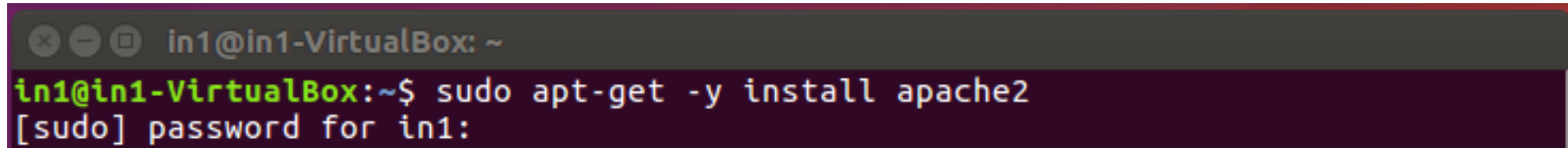


Hands-on

Set up web server

- Open terminal
- Type command : `sudo apt-get -y install apache2`

A terminal window with a dark purple background and a grey title bar. The title bar contains window control icons and the text 'in1@in1-VirtualBox: ~'. The terminal shows the command 'in1@in1-VirtualBox:~\$ sudo apt-get -y install apache2' in green and white text. Below it, the prompt '[sudo] password for in1:' is displayed in white text.

```
in1@in1-VirtualBox: ~  
in1@in1-VirtualBox:~$ sudo apt-get -y install apache2  
[sudo] password for in1:
```

