# Lab 2 – Packet Capture Analysis for Attackers

## Shrutika Joshi

## University of Maryland Baltimore County

## Presented To – Ian Coston

## Date – 21st SEP 2023

## Introduction

In this lab, get familiar with capturing and analyzing network traffic from the attacker's point of view and identify security vulnerabilities.

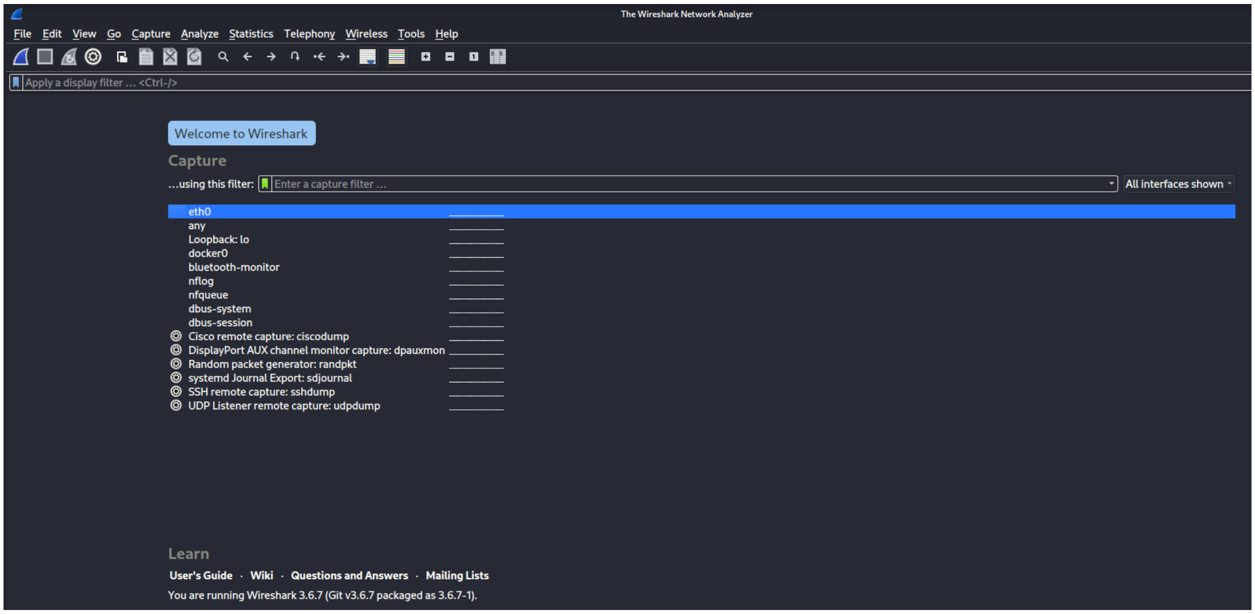
## Pre-Lab

For this lab, you will require Kali Linux and Wireshark

## Practical

### 1. Capturing live traffic and visiting a non-encrypted website.

Launch Wireshark, and start sniffing on your active network adapter. (You can tell by the 'heartrate monitor' at each interface)


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

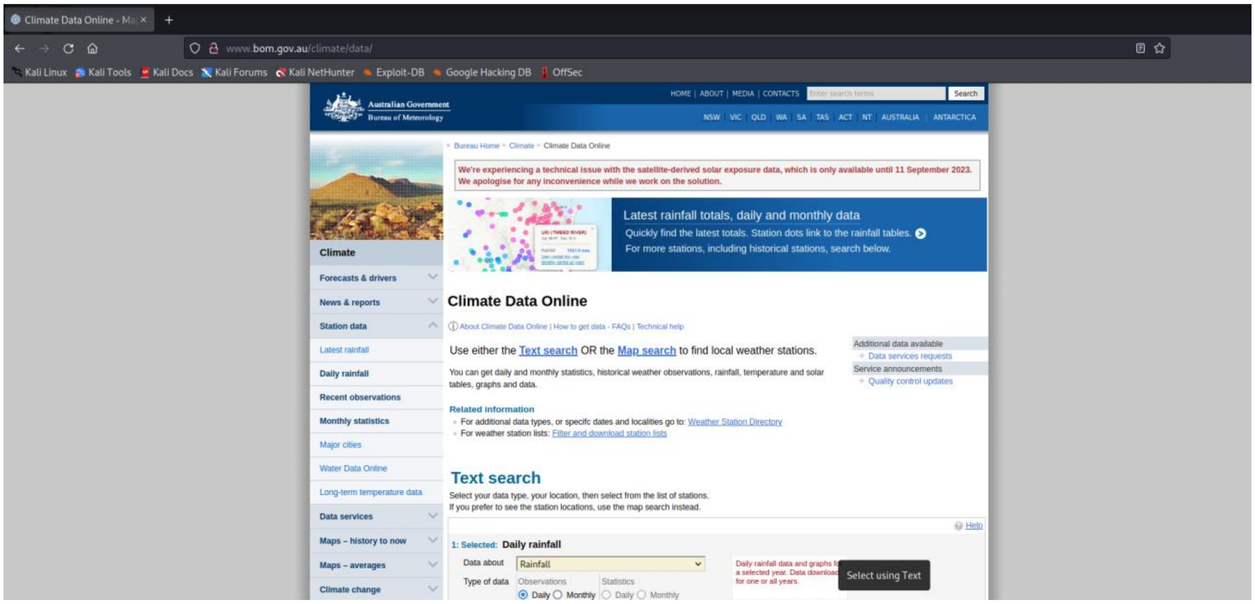
eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.7 (Git v3.6.7 packaged as 3.6.7-1).

Launch a web browser and go to http://www.bom.gov.au/ and perform a few random searches


Climate Data Online - Ma ×
www.bom.gov.au/climate/data/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Australian Government
Bureau of Meteorology
HOME | ABOUT | MEDIA | CONTACTS
Enter search terms
Search
NSW VIC QLD WA SA TAS ACT NT AUSTRALIA ANTARCTICA
Climate
Forecasts & drivers
News & reports
Station data
Latest rainfall
Daily rainfall
Recent observations
Monthly statistics
Major cities
Water Data Online
Long-term temperature data
Data services
Maps – history to now
Maps – averages
Climate change
Bureau Home › Climate › Climate Data Online

We're experiencing a technical issue with the satellite-derived solar exposure data, which is only available until 11 September 2023. We apologise for any inconvenience while we work on the solution.

Latest rainfall totals, daily and monthly data

Quickly find the latest totals. Station dots link to the rainfall tables.

For more stations, including historical stations, search below.

Climate Data Online

About Climate Data Online | How to get data - FAQs | Technical help

Use either the Text search OR the Map search to find local weather stations.

You can get daily and monthly statistics, historical weather observations, rainfall, temperature and solar tables, graphs and data.

Additional data available
- Data services requests

Service announcements
- Quality control updates

Related information
- For additional data types, or specifc dates and localities go to: Weather Station Directory
- For weather station lists: Filter and download station lists

Text search

Select your data type, your location, then select from the list of stations.
If you prefer to see the station locations, use the map search instead.

