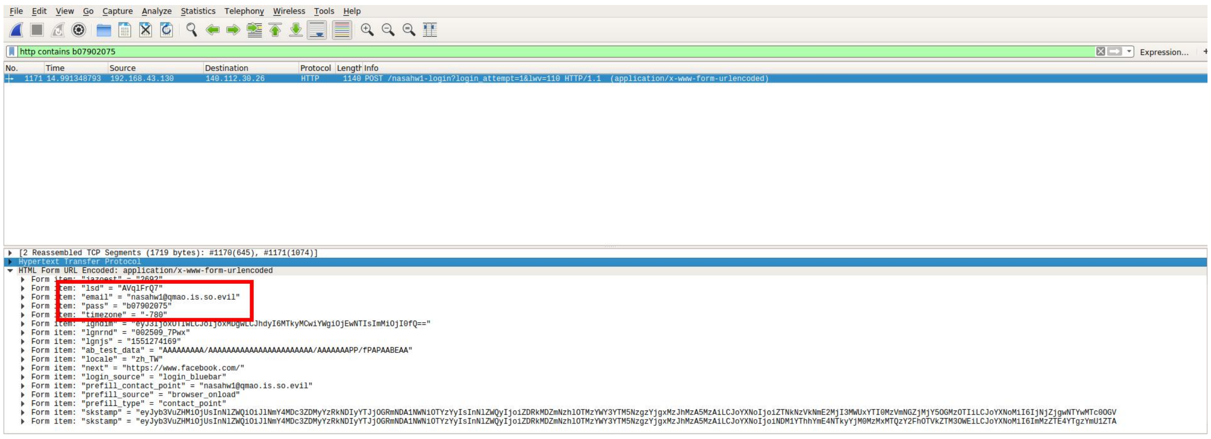
Network Administration

- Student Name: 林楷恩
- Student ID: b07902075

NANI? Is my uplink as evil as Q-mao? (15%)

1. Find the packet that contains the email and password you just typed, and screenshot it. (5%)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http contains b07902075
Expression…

```
No.   Time          Source          Destination    Protocol Length Info
1171 14.991348793 192.168.43.130  140.112.30.26  HTTP     1140 POST /nasahw1-login?login_attempt=1&lwv=110 HTTP/1.1  (application/x-www-form-urlencoded)
```

```
▶ [2 Reassembled TCP Segments (1719 bytes): #1170(645), #1171(1074)]
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "jazoest" = "2692"
  ▶ Form item: "lsd" = "AVqlFrQ7"
  ▶ Form item: "email" = "nasahw1@qmao.is.so.evil"
  ▶ Form item: "pass" = "b07902075"
  ▶ Form item: "timezone" = "-780"
  ▶ Form item: "lgndim" = "eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTkyMCwiYWgiOjEwNTIsImMiOjI0fQ=="
  ▶ Form item: "lgnrnd" = "002509_7Pwx"
  ▶ Form item: "lgnjs" = "1551274169"
  ▶ Form item: "ab_test_data" = "AAAAAAAAA/AAAAAAAAAAAAAAAAAAAAAAA/AAAAAAAPP/fPAPAABEAA"
  ▶ Form item: "locale" = "zh_TW"
  ▶ Form item: "next" = "https://www.facebook.com/"
  ▶ Form item: "login_source" = "login_bluebar"
  ▶ Form item: "prefill_contact_point" = "nasahw1@qmao.is.so.evil"
  ▶ Form item: "prefill_source" = "browser_onload"
  ▶ Form item: "prefill_type" = "contact_point"
  ▶ Form item: "skstamp" = "eyJyb3VuZHMiOjUsInNlZWQiOiJlNmY4MDc3ZDMyYzRkNDIyYTJjOGRmNDA1NWNiOTYzYyIsInNlZWQyIjoiZDRkMDZmNzhlOTMzYWY3YTM5NzgzYjgxMzJhMzA5MzAiLCJoYXNoIjoiZTNkNzVkNmE2MjI3MWUxYTI0MzVmNGZjMjY5OGMzOTIiLCJoYXNoMiI6IjNjZjgwNTYwMTc0OGV
  ▶ Form item: "skstamp" = "eyJyb3VuZHMiOjUsInNlZWQiOiJlNmY4MDc3ZDMyYzRkNDIyYTJjOGRmNDA1NWNiOTYzYyIsInNlZWQyIjoiZDRkMDZmNzhlOTMzYWY3YTM5NzgzYjgxMzJhMzA5MzAiLCJoYXNoIjoiNDM1YThhYmE4NTkyYjM0MzMxMTQzY2FhOTVkZTM3OWEiLCJoYXNoMiI6ImMzZTE4YTgzYmU1ZTA
```