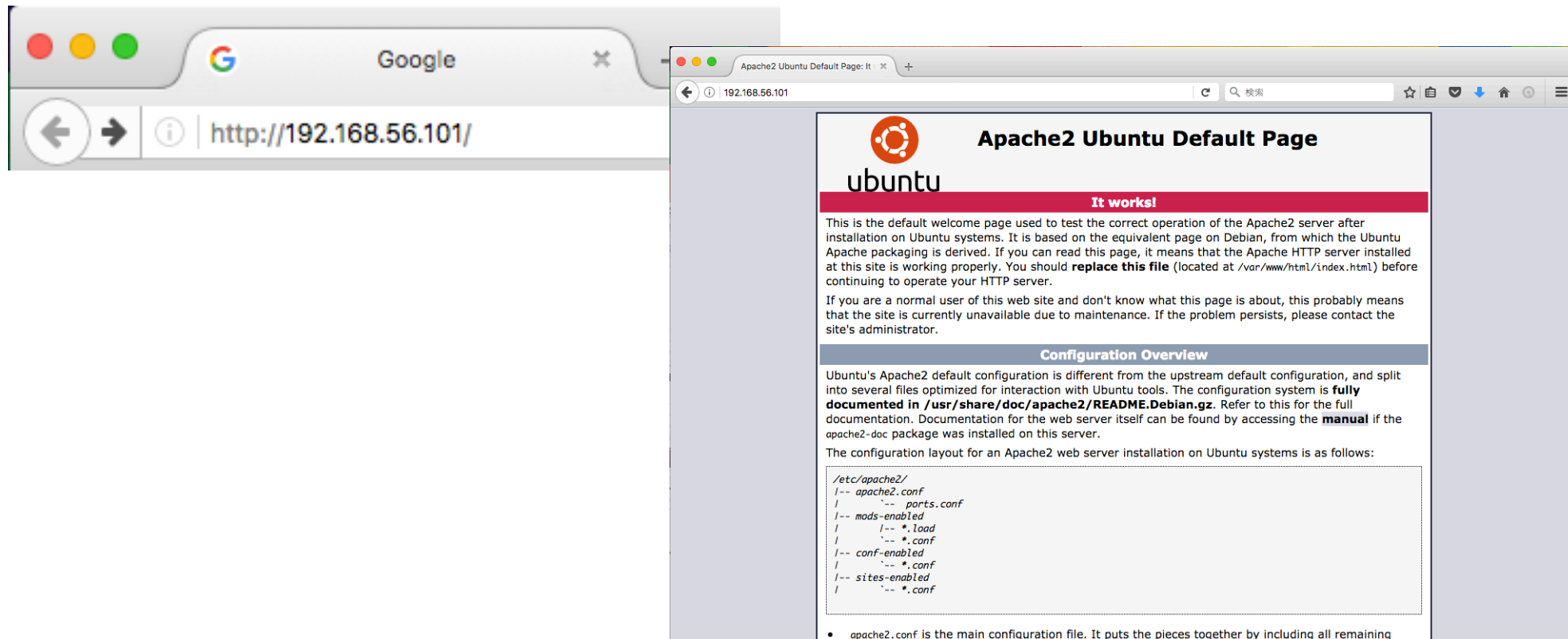
Set up web server

- By using netstat command, you can check apache2 is listening on port 80 with PID 4767.

```
in1@in1-VirtualBox: ~  
in1@in1-VirtualBox:~$ sudo netstat -tnlp  
[sudo] password for in1:  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name  
tcp        0      0 127.0.1.1:53           0.0.0.0:*                LISTEN      851/dnsmasq  
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      761/sshd  
tcp6       0      0 :::80                  :::*                    LISTEN      4767/apache2  
tcp6       0      0 :::22                  :::*                    LISTEN      761/sshd  
in1@in1-VirtualBox:~$
```

Set up web server

- Connect to your web server running on VM from your host machine. You can see default index page.



Monitoring web traffic

- While accessing web server, watch host-only interface.(in my environment, enp0s8)

The image shows a Wireshark packet capture window titled "Capturing from enp0s8". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for packet capture and analysis. Below the toolbar is a display filter field with the text "Apply a display filter ... <Ctrl-/>".

The main packet list table shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0a:00:27:00:00:00	Broadcast	ARP	60	Who has 192.168.56.101? Tell 192.168.56.1
2	0.000014579	PcsCompu_5f:49:da	0a:00:27:00:00:00	ARP	42	192.168.56.101 is at 08:00:27:5f:49:da
3	0.000140346	192.168.56.1	192.168.56.101	TCP	78	55733 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3
4	0.000160488	192.168.56.101	192.168.56.1	TCP	74	80 → 55733 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MS
5	0.000241221	192.168.56.1	192.168.56.101	TCP	66	55733 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=
6	0.000418516	192.168.56.1	192.168.56.101	HTTP	521	GET / HTTP/1.1
7	0.000440077	192.168.56.101	192.168.56.1	TCP	66	80 → 55733 [ACK] Seq=1 Ack=456 Win=30080 Len=0 TSval
8	0.002507979	192.168.56.101	192.168.56.1	HTTP	3591	HTTP/1.1 200 OK (text/html)

The packet details pane for the selected packet (No. 6) shows the following structure:

- Frame 6: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface 0
- Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu_5f:49:da (08:00:27:5f:49:da)
- Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
- Transmission Control Protocol, Src Port: 55733, Dst Port: 80, Seq: 1, Ack: 1, Len: 455
- Hypertext Transfer Protocol

