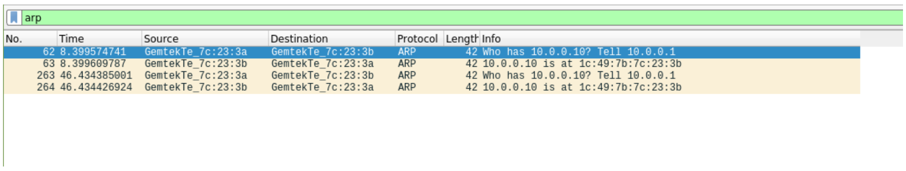
Практическая работа №9
Вариант 6

Кирилл Денисов ИВБО-02-19

16 декабря 2021 г.

Часть 1. Подготовка операционной системы компьютера content...

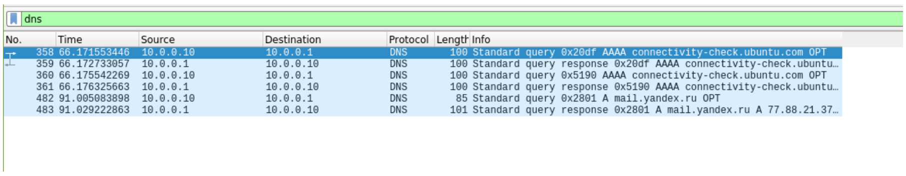
Подготовка операционной системы компьютера



arp

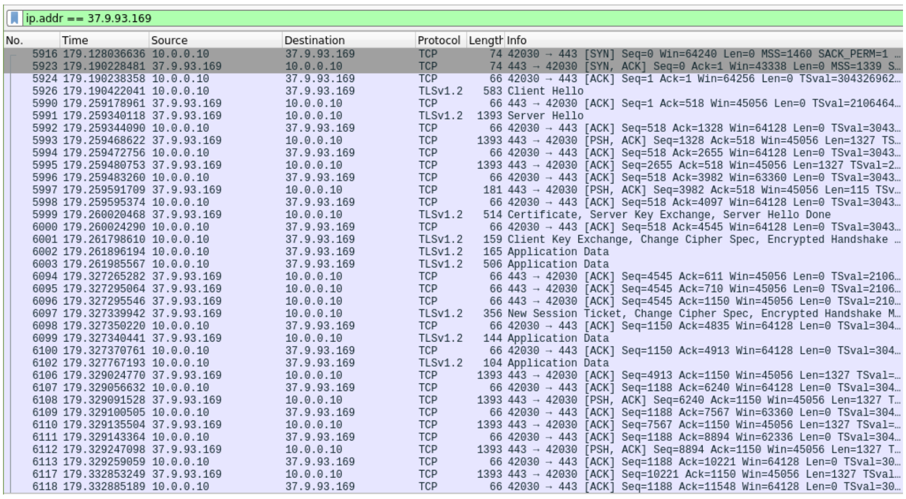
No.	Time	Source	Destination	Protocol	Length	Info
62	8.399574741	GemtekTe_7c:23:3a	GemtekTe_7c:23:3b	ARP	42	Who has 10.0.0.10? Tell 10.0.0.1
63	8.399609787	GemtekTe_7c:23:3b	GemtekTe_7c:23:3a	ARP	42	10.0.0.10 is at 1c:49:7b:7c:23:3b
263	46.434385001	GemtekTe_7c:23:3a	GemtekTe_7c:23:3b	ARP	42	Who has 10.0.0.10? Tell 10.0.0.1
264	46.434426924	GemtekTe_7c:23:3b	GemtekTe_7c:23:3a	ARP	42	10.0.0.10 is at 1c:49:7b:7c:23:3b

