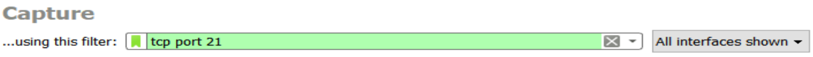
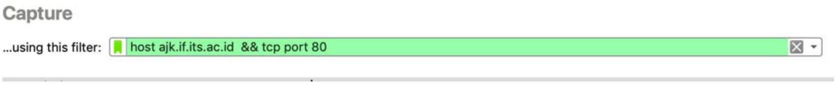
1.



Capture

...using this filter: tcp port 21

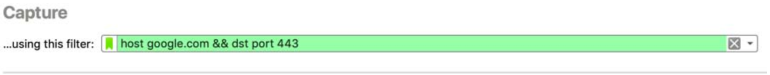
2.



Capture

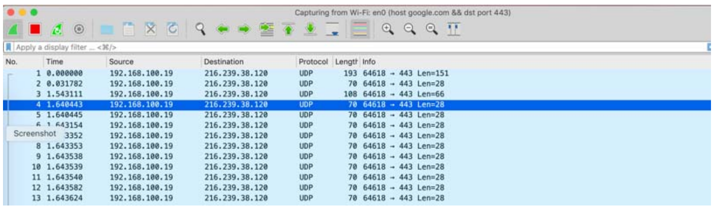
...using this filter: host ajk.if.its.ac.id && tcp port 80

3.



Capture

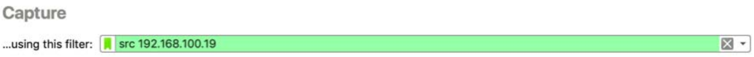
...using this filter: host google.com && dst port 443



Capturing from Wi-Fi: en0 (host google.com && dst port 443)

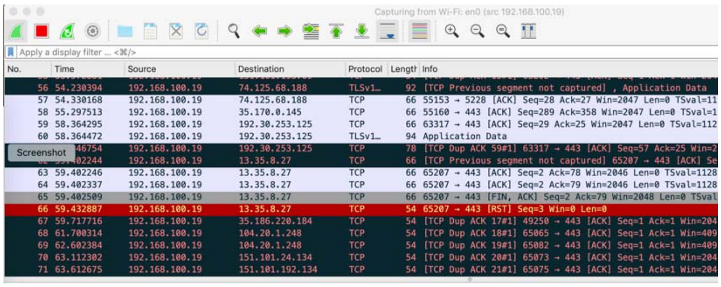
```
No.    Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.100.19   216.239.38.120   UDP      193 64618 → 443 Len=151
   2 0.031782   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
   3 1.543111   192.168.100.19   216.239.38.120   UDP      108 64618 → 443 Len=66
   4 1.640443   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
   5 1.640445   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
   6 1.643154   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
 Screenshot 3352  192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
   8 1.643353   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
   9 1.643538   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
  10 1.643539   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
  11 1.643540   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
  12 1.643582   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
  13 1.643624   192.168.100.19   216.239.38.120   UDP       70 64618 → 443 Len=28
```

4.



Capture

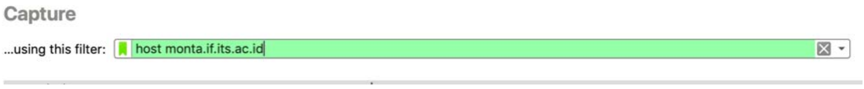
...using this filter: src 192.168.100.19



Capturing from Wi-Fi: en0 (src 192.168.100.19)

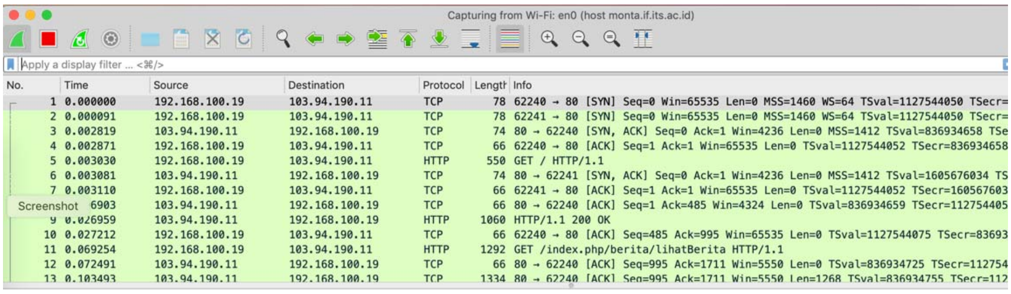
```
No.    Time        Source           Destination      Protocol Length Info
  56 54.230394   192.168.100.19   74.125.68.188    TLSv1…    92 [TCP Previous segment not captured] , Application Data
  57 54.330168   192.168.100.19   74.125.68.188    TCP       66 55153 → 5228 [ACK] Seq=28 Ack=27 Win=2047 Len=0 TSval=11
  58 55.297513   192.168.100.19   35.170.0.145     TCP       66 55160 → 443 [ACK] Seq=289 Ack=358 Win=2047 Len=0 TSval=1
  59 58.364295   192.168.100.19   192.30.253.125   TCP       66 63317 → 443 [ACK] Seq=29 Ack=25 Win=2047 Len=0 TSval=112
  60 58.364472   192.168.100.19   192.30.253.125   TLSv1…    94 Application Data
 Screenshot 46754  192.168.100.19   192.30.253.125   TCP       78 [TCP Dup ACK 59#1] 63317 → 443 [ACK] Seq=57 Ack=25 Win=2
        02244    192.168.100.19   13.35.8.27       TCP       66 [TCP Previous segment not captured] 65207 → 443 [ACK] Se
  63 59.402246   192.168.100.19   13.35.8.27       TCP       66 65207 → 443 [ACK] Seq=2 Ack=78 Win=2046 Len=0 TSval=1128
  64 59.402337   192.168.100.19   13.35.8.27       TCP       66 65207 → 443 [ACK] Seq=2 Ack=79 Win=2046 Len=0 TSval=1128
  65 59.402509   192.168.100.19   13.35.8.27       TCP       66 65207 → 443 [FIN, ACK] Seq=2 Ack=79 Win=2048 Len=0 TSval
  66 59.432887   192.168.100.19   13.35.8.27       TCP       54 65207 → 443 [RST] Seq=3 Win=0 Len=0
  67 59.717716   192.168.100.19   35.186.220.184   TCP       54 [TCP Dup ACK 17#1] 49250 → 443 [ACK] Seq=1 Ack=1 Win=204
  68 61.700314   192.168.100.19   104.20.1.248     TCP       54 [TCP Dup ACK 18#1] 65065 → 443 [ACK] Seq=1 Ack=1 Win=409
  69 62.602384   192.168.100.19   104.20.1.248     TCP       54 [TCP Dup ACK 19#1] 65082 → 443 [ACK] Seq=1 Ack=1 Win=409
  70 63.112302   192.168.100.19   151.101.24.134   TCP       54 [TCP Dup ACK 20#1] 65073 → 443 [ACK] Seq=1 Ack=1 Win=204
  71 63.612675   192.168.100.19   151.101.192.134  TCP       54 [TCP Dup ACK 21#1] 65075 → 443 [ACK] Seq=1 Ack=1 Win=204
```

5.



