Wroclaw 11.10.2018

# Secure Systems and Networks

Laboratory No. 1

Wiktor Lagiewka 219226

1. Check ping, traceroute, mtr -- what kind of packets do they send to discover the intermediate routers? Is it ICMP, TCP, UDP? What features they use to find routers?

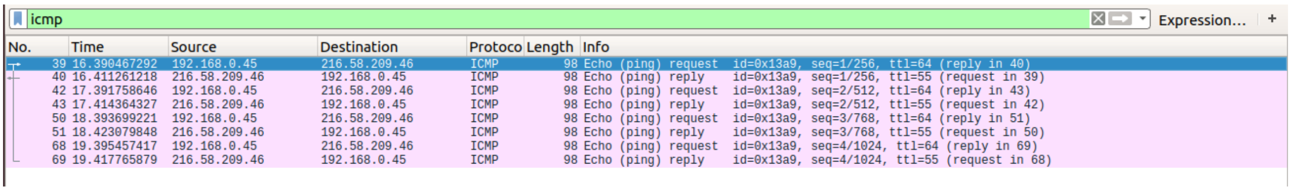
Ping – use ICMP protocol and send first ICMP echo Request and receive ICMP echo Replay

Usually servers that have public access serve ICMP echo Request and answer them, but not all hosts should respons and serve this packet. It depends on configuration r.g. firewall.

```
ING google.com (216.58.215.110) 56(84) bytes of data.
64 bytes from 216.58.215.110: icmp_seq=1 ttl=55 time=27.9 ms
64 bytes from 216.58.215.110: icmp_seq=2 ttl=55 time=54.3 ms
64 bytes from 216.58.215.110: icmp_seq=3 ttl=55 time=19.5 ms
64 bytes from 216.58.215.110: icmp_seq=4 ttl=55 time=40.7 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 19.587/35.664/54.365/13.161 ms
```

*Fig. Example of a google server response for ping command*



| No. | Time | Source | Destination | Protoco | Length | Info |
|---|---|---|---|---|---|---|
| 39 | 16.390467292 | 192.168.0.45 | 216.58.209.46 | ICMP | 98 | Echo (ping) request  id=0x13a9, seq=1/256, ttl=64 (reply in 40) |
| 40 | 16.411261218 | 216.58.209.46 | 192.168.0.45 | ICMP | 98 | Echo (ping) reply    id=0x13a9, seq=1/256, ttl=55 (request in 39) |
| 42 | 17.391758646 | 192.168.0.45 | 216.58.209.46 | ICMP | 98 | Echo (ping) request  id=0x13a9, seq=2/512, ttl=64 (reply in 43) |
| 43 | 17.414364327 | 216.58.209.46 | 192.168.0.45 | ICMP | 98 | Echo (ping) reply    id=0x13a9, seq=2/512, ttl=55 (request in 42) |
| 50 | 18.393699221 | 192.168.0.45 | 216.58.209.46 | ICMP | 98 | Echo (ping) request  id=0x13a9, seq=3/768, ttl=64 (reply in 51) |
| 51 | 18.423079848 | 216.58.209.46 | 192.168.0.45 | ICMP | 98 | Echo (ping) reply    id=0x13a9, seq=3/768, ttl=55 (request in 50) |
| 68 | 19.395457417 | 192.168.0.45 | 216.58.209.46 | ICMP | 98 | Echo (ping) request  id=0x13a9, seq=4/1024, ttl=64 (reply in 69) |
| 69 | 19.417765879 | 216.58.209.46 | 192.168.0.45 | ICMP | 98 | Echo (ping) reply    id=0x13a9, seq=4/1024, ttl=55 (request in 68) |

*Fig. Results from wireshark for ping command 4 ICMP request and 4 response*s.

When ICMP echo Request send via ping command do not receive any ICMP echo Response it either does not mean that we have problem with connection nor server is switched off. Example below show testing private company server site.

```
PING eshare.gemalto.com (91.241.42.157) 56(84) bytes of data.

--- eshare.gemalto.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3077ms
ping exited with status code 1
```

Fig. Example of testing private server site via ping command.

