**HW01**

0516208-黃郁恬

1.

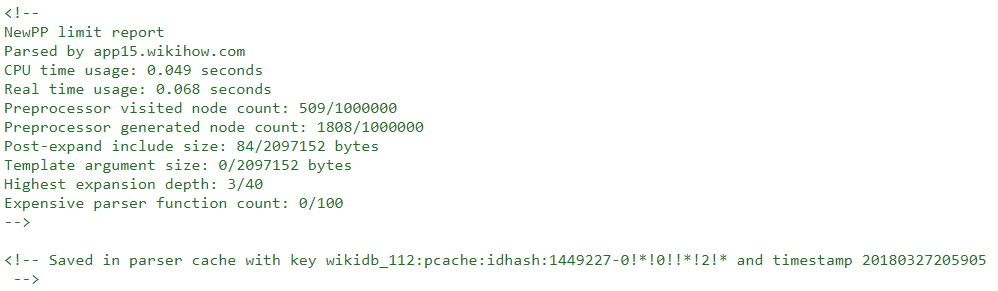
**(1)**

**cmd:**

**wget -m -np -p -P ./wget\_folder https://www.wikihow.com/Get-Slim-Naturally**

**target website:** [**https://www.wikihow.com/Get-Slim-Naturally**](https://www.wikihow.com/Get-Slim-Naturally)

**screen dumps:**

****







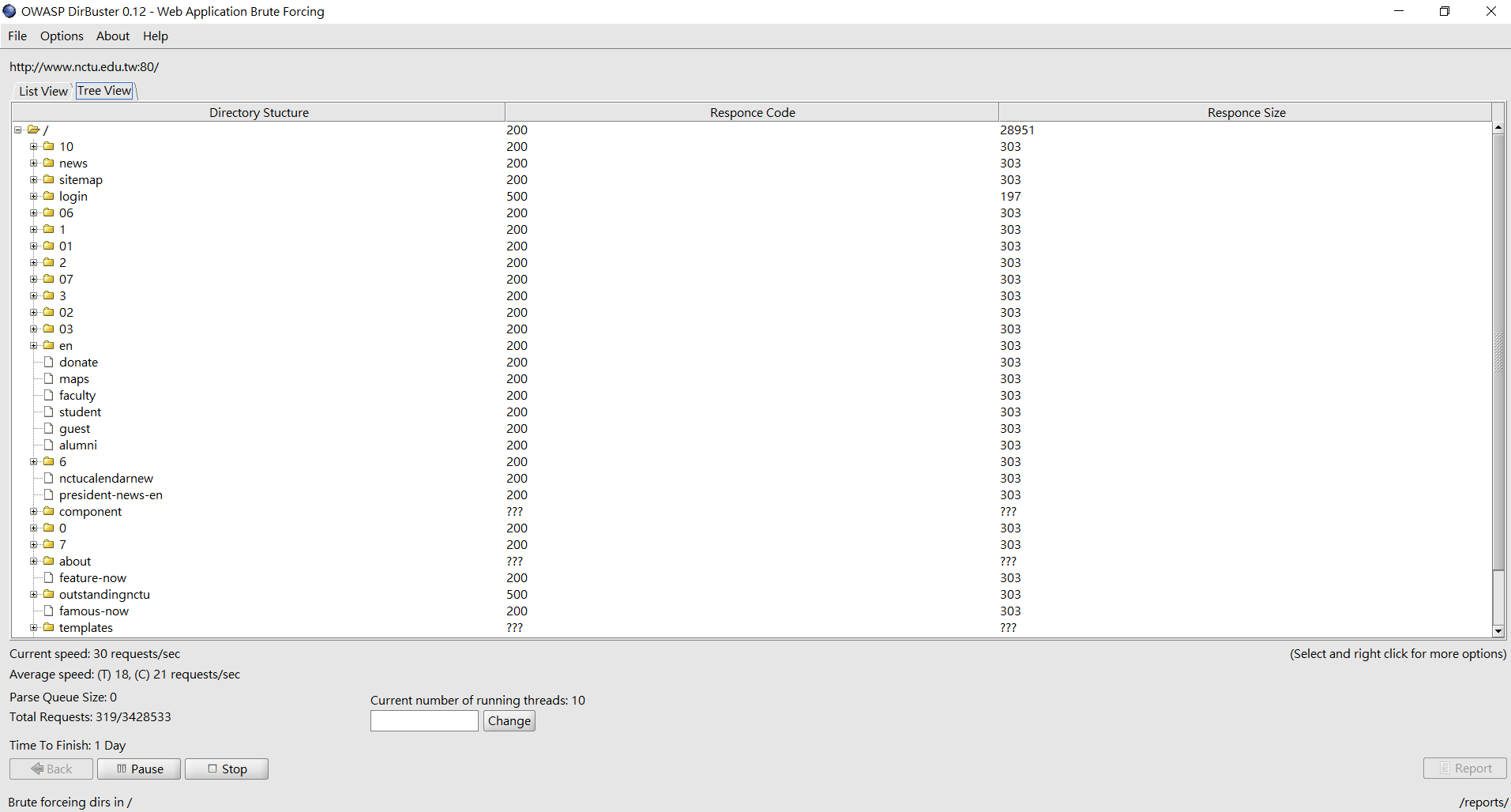


**Explanation of comment tags:**

**use keys(wikidb\_112) to get data(minify-css: removing redundant content)**

**(2)**

**target website:** [**https://www.facebook.com**](https://www.facebook.com)

****

2.

The speaker reduce the entropy from 160 bits(including: IP address-32 bits; epoch-32 bits; microseconds-32bits; random lcg\_value()-64 bits) to only 20 bits(microseconds: 32 bits -> 20 bits, IP address: 32 bits -> 0 bits (by chatting with the social networking sites), epoch: 32 bits -> 0 bits (the moment the user login), random lcg\_value(): 64 bits -> 0 bits). After that, he used “NAT Pinning” to confuse the router on protocol-level, then he used some skills such as html5-anti-waf xss and geolocation via xss and the results to find someone’s girlfriend!!!

3.