Help

1: Selected: Daily rainfall

Data about: Rainfall

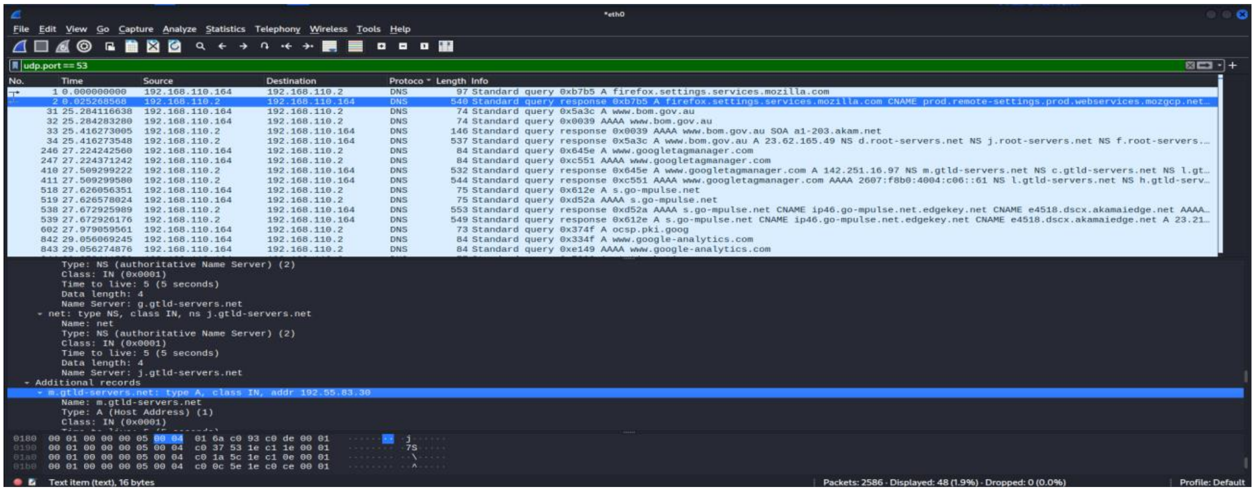
Type of data: Observations ● Daily ○ Monthly; Statistics ○ Daily ○ Monthly

Daily rainfall data and graphs f a selected year. Data download for one or all years.

Close your browser and stop Wireshark and review your network traffic

Take note of the DNS requests and responses

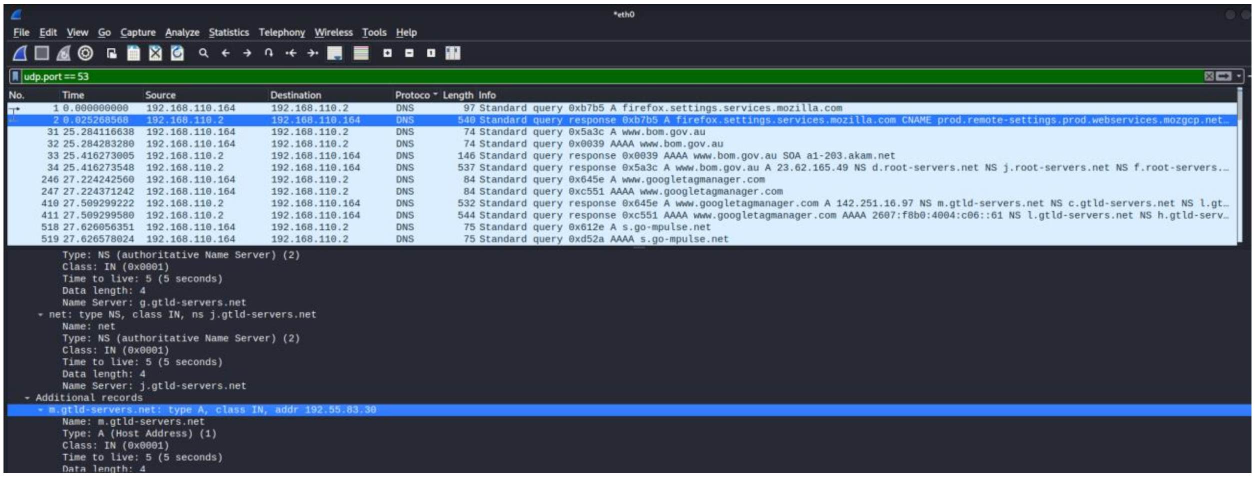
Use filter query ‘udp.port==53’ to check the DNS request and responses


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port == 53

No.   Time           Source            Destination       Protoco Length Info
    1 0.000000000    192.168.110.164   192.168.110.2     DNS      97 Standard query 0xb7b5 A firefox.settings.services.mozilla.com
    2 0.025268568    192.168.110.2     192.168.110.164   DNS     540 Standard query response 0xb7b5 A firefox.settings.services.mozilla.com CNAME prod.remote-settings.prod.webservices.mozgcp.net…
   31 25.284116638   192.168.110.164   192.168.110.2     DNS      74 Standard query 0x5a3c A www.bom.gov.au
   32 25.284283280   192.168.110.164   192.168.110.2     DNS      74 Standard query 0x0039 AAAA www.bom.gov.au
   33 25.416273005   192.168.110.2     192.168.110.164   DNS     146 Standard query response 0x0039 AAAA www.bom.gov.au SOA a1-203.akam.net
   34 25.416273548   192.168.110.2     192.168.110.164   DNS     537 Standard query response 0x5a3c A www.bom.gov.au A 23.62.165.49 NS d.root-servers.net NS j.root-servers.net NS f.root-servers.…
  246 27.224242560   192.168.110.164   192.168.110.2     DNS      84 Standard query 0x645e A www.googletagmanager.com
  247 27.224371242   192.168.110.164   192.168.110.2     DNS      84 Standard query 0xc551 AAAA www.googletagmanager.com
  410 27.509299222   192.168.110.2     192.168.110.164   DNS     532 Standard query response 0x645e A www.googletagmanager.com A 142.251.16.97 NS m.gtld-servers.net NS c.gtld-servers.net NS l.gt…
  411 27.509299580   192.168.110.2     192.168.110.164   DNS     544 Standard query response 0xc551 AAAA www.googletagmanager.com AAAA 2607:f8b0:4004:c06::61 NS l.gtld-servers.net NS h.gtld-serv…
  518 27.626056351   192.168.110.164   192.168.110.2     DNS      75 Standard query 0x612e A s.go-mpulse.net
  519 27.626578024   192.168.110.164   192.168.110.2     DNS      75 Standard query 0xd52a AAAA s.go-mpulse.net
  538 27.672925989   192.168.110.2     192.168.110.164   DNS     553 Standard query response 0xd52a AAAA s.go-mpulse.net CNAME ip46.go-mpulse.net.edgekey.net CNAME e4518.dscx.akamaiedge.net AAAA…
  539 27.672926176   192.168.110.2     192.168.110.164   DNS     549 Standard query response 0x612e A s.go-mpulse.net CNAME ip46.go-mpulse.net.edgekey.net CNAME e4518.dscx.akamaiedge.net A 23.21…
  602 27.979059561   192.168.110.164   192.168.110.2     DNS      73 Standard query 0x374f A ocsp.pki.goog
  842 29.056069245   192.168.110.164   192.168.110.2     DNS      84 Standard query 0x334f A www.google-analytics.com
  843 29.056274876   192.168.110.164   192.168.110.2     DNS      84 Standard query 0xe149 AAAA www.google-analytics.com