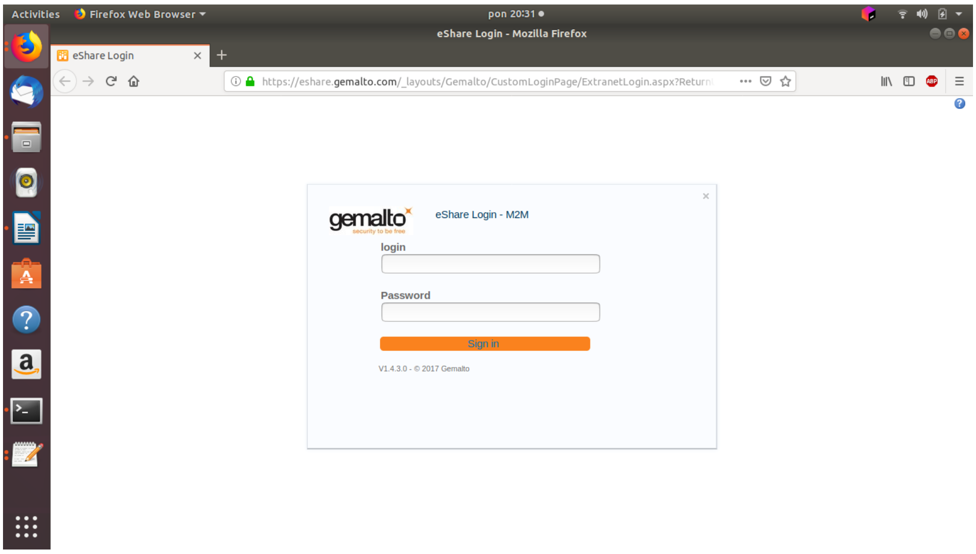

Activities
Firefox Web Browser
pon 20:31
eShare Login - Mozilla Firefox
eShare Login
https://eshare.gemalto.com/_layouts/Gemalto/CustomLoginPage/ExtranetLogin.aspx?Return
gemalto
security to be free
eShare Login - M2M
login
Password
Sign in
V1.4.3.0 - © 2017 Gemalto

Fig. Login panel to private company server site.

Above example depict that server is either not switched off nor our connection is failed, but it does not serve ICMP protocol.

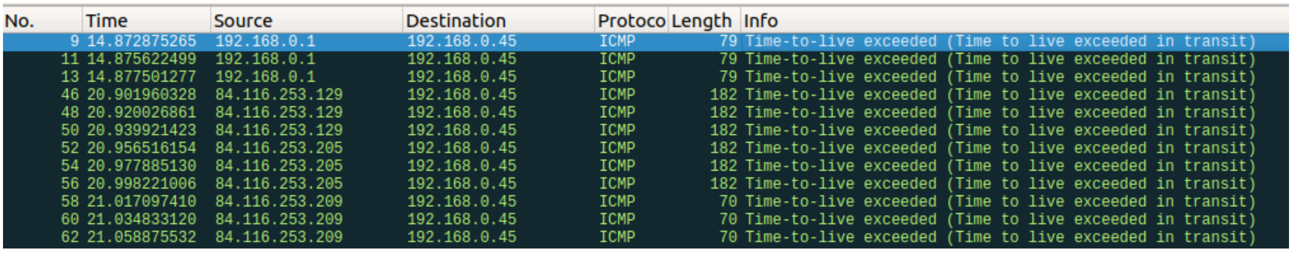
2. Traceroute - program which is use to search for the route of packets in network.
Program sends packet with TTL field equal to 1 to the first router on the road. When time will reach 0, packet is rejected and router send back ICMP response with IP address. In the next step program send packet with TTL equal to 2, when it reach first router decrease this value to 1 and forward it to the next router on the road. The mechnizm is repeatet over and over again and it depends on the number of nodes.
In the Linux based systems when the packet sent by the tracerout reach the destination host, information “Port Unrechable” is send back. Program wants to get that information, so intentionally send UDP packt with port number over 30000. It is very low probability that any devices work on that port.

To check out how it works below command was used:

```
# traceroute www.pwr.edu.pl

traceroute to www.pwr.edu.pl (156.17.16.240), 64 hops max
  1   192.168.0.1  3,376ms  2,723ms  1,859ms
  2   *  *  84.116.253.129  17,805ms
  3   84.116.253.129  17,858ms  19,715ms  84.116.253.205  16,471ms
  4   84.116.253.205  21,084ms  20,131ms  84.116.253.209  18,698ms
  5   84.116.253.209  17,449ms  23,963ms  62.179.3.242  17,808ms
  6   62.179.3.242  18,635ms  20,100ms  156.17.250.215  25,400ms
  7   156.17.250.215  25,009ms  22,609ms  156.17.254.112  20,086ms
  8   156.17.254.112  20,088ms  19,182ms  156.17.254.140  17,443ms
  9   156.17.254.140  19,997ms  17,299ms  156.17.18.244  19,337ms
 10   156.17.18.244  18,739ms  18,973ms  *
```

Wildcards in above example can be cause by firewall settings, or overload of network.



