

TASK 5
Jaringan Komputer



Nama : Indah Frisilina Putri
NIM : 09011181419010
Kelas : SK 5A
Dosen Pengampuh : Deris Setiawan M.T., Ph.D

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

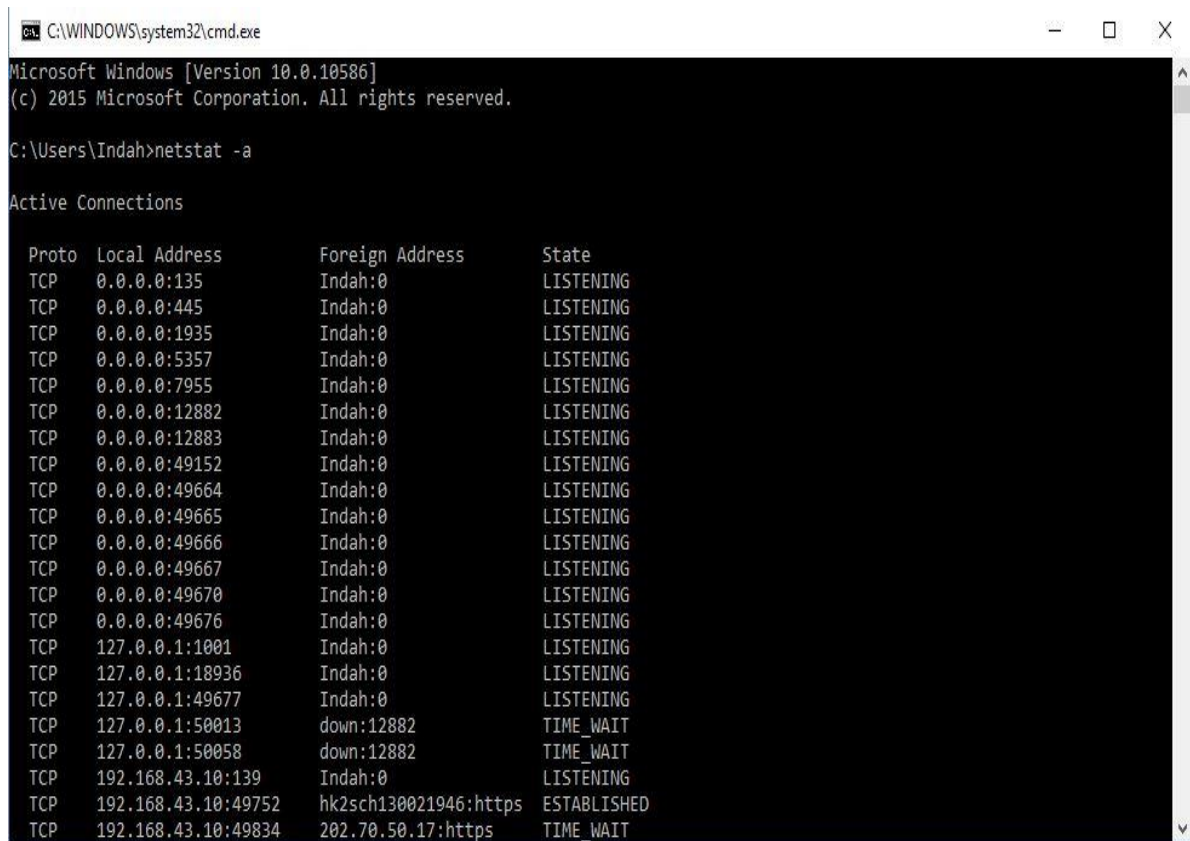
Universitas Sriwijaya

2016

Menggunakan command prompt.

Ketik perintah netstat -a di command prompt ketika web telah dibuat pada chrome.