Capture

...using this filter: host monta.if.its.ac.id

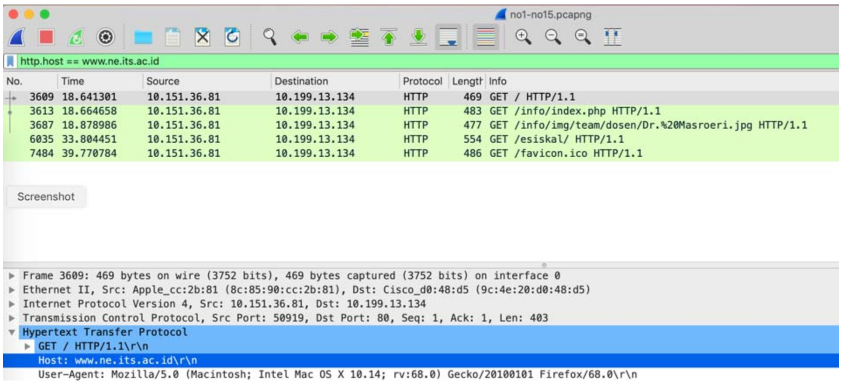


Capturing from Wi-Fi: en0 (host monta.if.its.ac.id)

```
No.    Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.100.19   103.94.190.11    TCP        78 62240 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1127544050 TSecr=
   2 0.000091   192.168.100.19   103.94.190.11    TCP        78 62241 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1127544050 TSecr=
   3 0.002819   103.94.190.11    192.168.100.19   TCP        74 80 → 62240 [SYN, ACK] Seq=0 Ack=1 Win=4236 Len=0 MSS=1412 TSval=836934658 TSe
   4 0.002871   192.168.100.19   103.94.190.11    TCP        66 62240 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=1127544052 TSecr=836934658
   5 0.003030   192.168.100.19   103.94.190.11    HTTP      550 GET / HTTP/1.1
   6 0.003081   103.94.190.11    192.168.100.19   TCP        74 80 → 62241 [SYN, ACK] Seq=0 Ack=1 Win=4236 Len=0 MSS=1412 TSval=1605676034 TS
   7 0.003110   192.168.100.19   103.94.190.11    TCP        66 62241 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=1127544052 TSecr=160567603
 Screenshot 6903  103.94.190.11    192.168.100.19   TCP        66 80 → 62240 [ACK] Seq=1 Ack=485 Win=4324 Len=0 TSval=836934659 TSecr=112754405
   9 0.026959   103.94.190.11    192.168.100.19   HTTP     1060 HTTP/1.1 200 OK
  10 0.027212   192.168.100.19   103.94.190.11    TCP        66 62240 → 80 [ACK] Seq=485 Ack=995 Win=65535 Len=0 TSval=1127544075 TSecr=83693
  11 0.069254   192.168.100.19   103.94.190.11    HTTP     1292 GET /index.php/berita/lihatBerita HTTP/1.1
  12 0.072491   103.94.190.11    192.168.100.19   TCP        66 80 → 62240 [ACK] Seq=995 Ack=1711 Win=5550 Len=0 TSval=836934725 TSecr=112754
  13 0.103493   103.94.190.11    192.168.100.19   TCP      1334 80 → 62240 [ACK] Seq=995 Ack=1711 Win=5550 Len=1268 TSval=836934755 TSecr=112
```

DISPLAY FILTER

1.



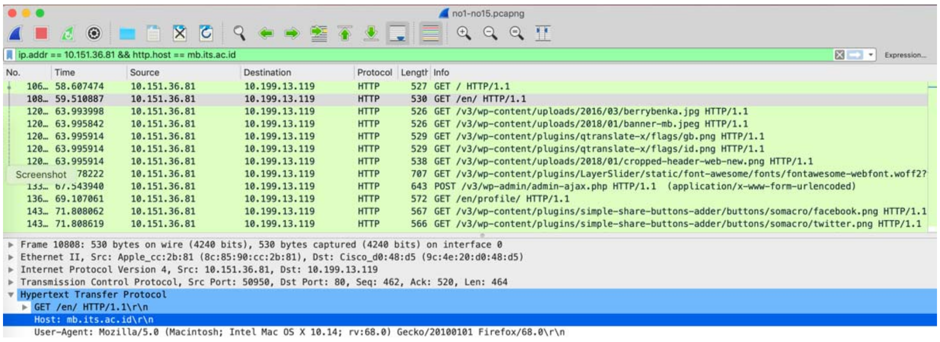
no1-no15.pcapng

http.host == www.ne.its.ac.id

```
No.   Time        Source          Destination     Protocol  Length  Info
 3609 18.641301   10.151.36.81    10.199.13.134   HTTP      469  GET / HTTP/1.1
 3613 18.664658   10.151.36.81    10.199.13.134   HTTP      483  GET /info/index.php HTTP/1.1
 3687 18.878986   10.151.36.81    10.199.13.134   HTTP      477  GET /info/img/team/dosen/Dr.%20Masroeri.jpg HTTP/1.1
 6035 33.804451   10.151.36.81    10.199.13.134   HTTP      554  GET /esiskal/ HTTP/1.1
 7484 39.770784   10.151.36.81    10.199.13.134   HTTP      486  GET /favicon.ico HTTP/1.1
```

```
▶ Frame 3609: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface 0
▶ Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: Cisco_d0:48:d5 (9c:4e:20:d0:48:d5)
▶ Internet Protocol Version 4, Src: 10.151.36.81, Dst: 10.199.13.134
▶ Transmission Control Protocol, Src Port: 50919, Dst Port: 80, Seq: 1, Ack: 1, Len: 403
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.ne.its.ac.id\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
```

2.