- Apply a display filter: **http contains b07902075.**
- The email and password is in a http POST packet.

2. Re-perform the above steps at fakebook-https2, can you find the email and password this time? (5%)

If the web server implements HSTS, I have the chance to do MitM only **the first time** a user connect to the website. It is because most users enter the url without specifying which scheme to use and the browser default to use HTTP. Thus, the web server runners who willing to enforce secure connections should redirect those users to HTTPS version, but this method is still subjected to MitM attack, while hackers can hijack the initial HTTP connection by converting the HTTPS link to HTTP, and he, as a man-in-the-middle, can eavesdrop all the plain text packets.

A way to avoid this is HSTS(HTTP Strict-Transport-Security). The HSTS mechanism ensures that the users will only access the website with HTTP and be redirected **only once**. However, hackers still can hijack the initial HTTP connection when users access it first time, though the risk has been considerably mitigated.

* References

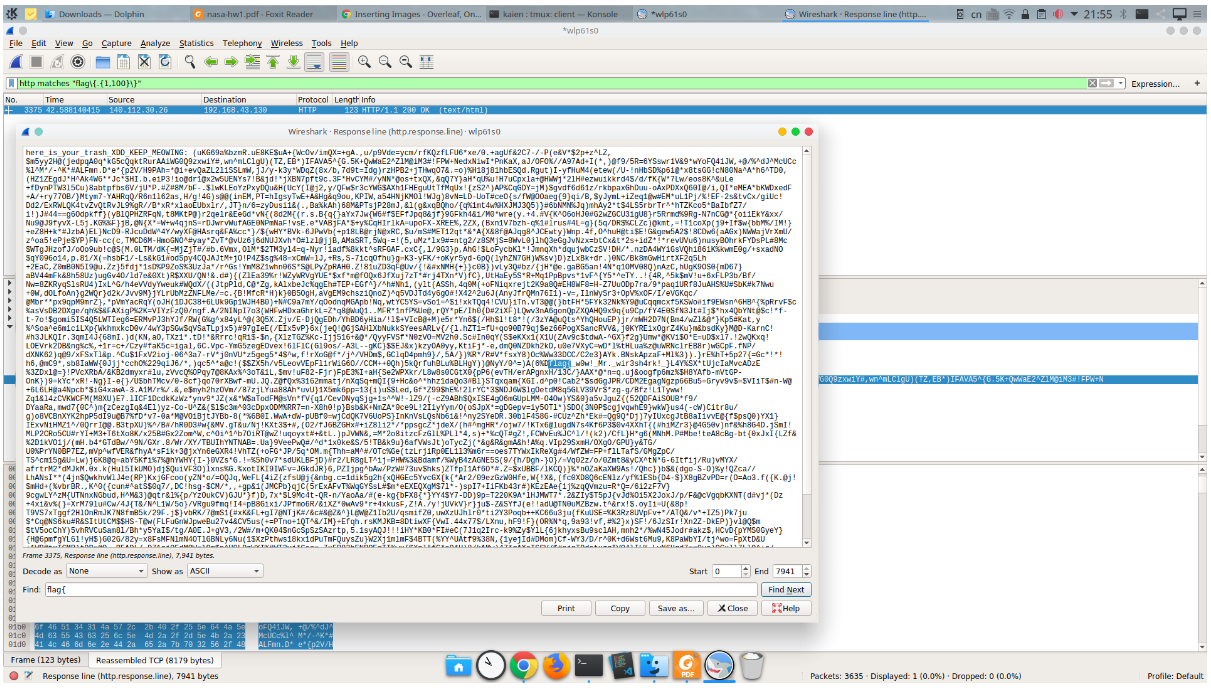
- https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