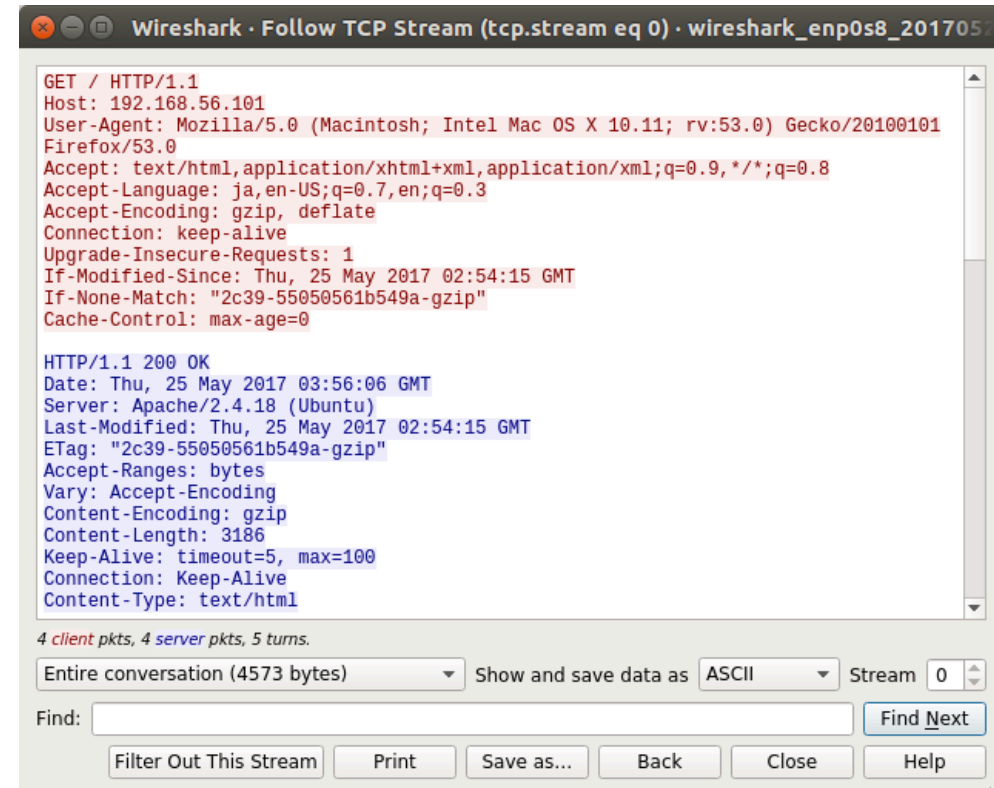
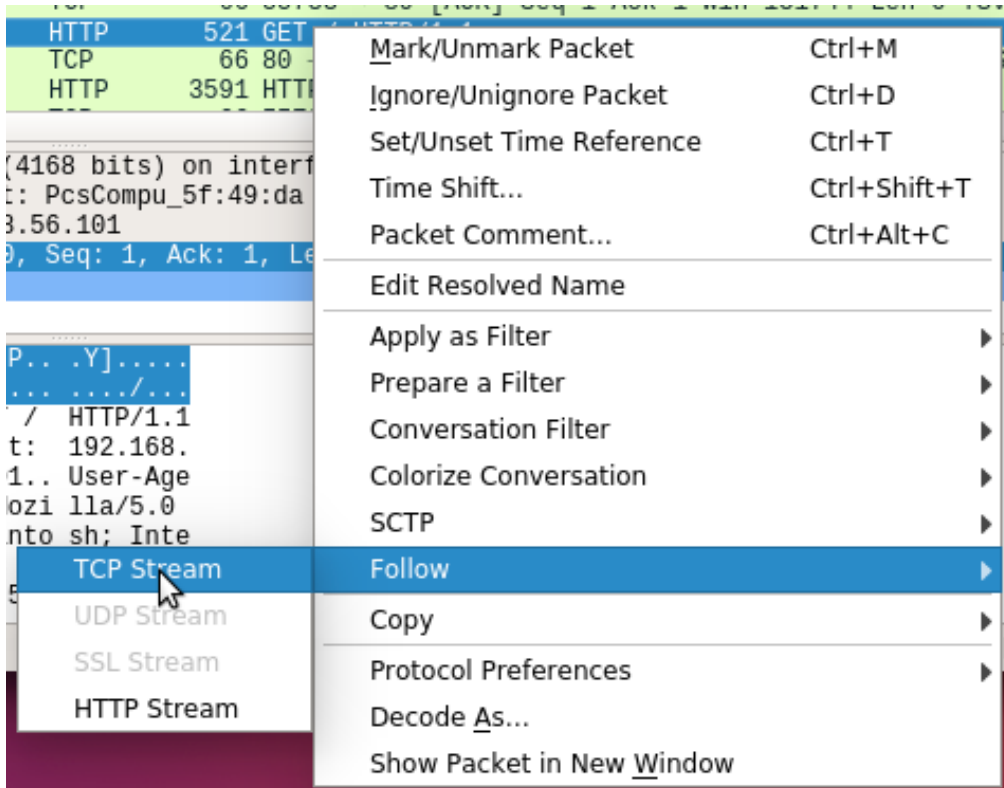
The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion of the packet is:

```
...P...Y]....  
...L.../...  
a.GET / HTTP/1.1  
..Host: 192.168.  
56.101.. User-Age  
nt: Mozi lla/5.0  
(Macinto sh; Inte  
l Mac OS X 10.11  
; rv:53. 0) Gecko
```

The status bar at the bottom indicates: Transmission Control Protocol (tcp), 32 bytes | Packets: 43 · Displayed: 43 (100.0%) | Profile: Default