**Name: Lily Collins(Lily Jane Collins)**

**Wikipedia:** [**https://en.wikipedia.org/wiki/Lily\_Collins**](https://en.wikipedia.org/wiki/Lily_Collins)

* **Information: name, job, relatives, age, birthday, citizenship**

****

**FB:** [**https://www.facebook.com/OfficialLilyCollins/**](https://www.facebook.com/OfficialLilyCollins/)

* **Information: her thoughts, her daily life**

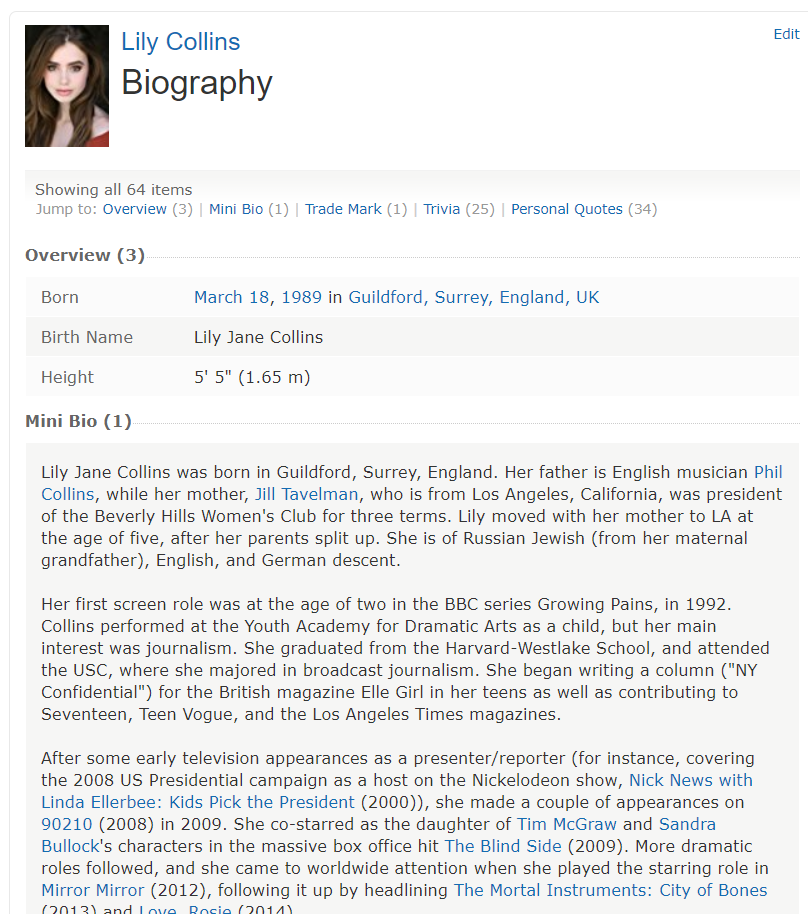
****

****

**IMDB:**

[**http://www.imdb.com/name/nm2934314/bio**](http://www.imdb.com/name/nm2934314/bio)

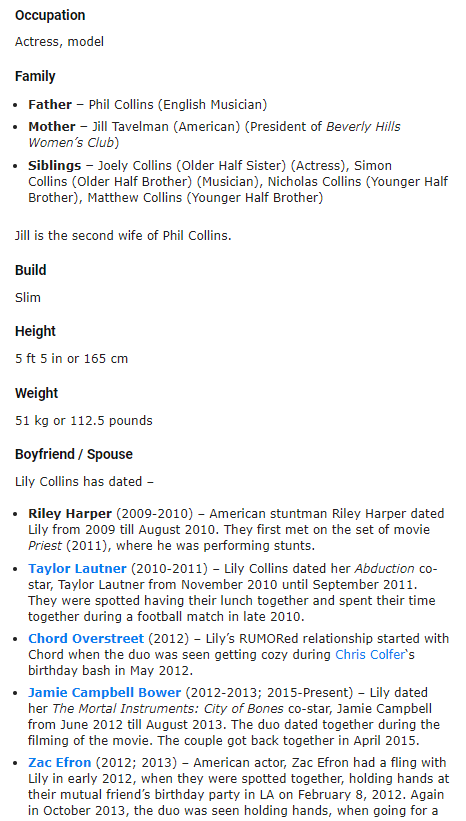
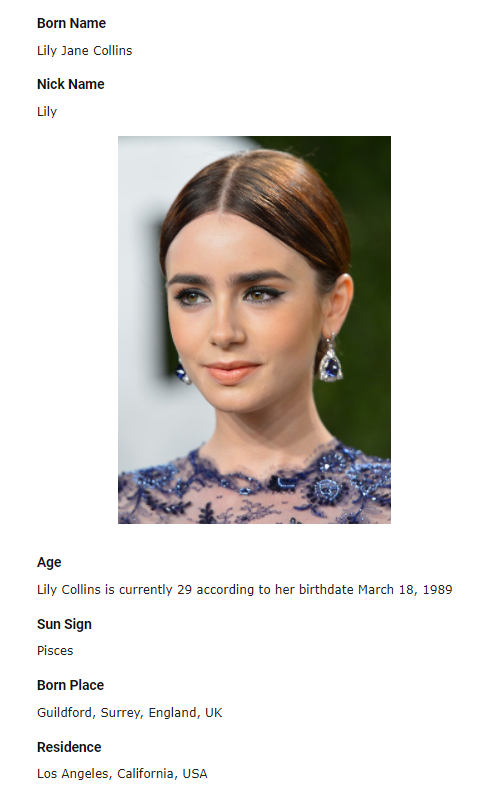
* **Information: works(movie, tv series: characters she played), birth name, birthday, height, mini-biography**

****

**HealthyCeleb:**

[**https://healthyceleb.com/lily-collins-height-weight-body-statistics/13175**](https://healthyceleb.com/lily-collins-height-weight-body-statistics/13175)

