

TOR 위협분석

김민영

minyoungk@outlook.com





1. About Tor

- TOR 소개
- Hidden Service
- TBB

2. Practical one

- Location Leaks
- 관련 도구들
- 익명성 실패 사례



Design Concepts

▪ Low Latency Anonymity

- 1981 Mix-Net Design : 근래 익명네트워크 구조의 시초. Chain of node 구조

▪ 전제 사항

- Not P2P : 공격자들의 다수 서버장악 우려
- End-to-end 공격에 취약 : 디자인 특성
- No Protocol normalization : TCP 에서'만' 동작
- Not steganographic : TOR에 연결되어 있는 것을 숨겨주지는 않음

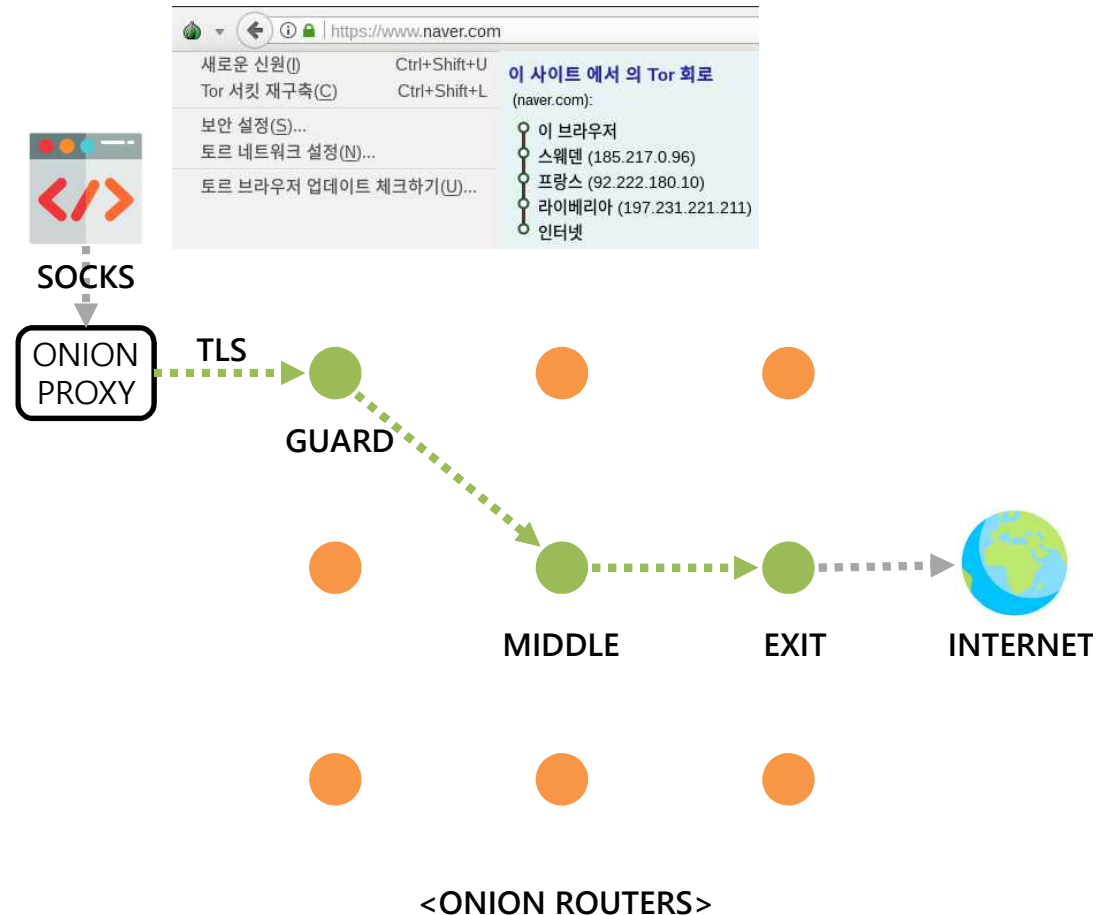
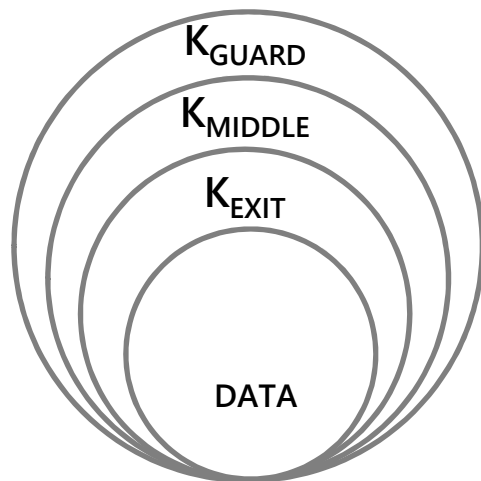
▪ 디자인 목표

- Deployability : Must be deployed and used in the real world.
- Usability : 다수가 있을 때 개인을 숨기기 쉬우므로 편리성 뿐만 아니라 보안성과 직결
- Flexibility : Flexible & well-specified. 향후 발전을 위한 테스트베드 역할 자처
- Simple Design : 검증되지 않은 추가기능들의 위협 견제



The Onion Router Network

- Onion Router
 - 일반 사용자에게 프로세스에서 동작
 - TLS 연결 관리
- Onion Proxy
 - 디렉토리로부터 토르네트워크 정보 수집
 - 서킷 연결
 - 사용자 프로그램의 접속 관리



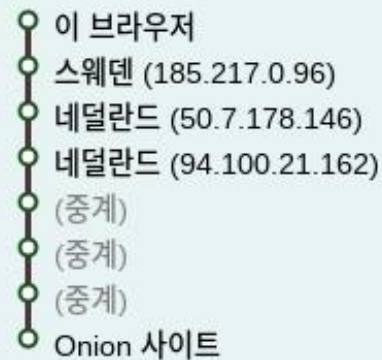


Relay Node 선택

- 동시에 여러 개 창을 띄웠을 때,
 - 동일한 Guard 노드

이 사이트 에서 의 Tor 회로

(highkorea5ou4wcy.onion):



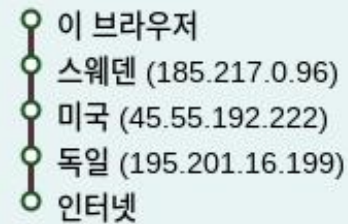
이 사이트 에서 의 Tor 회로

(h2ubt3eodqfpycc.onion):



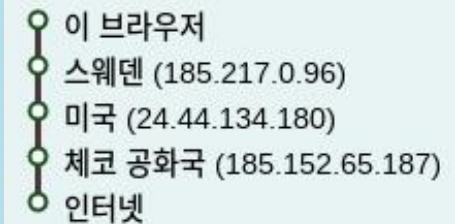
이 사이트 에서 의 Tor 회로

(daum.net):



이 사이트 에서 의 Tor 회로

(naver.com):





- Hidden Service
 - Responder anonymity : 서버의 익명성 제공
 - Client Authentication (Not yet implemented, 0.3.2.1-alpha)
 - Onion Address
 - ✓ Base 32 encoding
 - ✓ 옛날버전 : Master Identity Key의 public key.
 - ✓ 예전 : 16자, 현재 : 56자
- HS Descriptor
 - Hidden Service Directory에 업로드됨
 - 현재 Introduction Point들의 위치와 HS 컨택트 방법 등 포함
- Directory Authorities
 - DA 들은 정기적으로 합의된 RV 값을 생성함
 - 이 값들은 HS의 공개키와 합체되어 Descriptor가 저장될 HSDir의 위치를 결정함
- 설치 방법
 - TOR 설치 > 로컬 웹서버 설치 > torrc 수정

Add the following lines to your torrc:

```
HiddenServiceDir /Library/Tor/var/lib/tor/hidden_service/  
HiddenServicePort 80 127.0.0.1:8080
```




TBB (Tor Browser Bundle / Tor Bundle Browser)

- 다운로드 : <https://www.torproject.org/download/download-easy.html.en>
- Onion Proxy + Web Browser
- 그 외
 - <https://www.torproject.org/projects/projects.html.en>