Рисунок 1



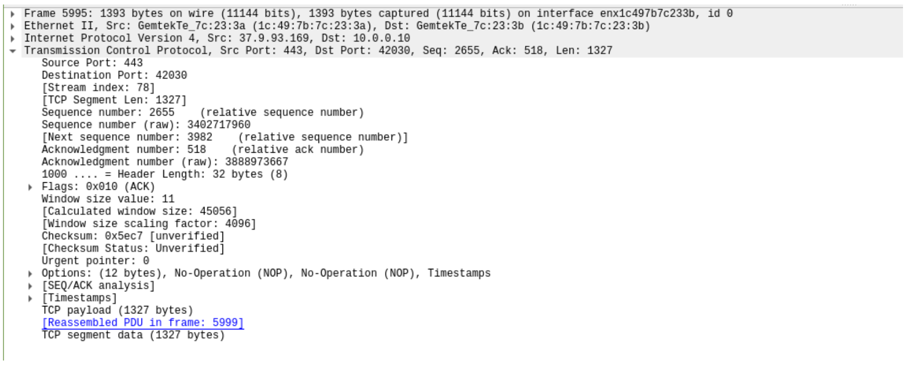
```
dns
No.  Time          Source     Destination Protocol Length Info
 358 66.171553446  10.0.0.10  10.0.0.1    DNS      100 Standard query 0x20df AAAA connectivity-check.ubuntu.com OPT
 359 66.172733057  10.0.0.1   10.0.0.10   DNS      100 Standard query response 0x20df AAAA connectivity-check.ubuntu…
 360 66.175542269  10.0.0.10  10.0.0.1    DNS      100 Standard query 0x5190 AAAA connectivity-check.ubuntu.com OPT
 361 66.176325663  10.0.0.1   10.0.0.10   DNS      100 Standard query response 0x5190 AAAA connectivity-check.ubuntu…
 482 91.005083898  10.0.0.10  10.0.0.1    DNS       85 Standard query 0x2801 A mail.yandex.ru OPT
 483 91.029222863  10.0.0.1   10.0.0.10   DNS      101 Standard query response 0x2801 A mail.yandex.ru A 77.88.21.37…
```