no1-no15.pcapng

ip.addr == 10.151.36.81 && http.host == mb.its.ac.id

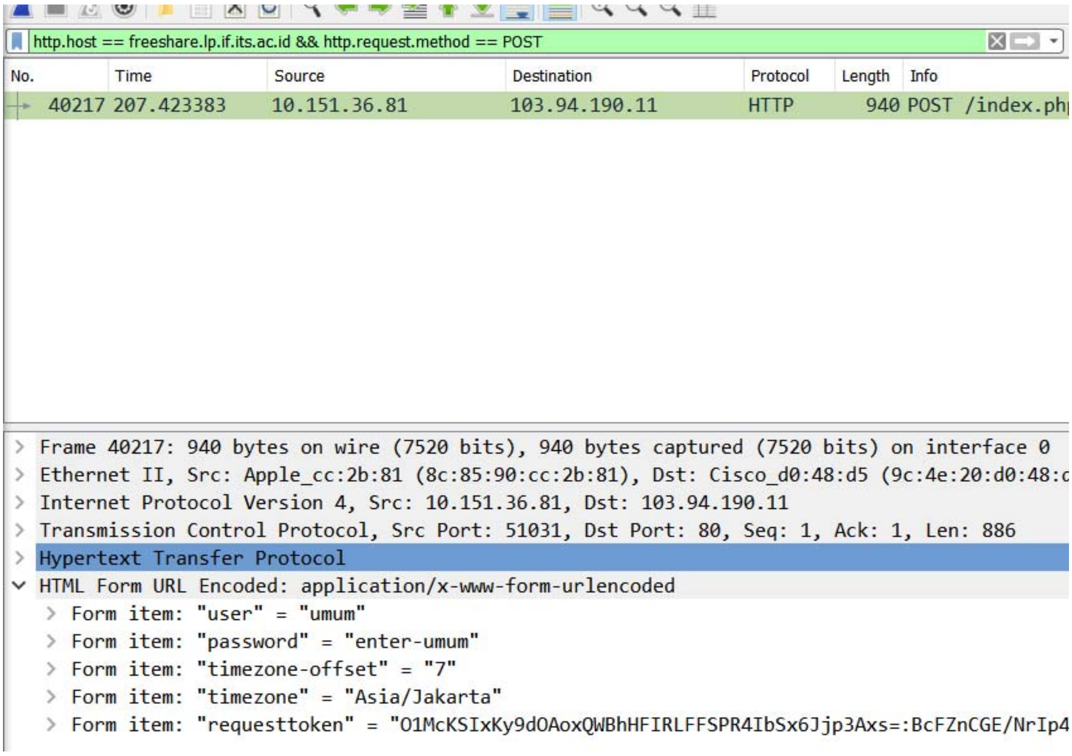
```
No.    Time        Source         Destination     Protocol  Length  Info
 106… 58.607474   10.151.36.81   10.199.13.119   HTTP      527  GET / HTTP/1.1
 108… 59.510887   10.151.36.81   10.199.13.119   HTTP      530  GET /en/ HTTP/1.1
 120… 63.993998   10.151.36.81   10.199.13.119   HTTP      526  GET /v3/wp-content/uploads/2016/03/berrybenka.jpg HTTP/1.1
 120… 63.995842   10.151.36.81   10.199.13.119   HTTP      526  GET /v3/wp-content/uploads/2018/01/banner-mb.jpeg HTTP/1.1
 120… 63.995914   10.151.36.81   10.199.13.119   HTTP      529  GET /v3/wp-content/plugins/qtranslate-x/flags/gb.png HTTP/1.1
 120… 63.995914   10.151.36.81   10.199.13.119   HTTP      529  GET /v3/wp-content/plugins/qtranslate-x/flags/id.png HTTP/1.1
 120… 63.995914   10.151.36.81   10.199.13.119   HTTP      538  GET /v3/wp-content/uploads/2018/01/cropped-header-web-new.png HTTP/1.1
Screenshot 78222  10.151.36.81   10.199.13.119   HTTP      707  GET /v3/wp-content/plugins/LayerSlider/static/font-awesome/fonts/fontawesome-webfont.woff2?
 133… 67.543940   10.151.36.81   10.199.13.119   HTTP      643  POST /v3/wp-admin/admin-ajax.php HTTP/1.1  (application/x-www-form-urlencoded)
 136… 69.107061   10.151.36.81   10.199.13.119   HTTP      572  GET /en/profile/ HTTP/1.1
 143… 71.808062   10.151.36.81   10.199.13.119   HTTP      567  GET /v3/wp-content/plugins/simple-share-buttons-adder/buttons/somacro/facebook.png HTTP/1.1
 143… 71.808619   10.151.36.81   10.199.13.119   HTTP      566  GET /v3/wp-content/plugins/simple-share-buttons-adder/buttons/somacro/twitter.png HTTP/1.1
```

```
▶ Frame 10808: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0
▶ Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: Cisco_d0:48:d5 (9c:4e:20:d0:48:d5)
▶ Internet Protocol Version 4, Src: 10.151.36.81, Dst: 10.199.13.119
▶ Transmission Control Protocol, Src Port: 50950, Dst Port: 80, Seq: 462, Ack: 520, Len: 464
▼ Hypertext Transfer Protocol
  ▶ GET /en/ HTTP/1.1\r\n
    Host: mb.its.ac.id\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
```

3. Bonus?

4.

5.

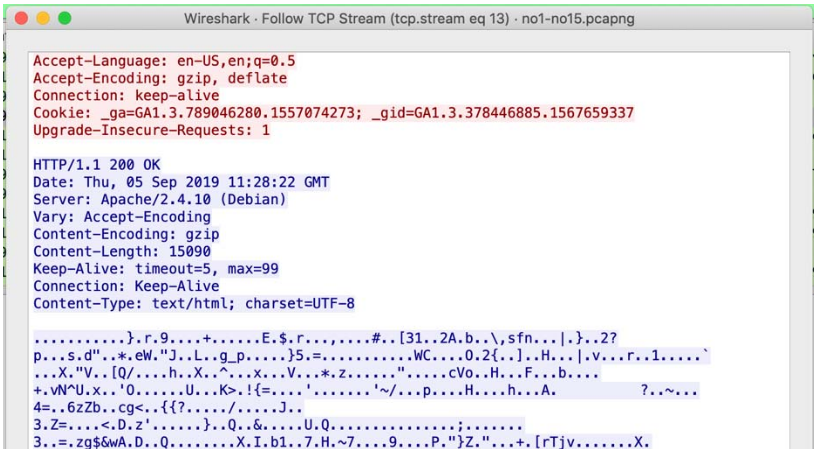


```
http.host == freeshare.lp.if.its.ac.id && http.request.method == POST

No.     Time        Source          Destination     Protocol  Length Info
  40217 207.423383  10.151.36.81    103.94.190.11   HTTP        940 POST /index.ph

> Frame 40217: 940 bytes on wire (7520 bits), 940 bytes captured (7520 bits) on interface 0
> Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: Cisco_d0:48:d5 (9c:4e:20:d0:48:c
> Internet Protocol Version 4, Src: 10.151.36.81, Dst: 103.94.190.11
> Transmission Control Protocol, Src Port: 51031, Dst Port: 80, Seq: 1, Ack: 1, Len: 886
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "user" = "umum"
  > Form item: "password" = "enter-umum"
  > Form item: "timezone-offset" = "7"
  > Form item: "timezone" = "Asia/Jakarta"
  > Form item: "requesttoken" = "O1McKSIxKy9dOAoxQWBhHFIRLFFSPR4IbSx6Jjp3Axs=:BcFZnCGE/NrIp4
```

6.



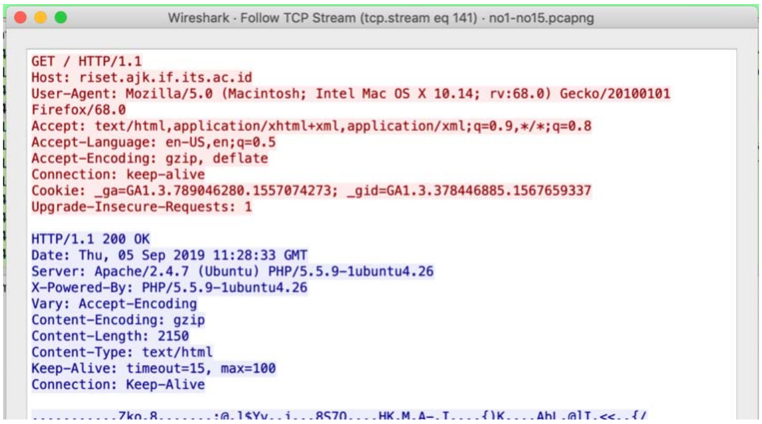
Wireshark · Follow TCP Stream (tcp.stream eq 13) · no1-no15.pcapng