Orbot
Tor on Android



Stem
Python Libs



Tails
Live CD/USB Distribution

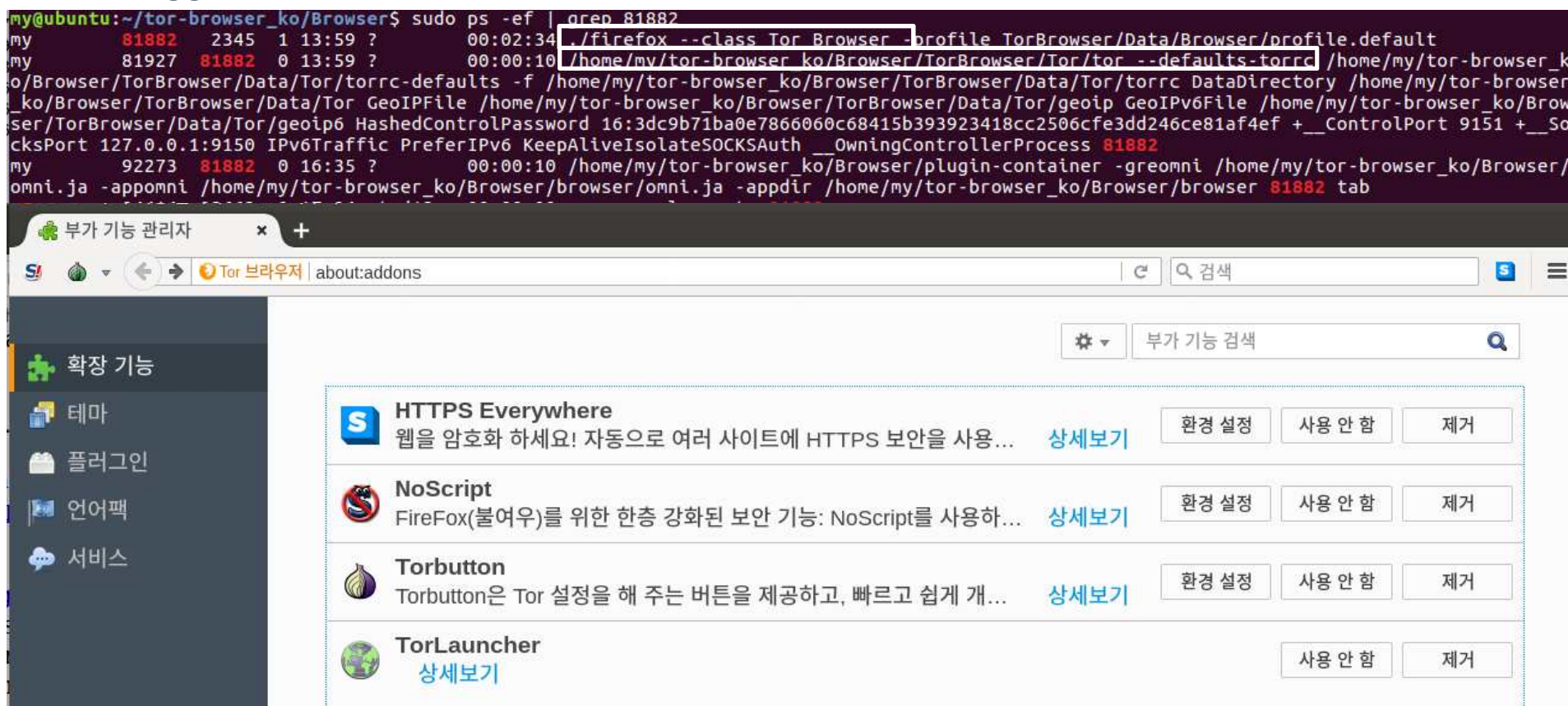


TorBirdy
Torbutton
for Thunderbird



TBB (Tor Bundle Browser)

- Based on Mozilla's Extended Support Release (ESR) Firefox branch
- Tor Launcher addon : Tor 프로세스 관리&설정
- HTTPS-Everywhere : Tor-Exit-Node 모니터링 방지
- Pluggable Transport : IP / 프로토콜 핑거프린트 차단 우회 (별도 패키지)





Tor Browser <> Onion Proxy

tcp.stream eq 2

No.	Time	Source	Destination	Protocol	Length	Info
23	0.681963943	127.0.0.1	127.0.0.1	Socks	485	Unknown
24	0.682026244	127.0.0.1	127.0.0.1	TCP	66	9150 →
33	1.217439310	127.0.0.1	127.0.0.1	Socks	246	Unknown
34	1.217503077	127.0.0.1	127.0.0.1	TCP	66	57008 →
35	1.314855573	127.0.0.1	127.0.0.1	Socks	453	Unknown
36	1.314874996	127.0.0.1	127.0.0.1	TCP	66	9150 →
45	1.848383674	127.0.0.1	127.0.0.1	Socks	246	Unknown
46	1.848409295	127.0.0.1	127.0.0.1	TCP	66	57008 →
47	1.849028683	127.0.0.1	127.0.0.1	Socks	450	Unknown
48	1.849041483	127.0.0.1	127.0.0.1	TCP	66	9150 →
66	2.360305198	127.0.0.1	127.0.0.1	Socks	246	Unknown
67	2.403907224	127.0.0.1	127.0.0.1	TCP	66	57008 →

Frame 24: 66 bytes on wire (528 bits), 66 bytes captured (528 b)
 Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00
 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 Transmission Control Protocol, Src Port: 9150, Dst Port: 57008,
 Source Port: 9150
 Destination Port: 57008
 [Stream index: 2]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Acknowledgment number: 420 (relative ack number)
 1000 = Header Length: 32 bytes (8)
 Flags: 0x010 (ACK)
 Window size value: 392
 [Calculated window size: 392]
 [Window size scaling factor: -1 (unknown)]

Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_lo_20180427163614_MHVB4T

GET / HTTP/1.1
 Host: whois.cymru.com
 User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
 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
 Upgrade-Insecure-Requests: 1
 If-Modified-Since: Wed, 21 Jun 2017 21:33:45 GMT
 If-None-Match: "594ae639-c15"
 Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
 Server: nginx/1.12.2
 Date: Fri, 27 Apr 2018 07:36:24 GMT
 Connection: keep-alive
 Last-Modified: Wed, 21 Jun 2017 21:33:45 GMT
 ETag: "594ae639-c15"

GET /style.css HTTP/1.1
 Host: whois.cymru.com
 User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
 Accept: text/css,*/*;q=0.1
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 Referer: http://whois.cymru.com/
 Connection: keep-alive
 If-Modified-Since: Thu, 08 Jun 2017 19:38:41 GMT
 If-None-Match: "5939a7c1-2eb"
 Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
 Server: nginx/1.12.2
 Date: Fri, 27 Apr 2018 07:36:25 GMT
 Connection: keep-alive
 Last-Modified: Thu, 08 Jun 2017 19:38:41 GMT
 ETag: "5939a7c1-2eb"

GET /images/dragon-big.gif HTTP/1.1
 Host: whois.cymru.com

```

graph TD
    TB[Tor Browser] -- SOCKS --> OP[ONION PROXY]
    OP -. TLS .-> G((GUARD))
    
```




Onion Proxy <> Onion Router

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
20	5.781869413	192.168.249.157	185.217.0.96	TCP	74	56646 → 9999
22	6.125153034	185.217.0.96	192.168.249.157	TCP	74	9999 → 56646
23	6.125234697	192.168.249.157	185.217.0.96	TCP	66	56646 → 9999
24	6.126200922	192.168.249.157	185.217.0.96	TLSv1.2	252	Client Hello
25	6.469243354	185.217.0.96	192.168.249.157	TCP	66	9999 → 56646
26	6.472799843	185.217.0.96	192.168.249.157	TLSv1.2	1087	Server Hello
27	6.472837255	192.168.249.157	185.217.0.96	TCP	66	56646 → 9999
28	6.474562533	192.168.249.157	185.217.0.96	TLSv1.2	192	Client Key Exchange
29	6.818652753	185.217.0.96	192.168.249.157	TLSv1.2	117	Change Cipher
31	6.819020633	192.168.249.157	185.217.0.96	TLSv1.2	106	Application Data
33	7.164398106	185.217.0.96	192.168.249.157	TLSv1.2	2149	Application Data
34	7.164445274	192.168.249.157	185.217.0.96	TCP	66	56646 → 9999
35	7.166238182	192.168.249.157	185.217.0.96	TLSv1.2	1637	Application Data
36	7.513688352	185.217.0.96	192.168.249.157	TCP	66	9999 → 56646
37	7.513835971	185.217.0.96	192.168.249.157	TLSv1.2	1123	Application Data
38	7.515209246	192.168.249.157	185.217.0.96	TLSv1.2	1123	Application Data
39	7.897742683	185.217.0.96	192.168.249.157	TCP	66	9999 → 56646
40	7.897786316	192.168.249.157	185.217.0.96	TLSv1.2	609	Application Data
41	7.934885108	185.217.0.96	192.168.249.157	TLSv1.2	609	Application Data
42	7.976648030	192.168.249.157	185.217.0.96	TCP	66	56646 → 9999
44	8.240763189	185.217.0.96	192.168.249.157	TCP	66	9999 → 56646

