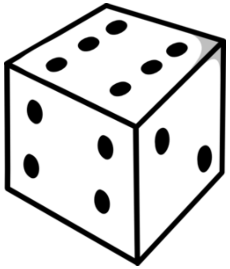


DICE - Deception of InterCommunication to Enemies

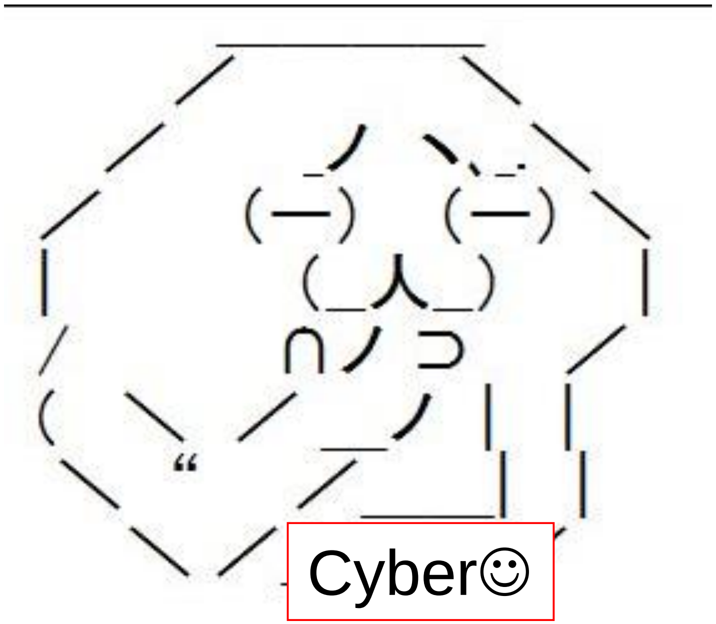
wakatono

wakatono@gmail.com

Twitter: @wakatono

Facebook: www.facebook.com/wakatono

Other side:



It’s a Joke ☺

Today’s Presentation

(Almost) All you need is…

- □ TCP/IP basic(knowledge of IP, UDP, TCP headers)
- □ DNS basic(knowledge of query – response)
- □ Speed of Light (300,000km/sec)

And some knowledge to develop, deploy

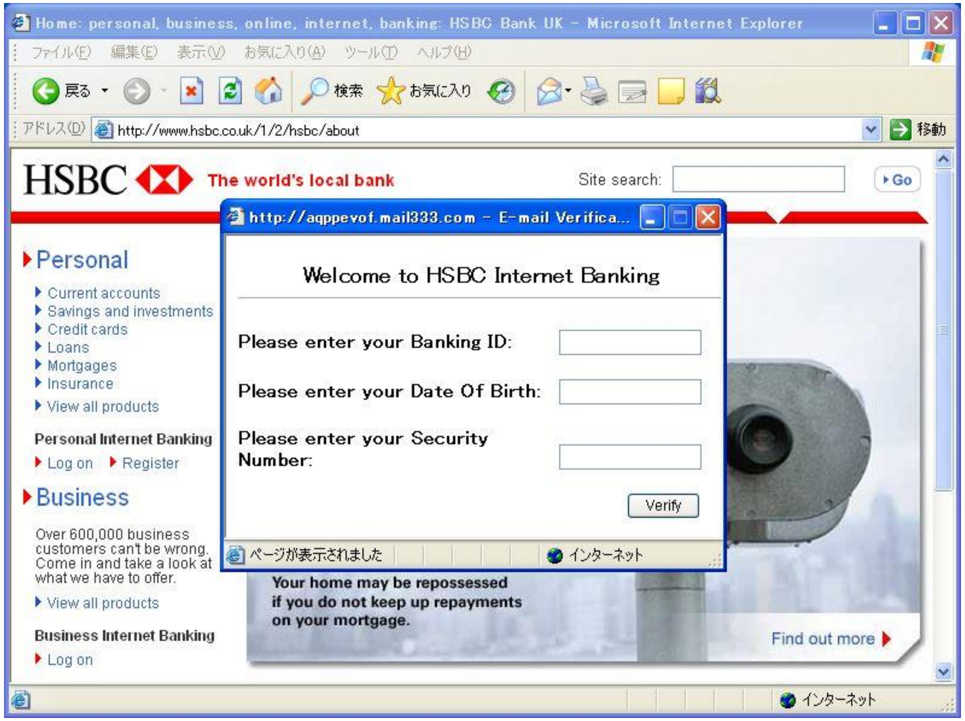
Table of Content

- ⚀ Various of attacks on internet
- ⚁ Popular solutions and issues
- ⚂ Focus to DNS query and response
- ⚃ Decept the Enemies! – DICE architecture, keys of implementation, and deployment
- ⚄ Protocol Deception – Joyful and Useful Decepting Technology
- ⚅ DICE Applications, Issues, and future

Various of attacks on internet

Assumption: Attackers use Malicious FQDNs, Domains, and FastFlus combination

Phishing makes malicious sites like a real service sites.



Home: personal, business, online, internet, banking: HSBC Bank UK - Microsoft Internet Explorer

http://www.hsbc.co.uk/1/2/hsbc/about

http://aqppevof.mail333.com - E-mail Verifica...

Welcome to HSBC Internet Banking

Please enter your Banking ID:

Please enter your Date Of Birth:

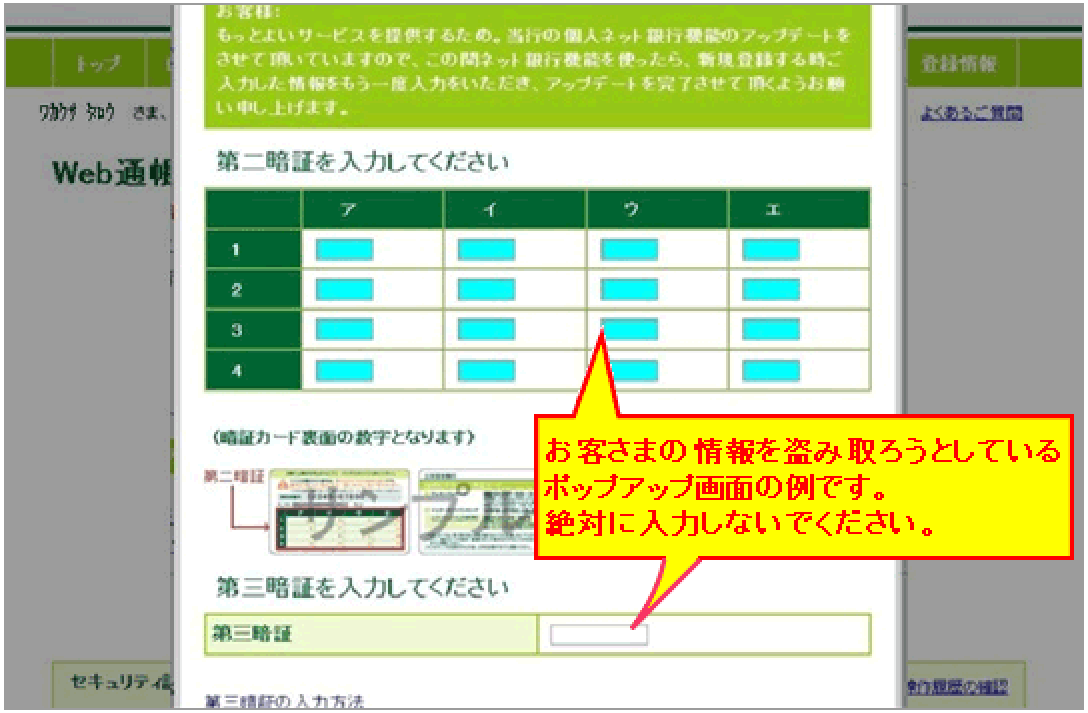
Please enter your Security Number:

Over 600,000 business customers can't be wrong. Come in and take a look at what we have to offer.

Your home may be repossessed if you do not keep up repayments on your mortgage.

Reference:
http://www.atmarkit.co.jp/fsecurity/special/65phishing/phishing01.html

MITB viruses inject malicious forms to real contents



お客様：
もっとよいサービスを提供するため。当行の個人ネット銀行機能のアップデートをさせて頂いていますので、この間ネット銀行機能を使ったら、新規登録する時ご入力した情報をもう一度入力をいただき、アップデートを完了させて頂くようお願い申し上げます。

第二暗証を入力してください

	ア	イ	ウ	エ
1				
2				
3				
4				

（暗証カード裏面の数字となります）

第二暗証

第三暗証を入力してください

第三暗証	

第三暗証の入力方法

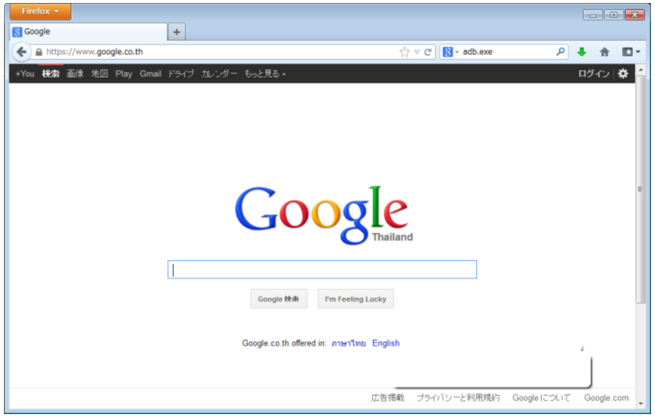
お客さまの情報を盗み取ろうとしている
ポップアップ画面の例です。
絶対に入力しないでください。

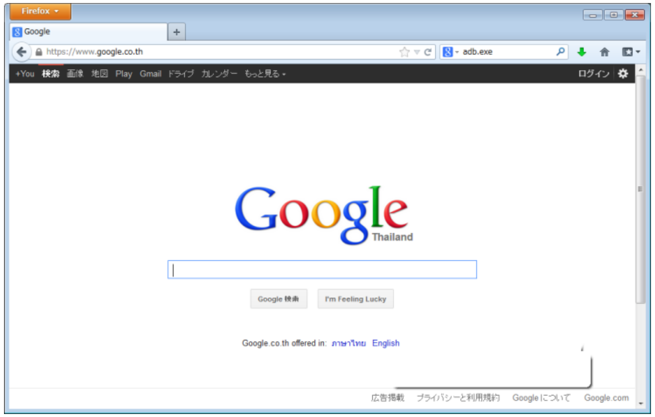
Reference: http://www.smbc.co.jp/security/popup.html

Common Spec:malicious hosts exist

- Attacker prepares the host to receive data of victims’ like banking information.
- Most of malicious host has own FQDN
- IP addresses is changed due to their lifecycle
  - Stopping access to malicious hosts that have fixed IP addresses is easy due to many technology to take down.

Modern Attacks triggered by Web Access

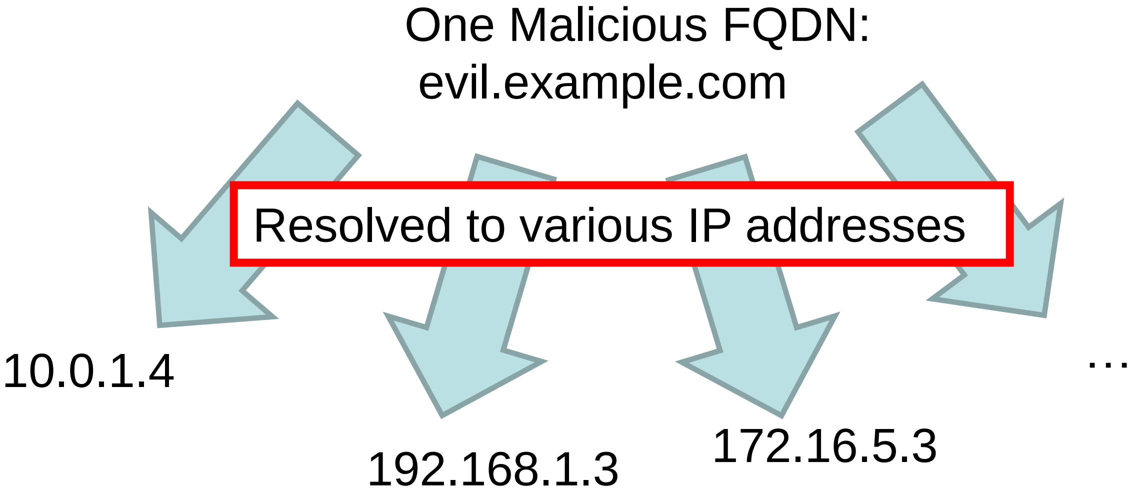

Firefox
Google
https://www.google.co.th
adb.exe
+You 検索 画像 地図 Play Gmail ドライブ カレンダー もっと見る
ログイン
Google Thailand
Google 検索
I'm Feeling Lucky
Google.co.th offered in: ภาษาไทย English
広告掲載 プライバシーと利用規約 Googleについて Google.com


Firefox
Google
https://www.google.co.th
adb.exe
+You 検索 画像 地図 Play Gmail ドライブ カレンダー もっと見る
ログイン
Google Thailand
Google 検索
I'm Feeling Lucky
Google.co.th offered in: ภาษาไทย English
広告掲載 プライバシーと利用規約 Googleについて Google.com

Which is better, left “Google” or right “Google” ?