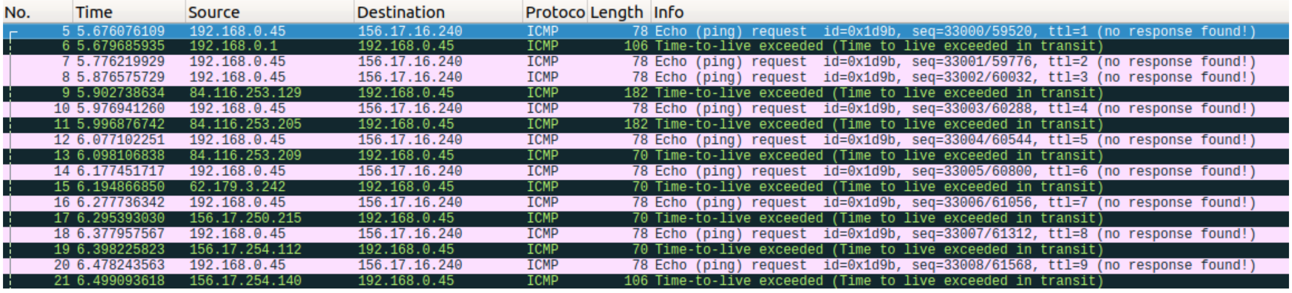
| No. | Time | Source | Destination | Protoco | Length | Info |
|---|---|---|---|---|---|---|
| 9 | 14.872875265 | 192.168.0.1 | 192.168.0.45 | ICMP | 79 | Time-to-live exceeded (Time to live exceeded in transit) |
| 11 | 14.875622499 | 192.168.0.1 | 192.168.0.45 | ICMP | 79 | Time-to-live exceeded (Time to live exceeded in transit) |
| 13 | 14.877501277 | 192.168.0.1 | 192.168.0.45 | ICMP | 79 | Time-to-live exceeded (Time to live exceeded in transit) |
| 46 | 20.901960328 | 84.116.253.129 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 48 | 20.920026861 | 84.116.253.129 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 50 | 20.939921423 | 84.116.253.129 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 52 | 20.956516154 | 84.116.253.205 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 54 | 20.977885130 | 84.116.253.205 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 56 | 20.998221006 | 84.116.253.205 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 58 | 21.017097410 | 84.116.253.209 | 192.168.0.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 60 | 21.034833120 | 84.116.253.209 | 192.168.0.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 62 | 21.058875532 | 84.116.253.209 | 192.168.0.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |

*Fig. Result of capturing ICMP packets for traceroute comand*

3. MTR - combines the functions of the traceroute and ping programs in one network diagnostic tool. It relies on ICMP packets coming back from routers, or ICMP Echo Reply packets when the packets have hit their destination host. MTR also has a UDP mode execute with -u option.

To run the program I used # mtr -r pwr.edu.pl command :

```
HOST: wiktor-Lenovo-B51-80       Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- compalhub.home            0.0%    10    3.7   2.6   2.1   3.7   0.6
  2.|-- 84.116.254.140           50.0%    10  6103. 6172. 5730. 6375. 269.8
  3.|-- pl-ktw01a-rc1-ae18-0.aort  0.0%    10   20.8  21.7  18.3  27.0   2.8
  4.|-- pl-wro02a-ra2-ae10-2120.a 10.0%    10   17.9  19.8  17.2  24.2   2.1
  5.|-- pl-wro02a-ra1-ae0-1430.ao  0.0%    10   30.1  22.0  18.6  30.1   3.5
  6.|-- chello062179003242.chello  0.0%    10   21.6  21.7  17.5  30.1   4.4
  7.|-- 156.17.250.215            0.0%    10   17.2  20.9  17.2  25.4   2.9
  8.|-- rolnik2-karkonosz.wask.wr  0.0%    10   18.2  20.8  17.8  26.5   3.1
  9.|-- wazniak-rolnik.wask.wroc.  0.0%    10   19.3  22.3  19.3  28.1   2.7
 10.|-- z-wask2-do-pwr2.pwrnet.pw  0.0%    10   17.3  19.6  17.3  23.0   1.6
```