Рисунок 2



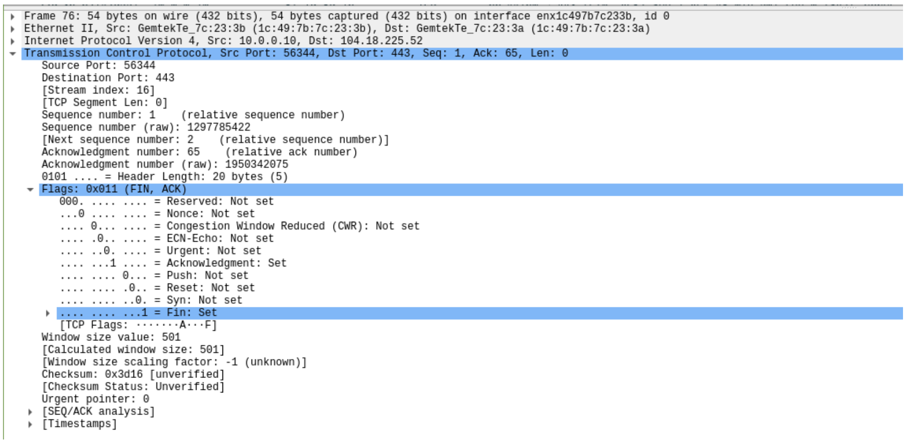
```
ip.addr == 37.9.93.169
No.   Time           Source       Destination  Protocol Length Info
 5916 179.128036636 10.0.0.10    37.9.93.169  TCP        74 42030 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 …
 5923 179.190228481 37.9.93.169  10.0.0.10    TCP        74 443 → 42030 [SYN, ACK] Seq=0 Ack=1 Win=43338 Len=0 MSS=1339 S…
 5924 179.190238358 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=304326962…
 5926 179.190422041 10.0.0.10    37.9.93.169  TLSv1.2   583 Client Hello
 5990 179.259178961 37.9.93.169  10.0.0.10    TCP        66 443 → 42030 [ACK] Seq=1 Ack=518 Win=45056 Len=0 TSval=2106464…
 5991 179.259340118 37.9.93.169  10.0.0.10    TLSv1.2  1393 Server Hello
 5992 179.259344090 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=518 Ack=1328 Win=64128 Len=0 TSval=3043…
 5993 179.259468622 37.9.93.169  10.0.0.10    TCP      1393 443 → 42030 [PSH, ACK] Seq=1328 Ack=518 Win=45056 Len=1327 TS…
 5994 179.259472756 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=518 Ack=2655 Win=64128 Len=0 TSval=3043…
 5995 179.259480753 37.9.93.169  10.0.0.10    TCP      1393 443 → 42030 [ACK] Seq=2655 Ack=518 Win=45056 Len=1327 TSval=2…
 5996 179.259483260 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=518 Ack=3982 Win=63360 Len=0 TSval=3043…
 5997 179.259591709 37.9.93.169  10.0.0.10    TCP       181 443 → 42030 [PSH, ACK] Seq=3982 Ack=518 Win=45056 Len=115 TSv…
 5998 179.259595374 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=518 Ack=4097 Win=64128 Len=0 TSval=3043…
 5999 179.260020468 37.9.93.169  10.0.0.10    TLSv1.2   514 Certificate, Server Key Exchange, Server Hello Done
 6000 179.260024290 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=518 Ack=4545 Win=64128 Len=0 TSval=3043…
 6001 179.261798610 10.0.0.10    37.9.93.169  TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake …
 6002 179.261896194 10.0.0.10    37.9.93.169  TLSv1.2   165 Application Data
 6003 179.261985567 10.0.0.10    37.9.93.169  TLSv1.2   506 Application Data
 6094 179.327265282 37.9.93.169  10.0.0.10    TCP        66 443 → 42030 [ACK] Seq=4545 Ack=611 Win=45056 Len=0 TSval=2106…
 6095 179.327295064 37.9.93.169  10.0.0.10    TCP        66 443 → 42030 [ACK] Seq=4545 Ack=710 Win=45056 Len=0 TSval=2106…
 6096 179.327295546 37.9.93.169  10.0.0.10    TCP        66 443 → 42030 [ACK] Seq=4545 Ack=1150 Win=45056 Len=0 TSval=210…
 6097 179.327339942 37.9.93.169  10.0.0.10    TLSv1.2   356 New Session Ticket, Change Cipher Spec, Encrypted Handshake M…
 6098 179.327350220 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1150 Ack=4835 Win=64128 Len=0 TSval=304…
 6099 179.327340441 37.9.93.169  10.0.0.10    TLSv1.2   144 Application Data
 6100 179.327370761 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1150 Ack=4913 Win=64128 Len=0 TSval=304…
 6102 179.327767193 10.0.0.10    37.9.93.169  TLSv1.2   104 Application Data
 6106 179.329024770 37.9.93.169  10.0.0.10    TCP      1393 443 → 42030 [ACK] Seq=4913 Ack=1150 Win=45056 Len=1327 TSval=…
 6107 179.329056632 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1188 Ack=6240 Win=64128 Len=0 TSval=304…
 6108 179.329091528 37.9.93.169  10.0.0.10    TCP      1393 443 → 42030 [PSH, ACK] Seq=6240 Ack=1150 Win=45056 Len=1327 T…
 6109 179.329100505 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1188 Ack=7567 Win=63360 Len=0 TSval=304…
 6110 179.329135504 37.9.93.169  10.0.0.10    TCP      1393 443 → 42030 [ACK] Seq=7567 Ack=1150 Win=45056 Len=1327 TSval=…
 6111 179.329143364 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1188 Ack=8894 Win=62336 Len=0 TSval=304…
 6112 179.329247098 37.9.93.169  10.0.0.10    TCP      1393 443 → 42030 [PSH, ACK] Seq=8894 Ack=1150 Win=45056 Len=1327 T…
 6113 179.329259059 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1188 Ack=10221 Win=64128 Len=0 TSval=30…
 6117 179.332853249 37.9.93.169  10.0.0.10    TCP      1393 443 → 42030 [ACK] Seq=10221 Ack=1150 Win=45056 Len=1327 TSval…
 6118 179.332885189 10.0.0.10    37.9.93.169  TCP        66 42030 → 443 [ACK] Seq=1188 Ack=11548 Win=64128 Len=0 TSval=30…
```