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: _ga=GA1.3.789046280.1557074273; _gid=GA1.3.378446885.1567659337
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Thu, 05 Sep 2019 11:28:22 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 15090
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...........}.r.9....+......E.$.r...,....#..[31..2A.b..\,sfn...|.}..2?
p...s.d"..*.eW."J..L..g_p.....}5.=...........WC....O.2{..]..H...|.v...r..1.....`
...X."V..[Q/....h..X..^...x...V...*.z......".....cVo..H...F...b....
+.vN^U.x..'O......U...K>.!{=....'.......'~/...p....H....h...A.        ?..~...
4=..6zZb..cg<..{{?...../.....J..
3.Z=....<.D.z'......}..Q..&.....U.Q...............;.......
3..=.zg$&wA.D..Q........X.I.b1..7.H.~7....9....P."}Z."...+.[rTjv.......X.
```

7.



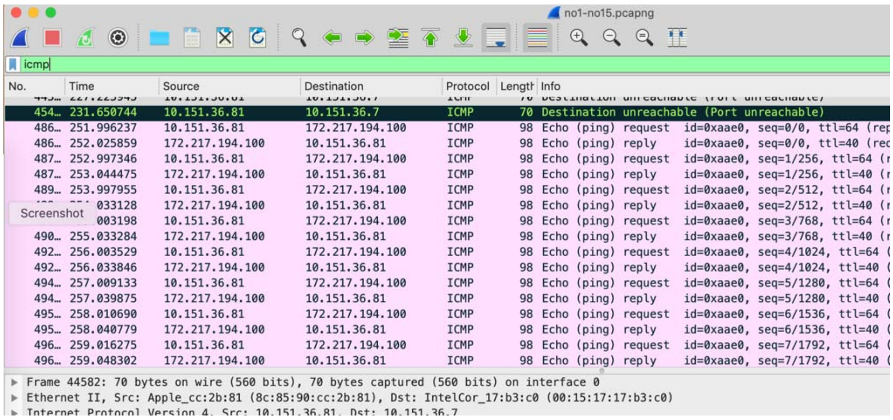
Wireshark · Follow TCP Stream (tcp.stream eq 141) · no1-no15.pcapng

```
GET / HTTP/1.1
Host: riset.ajk.if.its.ac.id
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: _ga=GA1.3.789046280.1557074273; _gid=GA1.3.378446885.1567659337
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Thu, 05 Sep 2019 11:28:33 GMT
Server: Apache/2.4.7 (Ubuntu) PHP/5.5.9-1ubuntu4.26
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2150
Content-Type: text/html
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive

...........7kq.8........:@.l$Yv..i...8S7O....HK.M.A-.I....{)K....AbL.@lI.<<..{/
```

8.

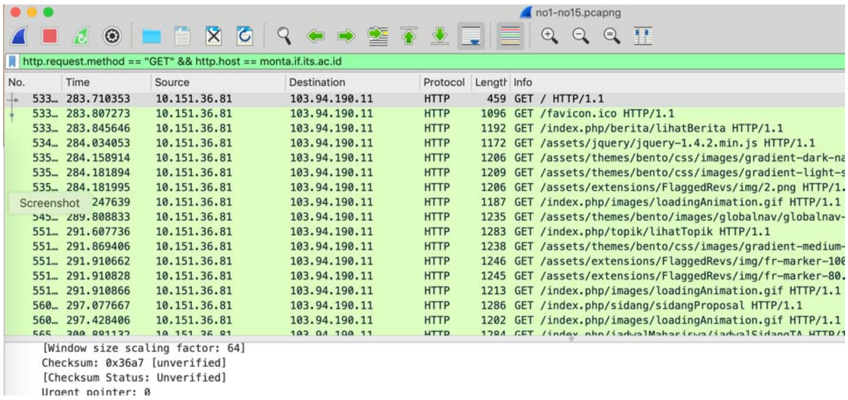


```
icmp
```

```
No.   Time        Source          Destination     Protocol Length Info
445…  227.225945  10.151.36.81    10.151.36.7     ICMP     70 Destination unreachable (Port unreachable)
454…  231.650744  10.151.36.81    10.151.36.7     ICMP     70 Destination unreachable (Port unreachable)
486…  251.996237  10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=0/0, ttl=64 (rep
486…  252.025859  172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=0/0, ttl=40 (rec
487…  252.997346  10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=1/256, ttl=64 (r
487…  253.044475  172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=1/256, ttl=40 (r
489…  253.997955  10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=2/512, ttl=64 (r
      033128      172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=2/512, ttl=40 (r
      003198      10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=3/768, ttl=64 (r
490…  255.033284  172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=3/768, ttl=40 (r
492…  256.003529  10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=4/1024, ttl=64 (
492…  256.033846  172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=4/1024, ttl=40 (
494…  257.009133  10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=5/1280, ttl=64 (
494…  257.039875  172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=5/1280, ttl=40 (
495…  258.010690  10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=6/1536, ttl=64 (
495…  258.040779  172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=6/1536, ttl=40 (
496…  259.016275  10.151.36.81    172.217.194.100 ICMP     98 Echo (ping) request  id=0xaae0, seq=7/1792, ttl=64 (
496…  259.048302  172.217.194.100 10.151.36.81    ICMP     98 Echo (ping) reply    id=0xaae0, seq=7/1792, ttl=40 (

▶ Frame 44582: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: IntelCor_17:b3:c0 (00:15:17:17:b3:c0)
▶ Internet Protocol Version 4, Src: 10.151.36.81, Dst: 10.151.36.7
```

9.

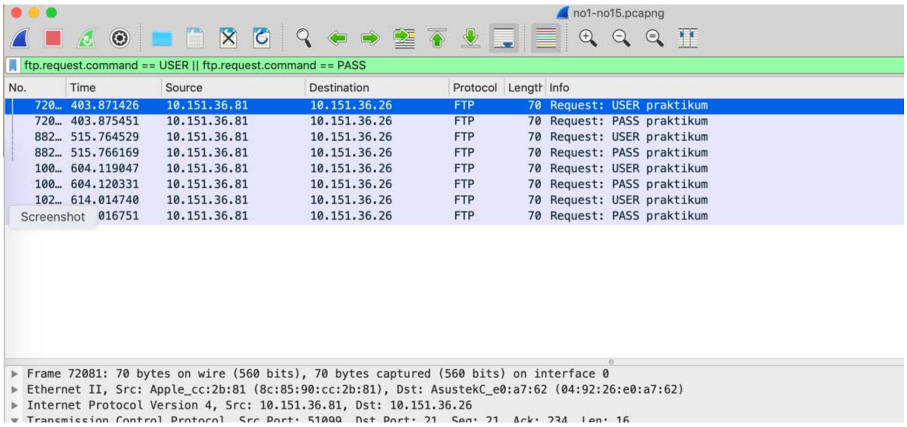


```
http.request.method == "GET" && http.host == monta.if.its.ac.id
```

```
No.   Time        Source        Destination    Protocol Length Info
533…  283.710353  10.151.36.81  103.94.190.11  HTTP      459 GET / HTTP/1.1
533…  283.807273  10.151.36.81  103.94.190.11  HTTP     1096 GET /favicon.ico HTTP/1.1
533…  283.845646  10.151.36.81  103.94.190.11  HTTP     1192 GET /index.php/berita/lihatBerita HTTP/1.1
534…  284.034053  10.151.36.81  103.94.190.11  HTTP     1172 GET /assets/jquery/jquery-1.4.2.min.js HTTP/1.1
535…  284.158914  10.151.36.81  103.94.190.11  HTTP     1206 GET /assets/themes/bento/css/images/gradient-dark-na
535…  284.181894  10.151.36.81  103.94.190.11  HTTP     1209 GET /assets/themes/bento/css/images/gradient-light-s
535…  284.181995  10.151.36.81  103.94.190.11  HTTP     1206 GET /assets/extensions/FlaggedRevs/img/2.png HTTP/1.
      247639      10.151.36.81  103.94.190.11  HTTP     1187 GET /index.php/images/loadingAnimation.gif HTTP/1.1
545…  289.808833  10.151.36.81  103.94.190.11  HTTP     1235 GET /assets/themes/bento/images/globalnav/globalnav-
551…  291.607736  10.151.36.81  103.94.190.11  HTTP     1283 GET /index.php/topik/lihatTopik HTTP/1.1
551…  291.869406  10.151.36.81  103.94.190.11  HTTP     1238 GET /assets/themes/bento/css/images/gradient-medium-
551…  291.910662  10.151.36.81  103.94.190.11  HTTP     1246 GET /assets/extensions/FlaggedRevs/img/fr-marker-100
551…  291.910828  10.151.36.81  103.94.190.11  HTTP     1245 GET /assets/extensions/FlaggedRevs/img/fr-marker-80.
551…  291.910866  10.151.36.81  103.94.190.11  HTTP     1213 GET /index.php/images/loadingAnimation.gif HTTP/1.1
560…  297.077667  10.151.36.81  103.94.190.11  HTTP     1286 GET /index.php/sidang/sidangProposal HTTP/1.1
560…  297.428406  10.151.36.81  103.94.190.11  HTTP     1202 GET /index.php/images/loadingAnimation.gif HTTP/1.1
565…  300.881132  10.151.36.81  103.94.190.11  HTTP     1284 GET /index.php/jadwalMahasiswa/jadwalSidangTA HTTP/1

    [Window size scaling factor: 64]
    Checksum: 0x36a7 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

10.