        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 5 (5 seconds)
        Data length: 4
        Name Server: g.gtld-servers.net
    - net: type NS, class IN, ns j.gtld-servers.net
        Name: net
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 5 (5 seconds)
        Data length: 4
        Name Server: j.gtld-servers.net
  - Additional records
    - m.gtld-servers.net: type A, class IN, addr 192.55.83.30
        Name: m.gtld-servers.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)

0180  00 01 00 00 00 05 00 04  01 6a c0 93 c0 de 00 01   ········ ·j······
0190  00 01 00 00 00 05 00 04  c0 37 53 1e c1 1e 00 01   ········ ·7S·····
01a0  00 01 00 00 00 05 00 04  c0 1a 5c 1e c1 0e 00 01   ········ ··\·····
01b0  00 01 00 00 00 05 00 04  c0 0c 5e 1e c0 ce 00 01   ········ ··^·····

Text item (text), 16 bytes        Packets: 2586 · Displayed: 48 (1.9%) · Dropped: 0 (0.0%)        Profile: Default
```

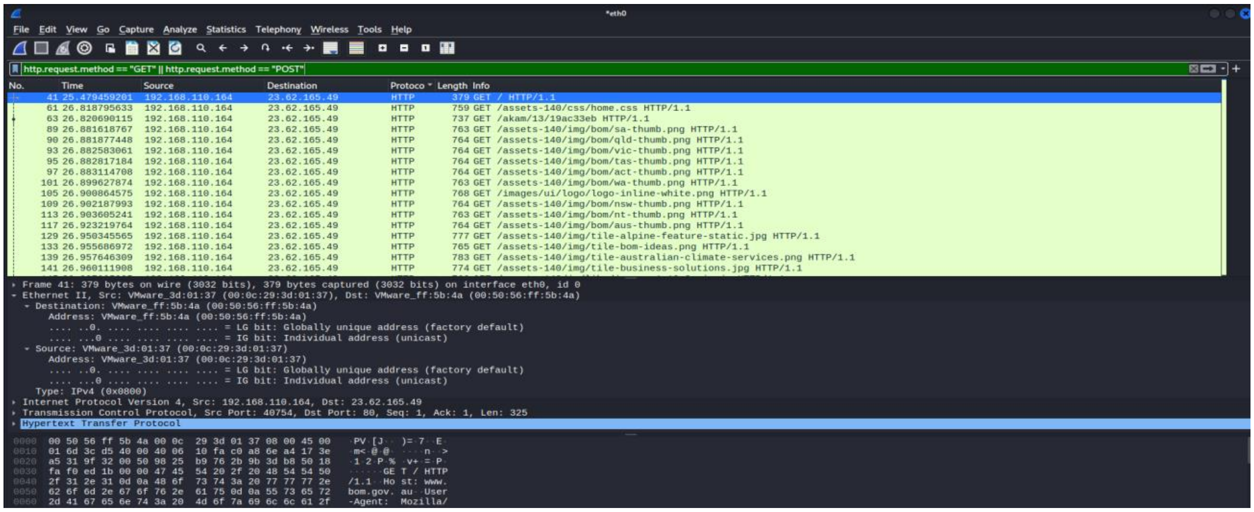
What is the DNS server for your computer?

- m.gtld-servers.net having IP address 192.55.83.30


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

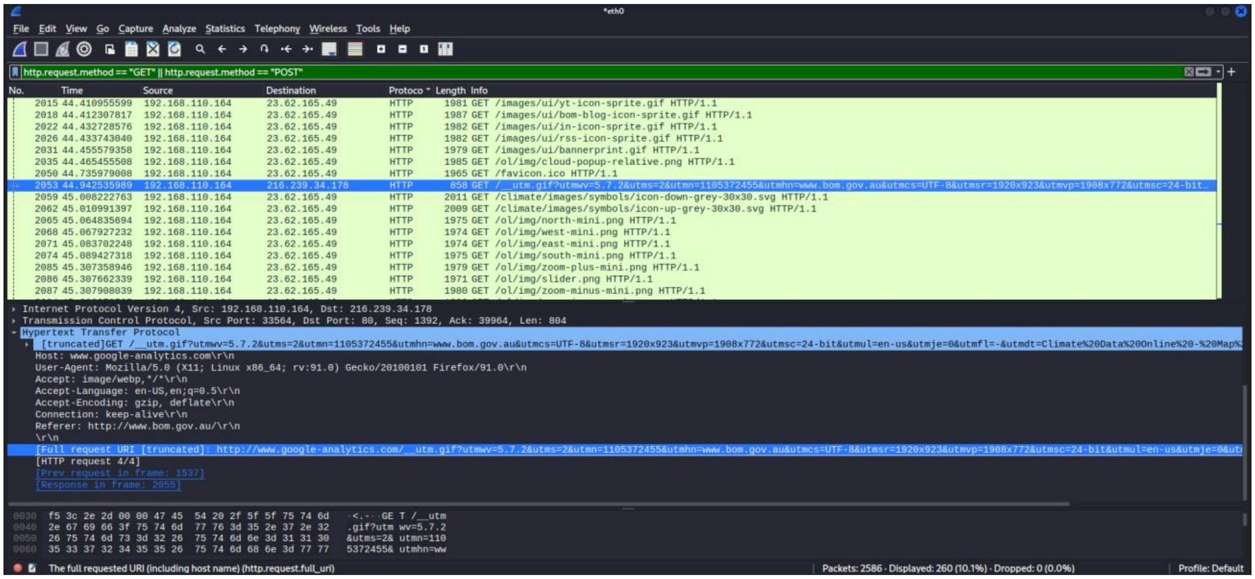
```
udp.port == 53

No.   Time           Source            Destination       Protoco Length Info
    1 0.000000000    192.168.110.164   192.168.110.2     DNS      97 Standard query 0xb7b5 A firefox.settings.services.mozilla.com
    2 0.025268568    192.168.110.2     192.168.110.164   DNS     540 Standard query response 0xb7b5 A firefox.settings.services.mozilla.com CNAME prod.remote-settings.prod.webservices.mozgcp.net…
   31 25.284116638   192.168.110.164   192.168.110.2     DNS      74 Standard query 0x5a3c A www.bom.gov.au
   32 25.284283280   192.168.110.164   192.168.110.2     DNS      74 Standard query 0x0039 AAAA www.bom.gov.au
   33 25.416273005   192.168.110.2     192.168.110.164   DNS     146 Standard query response 0x0039 AAAA www.bom.gov.au SOA a1-203.akam.net
   34 25.416273548   192.168.110.2     192.168.110.164   DNS     537 Standard query response 0x5a3c A www.bom.gov.au A 23.62.165.49 NS d.root-servers.net NS j.root-servers.net NS f.root-servers.…
  246 27.224242560   192.168.110.164   192.168.110.2     DNS      84 Standard query 0x645e A www.googletagmanager.com
  247 27.224371242   192.168.110.164   192.168.110.2     DNS      84 Standard query 0xc551 AAAA www.googletagmanager.com
  410 27.509299222   192.168.110.2     192.168.110.164   DNS     532 Standard query response 0x645e A www.googletagmanager.com A 142.251.16.97 NS m.gtld-servers.net NS c.gtld-servers.net NS l.gt…
  411 27.509299580   192.168.110.2     192.168.110.164   DNS     544 Standard query response 0xc551 AAAA www.googletagmanager.com AAAA 2607:f8b0:4004:c06::61 NS l.gtld-servers.net NS h.gtld-serv…
  518 27.626056351   192.168.110.164   192.168.110.2     DNS      75 Standard query 0x612e A s.go-mpulse.net
  519 27.626578024   192.168.110.164   192.168.110.2     DNS      75 Standard query 0xd52a AAAA s.go-mpulse.net