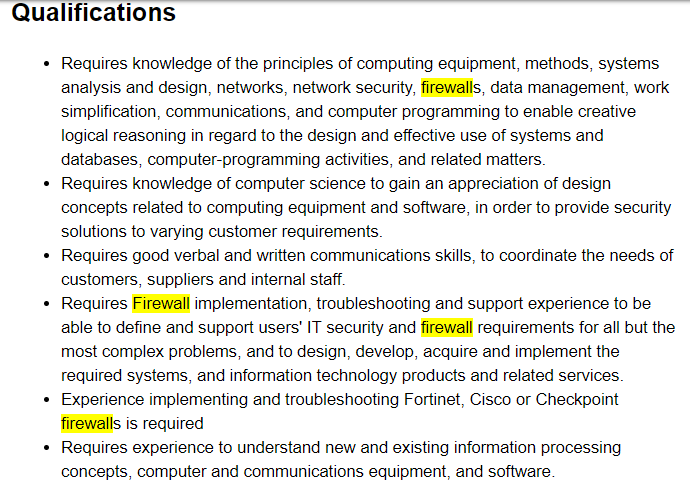
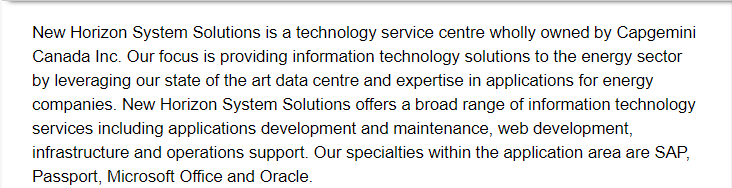
* **Information: nick name, age, family, job, birth place, height, weight, exboyfriends/boyfriend, etc.**

****

4.

Resume firewall:

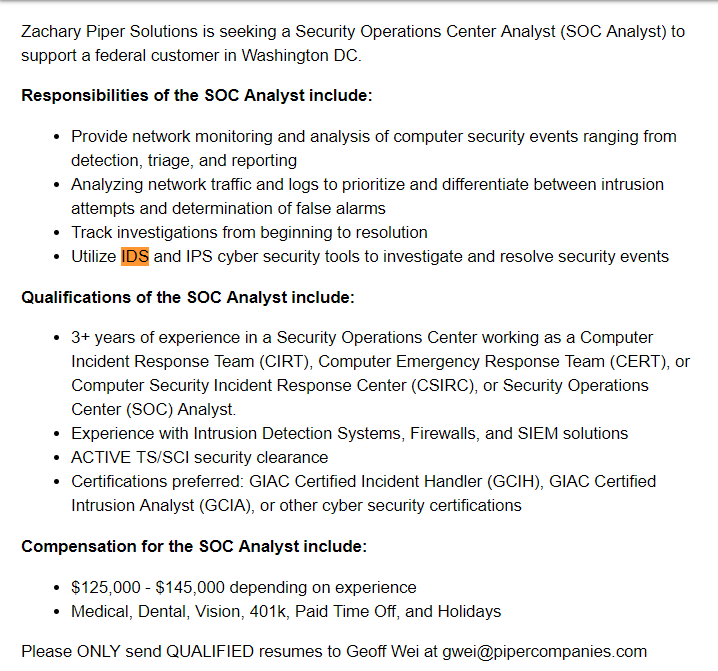
* Company Description:

****

* **Capgemini Canada Inc. is looking for someone who knows networks security and firewall well, and also has the experience of using troubleshooting Fortinet,**

**Cisco, or Checkpoint firewall.**

Resume Intrusion Detection:



* **Zachary Piper Solutions is looking for someone who has experience of ids and get some relating certifications.**

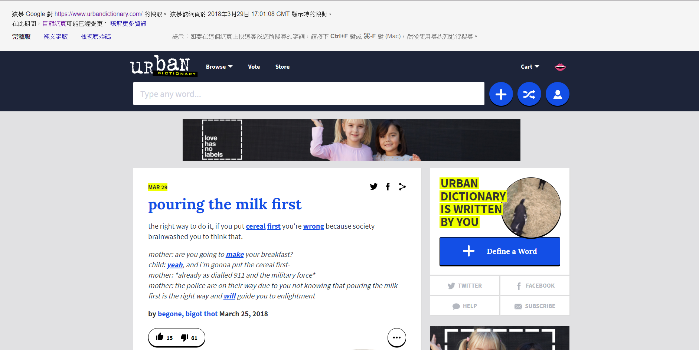
5.

Target website: <https://www.urbandictionary.com/>

* Archive.org(2018/03/28)



* Google Cache(2018/03/29)



* Current(2018/03/30)



* Difference:

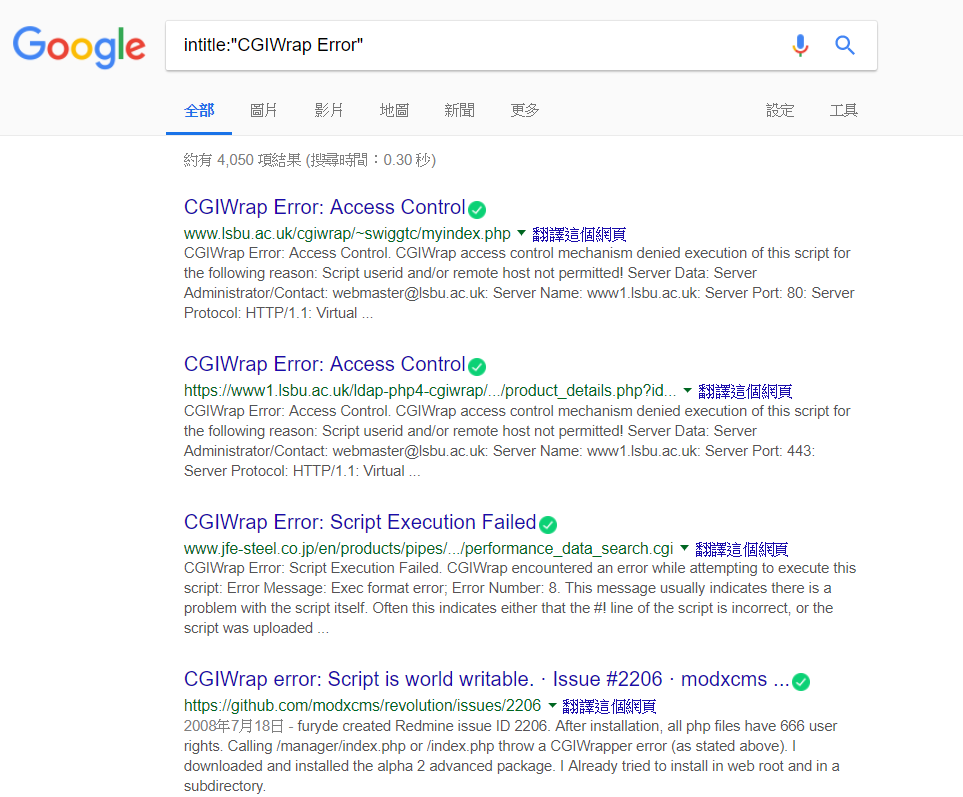
There is no much difference from archive.org, google cache, and the current website, cause the time is quite close.