Tampilannya seperti ini :



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Indah>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              Indah:0                 LISTENING
TCP   0.0.0.0:445              Indah:0                 LISTENING
TCP   0.0.0.0:1935             Indah:0                 LISTENING
TCP   0.0.0.0:5357             Indah:0                 LISTENING
TCP   0.0.0.0:7955             Indah:0                 LISTENING
TCP   0.0.0.0:12882            Indah:0                 LISTENING
TCP   0.0.0.0:12883            Indah:0                 LISTENING
TCP   0.0.0.0:49152            Indah:0                 LISTENING
TCP   0.0.0.0:49664            Indah:0                 LISTENING
TCP   0.0.0.0:49665            Indah:0                 LISTENING
TCP   0.0.0.0:49666            Indah:0                 LISTENING
TCP   0.0.0.0:49667            Indah:0                 LISTENING
TCP   0.0.0.0:49670            Indah:0                 LISTENING
TCP   0.0.0.0:49676            Indah:0                 LISTENING
TCP   127.0.0.1:1001           Indah:0                 LISTENING
TCP   127.0.0.1:18936          Indah:0                 LISTENING
TCP   127.0.0.1:49677          Indah:0                 LISTENING
TCP   127.0.0.1:50013          down:12882              TIME_WAIT
TCP   127.0.0.1:50058          down:12882              TIME_WAIT
TCP   192.168.43.10:139        Indah:0                 LISTENING
TCP   192.168.43.10:49752      hk2sch130021946:https  ESTABLISHED
TCP   192.168.43.10:49834      202.70.50.17:https     TIME_WAIT
```