Both sites are better(correct) web site ☺

FastFlux – common tech for attackers



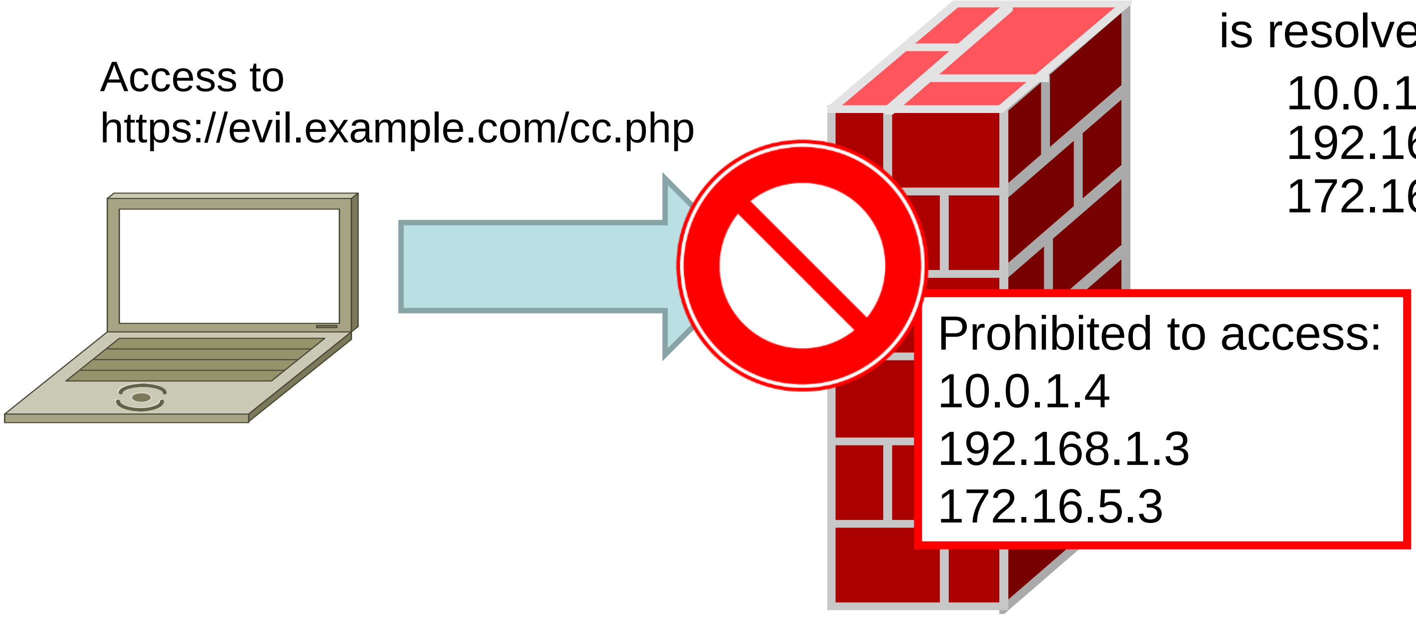
- One malicious FQDN has multiple IP addresses ☹

⚁

Popular solutions and issues

Firewall

Access to
https://evil.example.com/cc.php



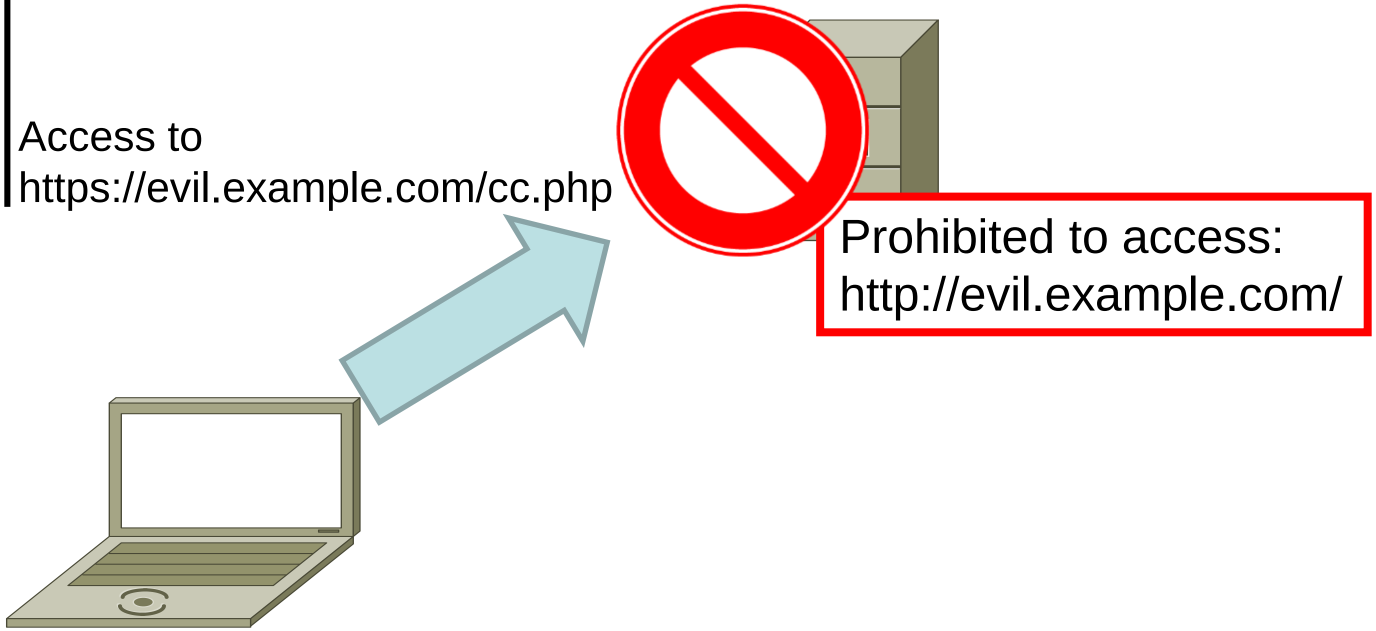
evil.example.com
is resolved to:

10.0.1.4
192.168.1.3
172.16.5.3

Prohibited to access:
10.0.1.4
192.168.1.3
172.16.5.3

URL Filtering by HTTP(S) Proxy

HTTP Proxy Server(e.g. Squid Proxy Server)



Access to
https://evil.example.com/cc.php

Prohibited to access:
http://evil.example.com/

IDS / IPS

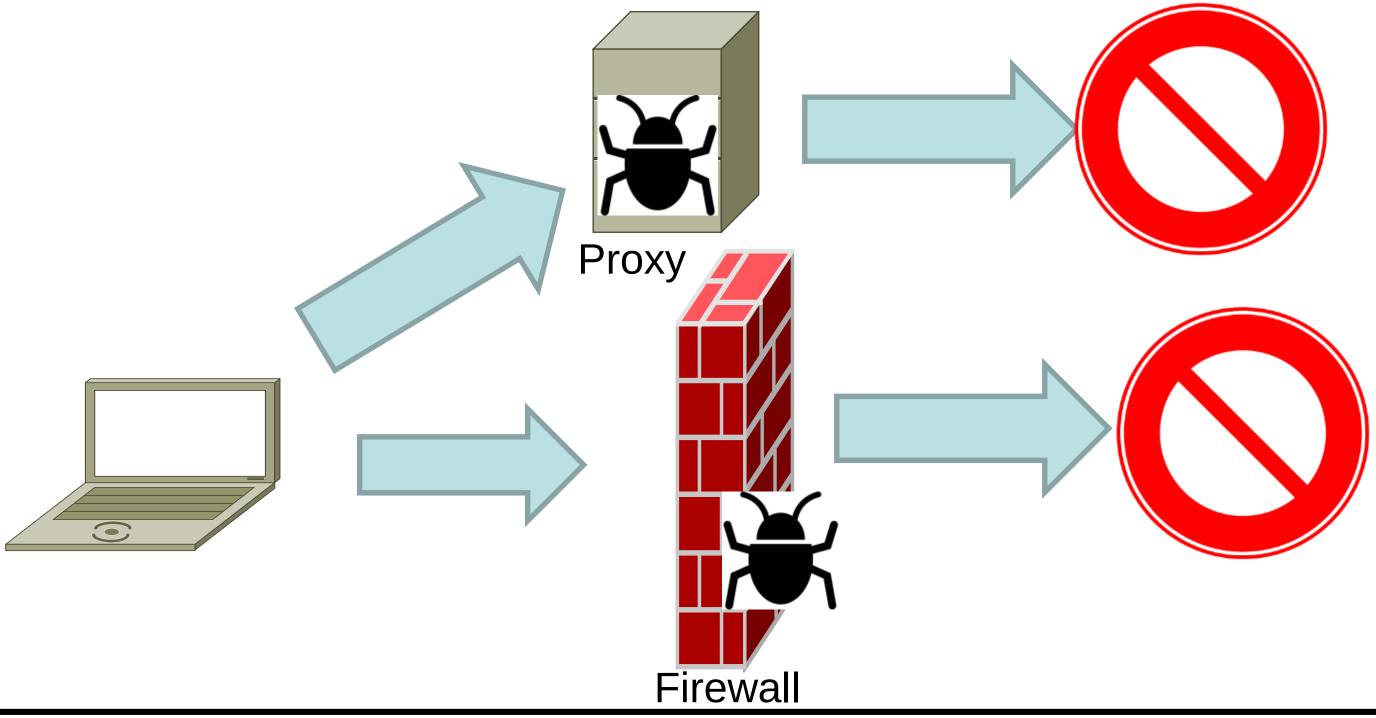
- (snip)

RPZ(Response Policy Zone)