3. Give a real-world examples that your password may be eavesdropped by Q-mao when still using the HTTP protocol. (assuming no eavesdropper in client and server-side software) (5%)

For example, `ipac.nlpi.edu.tw`（臺中市立圖書館）still use HTTP. If a hacker perform a man-in-the-middle attack(e.g. through arp spoofing), making the traffic between two ends pass through his device and sniff them. Since HTTP use plain text, my account-name and password will be exposed to the hacker.

In the vast sea, I see nobody but flag (10%)

1. Open Wireshark and start capturing packets.
2. Go to "nasa-hw1.csie.ntu.edu.tw/flagsea" and wait until the page is fully loaded.
3. Stop capturing packets.
4. Apply a display filter: **http matches "flag\{.{1,100}\}"**
5. Right click the data field which starts with `here_is_your_trash_XDD_KEEP_MEOWING:` and select "Show Packet Bytes"
6. Type "flag{" in the "Find: " input box below, then the flag pops up.
7. flag{_w0w!_Mr._wir3sh4rk!_}


Downloads — Dolphin
nasa-hw1.pdf - Foxit Reader
Inserting Images - Overleaf, On...
kaien : tmux: client — Konsole
*wlp61s0
Wireshark · Response line (http....
21:55
*wlp61s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Wireshark · Response line (http.response.line) · wlp61s0
Decode as None
Show as ASCII
Start 0
End 7941
Find: flag{
Find Next
Print
Copy
Save as...
Close
Help
Frame (123 bytes)
Reassembled TCP (8179 bytes)
Profile: Default

```
http matches "flag\{.{1,100}\}"

No.  Time         Source         Destination     Protocol Length Info
3375 42.588140415 140.112.30.26  192.168.43.130  HTTP     123 HTTP/1.1 200 OK  (text/html)
```

```
here_is_your_trash_XDD_KEEP_MEOWING: (uKG69a%bzmR.uE8KE$uA+{WcOv/imQX=+gA.,u/p9Vde=ycm/rfKQzfLFU6*xe/0.+agUf&2C7-/-P(e&V*$2p+z^LZ,
$m5yy2H@(jedpqA0q*kG5cQqktRurAAiWG0Q9zxwiY#,wn^mLClgU)(TZ,EB*)IFAVA5^{G.5K+QwWaE2^Z1M@iM3#!FPW+NedxNiwI*PnKaX,aJ/OFO%//A97Ad+I(*,)@f9/5R=6YSswr1V&9*wYoFQ41JW,+@/%^dJ^McUCc