```

TCP 127.0.0.1:49677 Indah:0 LISTENING
TCP 127.0.0.1:50013 down:12882 TIME_WAIT
TCP 127.0.0.1:50058 down:12882 TIME_WAIT
TCP 192.168.43.10:139 Indah:0 LISTENING
TCP 192.168.43.10:49752 hk2sch130021946:https ESTABLISHED
TCP 192.168.43.10:49834 202.70.50.17:https TIME_WAIT
TCP 192.168.43.10:49836 202.70.50.17:https TIME_WAIT
TCP 192.168.43.10:49837 202.70.50.17:https TIME_WAIT
TCP 192.168.43.10:49838 202.70.50.17:https TIME_WAIT
TCP 192.168.43.10:49927 a-0003:https ESTABLISHED
^C
C:\Users\Indah>

```

Percobaan menggunakan Wireshark.

Ke situs berniaga.com

Tampilan nya seperti ini :

1785	23.1842230	192.168.43.10	157.240.7.35	TCP	54	50099-443	[ACK] Seq=435 Ack=3550 win=261632 Len=0
1786	23.1844090	192.168.43.10	157.240.7.35	TLSv1.2	92		Application data
1787	23.2244560	104.68.32.229	192.168.43.10	TCP	1448		[TCP segment of a reassembled PDU]
1788	23.2245860	192.168.43.10	104.68.32.229	TCP	54	50117-80	[ACK] Seq=340 Ack=2789 win=262144 Len=0
1789	23.2444270	13.107.4.50	192.168.43.10	TCP	1448		[TCP Retransmission] [TCP segment of a reassembled PDU]
1790	23.2445290	192.168.43.10	13.107.4.50	TCP	66	49981-80	[ACK] Seq=3575 Ack=225359 win=604 Len=0 SLE=226753 SRE=228147
1791	23.2574540	31.13.78.17	192.168.43.10	TLSv1.2	135		[TCP Previous segment not captured] Application data
1792	23.2575000	31.13.78.17	192.168.43.10	TLSv1.2	312		[TCP out-of-order] New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1793	23.2575930	192.168.43.10	31.13.78.17	TCP	66	[TCP Dup Ack 1775#1]	50120-443 [ACK] Seq=649 Ack=3173 win=262144 Len=0 SLE=3431 SRE=3512
1794	23.2577800	192.168.43.10	31.13.78.17	TCP	54	50120-443	[ACK] Seq=649 Ack=3512 win=261632 Len=0
1795	23.2590590	192.168.43.10	31.13.78.17	TLSv1.2	92		Application data
1796	23.2738090	104.68.58.228	192.168.43.10	TCP	1448		[TCP out-of-order] [TCP segment of a reassembled PDU]
1797	23.2738110	31.13.78.17	192.168.43.10	TCP	54	443-50120	[ACK] Seq=3512 Ack=649 win=16384 Len=0
1798	23.2739350	192.168.43.10	104.68.58.228	TCP	66	50079-80	[ACK] Seq=749 Ack=79345 win=262144 Len=0 SLE=83527 SRE=84921
1799	23.3204310	104.68.32.229	192.168.43.10	TCP	1448		[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
1800	23.3305590	192.168.43.10	104.68.32.229	TCP	66	[TCP Dup Ack 1788#1]	50117-80 [ACK] Seq=340 Ack=2789 win=262144 Len=0 SLE=26487 SRE=27881
1801	23.3722910	104.68.32.229	192.168.43.10	TCP	1448		[TCP segment of a reassembled PDU]
1802	23.3722960	157.240.7.35	192.168.43.10	TCP	54	443-50099	[ACK] Seq=3550 Ack=473 win=30464 Len=0
1803	23.3723880	192.168.43.10	104.68.32.229	TCP	66	[TCP Dup Ack 1788#2]	50117-80 [ACK] Seq=340 Ack=2789 win=262144 Len=0 SLE=26487 SRE=29275
1804	23.4087900	13.107.4.50	192.168.43.10	TCP	1448		[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
1805	23.4088800	192.168.43.10	13.107.4.50	TCP	74	[TCP Dup Ack 1790#1]	49981-80 [ACK] Seq=3575 Ack=225359 win=604 Len=0 SLE=229541 SRE=230935 SLE=226
1806	23.4403650	104.68.32.229	192.168.43.10	TCP	1448		[TCP out-of-order] [TCP segment of a reassembled PDU]
1807	23.4405080	192.168.43.10	104.68.32.229	TCP	66	50117-80	[ACK] Seq=340 Ack=4183 win=262144 Len=0 SLE=26487 SRE=29275
1808	23.4444260	31.13.78.17	192.168.43.10	TCP	54	[TCP Previous segment not captured]	443-50120 [ACK] Seq=649 Ack=687 win=16384 Len=0
1809	23.5043230	13.107.4.50	192.168.43.10	TCP	1448		[TCP Retransmission] [TCP segment of a reassembled PDU]