        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 5 (5 seconds)
        Data length: 4
        Name Server: g.gtld-servers.net
    - net: type NS, class IN, ns j.gtld-servers.net
        Name: net
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 5 (5 seconds)
        Data length: 4
        Name Server: j.gtld-servers.net
  - Additional records
    - m.gtld-servers.net: type A, class IN, addr 192.55.83.30
        Name: m.gtld-servers.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 5 (5 seconds)
        Data length: 4
```

Take note of the HTTP requests and responses. User filter http.request.method==’GET’ || http.request.method==’POST’ and http.response to check http request and response

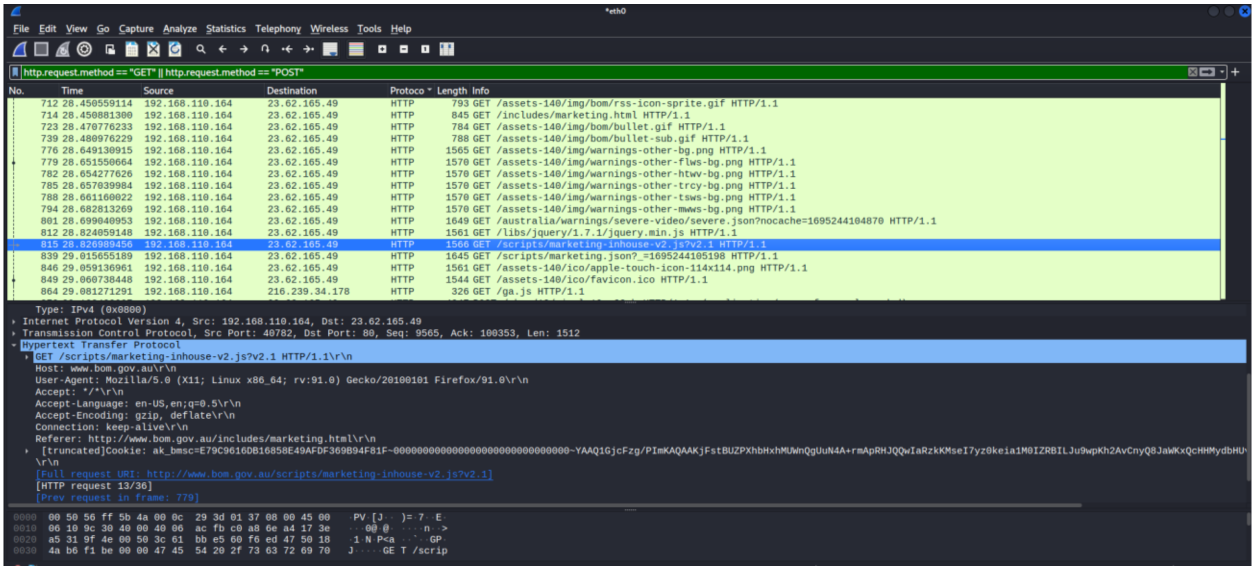

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "GET" || http.request.method == "POST"

No.   Time           Source            Destination       Protoco Length Info
   41 25.479459201   192.168.110.164   23.62.165.49      HTTP    379 GET / HTTP/1.1
   61 26.818795633   192.168.110.164   23.62.165.49      HTTP    759 GET /assets-140/css/home.css HTTP/1.1
   63 26.820690115   192.168.110.164   23.62.165.49      HTTP    737 GET /akam/13/19ac33eb HTTP/1.1
   89 26.881618767   192.168.110.164   23.62.165.49      HTTP    763 GET /assets-140/img/bom/sa-thumb.png HTTP/1.1
   90 26.881877448   192.168.110.164   23.62.165.49      HTTP    764 GET /assets-140/img/bom/qld-thumb.png HTTP/1.1
   93 26.882583061   192.168.110.164   23.62.165.49      HTTP    764 GET /assets-140/img/bom/vic-thumb.png HTTP/1.1
   95 26.882817184   192.168.110.164   23.62.165.49      HTTP    764 GET /assets-140/img/bom/tas-thumb.png HTTP/1.1
   97 26.883114708   192.168.110.164   23.62.165.49      HTTP    764 GET /assets-140/img/bom/act-thumb.png HTTP/1.1
  101 26.899627874   192.168.110.164   23.62.165.49      HTTP    763 GET /assets-140/img/bom/wa-thumb.png HTTP/1.1
  105 26.900864575   192.168.110.164   23.62.165.49      HTTP    768 GET /images/ui/logo/logo-inline-white.png HTTP/1.1
  109 26.902187993   192.168.110.164   23.62.165.49      HTTP    764 GET /assets-140/img/bom/nsw-thumb.png HTTP/1.1
  113 26.903605241   192.168.110.164   23.62.165.49      HTTP    763 GET /assets-140/img/bom/nt-thumb.png HTTP/1.1
  117 26.923219764   192.168.110.164   23.62.165.49      HTTP    764 GET /assets-140/img/bom/aus-thumb.png HTTP/1.1
  129 26.950345565   192.168.110.164   23.62.165.49      HTTP    777 GET /assets-140/img/tile-alpine-feature-static.jpg HTTP/1.1
  133 26.955686972   192.168.110.164   23.62.165.49      HTTP    765 GET /assets-140/img/tile-bom-ideas.png HTTP/1.1
  139 26.957646309   192.168.110.164   23.62.165.49      HTTP    783 GET /assets-140/img/tile-australian-climate-services.png HTTP/1.1
  141 26.960111908   192.168.110.164   23.62.165.49      HTTP    774 GET /assets-140/img/tile-business-solutions.jpg HTTP/1.1

> Frame 41: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface eth0, id 0
- Ethernet II, Src: VMware_3d:01:37 (00:0c:29:3d:01:37), Dst: VMware_ff:5b:4a (00:50:56:ff:5b:4a)
  - Destination: VMware_ff:5b:4a (00:50:56:ff:5b:4a)
      Address: VMware_ff:5b:4a (00:50:56:ff:5b:4a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  - Source: VMware_3d:01:37 (00:0c:29:3d:01:37)
      Address: VMware_3d:01:37 (00:0c:29:3d:01:37)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.110.164, Dst: 23.62.165.49
> Transmission Control Protocol, Src Port: 40754, Dst Port: 80, Seq: 1, Ack: 1, Len: 325
> Hypertext Transfer Protocol

0000  00 50 56 ff 5b 4a 00 0c  29 3d 01 37 08 00 45 00   ·PV·[J·· )=·7··E·
0010  01 6d 3c d5 40 00 40 06  10 fa c0 a8 6e a4 17 3e   ·m<·@·@· ····n··>
0020  a5 31 9f 32 00 50 98 25  b9 76 2b 9b 3d b8 50 18   ·1·2·P·% ·v+·=·P·
0030  fa f0 ed 1b 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0050  62 6f 6d 2e 67 6f 76 2e  61 75 0d 0a 55 73 65 72   bom.gov. au··User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
```