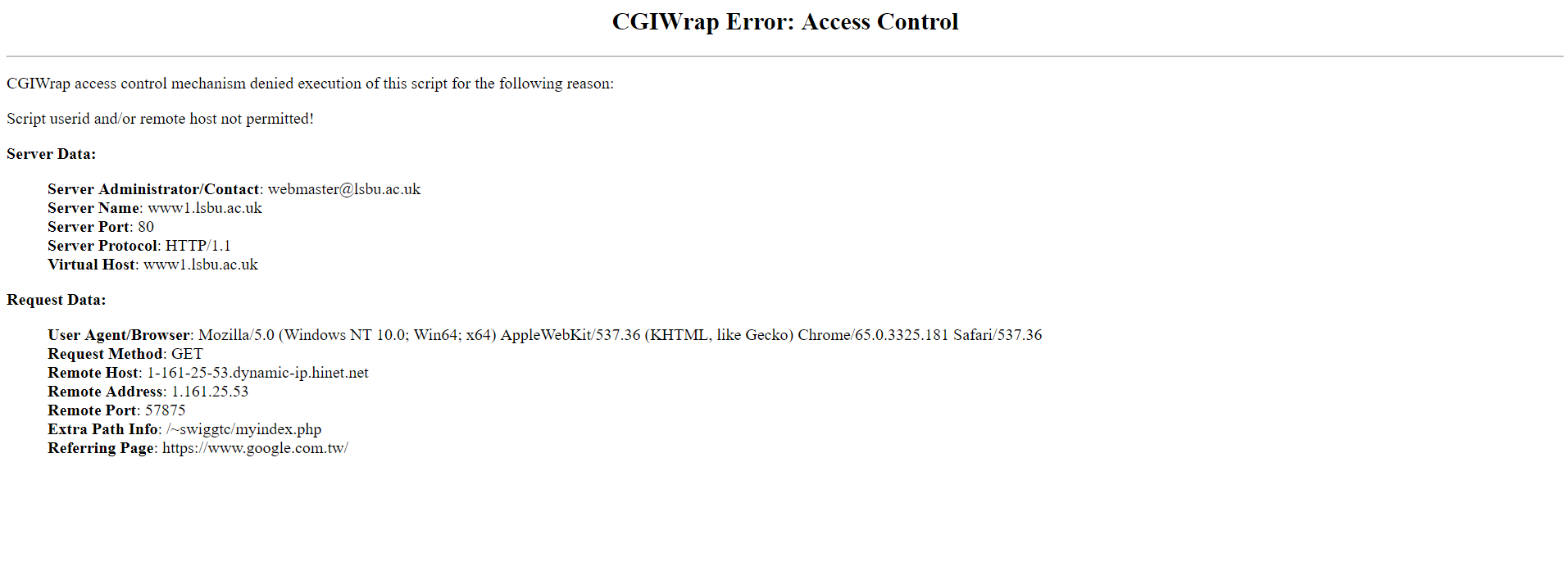
The tiny difference lies in advertisement and the pattern which changes every time you enter this website.

6.

Search:

Intitle:“CGIWrap Error”