- RPZ is the DNS blocking technology
- Implemented in newer BIND releases

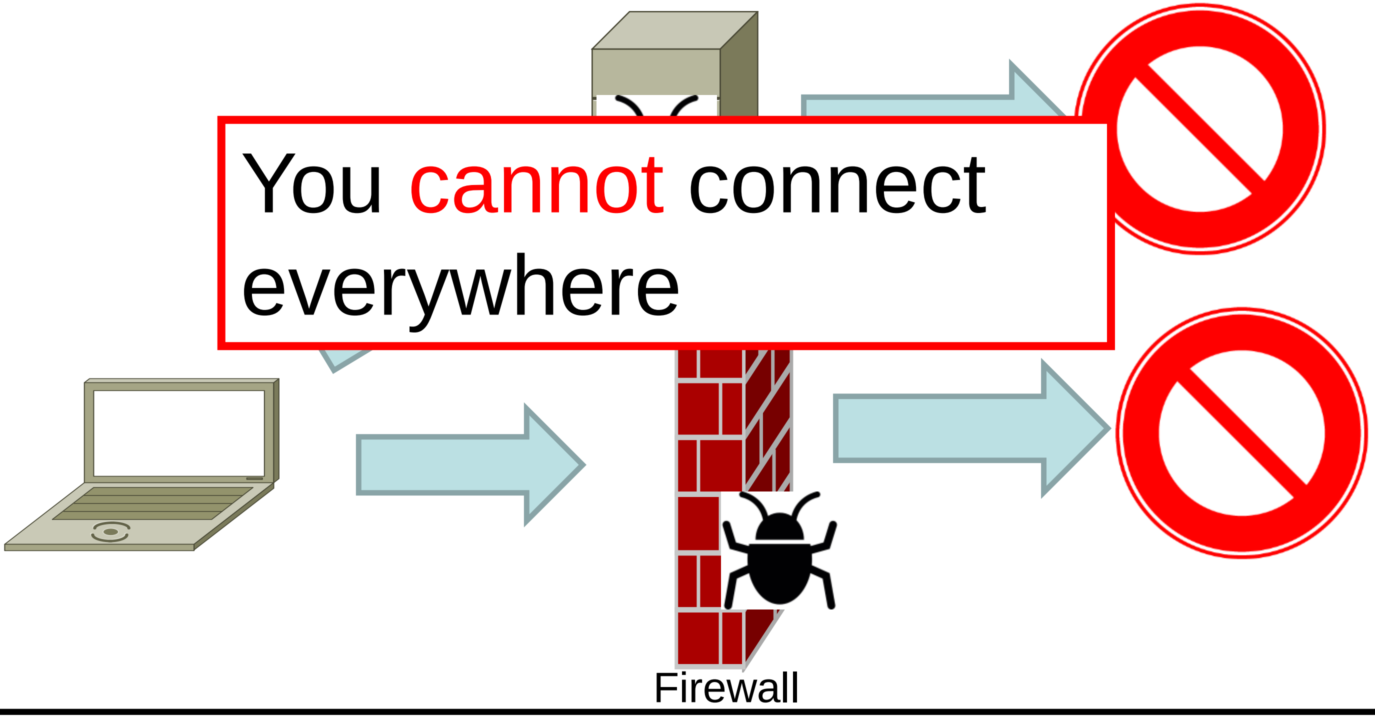
Generic Issues of Solutions

- Performance Bottleneck
- Reliability / Availability



Generic Issues of Solutions

- Performance Bottleneck
- Reliability / Availability



You cannot connect everywhere

How to avoid accessing to malicious host?

- HTTP/HTTPS Proxy Server access block by using Blacklist and/or Firewall
  - Load of Proxy (Servers & Operators) and/or Firewall(Servers & Operators) may be High!
- Takedown by ISP and Various Service Provider
  - Sometimes Long Term discussion is needed
- Temporarily:
  - Stop by using DNS response deception(example)
    - I assume this to use edge network(response from nearest DNS Cache Server is decepted)

Focus to DNS query and response

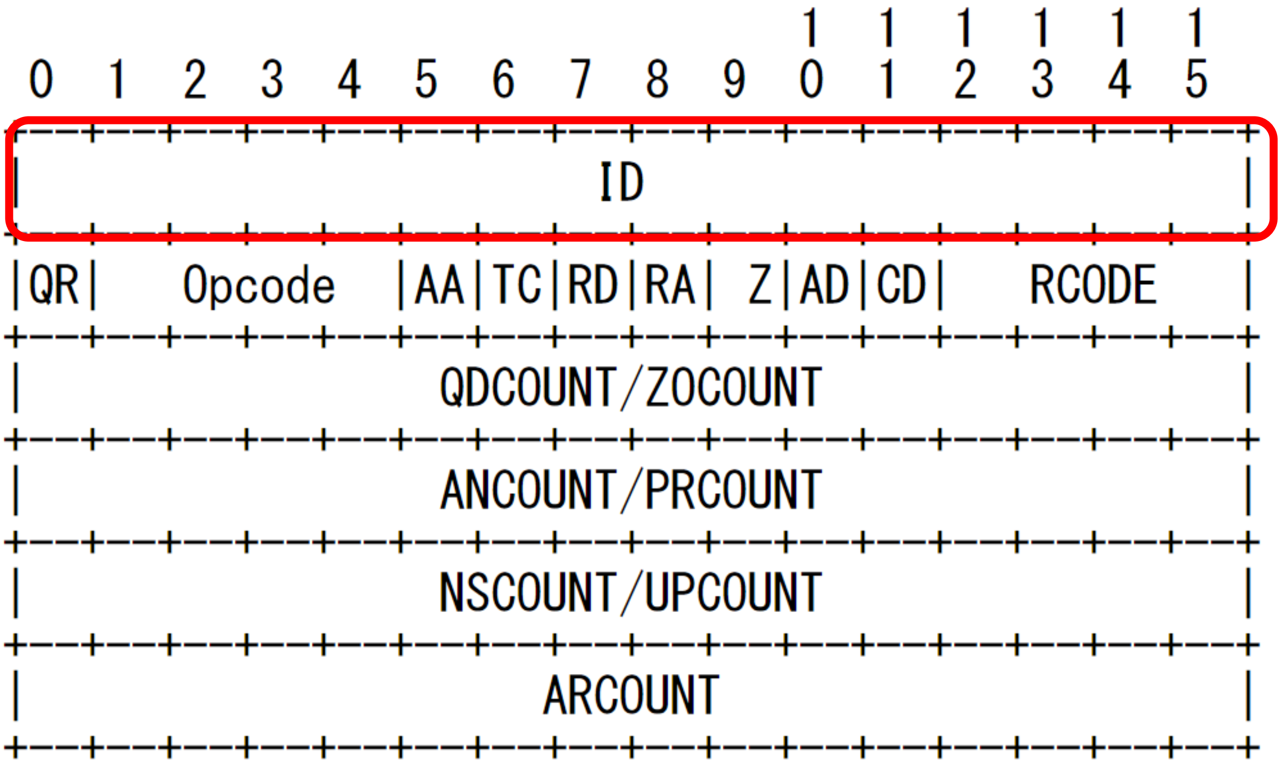
Assumption

- We have technology to identify malicious FQDN
  - By using SIEM, Domain Blacklist, URL Blacklist, etc…
- Network Operator and Security Operator are independent

DNS Response
- easily Deceptable Protocol Response

- Normal DNS Response can be decepted easily
  - Signed DNS Response (e.g. DNSSEC specification) is hard to be decepted.
  - TCP DNS Interaction is little a bit hard to be decepted.
- Applicable to various of deception
  - Various RR Type of Response(e.g. NS, MX) can be used for applying.