Рисунок 3



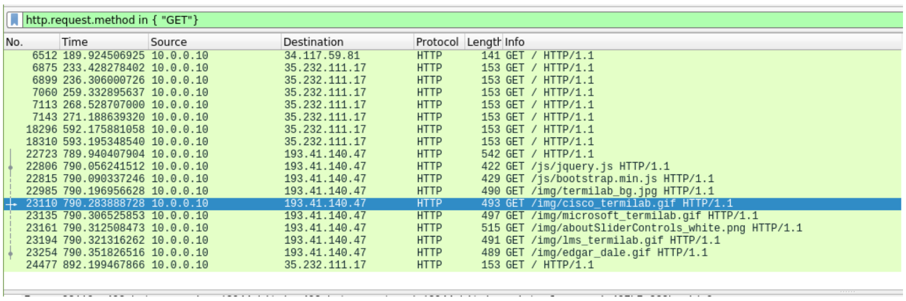
```
▸ Frame 5995: 1393 bytes on wire (11144 bits), 1393 bytes captured (11144 bits) on interface enx1c497b7c233b, id 0
▸ Ethernet II, Src: GemtekTe_7c:23:3a (1c:49:7b:7c:23:3a), Dst: GemtekTe_7c:23:3b (1c:49:7b:7c:23:3b)
▸ Internet Protocol Version 4, Src: 37.9.93.169, Dst: 10.0.0.10
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 42030, Seq: 2655, Ack: 518, Len: 1327
     Source Port: 443
     Destination Port: 42030
     [Stream index: 78]
     [TCP Segment Len: 1327]
     Sequence number: 2655    (relative sequence number)
     Sequence number (raw): 3402717960
     [Next sequence number: 3982    (relative sequence number)]
     Acknowledgment number: 518    (relative ack number)
     Acknowledgment number (raw): 3888973667
     1000 .... = Header Length: 32 bytes (8)
   ▸ Flags: 0x010 (ACK)
     Window size value: 11
     [Calculated window size: 45056]
     [Window size scaling factor: 4096]
     Checksum: 0x5ec7 [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
   ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
   ▸ [SEQ/ACK analysis]
   ▸ [Timestamps]
     TCP payload (1327 bytes)
     [Reassembled PDU in frame: 5999]
     TCP segment data (1327 bytes)
```

Рисунок 4



```
▸ Frame 76: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enx1c497b7c233b, id 0
▸ Ethernet II, Src: GemtekTe_7c:23:3b (1c:49:7b:7c:23:3b), Dst: GemtekTe_7c:23:3a (1c:49:7b:7c:23:3a)
▸ Internet Protocol Version 4, Src: 10.0.0.10, Dst: 104.18.225.52
▾ Transmission Control Protocol, Src Port: 56344, Dst Port: 443, Seq: 1, Ack: 65, Len: 0
     Source Port: 56344
     Destination Port: 443
     [Stream index: 16]
     [TCP Segment Len: 0]
     Sequence number: 1    (relative sequence number)
     Sequence number (raw): 1297785422
     [Next sequence number: 2    (relative sequence number)]
     Acknowledgment number: 65    (relative ack number)
     Acknowledgment number (raw): 1950342075
     0101 .... = Header Length: 20 bytes (5)
   ▾ Flags: 0x011 (FIN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
      ▸ .... .... ...1 = Fin: Set
        [TCP Flags: ·······A···F]
     Window size value: 501
     [Calculated window size: 501]
     [Window size scaling factor: -1 (unknown)]
     Checksum: 0x3d16 [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
   ▸ [SEQ/ACK analysis]
   ▸ [Timestamps]
```