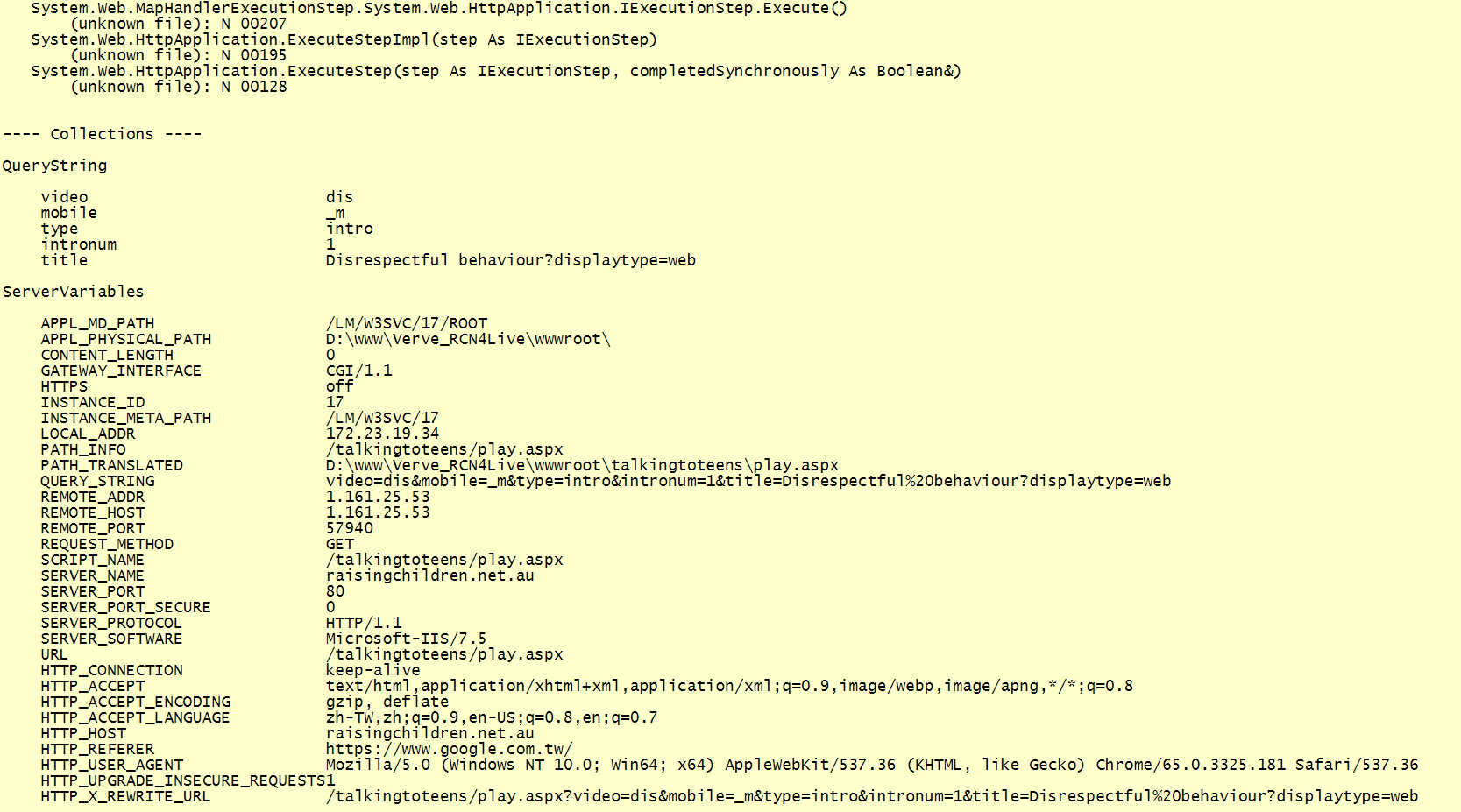
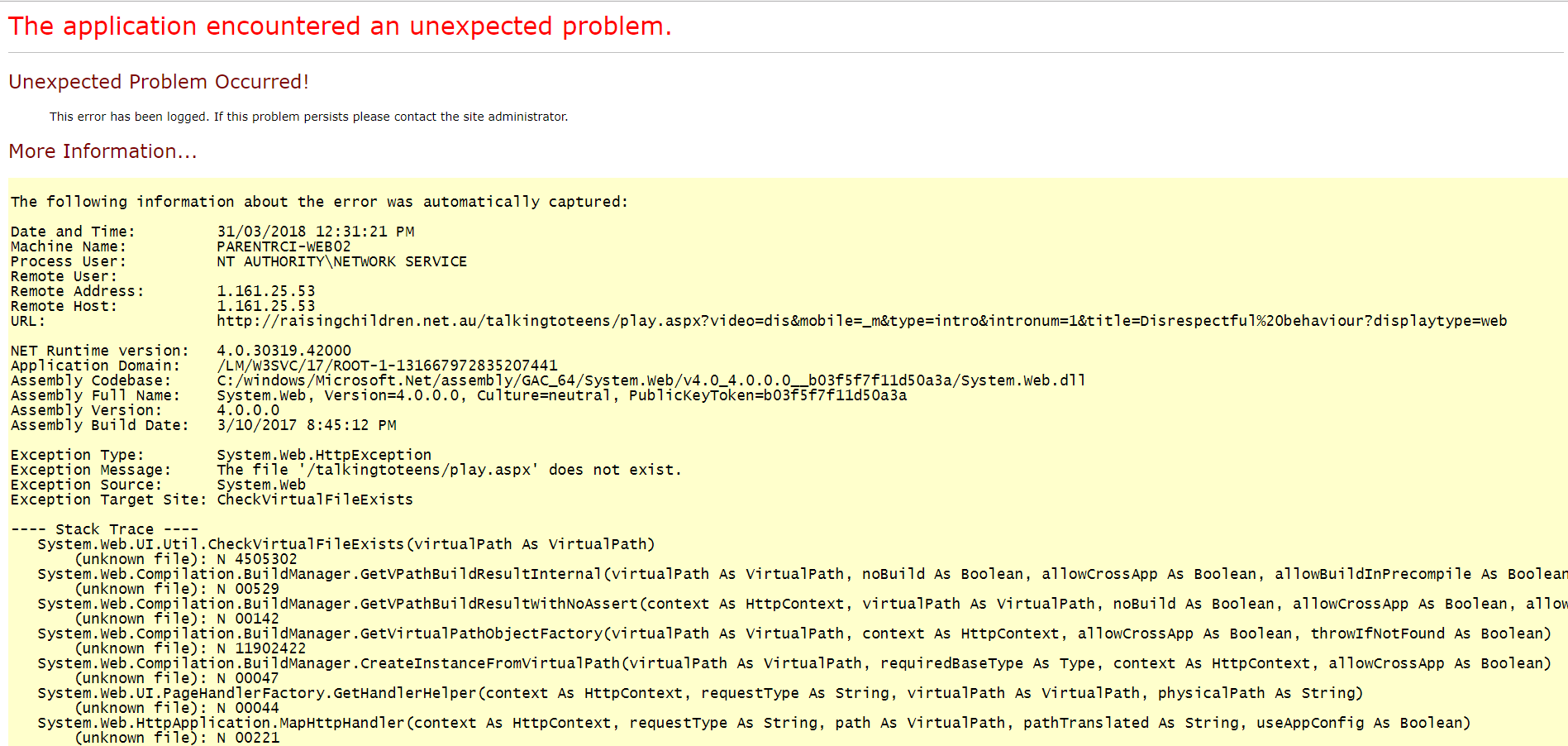
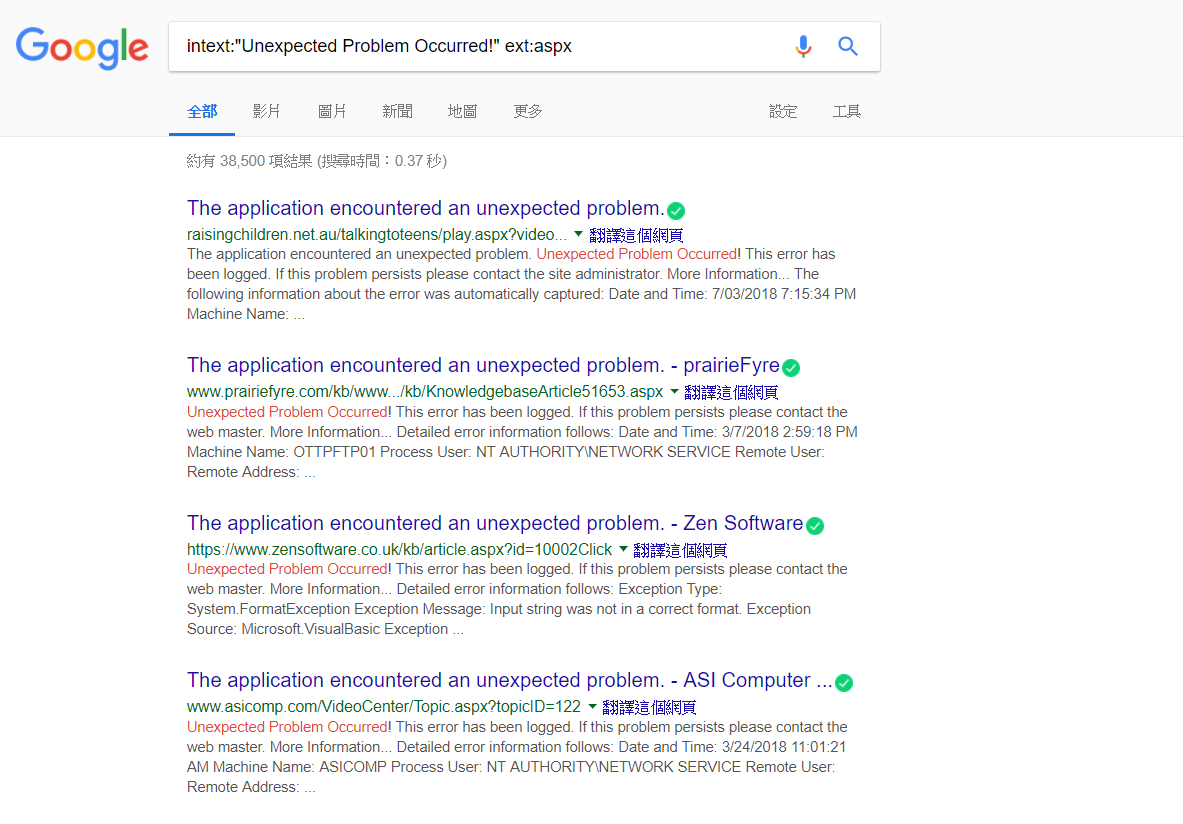