%l^M*/-^K*#ALFmn.D*e*{p2V/H9PAh=*@i+evQaZL2l1SSLmW,jJ/y-k3y*WDqZ(8x/b,7d9t=Idg)rzHPB2+jTHwq07&.=o)%H18j81hbESQd.Rgut)I-yfHuM4(etew(/U-!nHbSD%p6i@*x8tsGG!cN80Na^A*h6^TD0,
(HZ1ZEgdJ*H^Ak4W6**Jc*$HI.b.eiP3!io@dr1@x2w5UENYs7!B&jd!*jXBN7pft9c.3F*HvCYM#/yNN*@os+txQX,&qQ7Y}aH*qU%u!H7uCpxla+@HWWj*21H#ezwuikkrd4$/d/fK{W*7Lw/eos8K^&uLe
+fDynPTW3l5Cu)8abtpfbs6V/jU*P.#Z#8M/bF-.$lwKLEoYzPxyDQu&H(UcY(I@j2,y/QFw$r3cYWG$AXh1FHEguUtTfMqUx!{zS2^)AP%CqGDY=jM)$gvdf6d61z/rkbpaxGhDuu-oAxPDXxQ60I@/i,QI*eMEA*bKWDxedF
+A/+ry77OB/}Mtym7-YAHRqQ/R6n1l62as,H/g!4G)s@@(inEM,PT=hIgsyTwE+A&Hg&q9ou,KPIW,a54HNjKMOl!WJg)8vN=LD-UoT#ce0{s/fW@OOaeg{9}qi/B,$yJymL+iZeq1@w#EM*uL1Pj/%!EF-2s&tvCx/giUc!
Dd2/ExRWLQK4tvZvQtRvJL9%gR//B*xR*xlaoEUbxlr/,JT}n/6=zyDusi1&(.,Ba%kAh)68M&PTsjP28mJ,&l(g&xqBQho/{q%1mt4w%HXJMJ3Q5)}#6bNMN%Jq)mhAy2*t$4LS5rbrTr^*hTZKco5*BaIbfZ7/
i!)J#44==g60dpkff}(yBlQPHZRFqN,t8MKtP@)r2qelr&EeGd*vN{(8d2M{(r.s.B{q{}aYx7Jw{W6#f$EFfJpq8&jf}9GFkh4&i/M0*wre(y.+4.#V{K^O6oHJ0#G2wZGCU3igU8}r5Rrmd%9Rg-N7nCG@*{oi1EkY&xx/
Nu9@J9fyvX-L5j.KG%%F}jB,@N{X*=W+w4qjnS=rDJwrvWufAGE0NPmNaF!vsE.e*VABjFA*$+y%CqHIrlkA=upoFX-XREE%,2ZX,(Bxn1V7bzh-q%1#lrus#4L=g}(5q/DR$%CLZc)@kmt,=!T1coXp(j9+If$w{bbM%/IM!}
+eZ8H+k*#JzbA)EL}NcD9-RJcuDdW^4Y/wyXF@HAsrq&FA%cc*}/${wHY*BVk-6JPwVb(+p18LB@rjN@xRC,$u/mS#MET12qt*&*A{X&8f@AJqg8^JCEwty}Wnp.4f,O^huH@ti$E!G&gew5A2$!8CDw6(aAGx)NWWajVrXmU/
z^oa5!ePje$YP)FN-cc(c,TMCD6M-HmoGNO^#yay*ZvT*@vUz6j6dNUJXvh*O#lzl@jjB,AMaSRT,5Wq-=!(5,uMz*lx9#=ntg2/z8SMjS=8WvL0jlhQ3eGgJvNzx=btCx&t*2s+idZ*!*revUVu6)nusyBOhrkFYDsPL#8Mc
$WTgJHzofJ/oOo9ub!c@S(M.0LTM/dK{=MjZjT#/#b.6Vmx,O1M*$2TM3yl4=q-Nyr!iadf%8kkt^sRFGAF.cxC{,1/9G3}p,AhG!$LoFycbKl*!JmnqXh*dqujwbCzSV!DH/*.nzDA4WYiGsVQhi86iK%kwmE0g/+sxadNO
$qY096o14,p.81/X(=hsbF1/-Ls&kG1#odSpy4CQJAJtM+jO!P4Z$sg%48=xCmW=lJ,+Rs,S-7icqOfhu}g=K3-yFK/+oKyr5yd-6pQ(lyhZN7GH)W%sv)D)zLxBk+dr.)0NC/Bk8mGwHirtXF2q5Lh
+2EaC,Z0mB0N5I9@u.Zz}5fdj*1sD%P9ZoS%3UzJa*/r^Gs!YmM8Z1whn06S*S@LPyZpRAH0.Z!81uZD3qF@Uv/{!&#xNMH{+}}c0B})vLy3Q#bz/{jH*@e.gaBG5an!4N*q1OMV08Q)nAzC,hUgK9OS0{mD67}
[illegible]