In the below snapshot we can clearly see queries made in plaintext


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "GET" || http.request.method == "POST"

No.  Time           Source            Destination      Protoco Length Info
2015 44.410955599   192.168.110.164   23.62.165.49     HTTP    1981 GET /images/ui/yt-icon-sprite.gif HTTP/1.1
2018 44.412307817   192.168.110.164   23.62.165.49     HTTP    1987 GET /images/ui/bom-blog-icon-sprite.gif HTTP/1.1
2022 44.432728576   192.168.110.164   23.62.165.49     HTTP    1982 GET /images/ui/in-icon-sprite.gif HTTP/1.1
2026 44.433743040   192.168.110.164   23.62.165.49     HTTP    1982 GET /images/ui/rss-icon-sprite.gif HTTP/1.1
2031 44.455579358   192.168.110.164   23.62.165.49     HTTP    1979 GET /images/ui/bannerprint.gif HTTP/1.1
2035 44.465455508   192.168.110.164   23.62.165.49     HTTP    1985 GET /ol/img/cloud-popup-relative.png HTTP/1.1
2050 44.735979008   192.168.110.164   23.62.165.49     HTTP    1965 GET /favicon.ico HTTP/1.1
2053 44.942535989   192.168.110.164   216.239.34.178   HTTP     858 GET /__utm.gif?utmwv=5.7.2&utms=2&utmn=1105372455&utmhn=www.bom.gov.au&utmcs=UTF-8&utmsr=1920x923&utmvp=1908x772&utmsc=24-bit…
2059 45.008222763   192.168.110.164   23.62.165.49     HTTP    2011 GET /climate/images/symbols/icon-down-grey-30x30.svg HTTP/1.1
2062 45.010991397   192.168.110.164   23.62.165.49     HTTP    2009 GET /climate/images/symbols/icon-up-grey-30x30.svg HTTP/1.1
2065 45.064835694   192.168.110.164   23.62.165.49     HTTP    1975 GET /ol/img/north-mini.png HTTP/1.1
2068 45.067927232   192.168.110.164   23.62.165.49     HTTP    1974 GET /ol/img/west-mini.png HTTP/1.1
2071 45.083702248   192.168.110.164   23.62.165.49     HTTP    1974 GET /ol/img/east-mini.png HTTP/1.1
2074 45.089427318   192.168.110.164   23.62.165.49     HTTP    1975 GET /ol/img/south-mini.png HTTP/1.1
2085 45.307358946   192.168.110.164   23.62.165.49     HTTP    1979 GET /ol/img/zoom-plus-mini.png HTTP/1.1
2086 45.307662339   192.168.110.164   23.62.165.49     HTTP    1971 GET /ol/img/slider.png HTTP/1.1
2087 45.307908039   192.168.110.164   23.62.165.49     HTTP    1980 GET /ol/img/zoom-minus-mini.png HTTP/1.1

› Internet Protocol Version 4, Src: 192.168.110.164, Dst: 216.239.34.178
› Transmission Control Protocol, Src Port: 33564, Dst Port: 80, Seq: 1392, Ack: 39964, Len: 804
▾ Hypertext Transfer Protocol
  › [truncated]GET /__utm.gif?utmwv=5.7.2&utms=2&utmn=1105372455&utmhn=www.bom.gov.au&utmcs=UTF-8&utmsr=1920x923&utmvp=1908x772&utmsc=24-bit&utmul=en-us&utmje=0&utmfl=-&utmdt=Climate%20Data%20Online%20-%20Map%
    Host: www.google-analytics.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
    Accept: image/webp,*/*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.bom.gov.au/\r\n
    \r\n
    [Full request URI [truncated]: http://www.google-analytics.com/__utm.gif?utmwv=5.7.2&utms=2&utmn=1105372455&utmhn=www.bom.gov.au&utmcs=UTF-8&utmsr=1920x923&utmvp=1908x772&utmsc=24-bit&utmul=en-us&utmje=0&ut
    [HTTP request 4/4]
    [Prev request in frame: 1537]
    [Response in frame: 2055]

0030  f5 3c 2e 2d 00 00 47 45  54 20 2f 5f 5f 75 74 6d   ·<.-··GE T /__utm
0040  2e 67 69 66 3f 75 74 6d  77 76 3d 35 2e 37 2e 32   .gif?utm wv=5.7.2
0050  26 75 74 6d 73 3d 32 26  75 74 6d 6e 3d 31 31 30   &utms=2& utmn=110
0060  35 33 37 32 34 35 35 26  75 74 6d 68 6e 3d 77 77   5372455& utmhn=ww

