	640	Application Data, Application Data
21	0.310502	146.66.152.14	192.168.0.100	LSv1	640	Application Data, Application Data
22	4.181357	173.254.216.67	192.168.0.100	TCP	60	https > 23599 [ACK] Seq=587 Ack=1173 win=501 Len=0
23	4.181430	192.168.0.100	173.254.216.67	TLSv1	640	Application Data, Application Data
24	4.394273	173.254.216.67	192.168.0.100	TCP	60	https > 23599 [ACK] Seq=587 Ack=1759 win=501 Len=0
25	5.366243	192.168.0.100	87.240.188.249	HTTP	55	Continuation or non-HTTP traffic[Malformed Packet]
26	5.369257	87.240.188.249	192.168.0.100	TCP	66	http > 24590 [ACK] Seq=1 Ack=2 win=1803 Len=0 SLE=1 SRE=2
27	5.448474	fe80::902f:ac87:c51ff02::1:2		DHCPv6	152	solicit XID: 0xee5e03 CID: 00010001148bfe1f00241d8213ff
28	5.470323	173.254.216.67	192.168.0.100	TLSv1	640	Application Data, Application Data
29	5.670258	192.168.0.100	173.254.216.67	TCP	54	23599 > https [ACK] Seq=1759 Ack=1173 win=16278 Len=0

Wireshark: Find Packet

Find

By:  Display filter  Hex value  String

Filter: login

Search In:  Packet list  Packet details  Packet bytes

String Options:  Case sensitive

Character set: ASCII Unicode & Non-Unicode

Direction:  Up  Down

Buttons: Help Find Cancel

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2), Dst: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff)

Internet Protocol Version 4, Src: 50.16.189.191 (50.16.189.191), Dst: 192.168.0.100 (192.168.0.100)

Transmission Control Protocol, src Port: http (80), Dst Port: 24612 (24612), Seq: 1, Ack: 1, Len: 0

```

0000  00 24 1d 82 13 ff 1c af f7 49 94 c2 08 00 45 80  .$. . . . . .I. . . .E.
0010  00 28 6e e4 40 00 2c 06 2e 90 32 10 bd bf c0 a8  .(n.@. . .2. . . . .
0020  00 64 00 50 60 24 32 b5 54 44 c8 14 06 62 50 10  .d.P`$2. TD. . .bp.
0030  00 1b 48 f9 00 00 00 00 00 00 00 00  . .H. . . . . . . . .
    
```

57	7.297064	96	11.282604	192.168.0.100	178.140.129.184	TCP	947	20954	>	27292 [PSH, ACK] Seq=76 Ack=5 Win=63415 Len=893
58	7.509870									
71	8.258752									
72	8.260477									
74	8.473726									
76	8.686829									
77	8.686976									
79	8.937833									
81	9.203980									
85	9.622219									
88	10.04245									

- Frame 96: 947 bytes on wire (7576 bits), 947 bytes captured (7576 bits)
- Ethernet II, Src: Giga-Byt\_82:13:ff (00:24:1d:82:13:ff), Dst: D-LinkIn\_49:94:c2 (1c:af:f7:49:94:c2)
- Internet Protocol version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 178.140.129.184 (178.140.129.184)
- Transmission Control Protocol, Src Port: 20954 (20954), Dst Port: 27292 (27292), Seq: 76, Ack: 5, Len: 893
- Data (893 bytes)