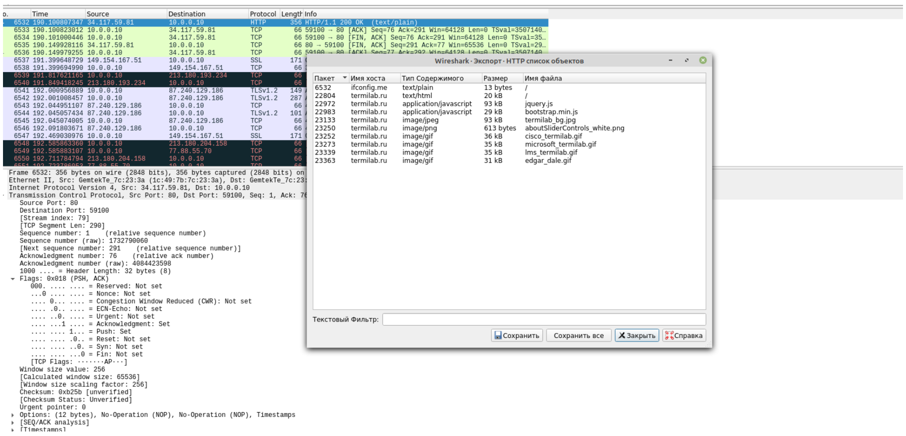
Рисунок 5



```
http.request.method in { "GET"}
```

```
No.   Time           Source      Destination      Protocol Length Info
 6512 189.924506925 10.0.0.10   34.117.59.81     HTTP      141 GET / HTTP/1.1
 6875 233.428278402 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
 6899 236.306000726 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
 7060 259.332895637 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
 7113 268.528707000 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
 7143 271.188639320 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
18296 592.175881058 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
18310 593.195348540 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
22723 789.940407904 10.0.0.10   193.41.140.47    HTTP      542 GET / HTTP/1.1
22806 790.056241512 10.0.0.10   193.41.140.47    HTTP      422 GET /js/jquery.js HTTP/1.1
22815 790.090337246 10.0.0.10   193.41.140.47    HTTP      429 GET /js/bootstrap.min.js HTTP/1.1
22985 790.196956628 10.0.0.10   193.41.140.47    HTTP      490 GET /img/termilab_bg.jpg HTTP/1.1
23110 790.283888728 10.0.0.10   193.41.140.47    HTTP      493 GET /img/cisco_termilab.gif HTTP/1.1
23135 790.306525853 10.0.0.10   193.41.140.47    HTTP      497 GET /img/microsoft_termilab.gif HTTP/1.1
23161 790.312508473 10.0.0.10   193.41.140.47    HTTP      515 GET /img/aboutSliderControls_white.png HTTP/1.1
23194 790.321316262 10.0.0.10   193.41.140.47    HTTP      491 GET /img/lms_termilab.gif HTTP/1.1
23254 790.351826516 10.0.0.10   193.41.140.47    HTTP      489 GET /img/edgar_dale.gif HTTP/1.1
24477 892.199467866 10.0.0.10   35.232.111.17    HTTP      153 GET / HTTP/1.1
```

Рисунок 6



```
o.    Time           Source           Destination      Protocol Length Info
 6532 190.100807347 34.117.59.81     10.0.0.10        HTTP      356 HTTP/1.1 200 OK  (text/plain)
 6533 190.100823012 10.0.0.10        34.117.59.81     TCP        66 59100 → 80 [ACK] Seq=76 Ack=291 Win=64128 Len=0 TSval=3507140…
 6534 190.101000446 10.0.0.10        34.117.59.81     TCP        66 59100 → 80 [FIN, ACK] Seq=76 Ack=291 Win=64128 Len=0 TSval=35…
 6535 190.149928116 34.117.59.81     10.0.0.10        TCP        66 80 → 59100 [FIN, ACK] Seq=291 Ack=77 Win=65536 Len=0 TSval=29…
 6536 190.149979255 10.0.0.10        34.117.59.81     TCP        66 59100 → 80 [ACK] Seq=77 Ack=292 Win=64128 Len=0 TSval=3507140…
 6537 191.399648729 149.154.167.51   10.0.0.10        SSL       171
 6538 191.399694990 10.0.0.10        149.154.167.51   TCP        66
 6539 191.817621165 10.0.0.10        213.180.193.234  TCP        66
 6540 191.849418245 213.180.193.234  10.0.0.10        TCP        66
 6541 192.000956889 10.0.0.10        87.240.129.186   TLSv1.2   149
 6542 192.001008457 10.0.0.10        87.240.129.186   TLSv1.2   287
 6543 192.044951107 87.240.129.186   10.0.0.10        TCP        66
 6544 192.045057434 87.240.129.186   10.0.0.10        TLSv1.2   101
 6545 192.045074005 10.0.0.10        87.240.129.186   TCP        66
 6546 192.091803671 87.240.129.186   10.0.0.10        TCP        66
 6547 192.469030976 10.0.0.10        149.154.167.51   SSL       171
 6548 192.585863360 10.0.0.10        213.180.204.158  TCP        66
 6549 192.585883107 10.0.0.10        77.88.55.70      TCP        66
 6550 192.711784794 213.180.204.158  10.0.0.10        TCP        66
```