The full requested URI (including host name) (http.request.full_uri)    Packets: 2586 · Displayed: 260 (10.1%) · Dropped: 0 (0.0%)    Profile: Default
```

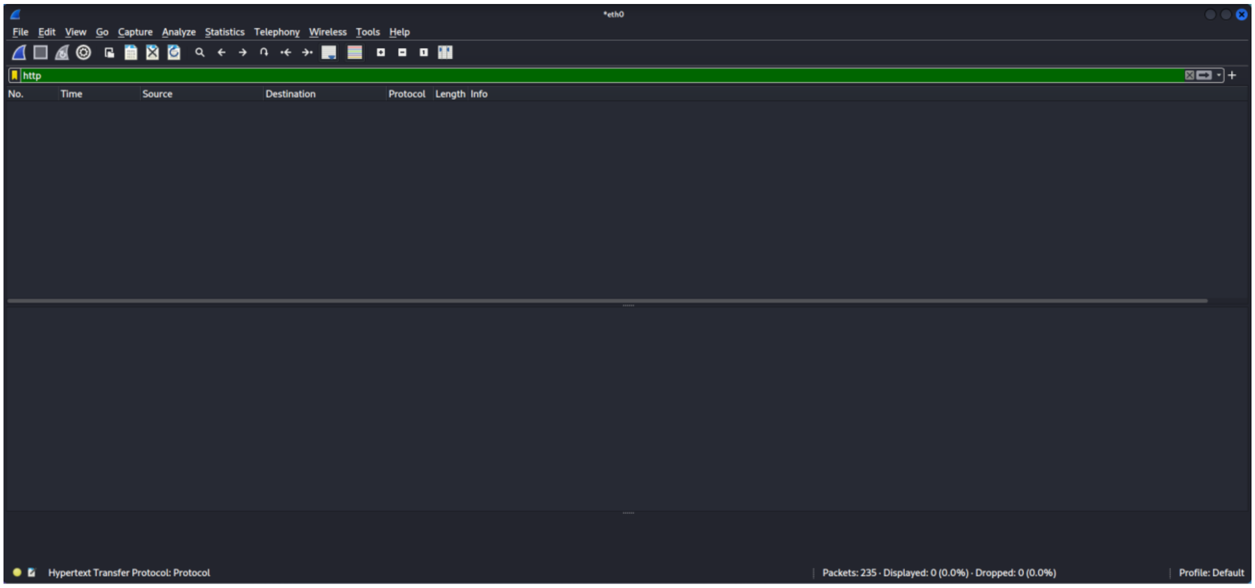

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "GET" || http.request.method == "POST"

No. Time           Source            Destination      Protoco Length Info
712 28.450559114   192.168.110.164   23.62.165.49     HTTP     793 GET /assets-140/img/bom/rss-icon-sprite.gif HTTP/1.1
714 28.450881300   192.168.110.164   23.62.165.49     HTTP     845 GET /includes/marketing.html HTTP/1.1
723 28.470776233   192.168.110.164   23.62.165.49     HTTP     784 GET /assets-140/img/bom/bullet.gif HTTP/1.1
739 28.480976229   192.168.110.164   23.62.165.49     HTTP     788 GET /assets-140/img/bom/bullet-sub.gif HTTP/1.1
776 28.649130915   192.168.110.164   23.62.165.49     HTTP    1565 GET /assets-140/img/warnings-other-bg.png HTTP/1.1
779 28.651550664   192.168.110.164   23.62.165.49     HTTP    1570 GET /assets-140/img/warnings-other-flws-bg.png HTTP/1.1
782 28.654277626   192.168.110.164   23.62.165.49     HTTP    1570 GET /assets-140/img/warnings-other-htwv-bg.png HTTP/1.1
785 28.657039984   192.168.110.164   23.62.165.49     HTTP    1570 GET /assets-140/img/warnings-other-trcy-bg.png HTTP/1.1
788 28.661160022   192.168.110.164   23.62.165.49     HTTP    1570 GET /assets-140/img/warnings-other-tsws-bg.png HTTP/1.1
794 28.682813269   192.168.110.164   23.62.165.49     HTTP    1570 GET /assets-140/img/warnings-other-mwws-bg.png HTTP/1.1
801 28.699040953   192.168.110.164   23.62.165.49     HTTP    1649 GET /australia/warnings/severe-video/severe.json?nocache=1695244104870 HTTP/1.1
812 28.824059148   192.168.110.164   23.62.165.49     HTTP    1561 GET /libs/jquery/1.7.1/jquery.min.js HTTP/1.1
815 28.826989456   192.168.110.164   23.62.165.49     HTTP    1566 GET /scripts/marketing-inhouse-v2.js?v2.1 HTTP/1.1
839 29.015655189   192.168.110.164   23.62.165.49     HTTP    1645 GET /scripts/marketing.json?_=1695244105198 HTTP/1.1
846 29.059136961   192.168.110.164   23.62.165.49     HTTP    1561 GET /assets-140/ico/apple-touch-icon-114x114.png HTTP/1.1
849 29.060738448   192.168.110.164   23.62.165.49     HTTP    1544 GET /assets-140/ico/favicon.ico HTTP/1.1
864 29.081271291   192.168.110.164   216.239.34.178   HTTP     326 GET /ga.js HTTP/1.1

    Type: IPv4 (0x0800)
› Internet Protocol Version 4, Src: 192.168.110.164, Dst: 23.62.165.49
› Transmission Control Protocol, Src Port: 40782, Dst Port: 80, Seq: 9565, Ack: 100353, Len: 1512
▾ Hypertext Transfer Protocol
  › GET /scripts/marketing-inhouse-v2.js?v2.1 HTTP/1.1\r\n
    Host: www.bom.gov.au\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.bom.gov.au/includes/marketing.html\r\n
  › [truncated]Cookie: ak_bmsc=E79C9616DB16858E49AFDF369B94F81F~000000000000000000000000000000~YAAQ1GjcFzg/PImKAQAAKjFstBUZPXhbHxhMUWnQgUuN4A+rmApRHJQQwIaRzkKMseI7yz0keia1M0IZRBILJu9wpKh2AvCnyQ8JaWKxQcHHMydbHU
    \r\n
    [Full request URI: http://www.bom.gov.au/scripts/marketing-inhouse-v2.js?v2.1]
    [HTTP request 13/36]
    [Prev request in frame: 779]

0000  00 50 56 ff 5b 4a 00 0c  29 3d 01 37 08 00 45 00   ·PV·[J·· )=·7··E·
0010  06 10 9c 30 40 00 40 06  ac fb c0 a8 6e a4 17 3e   ···0@·@· ····n··>
0020  a5 31 9f 4e 00 50 3c 61  bb e5 60 f6 ed 47 50 18   ·1·N·P<a ··`··GP·
0030  4a b6 f1 be 00 00 47 45  54 20 2f 73 63 72 69 70   J·····GE T /scrip
```

## 2. Capturing live traffic and visiting an encrypted website

I am not able to see any HTTP traffic after accessing site https://www.google.com as Google site we searched is using HTTP protocol which is an encrypted protocol

Also, you will not be able to see any actual content of the HTTPS requests and responses in plain text. This is because HTTPS traffic is encrypted for security reasons.