* **The reason why the error “CGIWrap Error” occurs – Access Control**

Search:

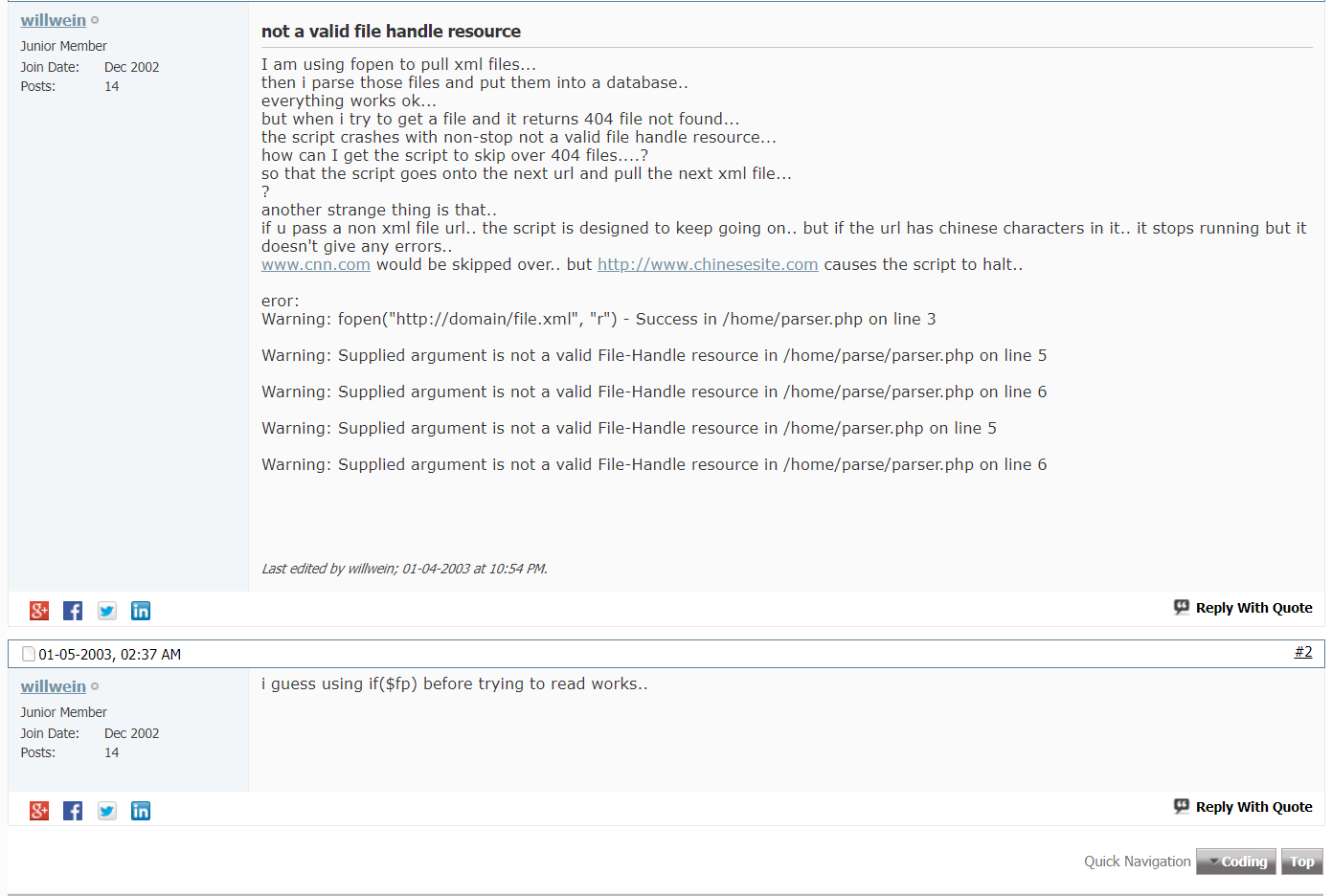
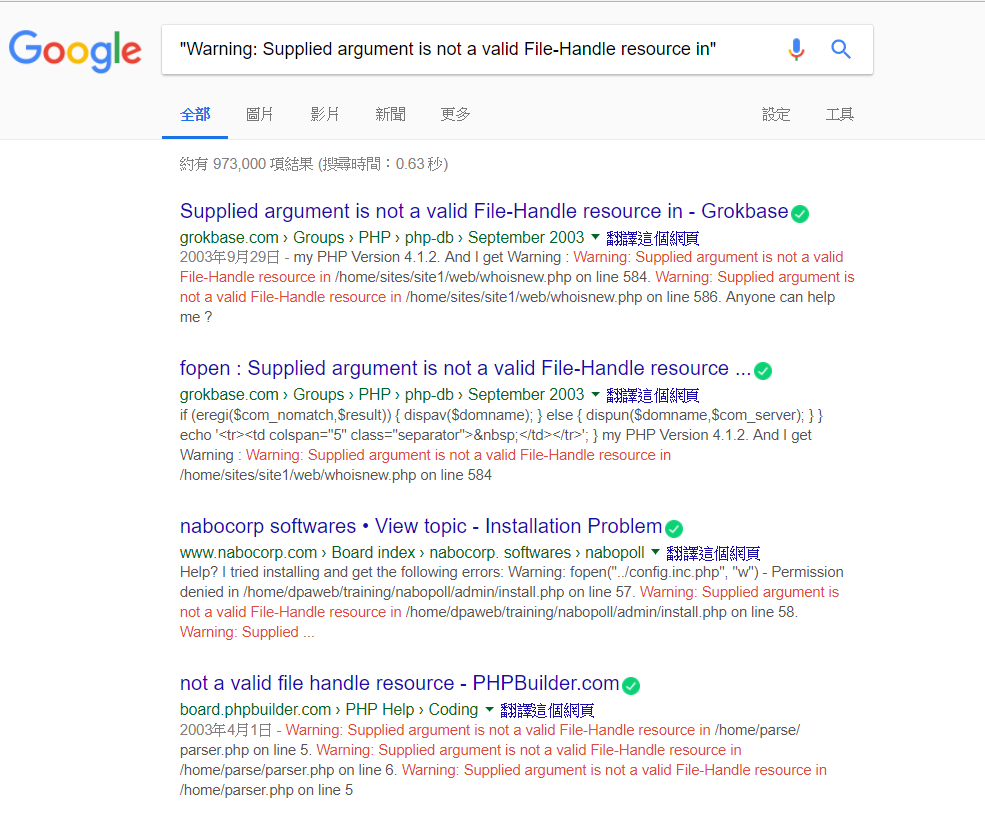
Intext:“Unexpected Problem Occurred!” ext:aspx