| No. | Time | Source | Destination | Protoco | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 5.676076109 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33000/59520, ttl=1 (no response found!) |
| 6 | 5.679685935 | 192.168.0.1 | 192.168.0.45 | ICMP | 106 | Time-to-live exceeded (Time to live exceeded in transit) |
| 7 | 5.776219929 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33001/59776, ttl=2 (no response found!) |
| 8 | 5.876575729 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33002/60032, ttl=3 (no response found!) |
| 9 | 5.902738634 | 84.116.253.129 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 10 | 5.976941260 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33003/60288, ttl=4 (no response found!) |
| 11 | 5.996876742 | 84.116.253.205 | 192.168.0.45 | ICMP | 182 | Time-to-live exceeded (Time to live exceeded in transit) |
| 12 | 6.077102251 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33004/60544, ttl=5 (no response found!) |
| 13 | 6.098106838 | 84.116.253.209 | 192.168.0.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 14 | 6.177451717 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33005/60800, ttl=6 (no response found!) |
| 15 | 6.194866850 | 62.179.3.242 | 192.168.0.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 16 | 6.277736342 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33006/61056, ttl=7 (no response found!) |
| 17 | 6.295393030 | 156.17.250.215 | 192.168.0.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 18 | 6.377957567 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33007/61312, ttl=8 (no response found!) |
| 19 | 6.398225823 | 156.17.254.112 | 192.168.0.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 20 | 6.478243563 | 192.168.0.45 | 156.17.16.240 | ICMP | 78 | Echo (ping) request  id=0x1d9b, seq=33008/61568, ttl=9 (no response found!) |
| 21 | 6.499093618 | 156.17.254.140 | 192.168.0.45 | ICMP | 106 | Time-to-live exceeded (Time to live exceeded in transit) |

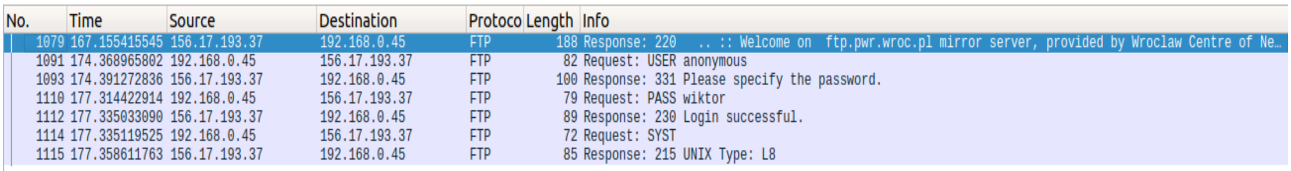
*Fig. Capturing ICMP packets fot MTR program execution.*

**Log in to some FTP site**

e.g ftp.icm.edu.pl or ftp.pwr.wroc.pl using "anonymous" acount, find out how this password information is sent over the network, use wireshark filters to get just the interesting packets, not all the rubbish that you can listen to on the network.

```
ftp> open ftp.pwr.wroc.pl
Connected to ftp.pwr.wroc.pl.
220   .. :: Welcome on  ftp.pwr.wroc.pl mirror server, provided by Wroclaw Centre of Networking
and Supercomputing :: ..
Name (ftp.pwr.wroc.pl:wiktor): anonymous
331 Please specify the password.
Password:
```

230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.