▼ RelativeDistinguishedName item (id-at-commonName=www.zca5jglxlqhb...
 Id: 2.5.4.3 (id-at-commonName)
 ▼ DirectoryString: printableString (1)
 printableString: www.zca5jglxlqhb...
 ▶ subjectPublicKeyInfo
 ▶ algorithmIdentifier (sha256WithRSAEncryption)
 Padding: 0
 encrypted: 78739c6f45c505eb6b2a931cf25d0364f873659b1a80754c...

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 333
 ▼ Handshake Protocol: Server Key Exchange
 Handshake Type: Server Key Exchange (12)
 Length: 329
 ▶ EC Diffie-Hellman Server Params

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 4
 ▼ Handshake Protocol: Server Hello Done
 Handshake Type: Server Hello Done (14)

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_ens33_20180428

```

.....D}T...../KY..26..(...0.....+./.,.0.
.....3.9./5.
.....1.....www.t6mmuy.com.....
.....
.....
.....
.....#...
.....>.....Z....Ip.
.....8..p.*Syb..e..J.....Y..
0.....Z...V..S..P0..L0.....:s=..60
.....*..H..
.....0&1$0"..U....www.6ejlg4n4ojck5u7xojk.com0..
180313000000Z.
181115235959Z0&1$0"..U....www.zca5jglxlqhb...net0.."0
.....*..H..
.....0..
.....?d...T...L"...8...9G.e1...y....m.x....S..S3...l..jk..0
..4u..I..!.....p..zq...L.....A.....-&
1P.G.V..D...hh.....9..xt.....)7.t@.L.H....a....
5...F.N.....j...&pSy...;K..w...r..5g..F..g.p2\...T...
%.o.....%k'7..L.
..WT..wS.....0
.....*..H..
.....xs.oE...k*...].d.se...uL..d...K.b-...<.....6...n.b.
.Xm&..m...gY=.7..BL.3xIu...3.D.sZV\...3W57...j....7....
+.....d...x.s...M...I...A...!..B...8.Ffw..CV*,
4U@..h..z....DJ.Sj..U.o..f..L.....hS.....7lS=...f.[
{=3.5..6.....
3.....|.'.0..l....aN..u..}z".0.}
H....(q....L&nH.g.lY,..`cv.@.}.k...D
@...z....1..8.....9....e.....cv$
8.3$H[...;.....v.....U.....zh...|.G.
..]
..u..@.....'.z.sn...j3.N.....F..FA>d
6...p...g...W...iz.....3.ok 1T
(...Y..v`g.[.9....[.h..4.....
+M..*.:Dwj1ay
Uj...!1....
      
```

SOCKS
ONION PROXY
GUARD

24 client pkts, 31 server pkts, 35 turns.
 Entire conversation (37 kB) Show and save data as ASCII Stream



- 웹페이지 검색 정보
 - IP / URL / 도메인
 - 이메일 / SNS 계정
 - Google Analytics / Adsense ID
 - 가상화폐 지갑 주소
 - 페이지 타이틀
- TOR private_key
- SSL 인증서
 - Common Name, SAN, hash(fingerprint), Public Key
- 다른 프로토콜들
 - SSH public key fingerprint
 - SMTP welcome message
- EXIF 이미지/동영상 메타데이터
 - Wordpress /wp-content/uploads 폴더
- Apache mod_status, .htaccess ...
- PHPmyadmin
- 기존 웹과 비교
 - 새로 등장한 위협
 - 일반 웹에서는 위협이 아님
 - 기존에 존재하던 위협



Feat. OSINT

[Contact us](#) [Prices](#) [Data removal](#)

Acc. type: "Guest" Requests: / User: Pass:

SameID.net

Acceptable ID types: Analytics, Adsense, Amazon affiliate/product, Clickbank affiliate/product, Addthis

SameID.net is not available now. Visit it later please.



https://opendata.rapid7.com/sonar.ssl/

Python Elasticsearch ... Kibana OnionScan Correlatio... Bitcoin Block Explore... PortSwigger Web Sec... Search APIs | Elastics... Elasticsearch Cheat S...

Download Now (No Account Required)

See below for datasets updated on the first of every month—no sign up required.

File Name	SHA1-Fingerprint	Size	Updated At
20180522/2018-05-22-1526950801-https_get_443_names.gz	9a9a2ed1f5b7a2a7c114aa977f093232c06c4e01	34.4 MB	May 24, 2018
20180522/2018-05-22-1526950801-https_get_443_hosts.gz	9a9a2ed1f5b7a2a7c114aa977f093232c06c4e01	1.1 GB	May 24, 2018
20180522/2018-05-22-1526950801-https_get_443_endpoints.gz	9a9a2ed1f5b7a2a7c114aa977f093232c06c4e01	1.2 GB	May 24, 2018
20180522/2018-05-22-1526950801-https_get_443_certs.gz	9a9a2ed1f5b7a2a7c114aa977f093232c06c4e01	874.3 MB	May 24, 2018





Crawler

- ACHE - Project of DARPA memex

- ES 버전 설정 : target/repository/ElasticSearchTargetRepository.java

```
String pageProperties = ( esVersion.startsWith("5.") | esVersion.startsWith("6.") ) ? pageMapping5x : targetMapping1x;
```

- 설정파일

```
# ElasticSearch

target_storage.data_formats:
- FILES
- ELASTICSEARCH

target_storage.data_format.elasticsearch.rest.hosts:
- http://127.0.0.1:9200

target_storage.data_format.elasticsearch.rest.connect_timeout: 30000
target_storage.data_format.elasticsearch.rest.socket_timeout: 30000
target_storage.data_format.elasticsearch.rest.max_retry_timeout_millis: 90000

#target_storage.data_format.type: FILESYSTEM_JSON

crawler_manager.downloader.torproxy: http://127.0.0.1:8118
```