MLP2CRo5CU#rYI+M3+T6tXo8K/x25B#Gx2Zom^W,c^O1^1^b7O1RT@wZ!uqoyxt#+&tL.)pJVWN&,=M*2o81tzcFzGlL%PLI*4,s)+*%cQT#gZ!,FCWvEu%JC^1/!(k2)/CfL}H*g6(MNhM.P#Mbe!teA8cBg-bt{0xJxI{LZf&
%2D1kVO1j/(mH.b4*GTdBw/^9N/GXr.8/Wr/XY/TBUIhYNTNAB=.Ua}9VeePwQ#/^d*1x0ke&S/5!TB&k9u}6afVWsJt)oTycZj(*&g&R&gmA&h!A%q.VIp29SxmH/OXgO/GPU}y&TG/
U0%PrYN0BP7EZ,mVp^wfVER&fhyA*sFik+3@jxYn6eGXR4!VhTZ(+oFG*JP/5q*OM.m{Thh=aM^#/OTc%Ge(tzLrjiRp0EL113%m6r==oes7TYWxIkReXg#4/WfZW=FP+flLTafS/GMgZpC/
TS^cm15g&U=Lw)j6K8@q=abY5Kfi%7%@hYWHY{I-}0VZs*G.!=%5h0v7*sdUKLBFjD)#r2/LR8gLT^ij=PHW%3&Bdamf/%WyB4zAGNE5S(9/{h/Dgh-}O}/=Vq02z/o/0Zmt8&yCX^tN*6-6Itfij/Ru)vMYX/
afrtrM2*dMJkM.0x.k(Hul5IkUMO)dj$QuiVF3O)lxns%G.%xotIKI9IWFv=JGkdJR}6,PZIjpg^bAw/PzW#73uv$hks)ZTfpI1Af6O*#.Z=$xUBBF/lKCQ)}%*nOZaKaXW9As!/Qhc}b$&(dgo-S-O)%y!QZca//
LhANsI**(4jn$QwkhvWlJ4e(RP)KxjGFcoo(yZN*o/=OQJq,WeFL{4iZ{zfsU@j{&nbg.c=1dik5g2h{xQHGEc5YvcGX{k{*Ar2/09ezGzW0Hfe,W{!X&,(fc0XD8Q6cENlz/yf%1ESb{D4-$}X8gBZvPD=r(O=Ao3.f({K.@j!
$mHd+(%vbrBR.,K^0({cun#^atS$0q7/,DC!hsg-$CM/*,,+gp&1(JMCPb}qjC(5rExAFvT%WqGYSsL#$m*eEXEQXgM$7l*-)spI7+IiFKb43r#)KEzEAe{1j%zqQVmzu=R*Q=/6i2zF7V}
9cgwLY^zM{UTNnxNGbud,H^M&3)@qtr&l%{p/YzOukCV)GJU*}f)D,7x*$L9Mc4t-QR-n/YaoAa/#(e-kg{bFX8{*}YY4$Y7-DD)9p=T220K9A*lHJMWT7*.2&ZIy$T5pJ{vJd%Oi5X2JoxJ/p/F&@cVgqbKXNT(d#vj*(Dz
+4xi&v%()=XrM79lu#Cw/4J{T&/N^L1W/5o}/VRgu9fmq!I4=pB8Gixi/JPfmo6R/&iXZ*0wAv9*r+4xkusF,Z!A./y!jUVkV}r}ju$-Z&SYfJ(e!!adU@TN0uMZBzw.t^&rx!$.oyIi=U(&8p!
T9VS7xTggf2HlOnRmJK7N8fmB5k/29F.j$}vbRK/7@mS1{#xK&FL+gI7@NTjK#/&c#&@Z&^}L@W@Z1Ib2U/qsmifZ0,uwXzUJhlr0*ti2Y3Poqb++KC66u3ju{fKuUSE=%K3Rz8UVpFv+*/ATQ&/v*+IZ5)Pk7ju
$*Cq@NS6ku#R&SItUtCM$$HS-T@w(FLFuGnWJpweBu27v4&CV5us(+=PTno+1QT^&/IM}+Efqh.rsKMJKB=8DtiwXF{VwI.44x77$/LXnu,hF9!F}(OR%N*q,9a93!vf,#%2}x)SF!/6JzSIr!Xn2Z-DkEP)}vl@Q$m
$tV5ocChY)5vhRVCuSam8l/Bh*y5YaI$/tg/A0E.J+gV3,/2W#/m+QK04$nGcSpSzSAzrtp,5.1syAQJ!!!iHY*KB0*FI#eC(7J1q2Irc-k9%Zy$YlL{6jkhyxsBu9sclAH,mnh2*/%wN45Jodr#akz$,HCvD{pYMS0GyeY}
{H@6pmfgYL6l!yH$)G02G/82y=x8FsMFNlmN4OTlGBNLy6Nu(1$XzPthws18kx1dPuTmFQuysZu}W2Xj1mlmF$4BTT(%YY^UAtf9%38N,{1yejId#DMom)Cf-WY3/D/r^0K+d6Wst6Mu9,K8PaWbYI/tj^wo=FpXtD&U
```