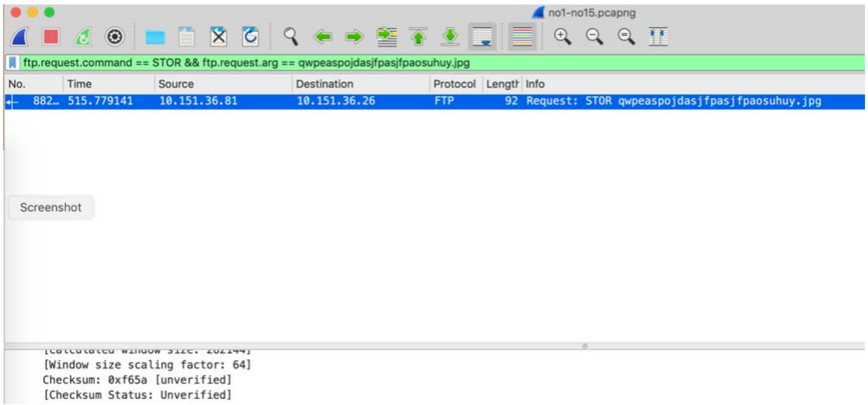


```
ftp.request.command == USER || ftp.request.command == PASS
```

```
No.   Time        Source        Destination   Protocol Length Info
720…  403.871426  10.151.36.81  10.151.36.26  FTP      70 Request: USER praktikum
720…  403.875451  10.151.36.81  10.151.36.26  FTP      70 Request: PASS praktikum
882…  515.764529  10.151.36.81  10.151.36.26  FTP      70 Request: USER praktikum
882…  515.766169  10.151.36.81  10.151.36.26  FTP      70 Request: PASS praktikum
100…  604.119047  10.151.36.81  10.151.36.26  FTP      70 Request: USER praktikum
100…  604.120331  10.151.36.81  10.151.36.26  FTP      70 Request: PASS praktikum
102…  614.014740  10.151.36.81  10.151.36.26  FTP      70 Request: USER praktikum
      016751      10.151.36.81  10.151.36.26  FTP      70 Request: PASS praktikum

▶ Frame 72081: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: AsustekC_e0:a7:62 (04:92:26:e0:a7:62)
▶ Internet Protocol Version 4, Src: 10.151.36.81, Dst: 10.151.36.26
▼ Transmission Control Protocol, Src Port: 51099, Dst Port: 21, Seq: 21, Ack: 234, Len: 16
```

11.

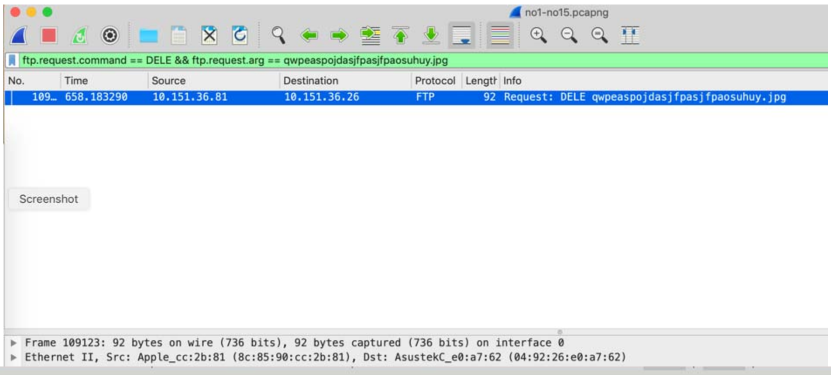


```
ftp.request.command == STOR && ftp.request.arg == qwpeaspojdasjfpasjfpaosuhuy.jpg
```

```
No.   Time        Source        Destination   Protocol Length Info
882…  515.779141  10.151.36.81  10.151.36.26  FTP      92 Request: STOR qwpeaspojdasjfpasjfpaosuhuy.jpg

    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0xf65a [unverified]
    [Checksum Status: Unverified]
```

12.

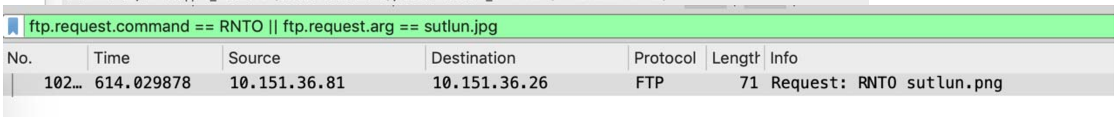


```
ftp.request.command == DELE && ftp.request.arg == qwpeaspojdasjfpasjfpaosuhuy.jpg
```

```
No.     Time         Source         Destination    Protocol  Length  Info
109…    658.183290   10.151.36.81   10.151.36.26   FTP           92  Request: DELE qwpeaspojdasjfpasjfpaosuhuy.jpg
```

```
▶ Frame 109123: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
▶ Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: AsustekC_e0:a7:62 (04:92:26:e0:a7:62)
```

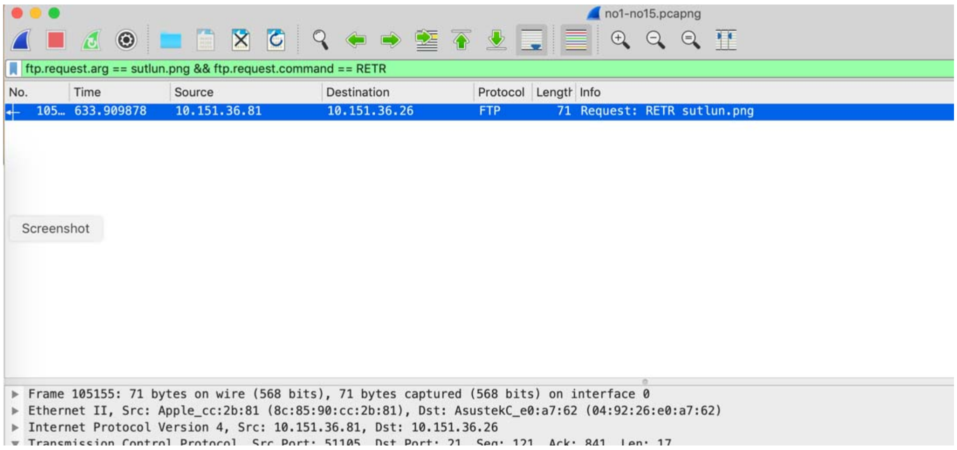
13.



```
ftp.request.command == RNTO || ftp.request.arg == sutlun.jpg
```

```
No.     Time         Source         Destination    Protocol  Length  Info
102…    614.029878   10.151.36.81   10.151.36.26   FTP           71  Request: RNTO sutlun.png
```

14.