* **Detailed information about the “unexpected problem” that the “application” encountered**

Search:

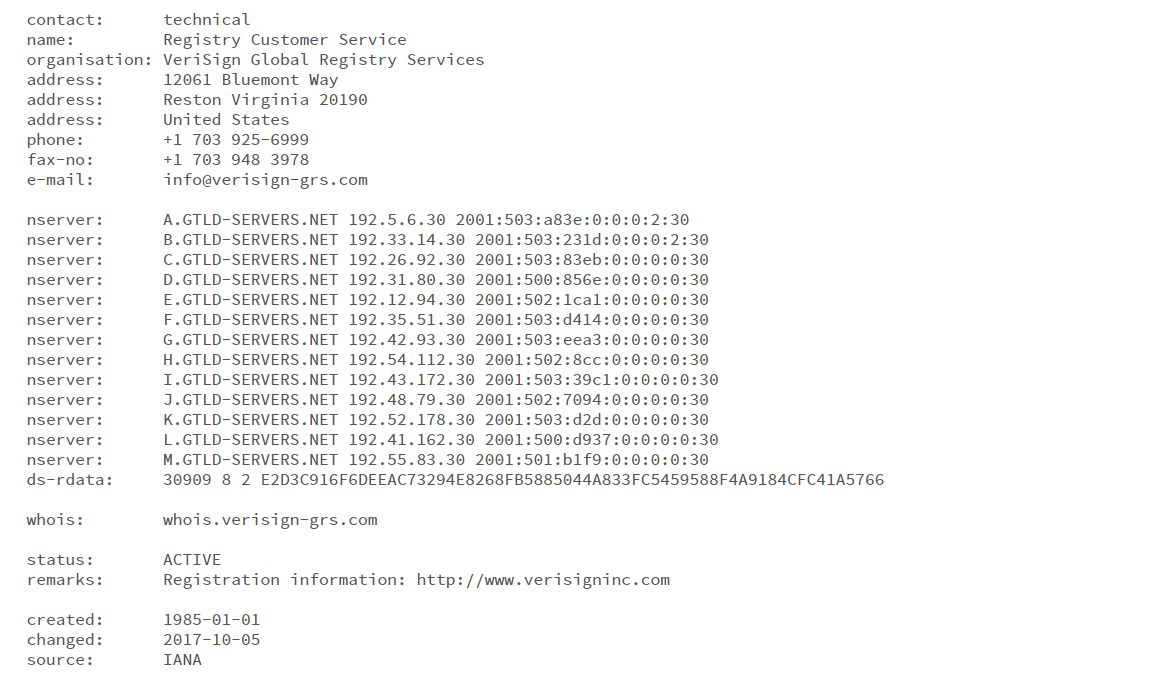
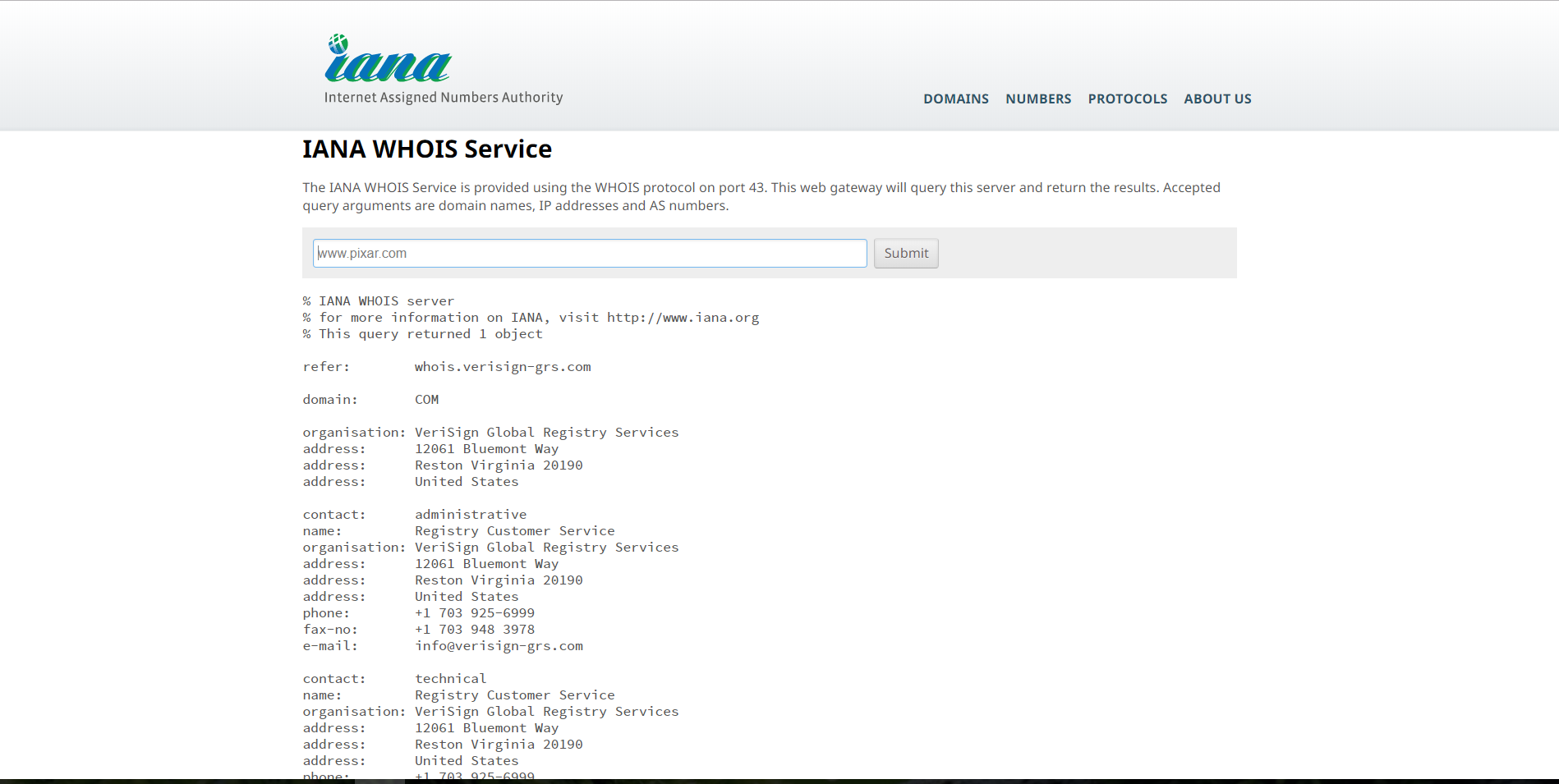
“Warning: Supplied argument is not a valid File-Handle resource in”