DNS Query/Response Header Format

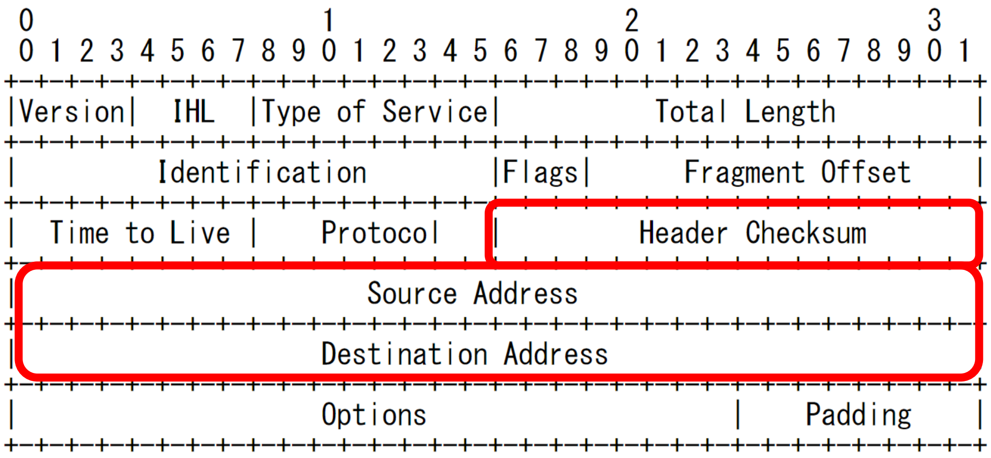


```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA| Z|AD|CD|   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                QDCOUNT/ZOCOUNT                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                ANCOUNT/PRCOUNT                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                NSCOUNT/UPCOUNT                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

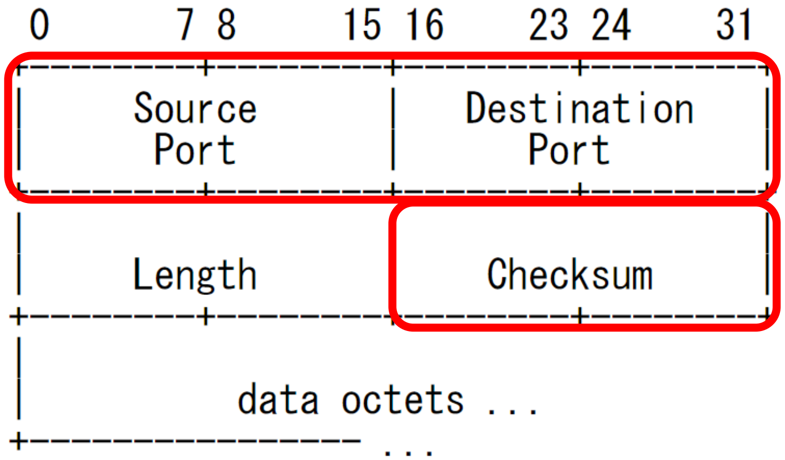
The ID field identifies the query and is echoed in the response so they can be matched.

Reference: RFC6895 Domain Name System (DNS) IANA Considerations

UDP and IP Header Format



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
 0      7 8     15 16    23 24    31
+--------+--------+--------+--------+
|     Source      |   Destination   |
|      Port       |      Port       |
+--------+--------+--------+--------+
|                 |                 |
|     Length      |    Checksum     |
+--------+--------+--------+--------+
|
|          data octets ...
+---------------- ...
```

References:
RFC768 User Datagram Protocol
RFC791 INTERNET PROTOCOL

DNS Response Deception Summary

- Response Packet is easy to decept
  - – Know pair of IP addresses(IP), Port numbers(UDP), (Transaction) ID(DNS)
  - – Send the decepted response packet to client(s) faster than “true” DNS response is sent
  - – Client(s) will access host(s) according to the decepted response

⚃

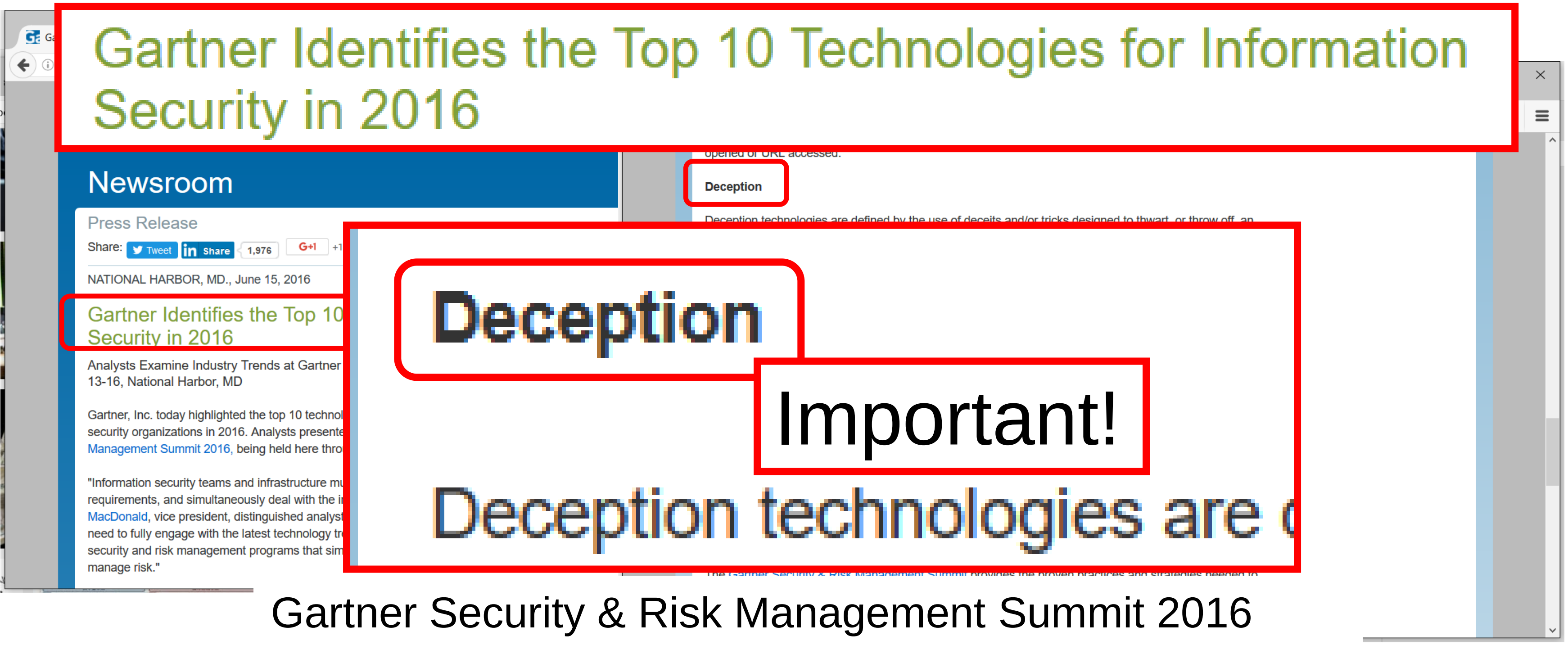
Decept the Enemies!
– DICE architecture, keys of implementation, and deployment

DICE architecture is simple, but implementation and deployment is difficult little a bit

What is DICE?