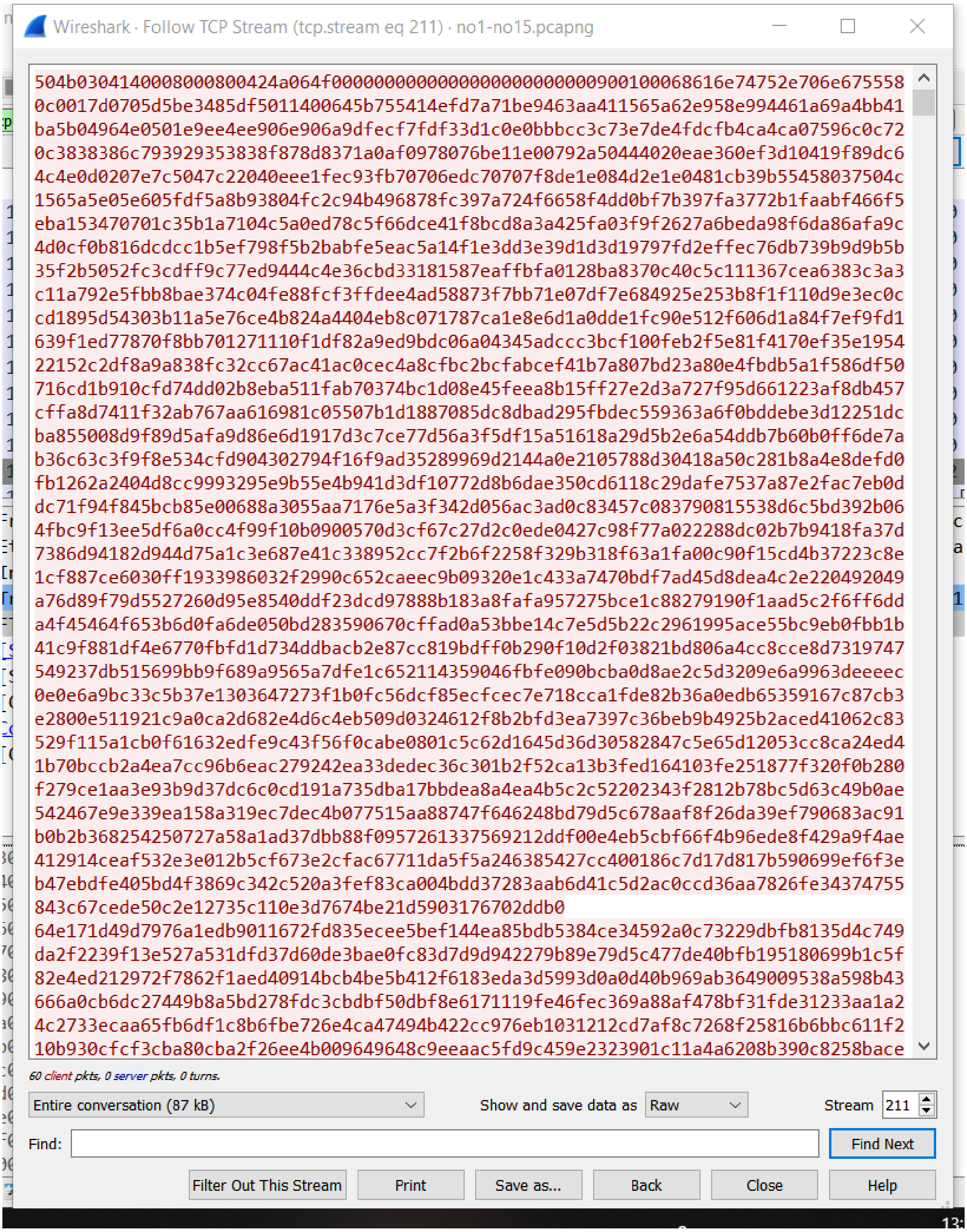


```
ftp.request.arg == sutlun.png && ftp.request.command == RETR
```

```
No.     Time         Source         Destination    Protocol  Length  Info
105…    633.909878   10.151.36.81   10.151.36.26   FTP           71  Request: RETR sutlun.png
```

```
▶ Frame 105155: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▶ Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: AsustekC_e0:a7:62 (04:92:26:e0:a7:62)
▶ Internet Protocol Version 4, Src: 10.151.36.81, Dst: 10.151.36.26
▼ Transmission Control Protocol, Src Port: 51105, Dst Port: 21, Seq: 121, Ack: 841, Len: 17
```

15.



Wireshark · Follow TCP Stream (tcp.stream eq 211) · no1-no15.pcapng

```
504b030414000800080424a064f000000000000000000000000900100068616e74752e706e675558
0c0017d0705d5be3485df5011400645b755414efd7a71be9463aa411565a62e958e994461a69a4bb41
ba5b04964e0501e9ee4ee906e906a9dfecf7fdf33d1c0e0bbbcc3c73e7de4fdcfb4ca4ca07596c0c72
0c3838386c79392935383 8f878d8371a0af0978076be11e00792a50444020eae360ef3d10419f89dc6
4c4e0d0207e7c5047c22040eee1fec93fb70706edc70707f8de1e084d2e1e0481cb39b55458037504c
1565a5e05e605fdf5a8b93804fc2c94b496878fc397a724f6658f4dd0bf7b397fa3772b1faabf466f5
eba153470701c35b1a7104c5a0ed78c5f66dce41f8bcd8a3a425fa03f9f2627a6beda98f6da86afa9c
4d0cf0b816dcdcc1b5ef798f5b2babfe5eac5a14f1e3dd3e39d1d3d19797fd2effec76db739b9d9b5b
35f2b5052fc3cdff9c77ed9444c4e36cbd33181587eaffbfa0128ba8370c40c5c111367cea6383c3a3
c11a792e5fbb8bae374c04fe88fcf3ffdee4ad58873f7bb71e07df7e684925e253b8f1f110d9e3ec0c
cd1895d54303b11a5e76ce4b824a4404eb8c071787ca1e8e6d1a0dde1fc90e512f606d1a84f7ef9fd1
639f1ed77870f8bb701271110f1df82a9ed9bdc06a04345adccc3bcf100feb2f5e81f4170ef35e1954
22152c2df8a9a838fc32cc67ac41ac0cec4a8cfbc2bcfabcef41b7a807bd23a80e4fbdb5a1f586df50
716cd1b910cfd74dd02b8eba511fab70374bc1d08e45feea8b15ff27e2d3a727f95d661223af8db457
cffa8d7411f32ab767aa616981c05507b1d1887085dc8dbad295fbdec559363a6f0bddebe3d12251dc
ba855008d9f89d5afa9d86e6d1917d3c7ce77d56a3f5df15a51618a29d5b2e6a54ddb7b60b0ff6de7a
b36c63c3f9f8e534cfd904302794f16f9ad35289969d2144a0e2105788d30418a50c281b8a4e8defd0
fb1262a2404d8cc9993295e9b55e4b941d3df10772d8b6dae350cd6118c29dafe7537a87e2fac7eb0d
dc71f94f845bcb85e00688a3055aa7176e5a3f342d056ac3ad0c83457c083790815538d6c5bd392b06
4fbc9f13ee5df6a0cc4f99f10b0900570d3cf67c27d2c0ede0427c98f77a022288dc02b7b9418fa37d
7386d94182d944d75a1c3e687e41c338952cc7f2b6f2258f329b318f63a1fa00c90f15cd4b37223c8e
1cf887ce6030ff1933986032f2990c652caeec9b09320e1c433a7470bdf7ad45d8dea4c2e220492049
a76d89f79d5527260d95e8540ddf23dcd97888b183a8fafa957275bce1c88279190f1aad5c2f6ff6dd
a4f45464f653b6d0fa6de050bd283590670cffad0a53bbe14c7e5d5b22c2961995ace55bc9eb0fbb1b
41c9f881df4e6770fbfd1d734ddbacb2e87cc819bdff0b290f10d2f03821bd806a4cc8cce8d7319747
549237db515699bb9f689a9565a7dfe1c652114359046fbfe090bcba0d8ae2c5d3209e6a9963deeeec
0e0e6a9bc33c5b37e1303647273f1b0fc56dcf85ecfcec7e718cca1fde82b36a0edb65359167c87cb3
e2800e511921c9a0ca2d682e4d6c4eb509d0324612f8b2bfd3ea7397c36beb9b4925b2aced41062c83
529f115a1cb0f61632edfe9c43f56f0cabe0801c5c62d1645d36d30582847c5e65d12053cc8ca24ed4
1b70bccb2a4ea7cc96b6eac279242ea33dedec36c301b2f52ca13b3fed164103fe251877f320f0b280
f279ce1aa3e93b9d37dc6c0cd191a735dba17bbdea8a4ea4b5c2c52202343f2812b78bc5d63c49b0ae
542467e9e339ea158a319ec7dec4b077515aa88747f646248bd79d5c678aaf8f26da39ef790683ac91
b0b2b368254250727a58a1ad37dbb88f0957261337569212ddf00e4eb5cbf66f4b96ede8f429a9f4ae
412914ceaf532e3e012b5cf673e2cfac67711da5f5a246385427cc400186c7d17d817b590699ef6f3e
b47ebdfe405bd4f3869c342c520a3fef83ca004bdd37283aab6d41c5d2ac0ccd36aa7826fe34374755
843c67cede50c2e12735c110e3d7674be21d5903176702ddb0
64e171d49d7976a1edb9011672fd835ecee5bef144ea85bdb5384ce34592a0c73229dbfb8135d4c749
da2f2239f13e527a531dfd37d60de3bae0fc83d7d9d942279b89e79d5c477de40bfb195180699b1c5f
82e4ed212972f7862f1aed40914bcb4be5b412f6183eda3d5993d0a0d40b969ab3649009538a598b43
666a0cb6dc27449b8a5bd278fdc3cbdbf50dbf8e6171119fe46fec369a88af478bf31fde31233aa1a2
4c2733ecaa65fb6df1c8b6fbe726e4ca47494b422cc976eb1031212cd7af8c7268f25816b6bbc611f2
10b930cfcf3cba80cba2f26ee4b009649648c9eeaac5fd9c459e2323901c11a4a6208b390c8258bace
```