1810	23.5043810	192.168.43.10	13.107.4.50	TCP	74	49981-80	[ACK] Seq=3575 Ack=225359 win=598 Len=0 SLE=229541 SRE=230935 SLE=226753 SRE=228147
1811	23.5807990	104.68.58.228	192.168.43.10	TCP	1448		[TCP Retransmission] [TCP segment of a reassembled PDU]

Wi-Fi [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	103.234.120.204	192.168.43.10	TCP	1448	80->50813 [ACK] Seq=1 Ack=1 win=1672 Len=1394
2	0.000068800	192.168.43.10	103.234.120.204	TCP	54	[TCP ACK] Previous segment not captured [TCP segment of a reassembled PDU]
3	0.347360000	192.168.43.10	103.234.120.204	HTTP	861	[TCP ACKed unseen segment] GET /edged/1/release2/13ymen2534c1fme1x1woet10czfnpjsod4bycsqwg9h908s1qrznd
4	0.419258000	103.234.120.204	192.168.43.10	TCP	1448	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
5	0.419354000	192.168.43.10	103.234.120.204	TCP	66	[TCP Dup ACK 3#1] [TCP ACKed unseen segment] 50813->80 [ACK] Seq=808 Ack=2493 win=386 Len=0 SLE=3887 SRE=6675
6	0.437513000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
7	0.437593000	192.168.43.10	103.234.120.204	TCP	66	[TCP Dup ACK 3#2] 50813->80 [ACK] Seq=808 Ack=2493 win=386 Len=0 SLE=3887 SRE=6675
8	0.448004000	103.234.120.204	192.168.43.10	TCP	1448	[TCP Fast Retransmission] [TCP segment of a reassembled PDU]
9	0.448134000	192.168.43.10	103.234.120.204	TCP	54	50813->80 [ACK] Seq=808 Ack=6675 win=381 Len=0
10	0.519059000	103.234.120.204	192.168.43.10	TCP	1448	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
11	0.519133000	192.168.43.10	103.234.120.204	TCP	66	[TCP Dup ACK 9#1] 50813->80 [ACK] Seq=808 Ack=6675 win=381 Len=0 SLE=8069 SRE=9463
12	0.530298000	103.234.120.204	192.168.43.10	TCP	1448	[TCP Retransmission] [TCP segment of a reassembled PDU]
13	0.530384000	192.168.43.10	103.234.120.204	TCP	54	50813->80 [ACK] Seq=808 Ack=9463 win=381 Len=0
14	0.566315000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
15	0.593434000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
16	0.595521000	192.168.43.10	103.234.120.204	TCP	54	50813->80 [ACK] Seq=808 Ack=12251 win=375 Len=0
17	0.609597000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
18	0.625252000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
19	0.625408000	192.168.43.10	103.234.120.204	TCP	54	50813->80 [ACK] Seq=808 Ack=15039 win=375 Len=0
20	0.665128000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
21	0.670115000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
22	0.670210000	192.168.43.10	103.234.120.204	TCP	54	50813->80 [ACK] Seq=808 Ack=17827 win=370 Len=0
23	0.704469000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
24	0.720348000	103.234.120.204	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
25	0.720427000	192.168.43.10	103.234.120.204	TCP	54	50813->80 [ACK] Seq=808 Ack=20615 win=370 Len=0
26	0.756729000	103.234.120.204	192.168.43.10	TCP	1448	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
27	0.756790000	192.168.43.10	103.234.120.204	TCP	66	[TCP Dup ACK 25#1] 50813->80 [ACK] Seq=808 Ack=20615 win=370 Len=0 SLE=22009 SRE=23403

Frame 160: 1126 bytes on wire (9008 bits), 1126 bytes captured (9008 bits) on Interface 0
 Ethernet II, Src: IntelCor_af:cc:02:92:af:cc:47, Dst: bc:20:10:4a:0c:88
 Internet Protocol Version 4, Src: 192.168.43.10, Dst: 210.210.179.94
 Hypertext Transfer Protocol, Content-Type: application/javascript