- Abbrev of:

Deception of InterCommunication to Enemies



Gartner Identifies the Top 10 Technologies for Information Security in 2016

Newsroom

Press Release

NATIONAL HARBOR, MD., June 15, 2016

Gartner Identifies the Top 10
Security in 2016

Analysts Examine Industry Trends at Gartner
13-16, National Harbor, MD

Gartner, Inc. today highlighted the top 10 technol
security organizations in 2016. Analysts presente
Management Summit 2016, being held here thro

"Information security teams and infrastructure mu
requirements, and simultaneously deal with the i
MacDonald, vice president, distinguished analyst
need to fully engage with the latest technology tr
security and risk management programs that sim
manage risk."

opened or URL accessed.

Deception

Deception technologies are defined by the use of deceits and/or tricks designed to thwart, or throw off, an

Deception

Important!

Deception technologies are

The Gartner Security & Risk Management Summit provides the proven practices and strategies needed to

Gartner Security & Risk Management Summit 2016

To Decept Protocol(s)

- Understand Protocol specification(s)
  - Connection sequence and requirement(TCP)
  - Communication sequence and fields of payloads
  - Transaction Relation Information(e,g,ID on DNS)
- Understand Protocol implementation(s)
  - TCP stack implementation UDP stack implementation, BIND on DNS, etc…
- Understand Target Application（s）
  - (snip)

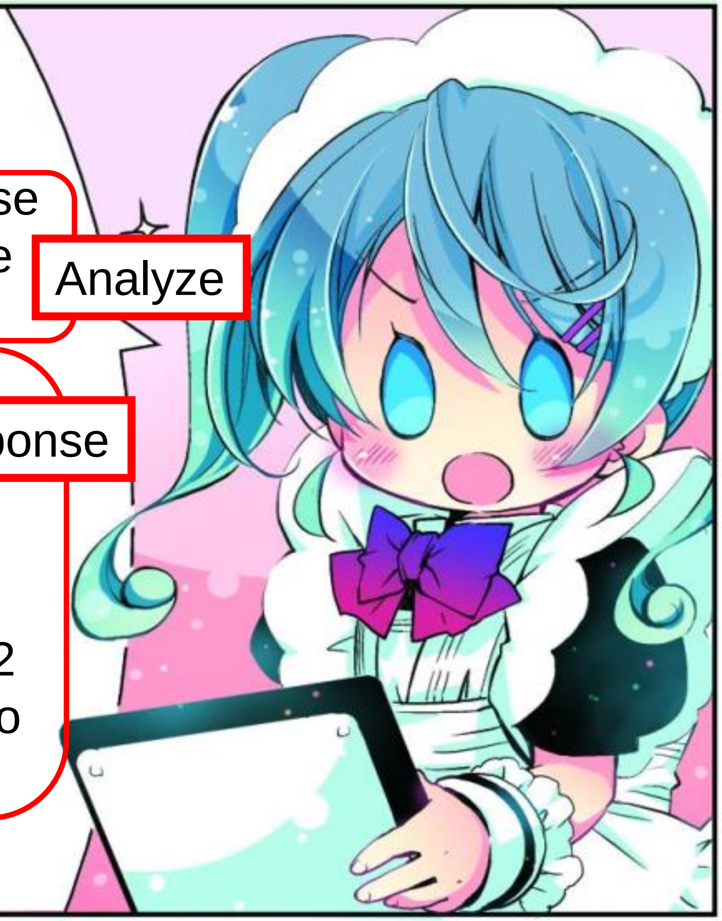
DICE architecture(simple!)

- Monitor subsystem
  - High-speed and lossless monitoring
  - Like tcpdump, wireshark, etc…(but simple)

- Analyze subsystem
  - Decede to Response

- Response Subsystem
  - High-speed and synchronous processing
  - Works like hping(but simple)