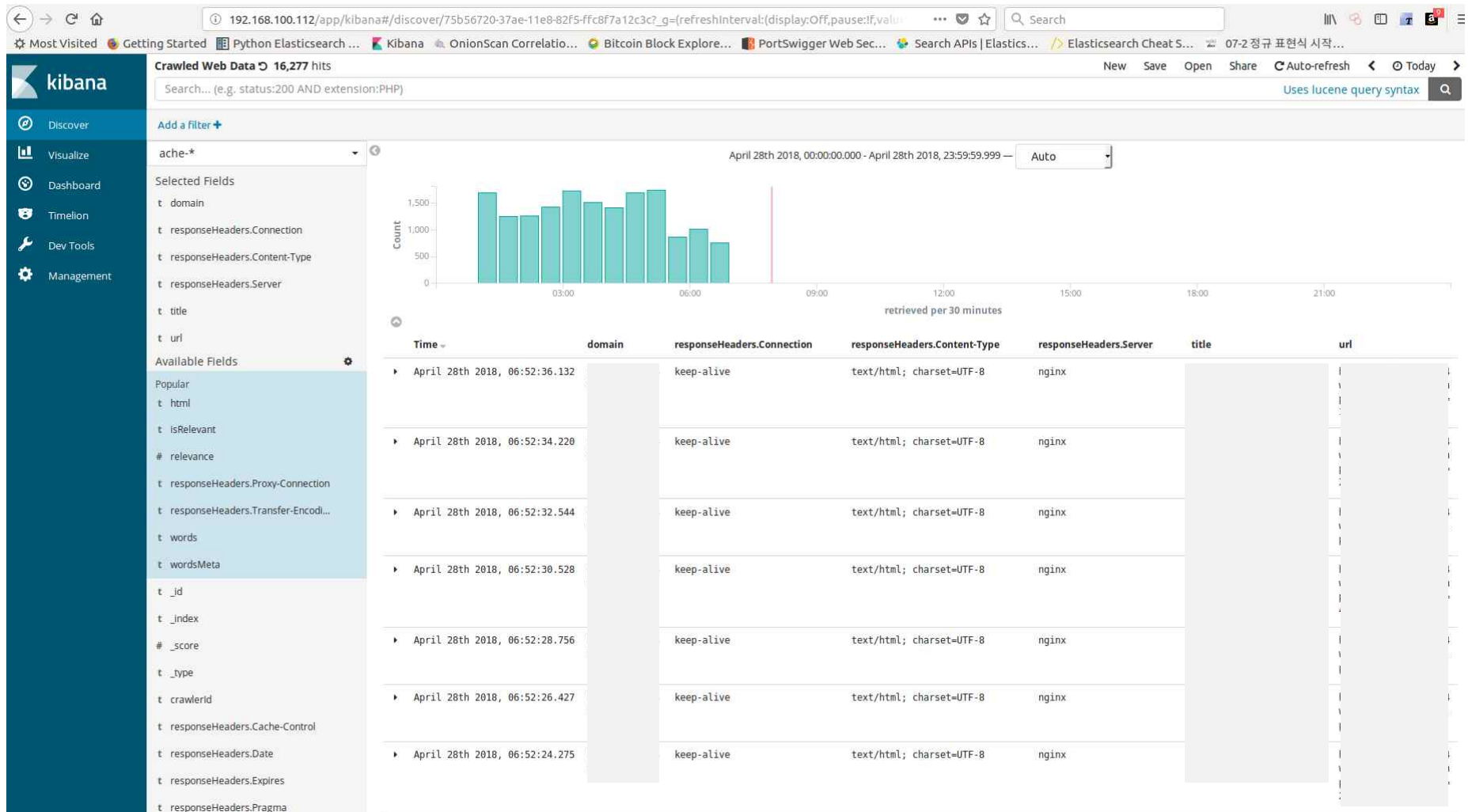
- 실행

```
./build/install/ache/bin/ache startCrawl -c /var/ache/config -o /var/ache -s ${CURDIR}/onion.seeds
-e ache-${day} -cid $day > /var/ache/${day}.log 2>&1
```




Crawler

■ ACHE





Crawler

■ ACHE

```
from elasticsearch import Elasticsearch
import json, re

config = {
    'host': '192.168.100.112',
    'port': 9200
}

es = Elasticsearch([config], timeout = 300)

if not es.indices.exists(index = 'ache-20180418'):
    print ("index ache-20180409 does not exists")
    exit()

squery = '{"query":{"regexp":{"html":"onion"}}}'

page = es.search(index='ache-20180418',size=1000,scroll='2m', body=squery)
sid = page['_scroll_id']
scroll_size = len(page['hits']['hits'])

p = re.compile('[a-z2-7]{16}\\.onion', re.IGNORECASE)
onion_list = []

while (scroll_size > 0):
    print ("scrolling...")
    page = es.scroll(scroll_id = sid, scroll = '2m')
    sid = page['_scroll_id']
    scroll_size = len(page['hits']['hits'])
    for d in page['hits']['hits']:
        # print(d['_source']['html'])
        onions = p.findall(d['_source']['html'])
        if (len(onions) > 0):
            onion_list += onions
    print ("scroll size: " + str(scroll_size))

unique_list = set(onion_list)
last = list(unique_list)
last.sort()
for link in last:
    print(link)
print(len(link))
```

```
26dnflhucnbiho42.onion
2gbawvvusqmwgy4y.onion
2kka4f23pcxgqkpv.onion
32pbf32xi6ccm63z.onion
344c6kbnjnljjzlz.onion
35khdgeiyit26syj.onion
3g2upl4pq6kufc4m.onion
3k4gwuc13cgch22k.onion
3xjowtfvv6tetjyt.onion
42bu3fd5gaxu3xbn.onion
46vnnzhwdvfe774.onion
46vnnzhwdvfg774.onion
4ojzyialtr2s4pvy.onion
4oy7nsv5713ragqz.onion
```

...

```
[minyoungk@localhost ~]$ curl -H "Content-Type: application/json" -XPOST http://localhost:9200/ache-20180403/_search
{"query":{"regexp":{"html":"[a-z2-7]{16}.onion"}}}
| more
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   Dload  Upload    Total   Spent    Left     Speed
  0     0    0     0     0     0      0      0  --:--:-- --:--:-- --:--:--    0
"took" : 18,
"timed_out" : false,
"_shards" : {
  "total" : 5,
  "successful" : 5,
  "skipped" : 0,
  "failed" : 0
},
"hits" : {
  "total" : 15266,
  "max_score" : 1.0,
  "hits" : [
    {
      "_index" : "ache-20180403",
      "_type" : "page",
```




Crawler

- Torscrapper : <https://github.com/dirtyfilthy/freshonions-torscraper>

FRESH ONIONS

[INDEX](#) [FAQ](#) [JSON](#) [SRC](#) [STATS](#) -- 768 certified fresh onions, 2 in the last 24 hours.

Information for **[REDACTED].onion**

[\[SITE\]](#) [\[JSON\]](#)

Open Ports:

- 80:http

Interesting Paths:

No interesting paths in database.

Emails:

No emails in database.

Bitcoin Addresses:

No bitcoin addresses in database.

SSH fingerprint

No SSH fingerprint in database.

Clones

This site appears to have no clones.

Status	Dead
Created At	2017-01-27 10:36:05
Visited At	2018-04-22 11:44:39
Last Seen	2018-04-21 21:38:41
Portscanned	2017-02-20 13:39:21
Language	English
Server	Apache 2.4.8.1 (ubuntu)
X-Powered-By	PHP/5.5.9-1ubuntu4.21
Useful 404 (Gen)	No
Useful 404 (PHP)	No
Useful 404 (Dir)	No



Crawler

- Onionscan: <https://onionscan.org>

OnionScan Correlations Lab - Chromium

OnionScan Correlat x

192.168.100.112:8080/?search=

Apps For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now...](#)

Summary Saved Searches

Summary for [search term] mod_status

Server Information

Email Addresses

Co-Hosted Clearnet Sites

HTTP Headers 39

Webpage Information 9

Links to External Sites 20

IP Addresses

Server Information linked to rrbm3jiflz3euxhp.onion (1)

Tag	Identifier	Onion	Other Links
mod_status	Apache/2.2.14 (Win32)	rrbm3jiflz3euxhp.onion	0

Email Addresses linked to rrbm3jiflz3euxhp.onion (1)