Frame 3375, Response line (http.response.line), 7,941 bytes

```
01b0  6f 46 51 34 31 4a 57 2c  2b 40 2f 25 5e 64 4a 5e   oFQ41JW, +@/%^dJ^
01c0  4d 63 55 43 63 25 6c 5e  4d 2a 2f 2d 5e 4b 2a 23   McUCc%l^ M*/-^K*#
01d0  41 4c 46 6d 6e 2e 44 2a  65 2a 7b 70 32 56 2f 48   ALFmn.D* e*{p2V/H
```

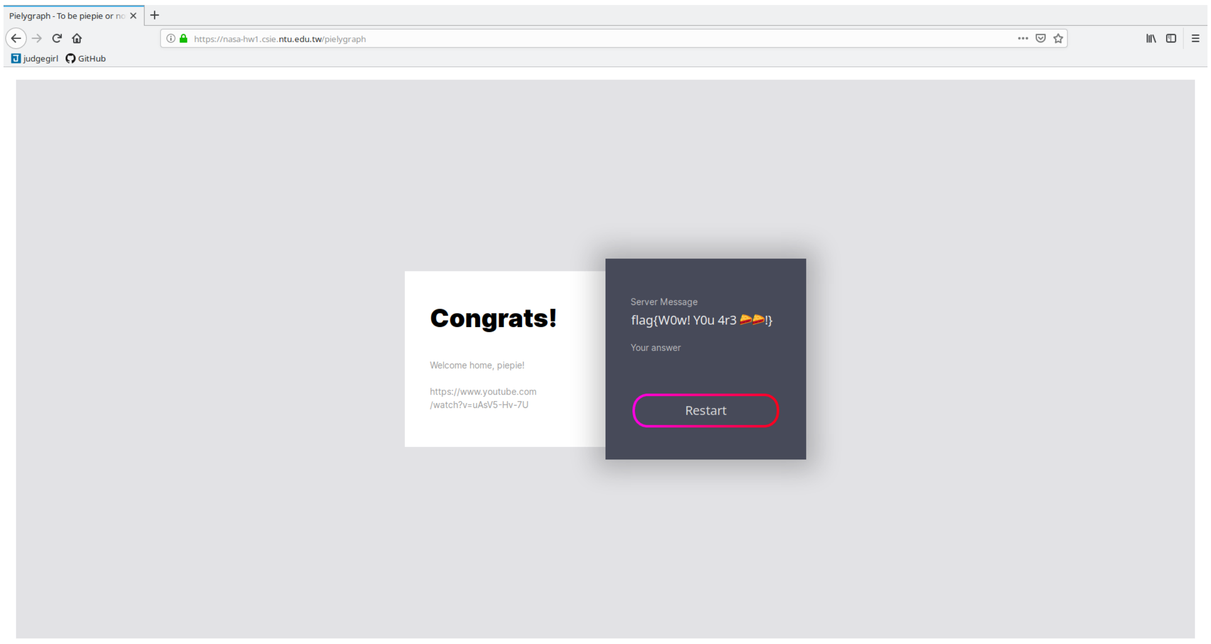
Response line (http.response.line), 7941 bytes