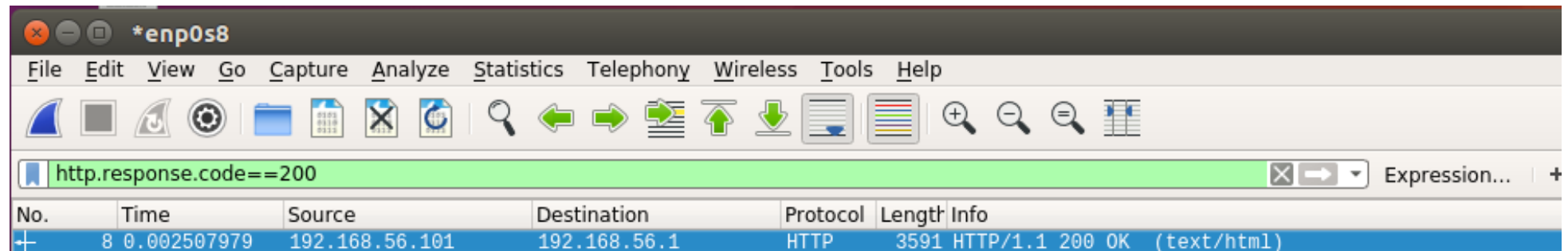
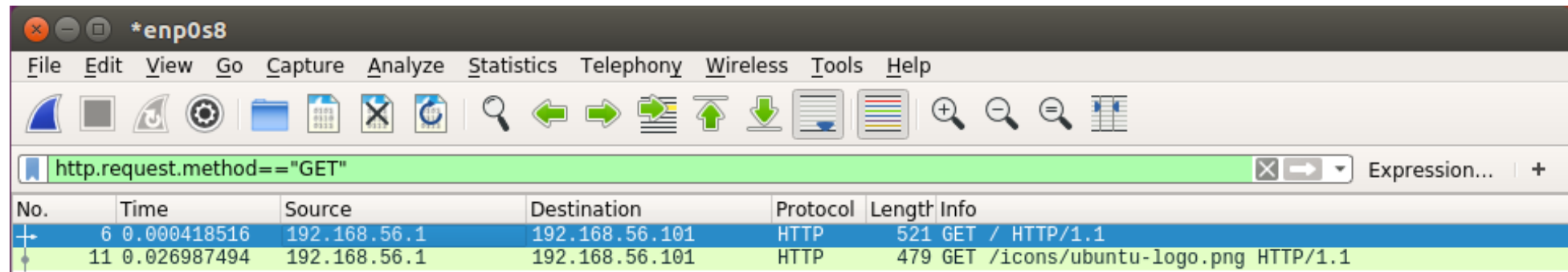
Monitoring web traffic

- Ctrl-click on web request packet, and choose “Follow-tcp stream”, you can extract content in specific tcp connection.



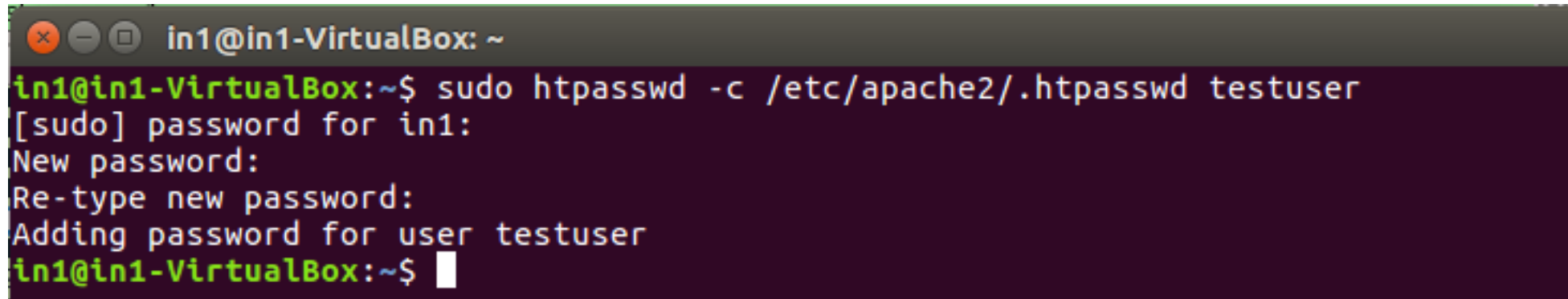
Tips

- By applying some filters, you can extract specific packet.