Tag	Identifier	Onion	Other Links
mailto	localhost	rrbm3jiflz3euxhp.onion	1



기존 도구들 + Tor Proxy

- Tor Proxy는 socks 프로토콜로 연결
 - SQLMap, NMAP 등 socks proxy 지원하는 프로그램은 모두 사용 가능

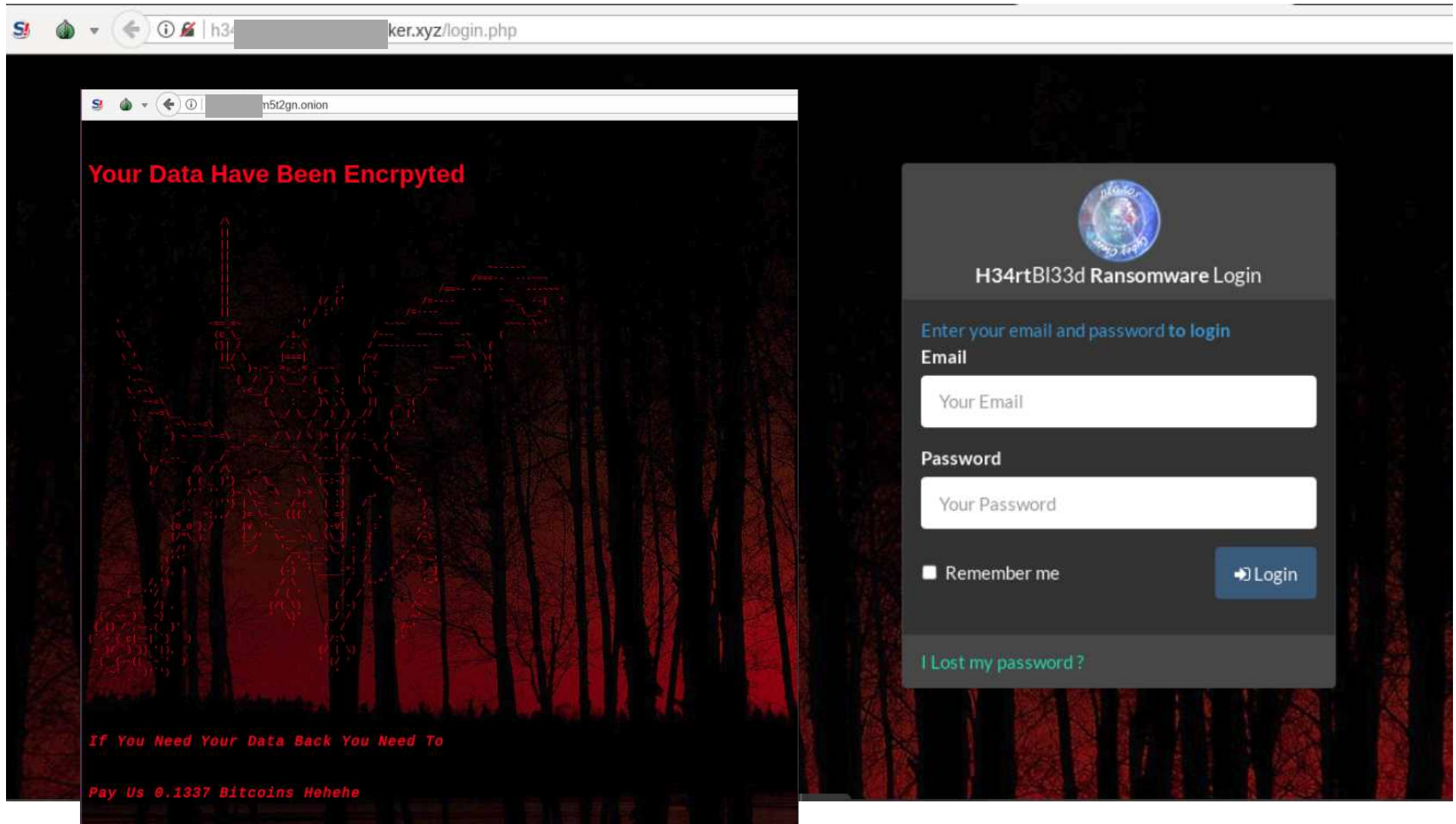
```
my@ubuntu:~/Downloads/drub$ sudo netstat -anp | grep tor
tcp        0      0 127.0.0.1:9050        0.0.0.0:*             LISTEN      1236/tor
tcp        0      0 127.0.0.1:9150        0.0.0.0:*             LISTEN      6477/tor
tcp        0      0 127.0.0.1:9151        0.0.0.0:*             LISTEN      6477/tor
```

- Torsocks

```
my@ubuntu:~/Downloads/drub$ torsocks curl http://[redacted].onion | head -5
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 162 100 162    0     0 121      0  0:00:01  0:00:01 --:--:-- 121
<html>
<head><title>[redacted]</title></head>
<body bgcolor="white">
<center><h1>[redacted]/h1></center>
<hr><center>nginx</center>
```

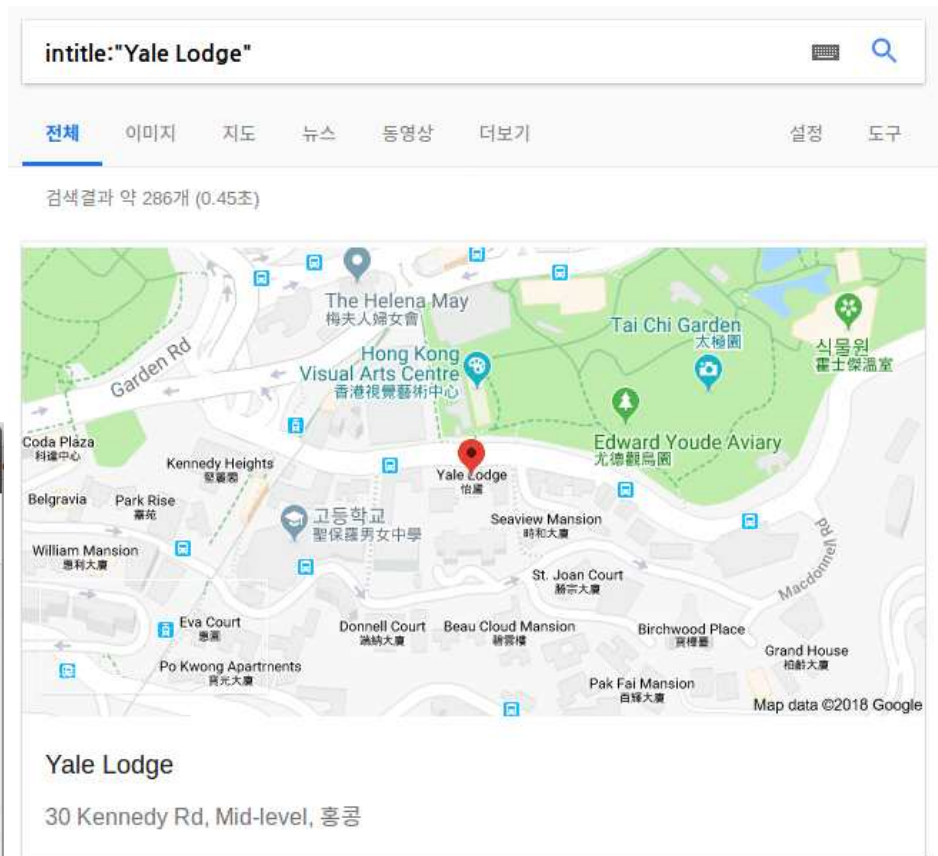
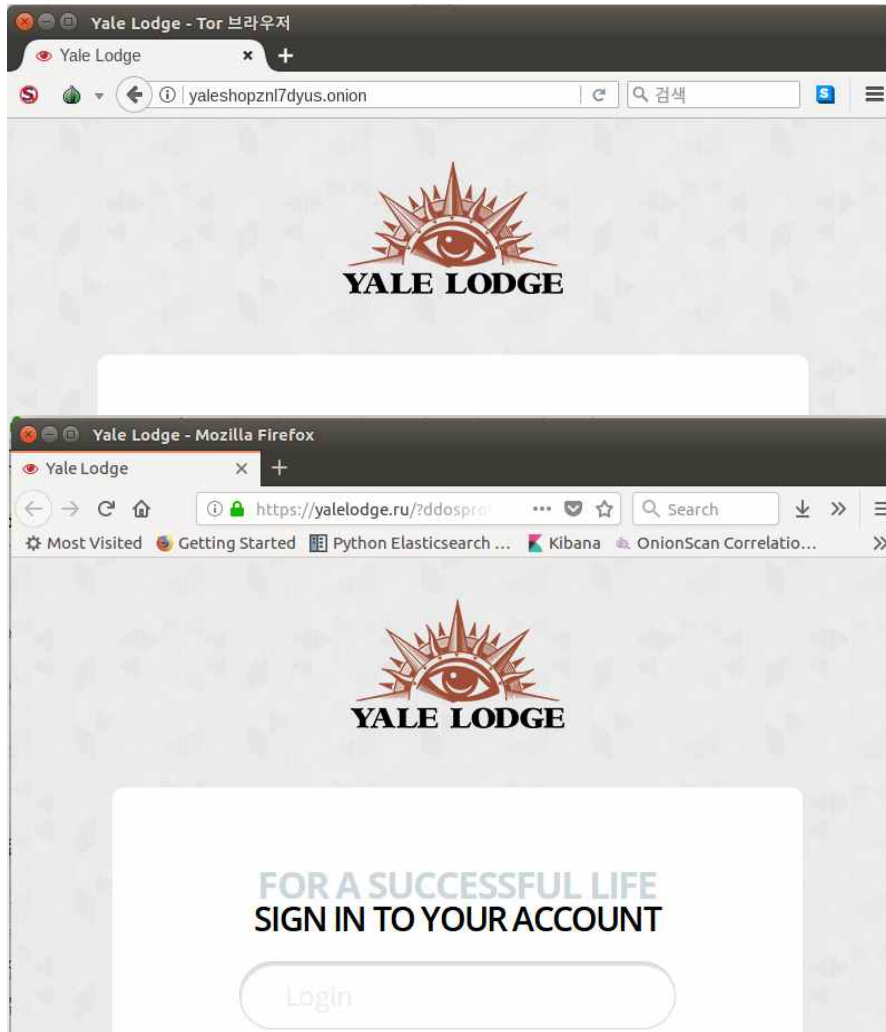


검색정보





HTTP 타이틀 검색



Yale Lodge
<https://yalelodge.ru/> 이 페이지 번역하기
for a successful life. Sign in to your account. Login. Registration is closed.