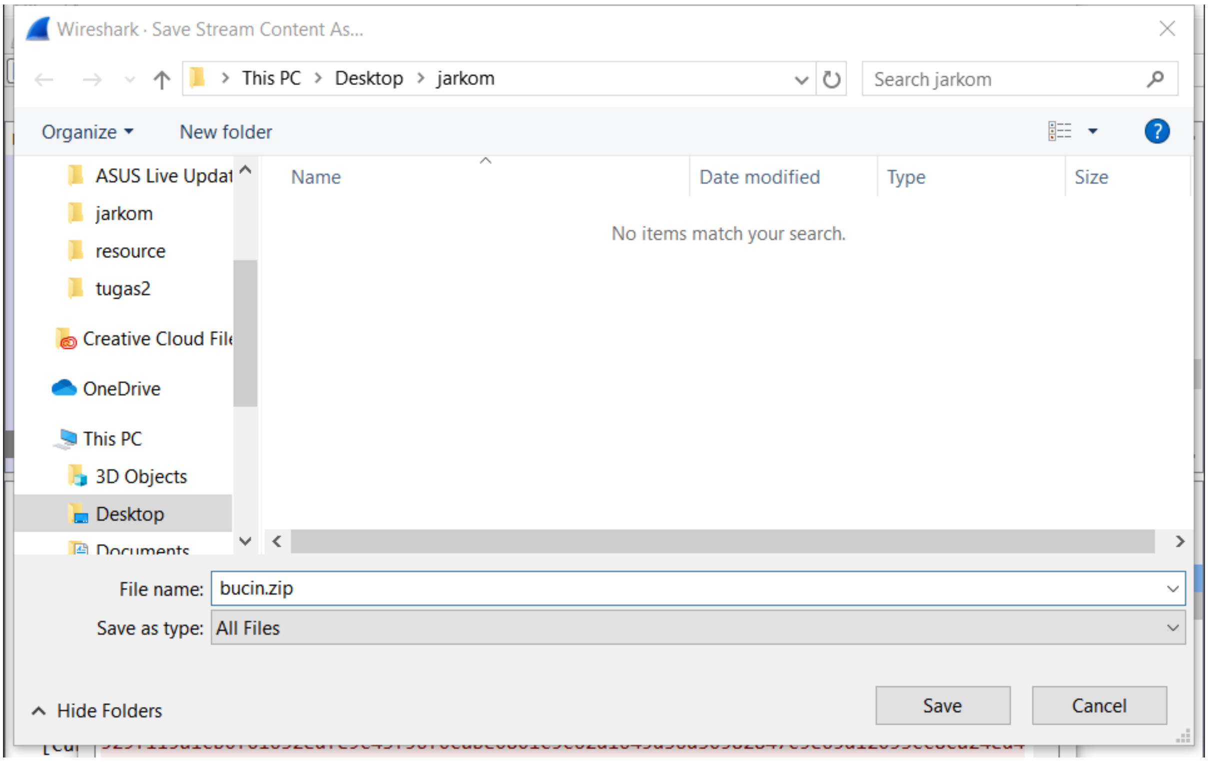
60 client pkts, 0 server pkts, 0 turns.

Entire conversation (87 kB)