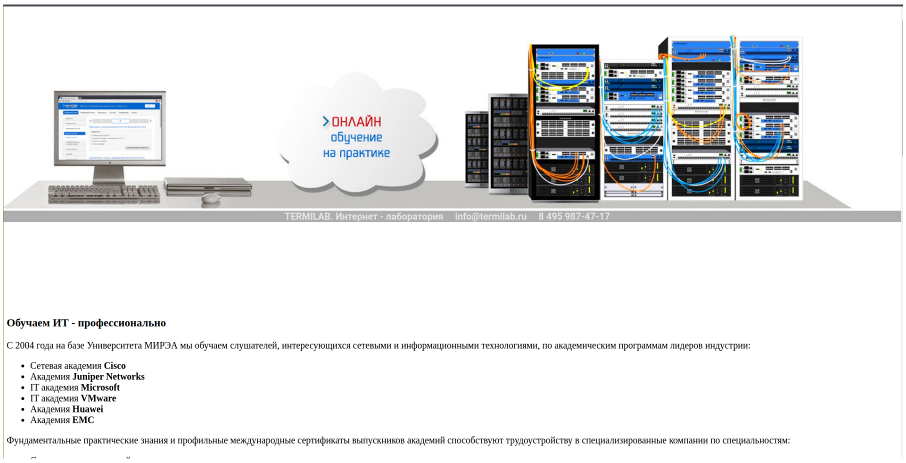
```
Frame 6532: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on
Ethernet II, Src: GemtekTe_7c:23:3a (1c:49:7b:7c:23:3a), Dst: GemtekTe_7c:23:
Internet Protocol Version 4, Src: 34.117.59.81, Dst: 10.0.0.10
Transmission Control Protocol, Src Port: 80, Dst Port: 59100, Seq: 1, Ack: 76
    Source Port: 80
    Destination Port: 59100
    [Stream index: 79]
    [TCP Segment Len: 290]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 1732790060
    [Next sequence number: 291    (relative sequence number)]
    Acknowledgment number: 76    (relative ack number)
    Acknowledgment number (raw): 4084423598
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x018 (PSH, ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Nonce: Not set
       .... 0... .... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...1 .... = Acknowledgment: Set
       .... .... 1... = Push: Set
       .... .... .0.. = Reset: Not set
       .... .... ..0. = Syn: Not set
       .... .... ...0 = Fin: Not set
       [TCP Flags: ·······AP···]
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0xb25b [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
```

Wireshark · Экспорт · HTTP список объектов

Пакет	Имя хоста	Тип Содержимого	Размер	Имя файла
6532	ifconfig.me	text/plain	13 bytes	/
22804	termilab.ru	text/html	20 kB	/
22972	termilab.ru	application/javascript	93 kB	jquery.js
22983	termilab.ru	application/javascript	29 kB	bootstrap.min.js
23133	termilab.ru	image/jpeg	93 kB	termilab_bg.jpg
23250	termilab.ru	image/png	613 bytes	aboutSliderControls_white.png
23252	termilab.ru	image/gif	36 kB	cisco_termilab.gif
23273	termilab.ru	image/gif	35 kB	microsoft_termilab.gif
23339	termilab.ru	image/gif	35 kB	lms_termilab.gif
23363	termilab.ru	image/gif	31 kB	edgar_dale.gif

Текстовый Фильтр:

Рисунок 7



> ОНЛАЙН
обучение
на практике
TERMILAB. Интернет - лаборатория info@termilab.ru 8 495 987-47-17

Обучаем ИТ - профессионально

С 2004 года на базе Университета МИРЭА мы обучаем слушателей, интересующихся сетевыми и информационными технологиями, по академическим программам лидеров индустрии:

- Сетевая академия **Cisco**
- Академия **Juniper Networks**
- IT академия **Microsoft**
- IT академия **VMware**
- Академия **Huawei**
- Академия **EMC**

Фундаментальные практические знания и профильные международные сертификаты выпускников академий способствуют трудоустройству в специализированные компании по специальностям:

Рисунок 8