- Google Analytics ID

Analytics IDs linked to analytics-id (1)			
Tag	Identifier	Onion	Other Links
snapshot	UA [REDACTED]-1	[REDACTED].onion	0

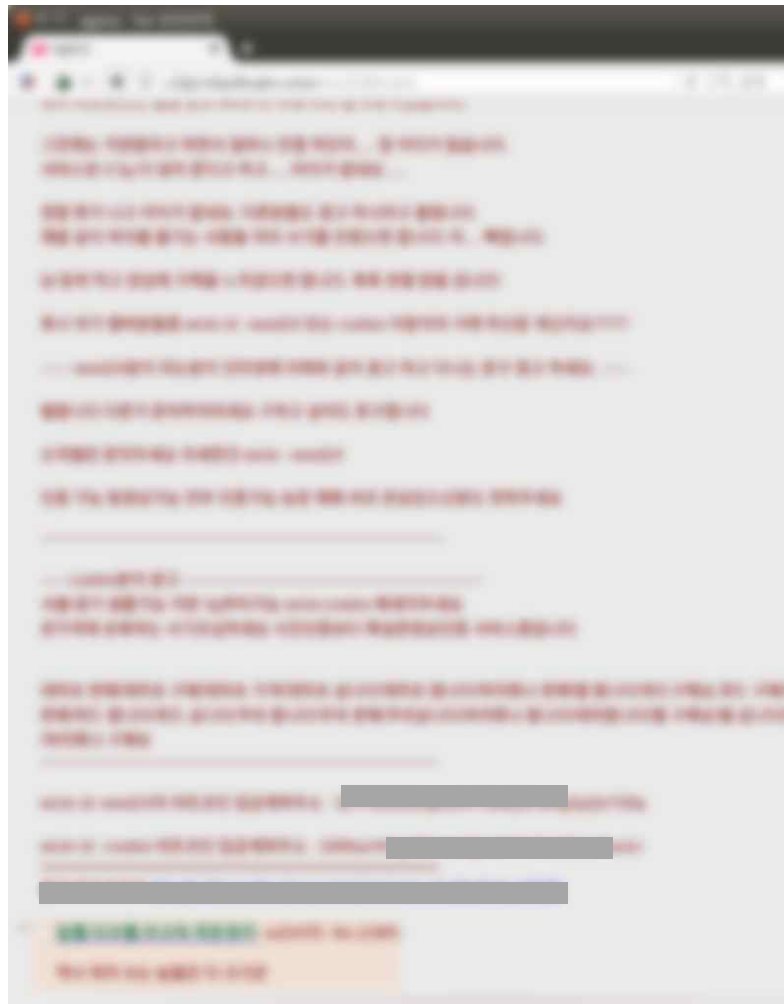
- SMTP Banner

Software Banners linked to smtp (5)			
Tag	Identifier	Onion	Other Links
smtp	220 [REDACTED] onion ESMTP Postfix (Debian/GNU)	[REDACTED].onion	-1
smtp	220 [REDACTED] onion ESMTP Postfix (Debian/GNU)	[REDACTED]z.onion	-1
smtp	220 [REDACTED] onion ESMTP Postfix (Debian/GNU)	[REDACTED].onion	-1
smtp	220 [REDACTED] onion ESMTP Postfix (Debian/GNU)	[REDACTED]4.onion	-1
smtp	220 [REDACTED] onion ESMTP Postfix (Debian/GNU)	[REDACTED].onion	-1



Bitcoin Address

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.



Summary

Address	1689acHrFgXDzHcIAQoVdUkMHh6WsaGack
Hash 160	3832b3d1d89625a06da0e1f256525532a839819b
Tools	Related Tags - Unspent Outputs

Transactions

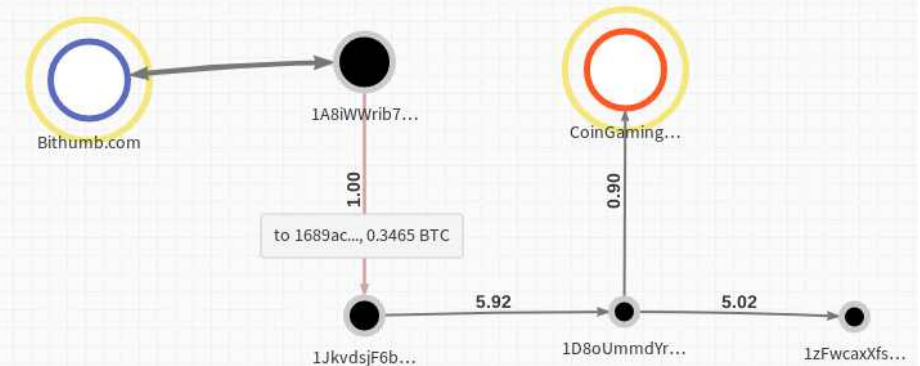
No. Transactions	2
Total Received	0.34649184 BTC
Final Balance	0 BTC

[Request Payment](#) [Donation Button](#)

Transactions (Oldest First) [Filter](#)

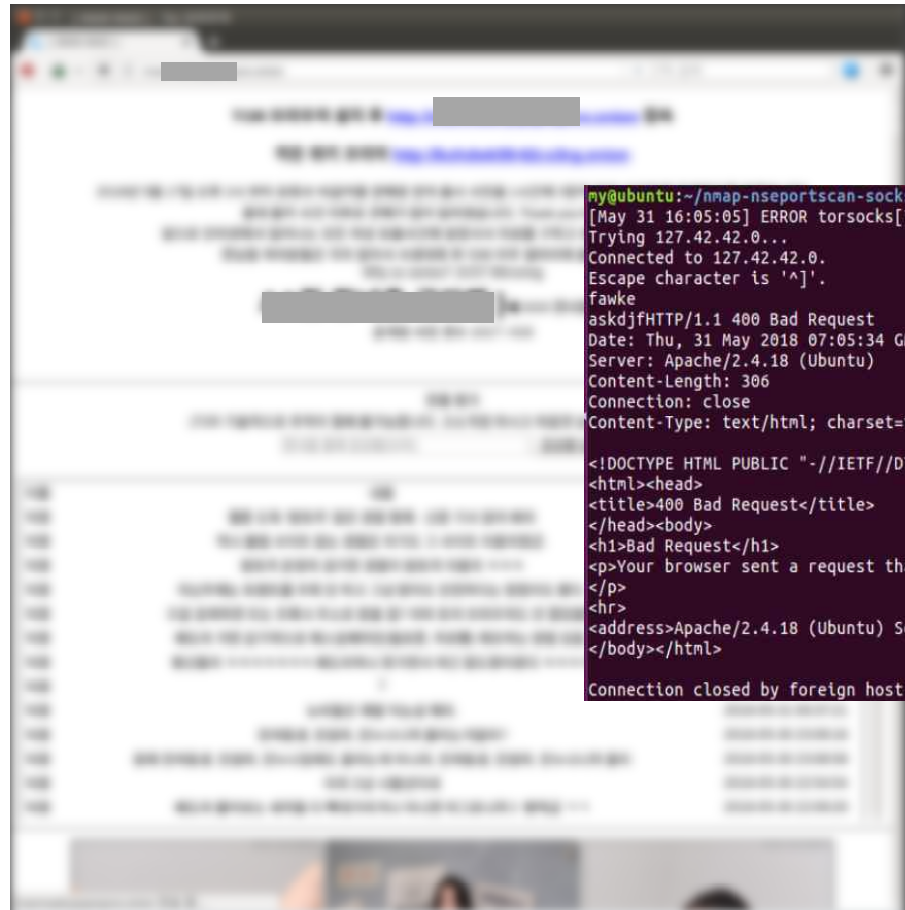
Buy Bitcoin and Ethereum with bank card via Changelly - instant cryptocurrency exchange with the best rates! [Buy Now](#)