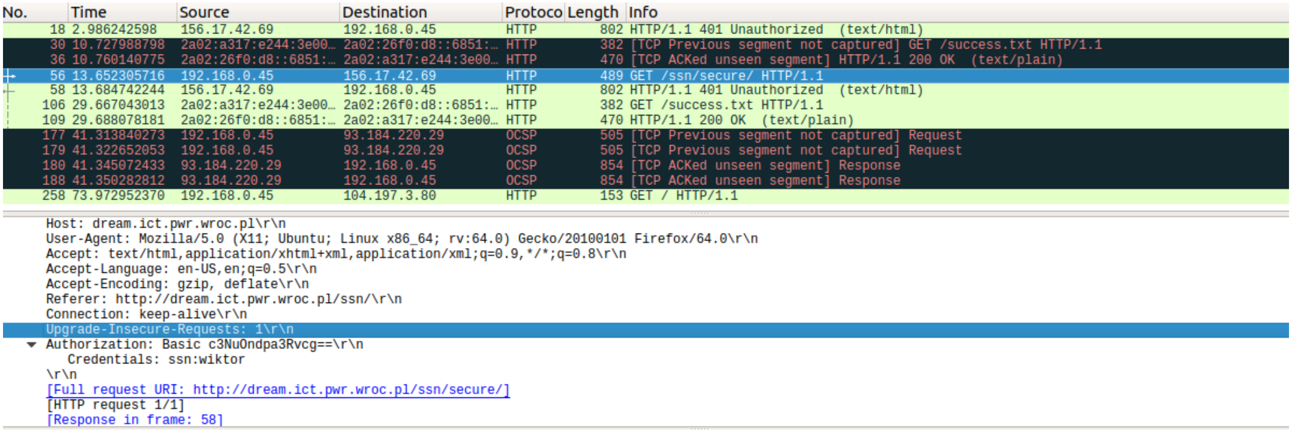
| No. | Time | Source | Destination | Protoco | Length | Info |
|---|---|---|---|---|---|---|
| 1079 | 167.155415545 | 156.17.193.37 | 192.168.0.45 | FTP | 188 | Response: 220   .. :: Welcome on  ftp.pwr.wroc.pl mirror server, provided by Wroclaw Centre of Ne… |
| 1091 | 174.368965802 | 192.168.0.45 | 156.17.193.37 | FTP | 82 | Request: USER anonymous |
| 1093 | 174.391272836 | 156.17.193.37 | 192.168.0.45 | FTP | 100 | Response: 331 Please specify the password. |
| 1110 | 177.314422914 | 192.168.0.45 | 156.17.193.37 | FTP | 79 | Request: PASS wiktor |
| 1112 | 177.335033090 | 156.17.193.37 | 192.168.0.45 | FTP | 89 | Response: 230 Login successful. |
| 1114 | 177.335119525 | 192.168.0.45 | 156.17.193.37 | FTP | 72 | Request: SYST |
| 1115 | 177.358611763 | 156.17.193.37 | 192.168.0.45 | FTP | 85 | Response: 215 UNIX Type: L8 |

Fig.  Wireshark captured FTP packet during connecting to ftp.pwr.wroc.pl server

Above screenshot depict that I used ‘anonymous’ username and password ‘wiktor’. Both names are visible during communication.

**Access a password protected WWW**

site: http://dream.ict.pwr.wroc.pl/ssn/secure/ -- use username "ssn" and password "secure". You may of course use a different password and see it fail. Observe how this user/pass information is sent from the web browser to the server.