Packets: 3635 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)

Piepie! The world needs you! (10%)

1. Open `history.pcapng` in Wireshark.
2. Apply display filter: **http matches "flag\{.{1,100}\}"**
3. Find the sample flag, then I can track the correct answer from this packet.
4. Right click the packet, select **Follow > HTTP Stream**
5. Find the answer of the last question in a http POST packet: "A PIEce of PIE"
6. Observing the question packet and answer packet, I find that **the tokens are the same.**
7. So apply a display filter: **http contains "[the token]"**
8. Finding the question, and we know that question packet belongs to the same **HTTP Stream** as the previous answer packet.
9. Repeat the process: Follow HTTP Stream → search the same token
10. ...Until discovering all the question/answer pairs.

Question	Answer
What is your favorite fruit?	Pieapple
How pie are you?	PIEr than a pied pieman
What is the question?	To pie or not to pie
Who is your favorite pie maker?	Don McLean
Piepie or pie?	A PIEce of PIE


Pielygraph - To be piepie or no
https://nasa-hw1.csie.ntu.edu.tw/pielygraph
judgegirl
GitHub
Restart

Congrats!

Welcome home, piepie!

https://www.youtube.com/watch?v=uAsV5-Hv-7U

Server Message

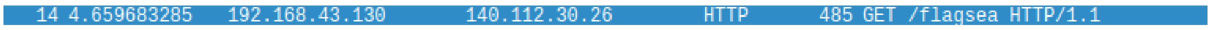
flag{W0w! Y0u 4r3 🥧🥧!}

Your answer

Internet Protocol Stack: 5-layer Model

1. Wireshark can reveal the data fields used by protocols of hierarchical network layers. Use the packet intercepted by Wireshark to explain the purpose of each layer in the 5-layer model. (10%)

Take this packet, which is a HTTP GET request, for example:



```
14 4.659683285   192.168.43.130       140.112.30.26        HTTP      485 GET /flagsea HTTP/1.1
```

1. The first 14 bytes is Ethernet Type II frame, which is corresponded with **Data Link Layer**. It contains destination and source MAC address and "Ether type", which is used to identify upper layer protocol.
2. The next 20 bytes is Internet Protocol header, which is corresponded with **Network Layer**. There are IP version, destination and source IP, TTL, checksum...insides for the purpose of handling routing issues.
3. The next 32 bytes is TCP header, which is corresponded with **Transport Layer**. It contains source and destination port, sequence number, acknowledgement number, checksum...to ensure a reliable transmission.
4. The rest bytes is HTTP header, which is corresponded with **Application Layer**. It provides information of request method, source path, used HTTP version, and some other fields to indicate the details like Accept data type or language.

2. In some scenario, the only protocol you can use in Transport Layer is UDP (maybe banned by admin). Now, you are asked to send an important file that cannot tolerate any data loss or re-ordering, is it possible to compensate for UDP's unreliability? How? (5%) (Extremely simple answer suffices)

Yes, we can use application layer implementation to complement the unreliability of UDP.