0581e9ee26d57769c0ed28123c3b773414f537602f2aaa7aaa8823289103055	2016-04-08 14:11:00
1689acHrFgXDzHcIAQoVdUkMHh6WsaGack → 1D8oUmmYr9PKdTDIM22nJvsJAZd5IEDTU	5.91938578 BTC
	-0.34649184 BTC
49336ac8f662742c7739ce0828bda20d22d7440ccea5c5f42f769c3b7f33063	2016-04-07 07:25:33
1A8iWWrib7nukhsFMhSFpZkcs2MWTWq8 → 1689acHrFgXDzHcIAQoVdUkMHh6WsaGack	0.34649184 BTC
	0.34649184 BTC





HTTP 에러 페이지



```
my@ubuntu:~/nmap-nseportscan-socks4a$ torsocks telnet [redacted] .onion 80
[May 31 16:05:05] ERROR torsocks[73509]: Unable to resolve. Status reply: 4 (in socks5_rcv_resolve_reply() at socks5.c:666)
Trying 127.42.42.0...
Connected to 127.42.42.0.
Escape character is '^]'.
fawke
askdjfHTTP/1.1 400 Bad Request
Date: Thu, 31 May 2018 07:05:34 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 306
Connection: close
Content-Type: text/html; charset=iso-8859-1

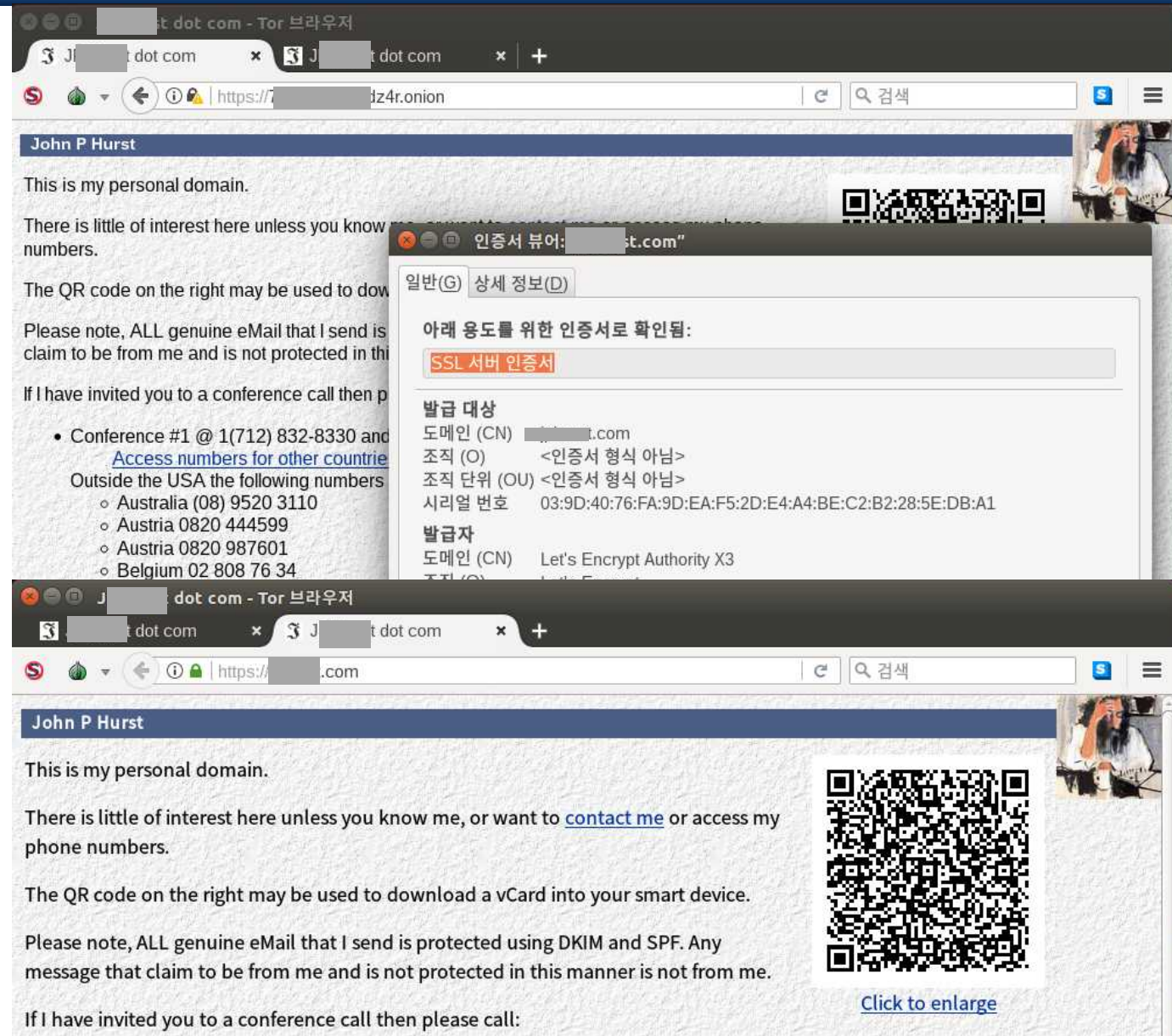
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 172.[redacted].178 Port 80</address>
</body></html>

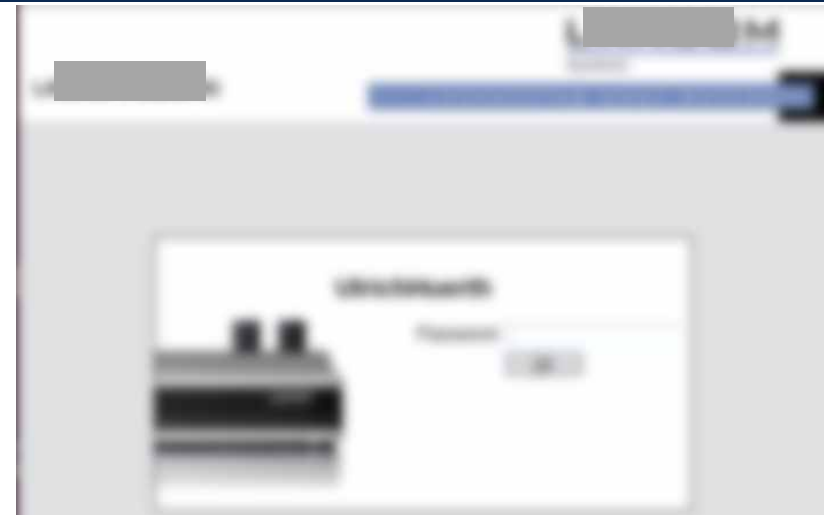
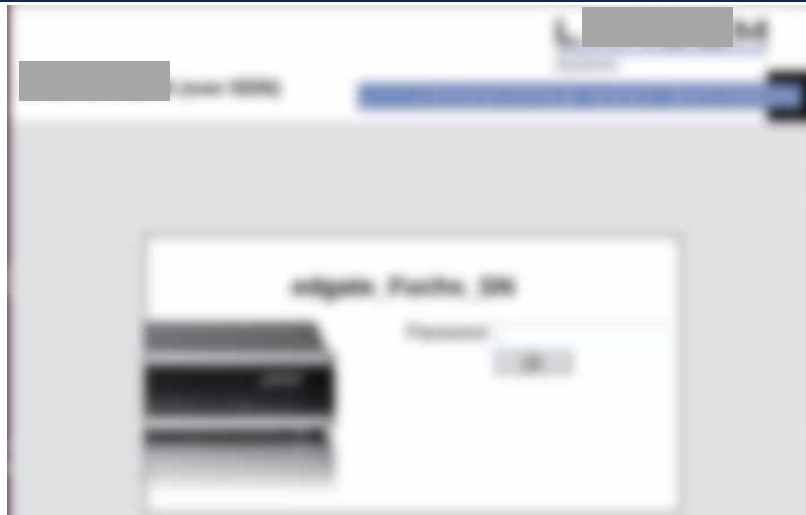
Connection closed by foreign host.
```