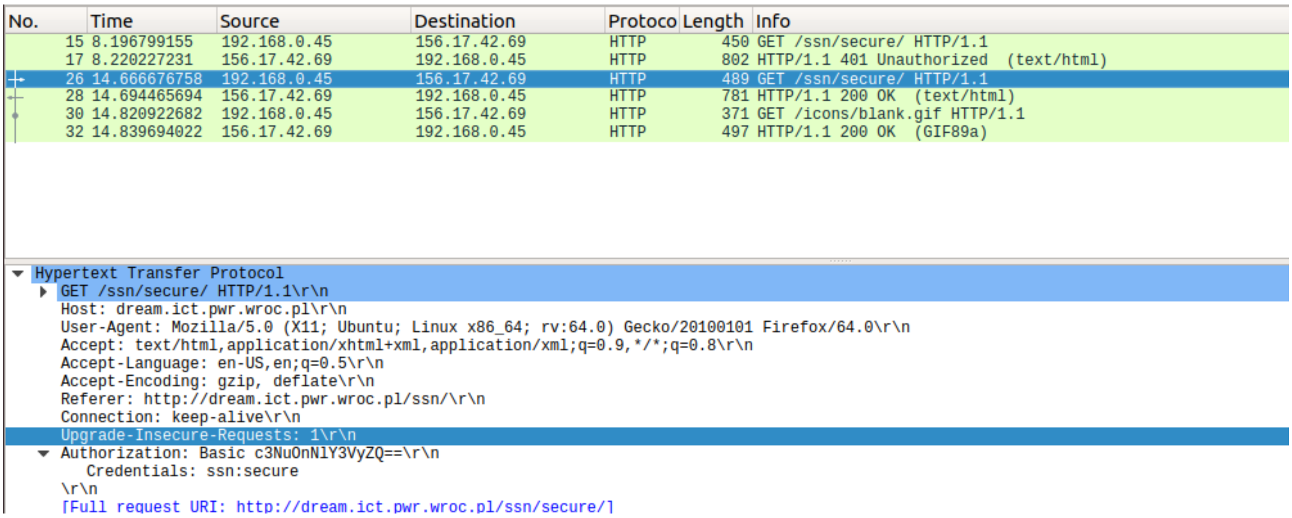


| No. | Time | Source | Destination | Protoco | Length | Info |
|---|---|---|---|---|---|---|
| 18 | 2.986242598 | 156.17.42.69 | 192.168.0.45 | HTTP | 802 | HTTP/1.1 401 Unauthorized  (text/html) |
| 30 | 10.727988798 | 2a02:a317:e244:3e00… | 2a02:26f0:d8::6851:… | HTTP | 382 | [TCP Previous segment not captured] GET /success.txt HTTP/1.1 |
| 36 | 10.760140775 | 2a02:26f0:d8::6851:… | 2a02:a317:e244:3e00… | HTTP | 470 | [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/plain) |
| 56 | 13.652305716 | 192.168.0.45 | 156.17.42.69 | HTTP | 489 | GET /ssn/secure/ HTTP/1.1 |
| 58 | 13.684742244 | 156.17.42.69 | 192.168.0.45 | HTTP | 802 | HTTP/1.1 401 Unauthorized  (text/html) |
| 106 | 29.667043013 | 2a02:a317:e244:3e00… | 2a02:26f0:d8::6851:… | HTTP | 382 | GET /success.txt HTTP/1.1 |
| 109 | 29.688078181 | 2a02:26f0:d8::6851:… | 2a02:a317:e244:3e00… | HTTP | 470 | HTTP/1.1 200 OK  (text/plain) |
| 177 | 41.313840273 | 192.168.0.45 | 93.184.220.29 | OCSP | 505 | [TCP Previous segment not captured] Request |
| 179 | 41.322652053 | 192.168.0.45 | 93.184.220.29 | OCSP | 505 | [TCP Previous segment not captured] Request |
| 180 | 41.345072433 | 93.184.220.29 | 192.168.0.45 | OCSP | 854 | [TCP ACKed unseen segment] Response |
| 188 | 41.350282812 | 93.184.220.29 | 192.168.0.45 | OCSP | 854 | [TCP ACKed unseen segment] Response |
| 258 | 73.972952370 | 192.168.0.45 | 104.197.3.80 | HTTP | 153 | GET / HTTP/1.1 |

```
    Host: dream.ict.pwr.wroc.pl\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://dream.ict.pwr.wroc.pl/ssn/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  ▾ Authorization: Basic c3NuOndpa3Rvcg==\r\n
       Credentials: ssn:wiktor
    \r\n
    [Full request URI: http://dream.ict.pwr.wroc.pl/ssn/secure/]
    [HTTP request 1/1]
    [Response in frame: 58]
```

Fig. Wireshark captured HTTP packets during connecting to http://dream.ict.pwr.wroc.pl/ssn/secure/ server site with wrong password.

Above screenshot from wireshark depict situation when I typed ‘ssn’ as a username and ‘wiktor’ as a password. Connection fail, but password which I typed is visible in Authorization section.



| No. | Time | Source | Destination | Protoco | Length | Info |
|---|---|---|---|---|---|---|
| 15 | 8.196799155 | 192.168.0.45 | 156.17.42.69 | HTTP | 450 | GET /ssn/secure/ HTTP/1.1 |
| 17 | 8.220227231 | 156.17.42.69 | 192.168.0.45 | HTTP | 802 | HTTP/1.1 401 Unauthorized  (text/html) |
| 26 | 14.666676758 | 192.168.0.45 | 156.17.42.69 | HTTP | 489 | GET /ssn/secure/ HTTP/1.1 |
| 28 | 14.694465694 | 156.17.42.69 | 192.168.0.45 | HTTP | 781 | HTTP/1.1 200 OK  (text/html) |
| 30 | 14.820922682 | 192.168.0.45 | 156.17.42.69 | HTTP | 371 | GET /icons/blank.gif HTTP/1.1 |
| 32 | 14.839694022 | 156.17.42.69 | 192.168.0.45 | HTTP | 497 | HTTP/1.1 200 OK  (GIF89a) |

```
▾ Hypertext Transfer Protocol
  ▸ GET /ssn/secure/ HTTP/1.1\r\n
    Host: dream.ict.pwr.wroc.pl\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://dream.ict.pwr.wroc.pl/ssn/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  ▾ Authorization: Basic c3NuOnNlY3VyZQ==\r\n
       Credentials: ssn:secure
    \r\n
    [Full request URI: http://dream.ict.pwr.wroc.pl/ssn/secure/]
```

Fig. Wireshark captured HTTP packets during connecting to http://dream.ict.pwr.wroc.pl/ssn/secure/ server site with correct password.