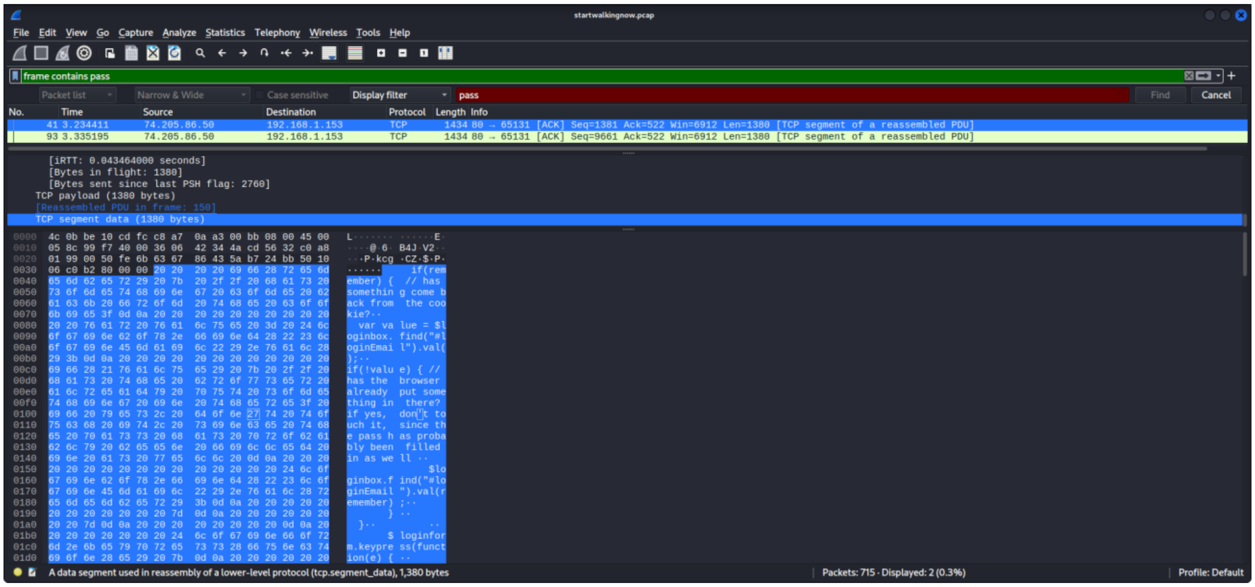
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time   Source   Destination   Protocol   Length   Info
```

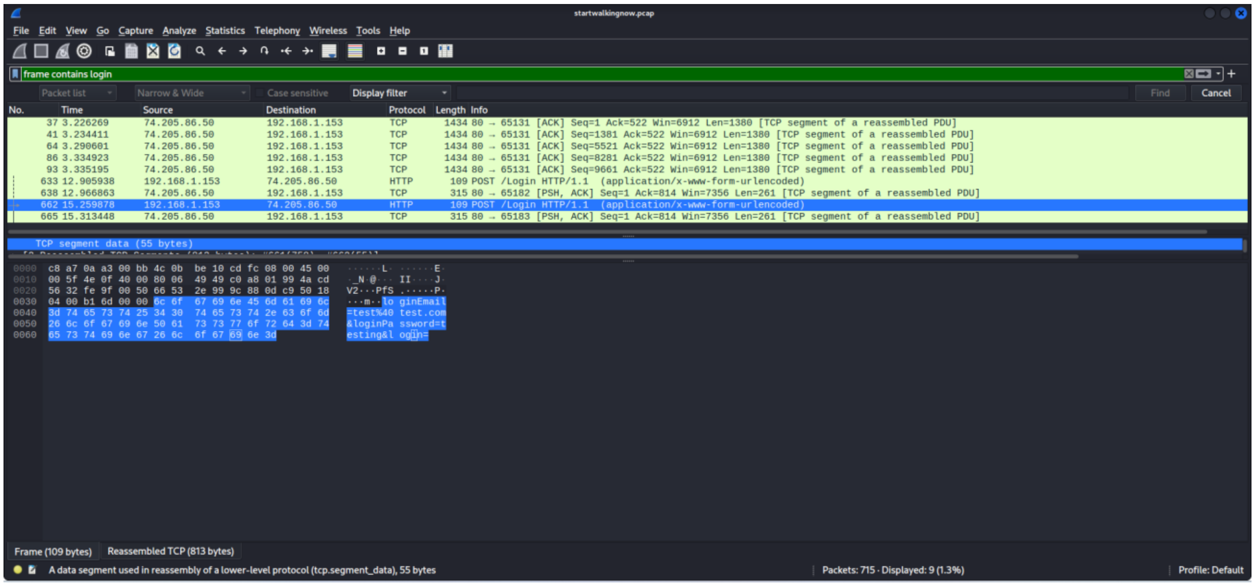
```
Hypertext Transfer Protocol: Protocol      Packets: 235 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)      Profile: Default
```

### 3. Analyzing a saved packet capture to determine a vulnerability in a website

I can see javascript code and considering the all snapshots it looks like password spraying attack which is a brute-force can be possible on this site as it is showing the response to a login attempt



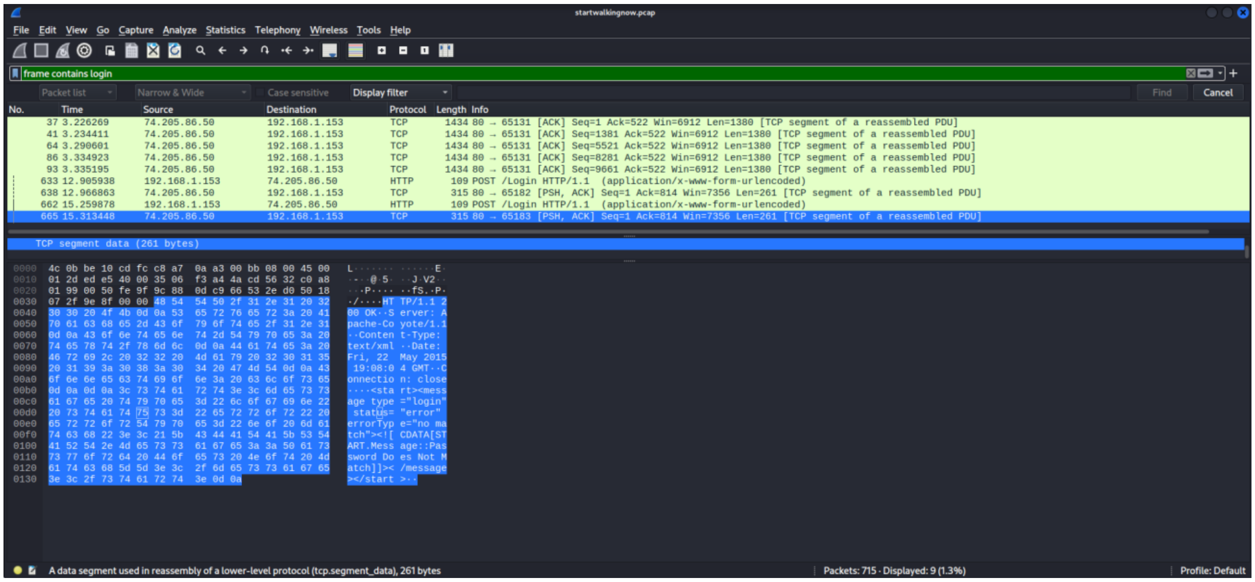
```
frame contains pass
pass

No.   Time       Source        Destination    Protocol Length Info
   41 3.234411   74.205.86.50  192.168.1.153  TCP      1434 80 → 65131 [ACK] Seq=1381 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
   93 3.335195   74.205.86.50  192.168.1.153  TCP      1434 80 → 65131 [ACK] Seq=9661 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]

      [iRTT: 0.043464000 seconds]
      [Bytes in flight: 1380]
      [Bytes sent since last PSH flag: 2760]
    TCP payload (1380 bytes)
    [Reassembled PDU in frame: 150]
    TCP segment data (1380 bytes)

0000  4c 0b be 10 cd fc c8 a7  0a a3 00 bb 08 00 45 00   L······· ······E·
0010  05 8c 99 f7 40 00 36 06  42 34 4a cd 56 32 c0 a8   ····@·6· B4J·V2··
0020  01 99 00 50 fe 6b 63 67  86 43 5a b7 24 bb 50 10   ···P·kcg ·CZ·$·P·
0030  06 c0 b2 80 00 00 20 20  20 20 69 66 28 72 65 6d   ······     if(rem
0040  65 6d 62 65 72 29 20 7b  20 2f 2f 20 68 61 73 20   ember) {  // has 
0050  73 6f 6d 65 74 68 69 6e  67 20 63 6f 6d 65 20 62   somethin g come b
0060  61 63 6b 20 66 72 6f 6d  20 74 68 65 20 63 6f 6f   ack from  the coo
0070  6b 69 65 3f 0d 0a 20 20  20 20 20 20 20 20 20 20   kie?··          
0080  20 20 76 61 72 20 76 61  6c 75 65 20 3d 20 24 6c     var va lue = $l
0090  6f 67 69 6e 62 6f 78 2e  66 69 6e 64 28 22 23 6c   oginbox. find("#l
00a0  6f 67 69 6e 45 6d 61 69  6c 22 29 2e 76 61 6c 28   oginEmai l").val(
00b0  29 3b 0d 0a 20 20 20 20  20 20 20 20 20 20 20 20   );··            
00c0  69 66 28 21 76 61 6c 75  65 29 20 7b 20 2f 2f 20   if(!valu e) { // 
00d0  68 61 73 20 74 68 65 20  62 72 6f 77 73 65 72 20   has the  browser 
00e0  61 6c 72 65 61 64 79 20  70 75 74 20 73 6f 6d 65   already  put some
00f0  74 68 69 6e 67 20 69 6e  20 74 68 65 72 65 3f 20   thing in  there? 
0100  69 66 20 79 65 73 2c 20  64 6f 6e 27 74 20 74 6f   if yes,  don't to
0110  75 63 68 20 69 74 2c 20  73 69 6e 63 65 20 74 68   uch it,  since th
0120  65 20 70 61 73 73 20 68  61 73 20 70 72 6f 62 61   e pass h as proba
0130  62 6c 79 20 62 65 65 6e  20 66 69 6c 6c 65 64 20   bly been  filled 
0140  69 6e 20 61 73 20 77 65  6c 6c 20 0d 0a 20 20 20   in as we ll ··   
0150  20 20 20 20 20 20 20 20  20 20 20 20 20 24 6c 6f                $lo
0160  67 69 6e 62 6f 78 2e 66  69 6e 64 28 22 23 6c 6f   ginbox.f ind("#lo
0170  67 69 6e 45 6d 61 69 6c  22 29 2e 76 61 6c 28 72   ginEmail ").val(r
0180  65 6d 65 6d 62 65 72 29  3b 0d 0a 20 20 20 20 20   emember) ;··     
0190  20 20 20 20 20 20 20 7d  0d 0a 20 20 20 20 20 20          } ··      
01a0  20 20 7d 0d 0a 20 20 20  20 20 20 20 20 0d 0a 20     }··        ·· 
01b0  20 20 20 20 20 20 20 24  6c 6f 67 69 6e 66 6f 72          $ loginfor
01c0  6d 2e 6b 65 79 70 72 65  73 73 28 66 75 6e 63 74   m.keypre ss(funct
01d0  69 6f 6e 28 65 29 20 7b  0d 0a 20 20 20 20 20 20   ion(e) { ··      