```

0000  bc 20 10 4a 0c 88 0c d2 92 af cc 47 08 00 45 00  . . . . .G..E.
0010  04 58 48 00 40 00 80 06 3b ed 0c a8 20 0a d2    .M.8...+...
0020  b3 se ce dd 00 50 da d6 99 57 48 2f 17 bb 50 18  .A...P.
0030  04 00 bb 22 00 00 47 45 54 20 2f 20 48 54 54 50  . . . . .GE T / HTTP
0040  2f 11 2e 31 0f 0a 41 63 63 63 70 74 3a 20 74 65  /1...ACAPT:te
0050  78 2f 7f e8 71 6d 6c 7c 70 61 70 70 6c 63 61  .f/rt1c...
  
```

File: C:\Users\linda\AppData\Local\Temp\... Packets: 1259 - Displayed: 1259 (100.0%) - Dropped: 0 (0.0%)

Wi-Fi [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
154	3.075359000	192.168.43.10	210.210.179.94	TCP	66	50909->80 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
156	3.130293000	210.210.179.94	192.168.43.10	TCP	66	80->50909 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512
157	3.130478000	192.168.43.10	210.210.179.94	TCP	54	50909->80 [ACK] Seq=1 Ack=1 win=262144 Len=0
160	3.310309000	192.168.43.10	210.210.179.94	HTTP	1126	GET / HTTP/1.1
161	3.214515000	210.210.179.94	192.168.43.10	TCP	1448	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
162	3.214559000	192.168.43.10	210.210.179.94	TCP	66	[TCP Dup ACK 160#1] 50909->80 [ACK] Seq=1073 Ack=1 win=262144 Len=0 SLE=4183 SRE=5577
163	3.214781000	210.210.179.94	192.168.43.10	TCP	1448	[TCP out-of-order] [TCP segment of a reassembled PDU]
164	3.214832000	192.168.43.10	210.210.179.94	TCP	66	[TCP Dup ACK 160#2] 50909->80 [ACK] Seq=1073 Ack=1 win=262144 Len=0 SLE=2789 SRE=5577
167	3.237231000	210.210.179.94	192.168.43.10	TCP	1448	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
168	3.237325000	192.168.43.10	210.210.179.94	TCP	74	[TCP Dup ACK 160#3] 50909->80 [ACK] Seq=1073 Ack=1 win=262144 Len=0 SLE=6971 SRE=8365 SLE=2789 SRE=5577
169	3.248223000	210.210.179.94	192.168.43.10	TCP	1448	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
170	3.248294000	192.168.43.10	210.210.179.94	TCP	82	[TCP Dup ACK 160#4] 50909->80 [ACK] Seq=1073 Ack=1 win=262144 Len=0 SLE=9759 SRE=11153 SLE=6971 SRE=8365
171	3.256629000	210.210.179.94	192.168.43.10	TCP	1448	[TCP out-of-order] [TCP segment of a reassembled PDU]
172	3.256745000	192.168.43.10	210.210.179.94	TCP	82	[TCP Dup ACK 160#5] 50909->80 [ACK] Seq=1073 Ack=1 win=262144 Len=0 SLE=1395 SRE=5577 SLE=9759 SRE=8365
173	3.279563000	210.210.179.94	192.168.43.10	TCP	1448	[TCP out-of-order] [TCP segment of a reassembled PDU]
174	3.279840000	192.168.43.10	210.210.179.94	TCP	74	50909->80 [ACK] Seq=1073 Ack=5577 win=262144 Len=0 SLE=9759 SRE=11153 SLE=6971 SRE=8365
175	3.290333000	210.210.179.94	192.168.43.10	TCP	1448	[TCP out-of-order] [TCP segment of a reassembled PDU]
176	3.290329000	192.168.43.10	210.210.179.94	TCP	66	[TCP Dup ACK 174#1] 50909->80 [ACK] Seq=1073 Ack=5577 win=262144 Len=0 SLE=6971 SRE=11153
177	3.300427000	210.210.179.94	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
178	3.300523000	192.168.43.10	210.210.179.94	TCP	66	[TCP Dup ACK 174#2] 50909->80 [ACK] Seq=1073 Ack=5577 win=262144 Len=0 SLE=6971 SRE=12547
179	3.320313000	210.210.179.94	192.168.43.10	TCP	1448	[TCP Fast Retransmission] [TCP segment of a reassembled PDU]
180	3.320510000	192.168.43.10	210.210.179.94	TCP	54	50909->80 [ACK] Seq=1073 Ack=12547 win=262144 Len=0
182	3.336490000	210.210.179.94	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]
183	3.336640000	192.168.43.10	210.210.179.94	TCP	54	50909->80 [ACK] Seq=1073 Ack=13941 win=262144 Len=0
184	3.339894000	210.210.179.94	192.168.43.10	TCP	1448	[TCP out-of-order] 80->50909 [ACK] Seq=1 Ack=1073 win=31744 Len=1394
185	3.339967000	192.168.43.10	210.210.179.94	TCP	66	[TCP Dup ACK 183#1] 50909->80 [ACK] Seq=1073 Ack=13941 win=262144 Len=0 SLE=1 SRE=1395
187	3.366423000	210.210.179.94	192.168.43.10	TCP	1448	[TCP segment of a reassembled PDU]

The screenshot shows the 'Follow TCP Stream' window in Wireshark, titled 'Follow TCP Stream (tcp.stream eq 10)'. The window displays the 'Stream Content' for a selected packet. The content is an HTTP 301 Moved Permanently response. The request part shows a GET request for '/ HTTP/1.1' with various headers including Accept, Accept-Language, User-Agent (Mozilla/5.0), and Host (berniaga.com). The response part shows 'HTTP/1.1 301 Moved Permanently' with headers like Date, Content-Type, Content-Length, Location (http://olx.co.id/), Expires, Cache-Control, and Access-Control-Allow-Origin. The body of the response is HTML code indicating a permanent move to http://olx.co.id/.

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586
Accept-Encoding: gzip, deflate
Host: berniaga.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Mon, 19 Sep 2016 09:32:35 GMT
Content-Type: text/html
Content-Length: 178
Connection: close
Location: http://olx.co.id/
Expires: Thu, 31 Dec 2037 23:55:55 GMT
Cache-Control: max-age=315360000
Req-Time: 0.000
Access-Control-Allow-Origin: *
Allow: GET, POST, HEAD

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Analisa

Wireshark, perangkat lunak ini membantu untuk menangkap/merekam dan melihat traffic yang sedang berjalan di sebuah jaringan komputer. Wireshark digunakan untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap data/informasi yang melewati jaringan yang sedang kita amati. Dengan wireshark dapat dilihat proses pengiriman data dari komputer ke web yang dituju.

Ketika kita mengetik **http** dan tekan enter, kita tidak perlu lagi untuk mengingat setiap kali mnyaring paket. Klik kanan pada paket yang ingin di analisis lalu pilih Follow TCP Stream.

Get menunjukkan permintaan data yang dikirim dari sumber tertentu.

Post → Data yang diserahkan untuk di proses ke sumber daya tertentu dengan login.

Respon → mengirim data ke web.

Kita dapat menemukan seluruh kode status HTTP tanggal menunjukkan waktu selama respon yang dikeluarkan.