Show and save data as Raw

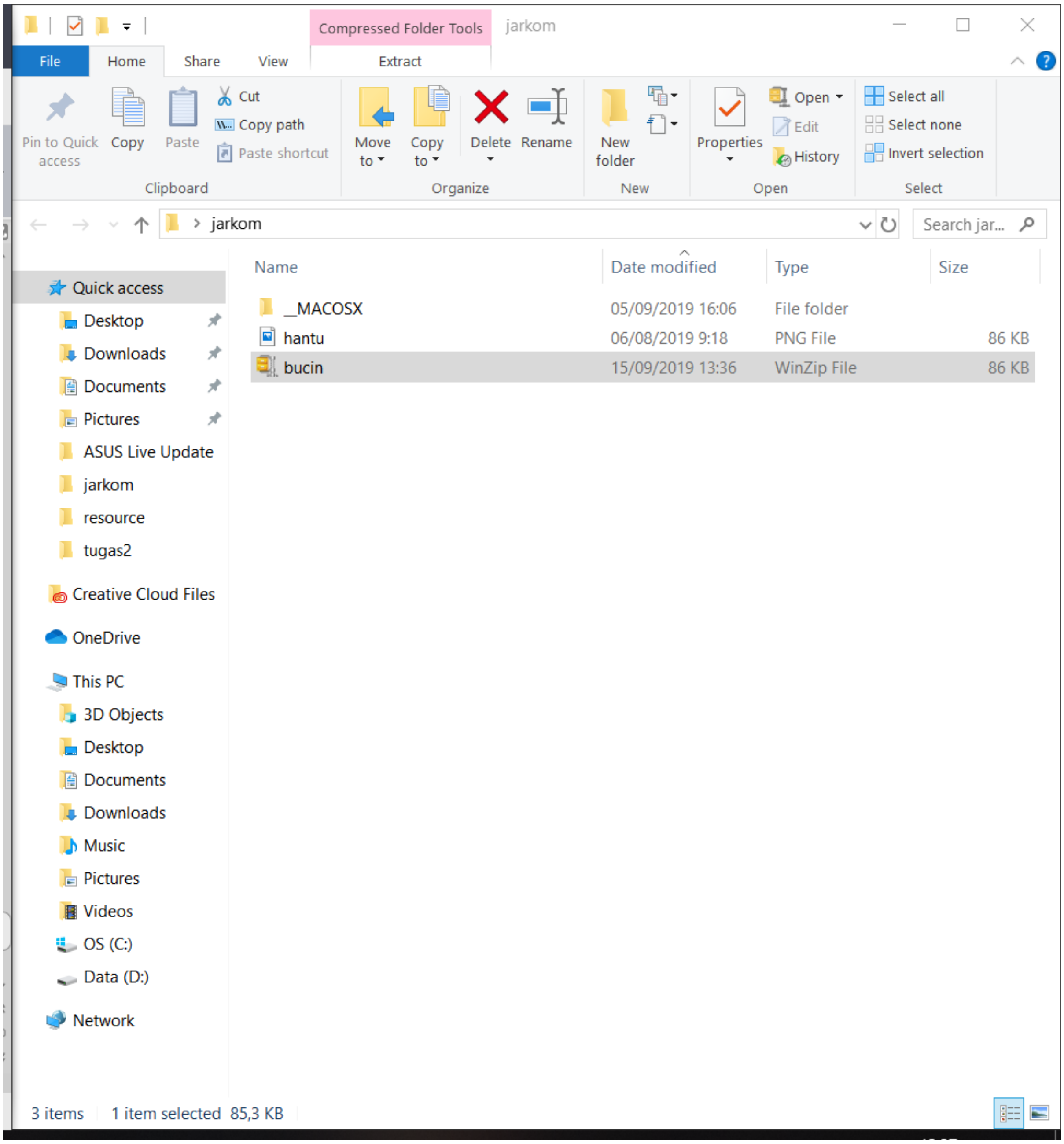
Stream 211

Find:



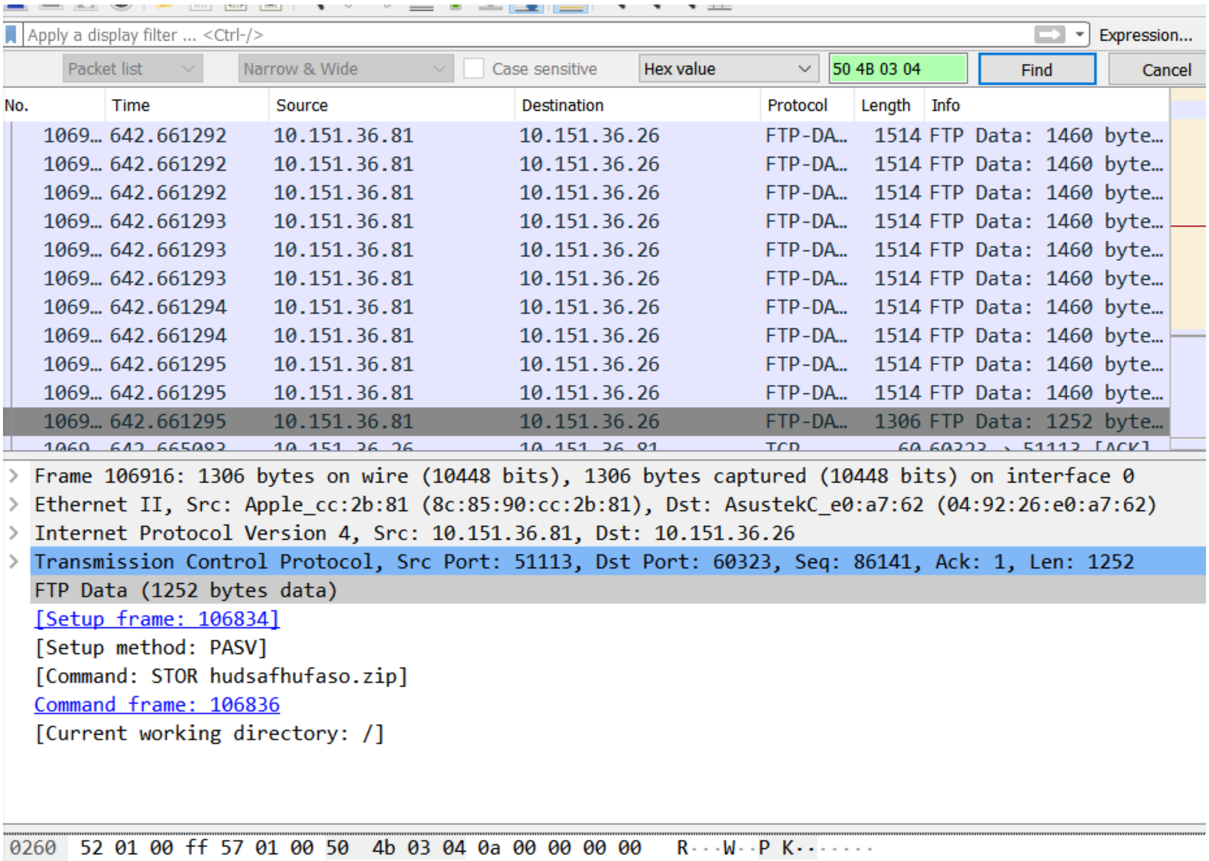
File name: bucin.zip

Save as type: All Files



Name	Date modified	Type	Size
__MACOSX	05/09/2019 16:06	File folder	
hantu	06/08/2019 9:18	PNG File	86 KB
bucin	15/09/2019 13:36	WinZip File	86 KB

3 items 1 item selected 85,3 KB



Apply a display filter ... <Ctrl-/>   Expression...

Packet list   Narrow & Wide   □ Case sensitive   Hex value   50 4B 03 04   Find   Cancel

```
No.      Time         Source          Destination     Protocol  Length Info
1069…    642.661292   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661292   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661292   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661293   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661293   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661293   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661294   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661294   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661295   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661295   10.151.36.81    10.151.36.26    FTP-DA…   1514 FTP Data: 1460 byte…
1069…    642.661295   10.151.36.81    10.151.36.26    FTP-DA…   1306 FTP Data: 1252 byte…
1069     642.665083   10.151.36.26    10.151.36.81    TCP         60 60323 → 51113 [ACK]
```

```
> Frame 106916: 1306 bytes on wire (10448 bits), 1306 bytes captured (10448 bits) on interface 0
> Ethernet II, Src: Apple_cc:2b:81 (8c:85:90:cc:2b:81), Dst: AsustekC_e0:a7:62 (04:92:26:e0:a7:62)
> Internet Protocol Version 4, Src: 10.151.36.81, Dst: 10.151.36.26
> Transmission Control Protocol, Src Port: 51113, Dst Port: 60323, Seq: 86141, Ack: 1, Len: 1252
  FTP Data (1252 bytes data)
  [Setup frame: 106834]
  [Setup method: PASV]
  [Command: STOR hudsafhufaso.zip]
  Command frame: 106836
  [Current working directory: /]
```

```
0260  52 01 00 ff 57 01 00 50  4b 03 04 0a 00 00 00 00   R···W··P K·······
```