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1,380 bytes      Packets: 715 · Displayed: 2 (0.3%)      Profile: Default
```


startwalkingnow.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel
Frame (109 bytes)
Reassembled TCP (813 bytes)

frame contains login

```
No.  Time       Source          Destination     Protocol Length Info
  37 3.226269   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=1 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  41 3.234411   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=1381 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  64 3.290601   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=5521 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  86 3.334923   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=8281 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  93 3.335195   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=9661 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
 633 12.905938  192.168.1.153   74.205.86.50    HTTP      109 POST /Login HTTP/1.1  (application/x-www-form-urlencoded)
 638 12.966863  74.205.86.50    192.168.1.153   TCP       315 80 → 65182 [PSH, ACK] Seq=1 Ack=814 Win=7356 Len=261 [TCP segment of a reassembled PDU]
 662 15.259878  192.168.1.153   74.205.86.50    HTTP      109 POST /Login HTTP/1.1  (application/x-www-form-urlencoded)
 665 15.313448  74.205.86.50    192.168.1.153   TCP       315 80 → 65183 [PSH, ACK] Seq=1 Ack=814 Win=7356 Len=261 [TCP segment of a reassembled PDU]

    TCP segment data (55 bytes)

0000  c8 a7 0a a3 00 bb 4c 0b  be 10 cd fc 08 00 45 00   ······L· ······E·
0010  00 5f 4e 0f 40 00 80 06  49 49 c0 a8 01 99 4a cd   ·_N·@··· II····J·
0020  56 32 fe 9f 00 50 66 53  2e 99 9c 88 0d c9 50 18   V2···PfS .·····P·
0030  04 00 b1 6d 00 00 6c 6f  67 69 6e 45 6d 61 69 6c   ···m··lo ginEmail
0040  3d 74 65 73 74 25 34 30  74 65 73 74 2e 63 6f 6d   =test%40 test.com
0050  26 6c 6f 67 69 6e 50 61  73 73 77 6f 72 64 3d 74   &loginPa ssword=t
0060  65 73 74 69 6e 67 26 6c  6f 67 69 6e 3d            esting&l ogin=
```

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 55 bytes | Packets: 715 · Displayed: 9 (1.3%) | Profile: Default



frame contains login

```
No.  Time       Source          Destination     Protocol Length Info
  37 3.226269   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=1 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  41 3.234411   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=1381 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  64 3.290601   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=5521 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  86 3.334923   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=8281 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
  93 3.335195   74.205.86.50    192.168.1.153   TCP      1434 80 → 65131 [ACK] Seq=9661 Ack=522 Win=6912 Len=1380 [TCP segment of a reassembled PDU]
 633 12.905938  192.168.1.153   74.205.86.50    HTTP      109 POST /Login HTTP/1.1  (application/x-www-form-urlencoded)
 638 12.966863  74.205.86.50    192.168.1.153   TCP       315 80 → 65182 [PSH, ACK] Seq=1 Ack=814 Win=7356 Len=261 [TCP segment of a reassembled PDU]
 662 15.259878  192.168.1.153   74.205.86.50    HTTP      109 POST /Login HTTP/1.1  (application/x-www-form-urlencoded)
 665 15.313448  74.205.86.50    192.168.1.153   TCP       315 80 → 65183 [PSH, ACK] Seq=1 Ack=814 Win=7356 Len=261 [TCP segment of a reassembled PDU]

    TCP segment data (261 bytes)

0000  4c 0b be 10 cd fc c8 a7  0a a3 00 bb 08 00 45 00   L······· ······E·
0010  01 2d ed e5 40 00 35 06  f3 a4 4a cd 56 32 c0 a8   ·-··@·5· ··J·V2··
0020  01 99 00 50 fe 9f 9c 88  0d c9 66 53 2e d0 50 18   ···P···· ··fS.·P·
0030  07 2f 9e 8f 00 00 48 54  54 50 2f 31 2e 31 20 32   ·/····HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 41   00 OK··S erver: A
0050  70 61 63 68 65 2d 43 6f  79 6f 74 65 2f 31 2e 31   pache-Co yote/1.1
0060  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0070  74 65 78 74 2f 78 6d 6c  0d 0a 44 61 74 65 3a 20   text/xml ··Date: 
0080  46 72 69 2c 20 32 32 20  4d 61 79 20 32 30 31 35   Fri, 22  May 2015
0090  20 31 39 3a 30 38 3a 30  34 20 47 4d 54 0d 0a 43    19:08:0 4 GMT··C
00a0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 63 6c 6f 73 65   onnectio n: close
00b0  0d 0a 0d 0a 3c 73 74 61  72 74 3e 3c 6d 65 73 73   ····<sta rt><mess
00c0  61 67 65 20 74 79 70 65  3d 22 6c 6f 67 69 6e 22   age type ="login"
00d0  20 73 74 61 74 75 73 3d  22 65 72 72 6f 72 22 20    status= "error" 
00e0  65 72 72 6f 72 54 79 70  65 3d 22 6e 6f 20 6d 61   errorTyp e="no ma
00f0  74 63 68 22 3e 3c 21 5b  43 44 41 54 41 5b 53 54   tch"><![ CDATA[ST
0100  41 52 54 2e 4d 65 73 73  61 67 65 3a 3a 50 61 73   ART.Mess age::Pas
0110  73 77 6f 72 64 20 44 6f  65 73 20 4e 6f 74 20 4d   sword Do es Not M
0120  61 74 63 68 5d 5d 3e 3c  2f 6d 65 73 73 61 67 65   atch]]>< /message
0130  3e 3c 2f 73 74 61 72 74  3e 0d 0a                  ></start >··
```

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 261 bytes | Packets: 715 · Displayed: 9 (1.3%) | Profile: Default