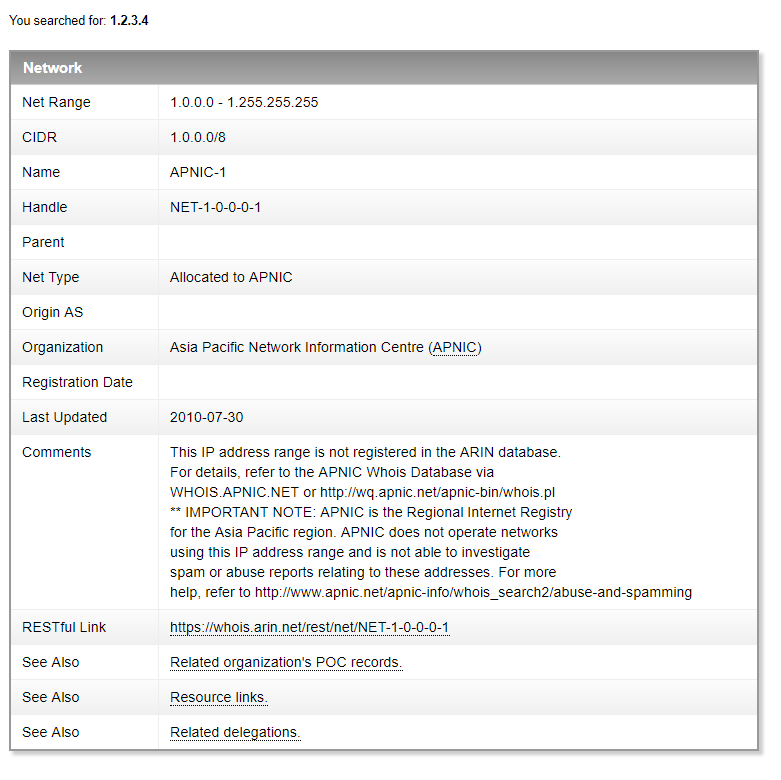
* **The problem “Supplied argument is not a valid File-Handle resource” of “fopen” one encountered and the solutions.**

7.

* whois.iana.org – [www.pixar.com](http://www.pixar.com)



* **Registry(註冊處): verisign-grs**
* **Registrar(註冊商): verisigninc.com**
* **Registrant(註冊人): Registry customer service**
* arin.net – 1.2.3.4



* **1.2.3.4 is Asia Pacific Network Information Centre**

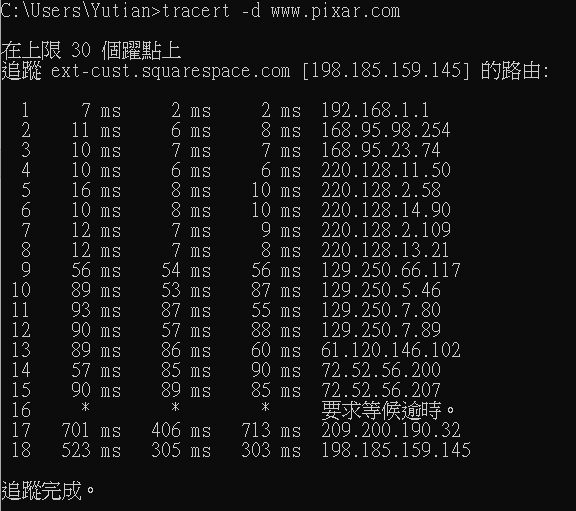
8.

****

* **PIXAR has four IP addresses for the balance loading**

9.

Use “tracert”:



* **Use 18 steps to arrive the destination IP address (198.185.159.145).**
* **At the 16th step, it wait more than the default waiting time (4s), so it didn’t show on the screen!**