Basic Authentication

- Let's create authenticated web page.
- Create the password file for basic authentication. Set username "testuser", and password "testpass".



```
in1@in1-VirtualBox: ~  
in1@in1-VirtualBox:~$ sudo htpasswd -c /etc/apache2/.htpasswd testuser  
[sudo] password for in1:  
New password:  
Re-type new password:  
Adding password for user testuser  
in1@in1-VirtualBox:~$
```

Basic Authentication

- Edit /etc/apache2/apache2.conf
- Add these lines and restart apache2.

```
in1@in1-VirtualBox: ~  
in1@in1-VirtualBox:~$ sudo vi /etc/apache2/apache2.conf  
[sudo] password for in1:  
in1@in1-VirtualBox:~$  
in1@in1-VirtualBox:~$ sudo service apache2 restart  
in1@in1-VirtualBox:~$
```

```
<Directory "/var/www/html">  
    AuthType Basic  
    AuthName "Hands-on BasicAuth"  
    AuthUserFile /etc/apache2/.htpasswd  
    Require valid-user  
</Directory>
```

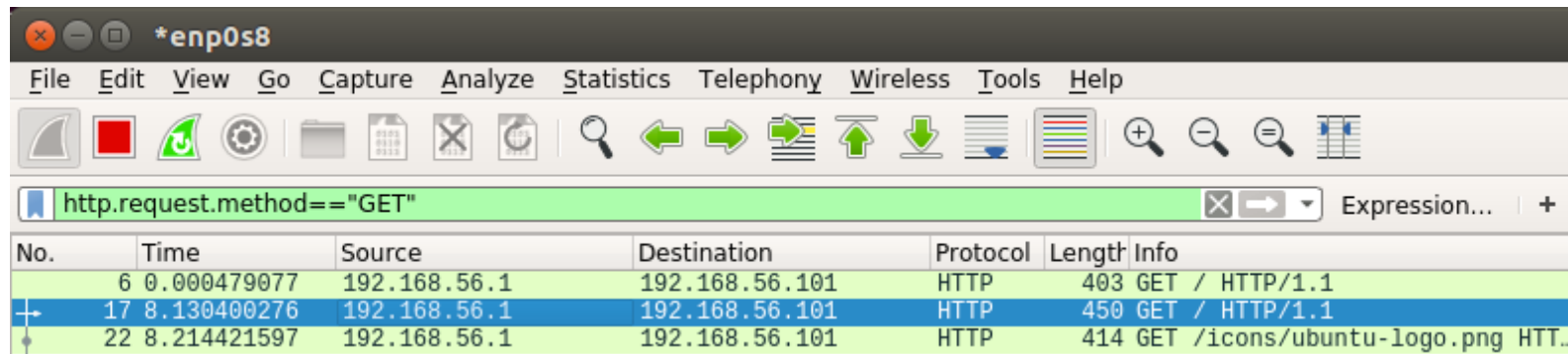
Basic Authentication

- Connect to web server.
- To access web page, type username and password.



Basic Authentication

- Using wireshark, you can see authentication packet.