SSL

- Common Name
- SAN
- Fingerprint
- Public Key

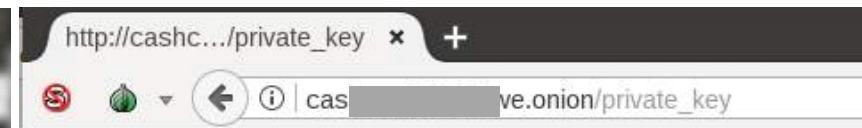




```
my@ubuntu:~/SSL$ echo "" | openssl s_client -connect [REDACTED]:443 2>/dev/null | openssl x509 -subject -fingerprint -pubkey -noout
subject= /C=DE/ST=NRW/L=Wuerselen/O=[REDACTED]ems/OU=Engineering/emailAddress=info@[REDACTED].ms.de/CN=[REDACTED]32
SHA1 Fingerprint=A9:F7:A6:E7:25:C9:B1:A1:77:EF:BF:F3:64:79:12:C5:E6:42:05:51
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEASu0zUg1PBVpmw99HffcE
qPaGku2M6r3e8NC/+Ph2dTLL1hkJefZXM9NF0BgzMqkkZk6eLdFXf8uAVttfs72k
TT/muwr6dOwFeyltVQ7kk66hFQ33E/YQ1L0s1q800qil7esoDXY4prcant0ZfkTM
puIeZFraKnyCGfsINJtPtssdXltG1vCgGdU3dTlys85MXoY2SqqQhMMQgjDNwzj+
cz0GSgg/FT99/unwmZ4fUScLBXdvEzyckwd+8UCVDgXbZMXtKU+g6+SSv9HkDRTv
qqX5jPUMpK6Secr1HNWdG/+5GLhgG532onyFnEZnFvet3meMPRVGW3YfktB928Rx
FQIDAQAB
-----END PUBLIC KEY-----
my@ubuntu:~/SSL$ echo "" | openssl s_client -connect [REDACTED]:18:443 2>/dev/null | openssl x509 -subject -fingerprint -pubkey -noout
subject= /C=DE/ST=NRW/L=Wuerselen/O=[REDACTED]ems/OU=Engineering/emailAddress=info@[REDACTED].ms.de/CN=[REDACTED]18
SHA1 Fingerprint=10:DA:B6:C7:38:6D:3D:AF:B7:ED:F8:8D:F0:E3:7C:4A:B2:5F:D4:9F
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEASu0zUg1PBVpmw99HffcE
qPaGku2M6r3e8NC/+Ph2dTLL1hkJefZXM9NF0BgzMqkkZk6eLdFXf8uAVttfs72k
TT/muwr6dOwFeyltVQ7kk66hFQ33E/YQ1L0s1q800qil7esoDXY4prcant0ZfkTM
puIeZFraKnyCGfsINJtPtssdXltG1vCgGdU3dTlys85MXoY2SqqQhMMQgjDNwzj+
cz0GSgg/FT99/unwmZ4fUScLBXdvEzyckwd+8UCVDgXbZMXtKU+g6+SSv9HkDRTv
qqX5jPUMpK6Secr1HNWdG/+5GLhgG532onyFnEZnFvet3meMPRVGW3YfktB928Rx
FQIDAQAB
-----END PUBLIC KEY-----
```



HS private_key



```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC1QShsmTDkyRvSa6x2qgmRIhivz6ECB9X0VMfmbH5U8MOCRUL
e13MZiAu0d3Sq1NfWShpwMhhfckt03+Im93FR1NM1NMZDN/vrW15p3vxq8CYfLk
F6cwzJfMCvdYPr0q03G3klIgMSdQRYmK2kj+cKHvNCUFjQ31BUG5mGnDqQIDAQAB
AoGBAKIMTYycuwWfHMCerrpCVK2J/ins8/CVVnhsJJYPEohoM+67ff46+Lyc3eke
JuVv2WVYyjiZ8rL/A7sWA8q+F8IE0FUZbTlDCf0vf2b2tXgDJxitPwZAewxthzIZ
ZrJmsdv+wwQ2ns/RrG7xb+jTlx1qyKsGclSE+sGbQRVhwzLVAKA3c6qlbBXXrZW
36LX8uI/NrUwbrb+f6N37QiVXEbk6AyaFBMat9wUnXFduXjq50z70pynZF8U+rGY
1uNm5SIPFwJBANEyIun5zUC8tXUQsENNgNJSdfG2UvSB1P0medrjQ6k66s/US09v
s9Pdp5QmuaQMhew3WjtQEwULE3o4IN4ez8CQBCJuzAXA8wkQxExYcqpczVkdmyU
SDrLqM4m4RSxjHkJrgs9ugpeFbsQrNJx27wwg7ufv8cuFQjA34YaUnqkIfsCQDfA
fuGQe403PbZ3N6KYM524MEq85prXRyOwSGV3j/63/wBoeq+m22wpdFjgLogoAdGb
mWJvaG0iu7P/zmX7ZA0CQFDP+kn1TnuwiGuDkYJlgL0Uz1Tv+BugJJn4uLB4/XAN
mm8Vrfy58kxFTbICBXqJrAv2gNh3YXJUGBQH4FzDErg=
-----END RSA PRIVATE KEY-----
```



Apache Server Status for [REDACTED] .onion (via 192.168.0.8)

```
Parent Server Config: Generation: 10
Parent Server IP: Generation: 9
Server IP: 0.0.0.0
Total accesses: 20000 Total Traffic: 900.1 MB
CPU Usage: 19.9 523.4 MB 30.00% CPU load:
0.30 requests: 1070 Requests: 29.0 Kbytes/request
1 requests currently being processed: 40 idle workers
```

99)	Connections	Threads		Active connections	
	total/accepting	busy	idle	keep-alive	closing
20/48/0/0	yes	0	26	0	0
20/48/0/0	yes	1	24	0	0
Sum		1	49	0	0

Scoreboard Key:

- Waiting for Connection
- Starting up
- Reading Request
- Sending Reply
- Keepalive (read)
- DRS Lookup
- Closing connection
- Logging
- Gracefully finishing
- Idle cleanup or error
- Open work with no current process

SVR	IPD	ACC	W	CPU	OS	Req.Conn	Child Size	Child	VMSize	Request
0-9	20490	0/130/597	11:50	322	0	0.0	12:32 19:45 192 168 1.1			
0-9	20490	0/140/632	11:50	328	0	0.0	13:12 18:50 192 168 1.1			option 0000 GET /charlie/first2weeks/P2200005.jpg HTTP/1.1
0-9	20490	0/145/620	11:44	318	0	0.0	12:10 18:54 192 168 1.1			
0-9	20490	0/142/633	11:50	324	0	0.0	10:51 18:30 192 168 1.1			
0-9	20490	0/140/612	11:50	326	0	0.0	14:57 19:36 192 168 1.1			
0-9	20490	0/130/592	11:42	327	1	0.0	18:37 20:06 192 168 1.1			
0-9	20490	0/139/623	11:51	317	0	0.0	15:64 20:18 192 168 1.1			
0-9	20490	0/140/614	11:52	312	0	0.0	16:52 20:19 192 168 1.1			option 0000 GET /charlie/first2weeks/P22000011.jpg HTTP/1.1
0-9	20490	0/152/616	11:51	314	0	0.0	16:02 13:52 192 168 1.1			option 0000 GET /charlie/first2weeks/P22000010.jpg HTTP/1.1

Apache Server Status for www. [REDACTED] .com (via 192.168.1.31)

www. [REDACTED] .com:80.6E7/charlie?first2weeks=72280008;oe HTTP/1.1

00이랑 아고라랑 같은 VPS 회사 쓰는 거냐? 아니면 두 사이트 운영자가 동일원?



EXIF





- OnionScan report : <https://mascherari.press/Tor>
- Documentation : <https://www.torproject.org/docs/documentation>
- "CARONTE: Detecting Location Leaks for Deanonymizing Tor Hidden Services"
 - CCS '15 Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security
- <https://darkwebnews.com/>