0000	1c	af	f7	49	94	c2	00	24	1d	82	13	ff	08	00	45	00	...	I...	\$	.....	E.
0010	03	a5	35	ce	40	00	80	06	00	00	c0	a8	00	64	b2	8c	...	.5@.	.....	d.	
0020	81	b8	51	da	6a	9c	07	c7	9c	19	bd	50	03	aa	50	18	...	.Q.j...	.....	P.P.	
0030	f7	b7	f8	e8	00	00	0a	56	85	31	d0	9c	14	74	49	1f	...	...Q...	.....	V	1...tI.
0040	fa	4b	95	87	ac	55	c2	45	12	c0	ab	6e	10	b1	85	5e	...	.K...U.E	.....	n...A	
0050	07	f6	e8	65	fd	8a	ce	b0	ea	6e	47	05	a7	a7	77	53	...	.e....	.....	ng...	wS
0060	d0	62	2a	e3	f1	dc	0d	11	5d	86	ab	73	5f	d7	72	ec	...	.b*....	.....	].s_r.	
0070	6b	6a	78	f6	e6	c3	d8	db	f0	a0	73	c8	7e	1d	d5	40	...	kjx....	.....	s...@	
0080	ce	30	f3	ff	dc	b3	05	f5	3f	60	a9	09	53	bd	48	82	...	.0.....	?	.....	S.H.
0090	cf	47	24	5e	f2	de	54	f4	59	be	55	03	1c	d4	89	99	...	.G\$^..T.	.....	Y.U....	
00a0	6e	23	58	76	b0	1d	30	64	7e	31	e4	bd	63	38	9d	4c	...	n#Xv...Od	~1..c8.L		
00b0	7c	66	29	e7	71	46	4f	e3	5a	1d	21	2d	9b	31	eb	6f	...	[f)wqFO.	Z.!--1.o		
00c0	9a	8a	5c	e9	7f	30	1e	c3	16	c1	dd	e0	74	28	ef	ee	...	...\\..	.....	t(..	
00d0	0b	4e	a2	39	be	c3	a2	94	b7	e3	be	dc	e2	35	40	3f	...	.N.9....	.....	5@?n	
00e0	67	bd	e1	ab	8a	8e	53	d2	96	6a	c5	ba	fd	fe	9d	6e	...	g.....	S.	.....	j.....n
00f0	a0	3a	70	1e	5d	7d	85	2f	44	69	0a	fc	09	f8	c1	21	...	.:p.]]./	D[.....!		
0100	37	29	d2	a5	be	ae	98	93	2b	df	1e	7f	23	76	34	de	...	7).....	+	.....	#v4.
0110	bc	28	2b	9e	0c	09	de	18	50	76	c2	4f	43	aa	1f	ca	...	.(+.....	.....	Pv.OC...	
0120	90	4d	39	ad	1d	dd	6c	57	23	ee	20	68	be	68	2a	da	...	.M9...lw	#.	h.h*..	
0130	20	83	1e	7a	90	5c	3a	bf	3e	92	2d	bc	0c	f3	88	eb	...	.z.\:.	>.....	-.....	
0140	73	e6	79	a4	d8	e4	a7	55	9d	28	b6	db	70	f6	8b	4b	...	s.y....U	(.p..K		
0150	ec	0c	9d	bc	eb	ab	ea	99	b0	ea	71	b2	b8	0a	0c	eb	...	.....	.....	q.....	
0160	1e	d8	4c	bb	1f	a3	28	44	2e	d9	59	8e	9e	b5	2f	52	...	..L...D	.....	Y.../R	
0170	38	4b	00	d8	5c	e5	98	1c	95	34	5f	c3	d5	ae	0e	0a	...	8K.\:.	4_	.....	
0180	39	d9	57	3d	aa	e2	79	d4	ea	36	33	7b	f0	7f	87	a5	...	9.W=..by.	.63{....		
0190	45	c4	ef	56	e7	18	8c	d6	ee	ad	8f	ac	01	fc	b7	3c	...	E..V....	.....	A	.....<
01a0	df	cf	e3	fd	c1	57	e6	41	62	7c	9e	2e	95	6a	ae	ac	...	.....	w.A	b ...j.	
01b0	7e	60	98	fe	db	08	e4	85	9a	08	49	f5	19	02	ec	35	...	.....	I....5		
01c0	01	fa	1e	c1	67	ad	28	67	0c	5e	42	82	92	47	ac	7f	...	.....	g.(g	^B..G.	
01d0	a9	ec	3e	86	dd	3d	e4	2d	0a	41	c0	22	ac	a9	78	80	...	.....	.-=.	A"....x.	
01e0	4f	20	ba	7b	d5	59	6d	58	46	3c	16	91	68	4c	72	c6	...	O...{.	YmX	F<...hLr.	
01f0	e6	51	f4	5a	64	b8	78	3c	8e	83	67	d2	8b	75	70	ea	...	.Q.Zd.x<	.....	g..up.	
0200	fd	dc	c1	d4	32	8b	76	be	7d	2b	9a	0f	ef	12	27	10	...	.....	.2.v.	}+.....	
0210	db	5e	1f	37	cd	72	c5	25	28	42	ad	05	43	ce	bd	c7	...	..^..7.r.%	(B..C..%		
0220	34	50	5b	0e	9b	54	f2	ae	38	3e	63	43	dd	25	6c	6f	...	4P[...T..	>8>cC.%lo		
0230	44	13	c0	a6	b2	f1	96	e5	94	19	97	37	88	dd	85	25	...	D.....	.....	7...%	
0240	5c	e6	a2	10	3b	63	8b	74	b9	b0	62	c2	7c	62	59	60	...	\\...;c.t	.....	b.  by"	
0250	5d	c3	ae	f7	c0	f6	31	a3	92	bc	b4	57	4b	f1	2f	e9	...	].....1.	.....	WK./.	
0260	4f	d4	2b	9a	ce	ab	66	9f	d6	ed	cb	bf	83	94	25	49	...	O+...f.	.....	%I	
0270	f2	4f	70	0b	13	38	f7	f0	9e	74	29	71	8a	44	51	f7	...	.Op..8..	.....	t)q.DQ.	
0280	72	12	19	c8	88	a3	62	09	60	24	fa	fb	a6	6f	0d	bc	...	r.....b.	.....	\$.o...	
0290	8e	4b	aa	6e	23	b5	9f	fc	3f	9a	ab	b8	fb	fb	bc	14	...	.K.n#...	.....	?.....	
02a0	03	ad	ba	82	a6	14	ba	cb	df	37	46	64	19	94	de	e2	...	.....	.7Fd...		
02b0	0c	86	4d	b6	00	49	db	e1	a6	66	0b	48	be	b8	12	bc	...	.M..I..	.....	f.H....	
02c0	22	a9	6b	9c	e7	d2	7e	17	5e	8d	f3	af	b4	08	5e	fa	...	.k....~.	.....	^.....^.	
02d0	8a	4b	e8	91	a1	b3	90	9f	16	c2	61	ca	e0	f3	01	4b	...	.k.....	.....	a...K	
02e0	2c	74	f8	35	0d	53	8f	68	31	68	0d	b6	8c	7b	d0	7a	...	.t.5.s.h	1h...{.z		
02f0	69	17	77	78	19	37	a5	20	aa	fa	1f	8c	2d	36	91	56	...	.;w..7.	.....	-6.V	