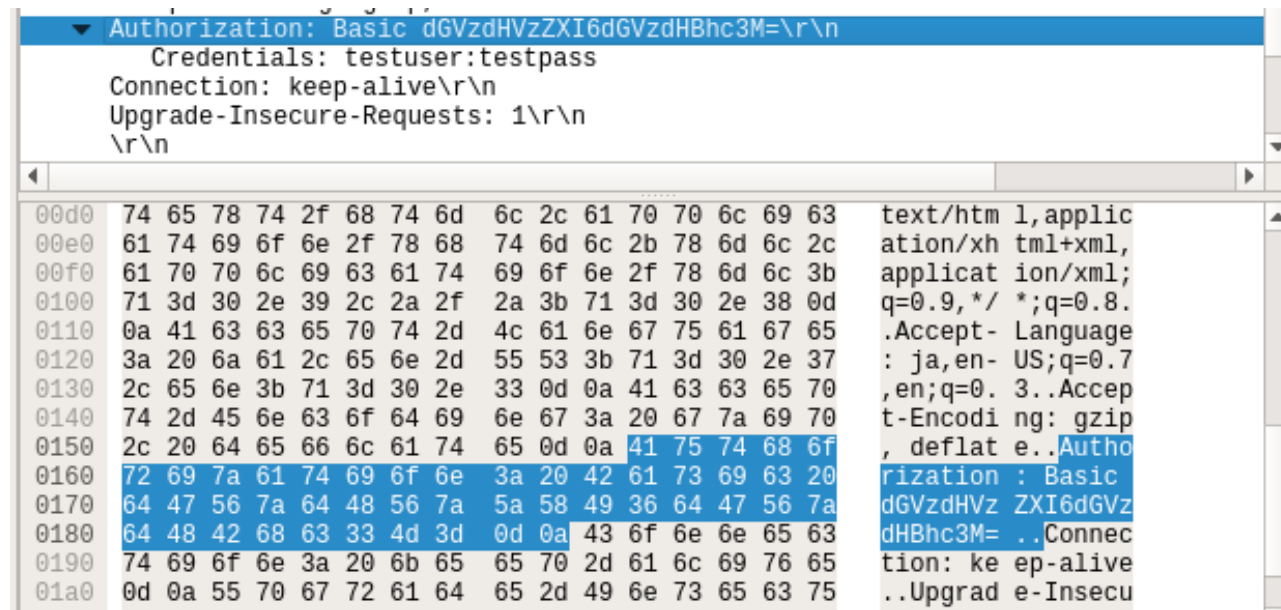


No.	Time	Source	Destination	Protocol	Length	Info
6	0.000479077	192.168.56.1	192.168.56.101	HTTP	403	GET / HTTP/1.1
17	8.130400276	192.168.56.1	192.168.56.101	HTTP	450	GET / HTTP/1.1
22	8.214421597	192.168.56.1	192.168.56.101	HTTP	414	GET /icons/ubuntu-logo.png HTTP/1.1

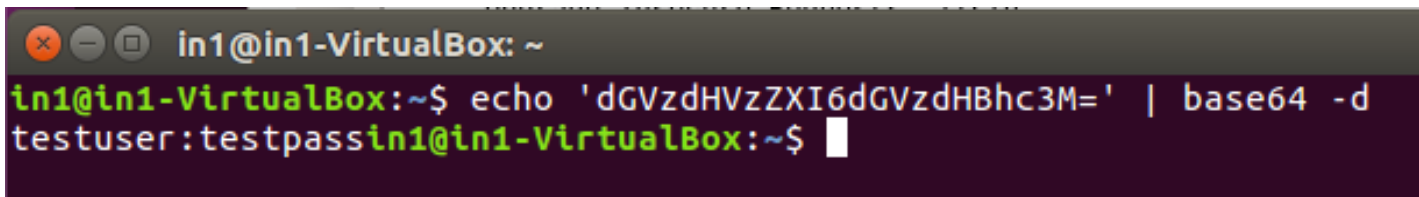
```
▶ Frame 17: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits) on interface 0
▶ Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu_5f:49:da (08:00:27:5f:49:da)
▶ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
▶ Transmission Control Protocol, Src Port: 59320, Dst Port: 80, Seq: 1, Ack: 1, Len: 384
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: 192.168.56.101\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:53.0) Gecko/20100101 Firefox/53.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: ja,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  ▶ Authorization: Basic dGVzdHVzZXI6dGVzdHBhc3M=\r\n
    \r\n
    [Full request URI: http://192.168.56.101/]
    [HTTP request 1/2]
```

Basic Authentication

- You can see username and password in packet.
- These information are encoded with base64.



```
▼ Authorization: Basic dGVzdHVzZXI6dGVzdHBhc3M=\r\n
  Credentials: testuser:testpass
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
00d0 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8.
00e0 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c
00f0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b
0100 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d
0110 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65
0120 3a 20 6a 61 2c 65 6e 2d 55 53 3b 71 3d 30 2e 37
0130 2c 65 6e 3b 71 3d 30 2e 33 0d 0a 41 63 63 65 70
0140 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70
0150 2c 20 64 65 66 6c 61 74 65 0d 0a 41 75 74 68 6f
0160 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20
0170 64 47 56 7a 64 48 56 7a 5a 58 49 36 64 47 56 7a
0180 64 48 42 68 63 33 4d 3d 0d 0a 43 6f 6e 6e 65 63
0190 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65
01a0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75
..Accept-Language: ja,en-US;q=0.7,en;q=0.3..Accept-Encoding: gzip, deflate..Autho
rization: Basic
dGVzdHVz ZXI6dGVz
dHBhc3M= ..Connec
tion: ke ep-alive
..Upgrad e-Insecu
```



```
in1@in1-VirtualBox: ~
in1@in1-VirtualBox:~$ echo 'dGVzdHVzZXI6dGVzdHBhc3M=' | base64 -d
testuser:testpassin1@in1-VirtualBox:~$
```