Applied DICE architecture to DNS client deception



Monitor

1. Capture DNS request
2. Decide whether the response of captured request must be decepted or not.

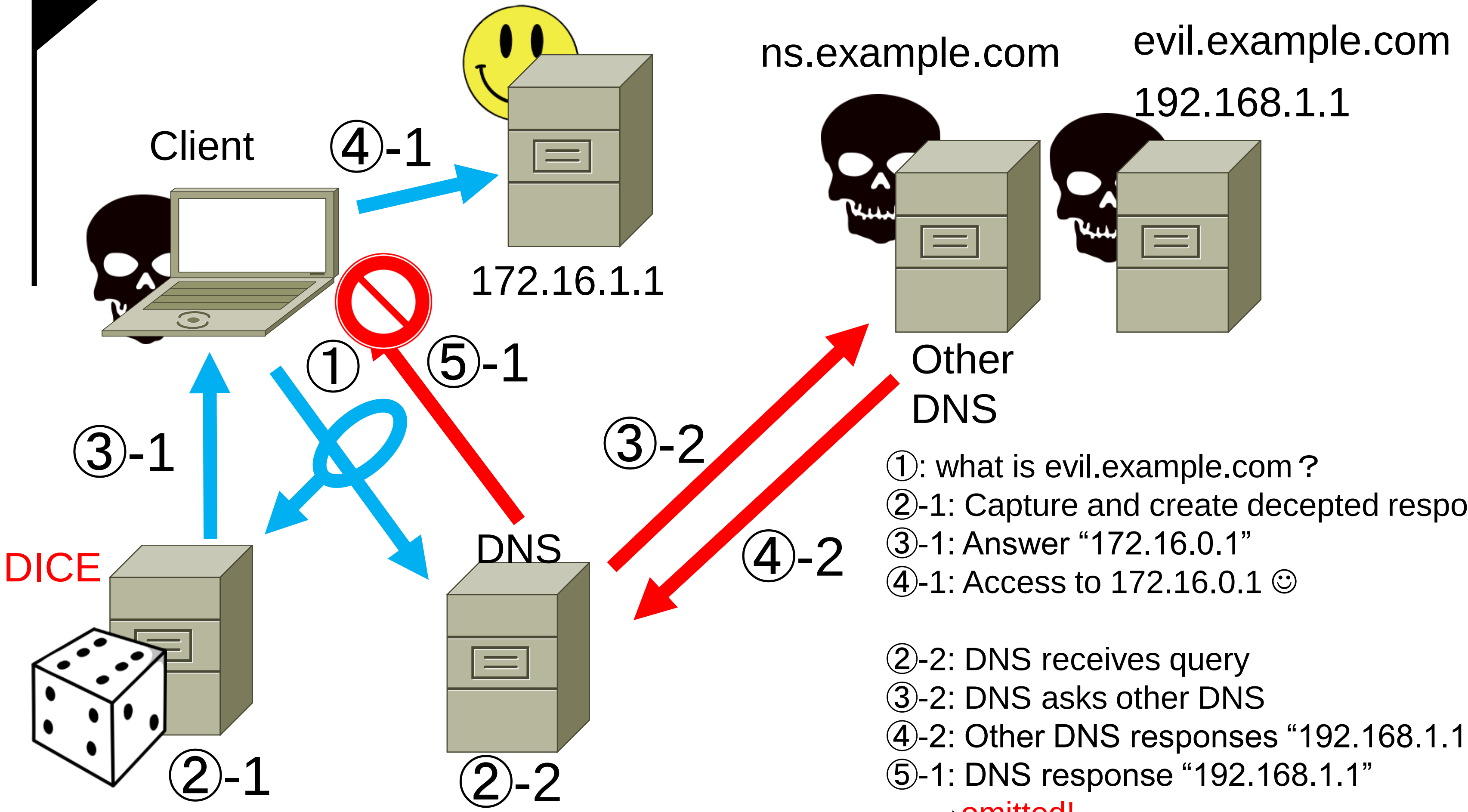
Analyze

3. Get Request ID, Source IP/PORT, Destination IP/PORT, and request content.

Response

4. Make Decepted Response Packet from information of 2
5. Send Response response to client as soon as possible!

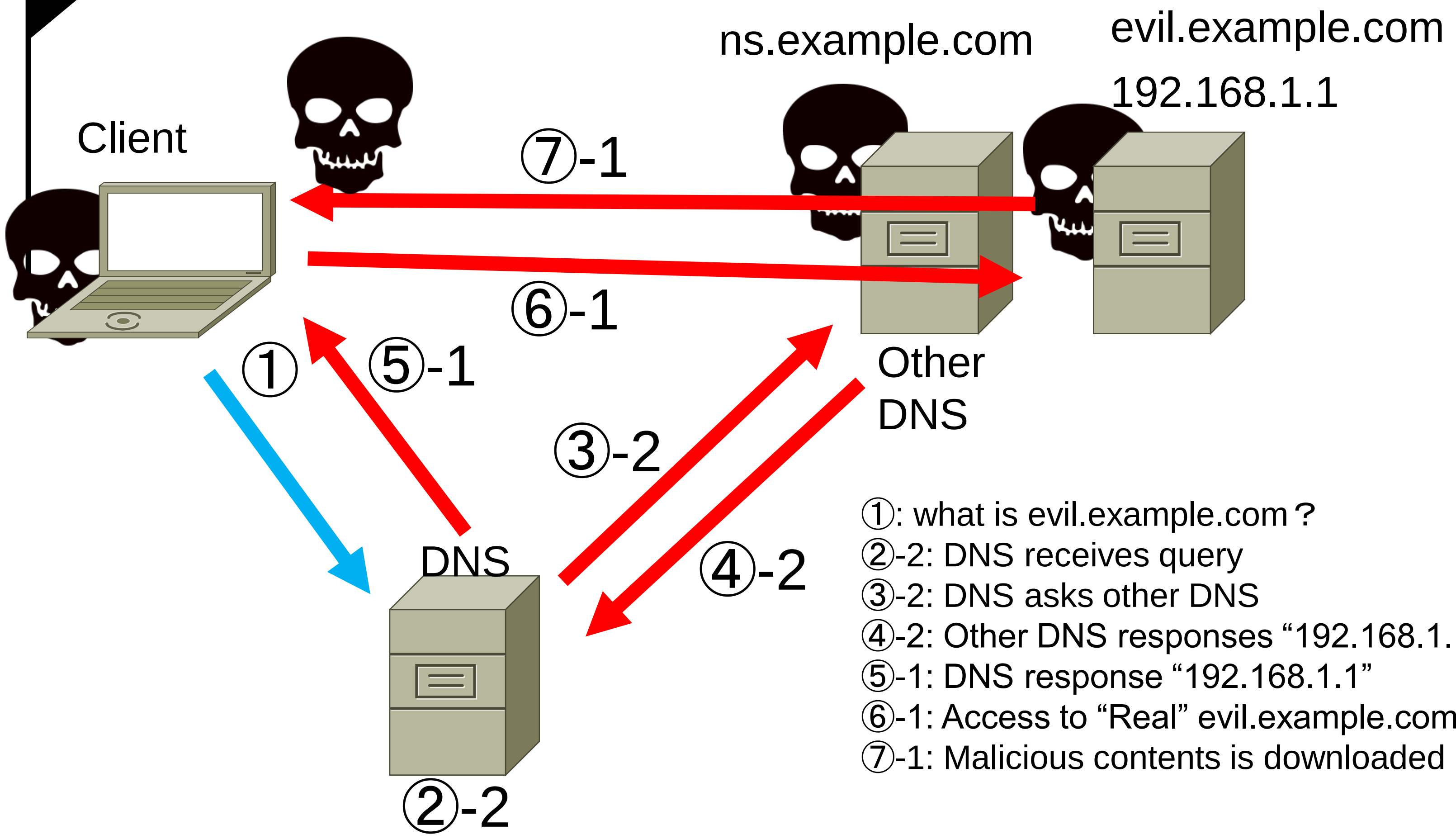
Concept Diagram



①: what is evil.example.com？
②-1: Capture and create decepted response
③-1: Answer “172.16.0.1”
④-1: Access to 172.16.0.1 ☺

②-2: DNS receives query
③-2: DNS asks other DNS
④-2: Other DNS responses “192.168.1.1”
⑤-1: DNS response “192.168.1.1”
→omitted!

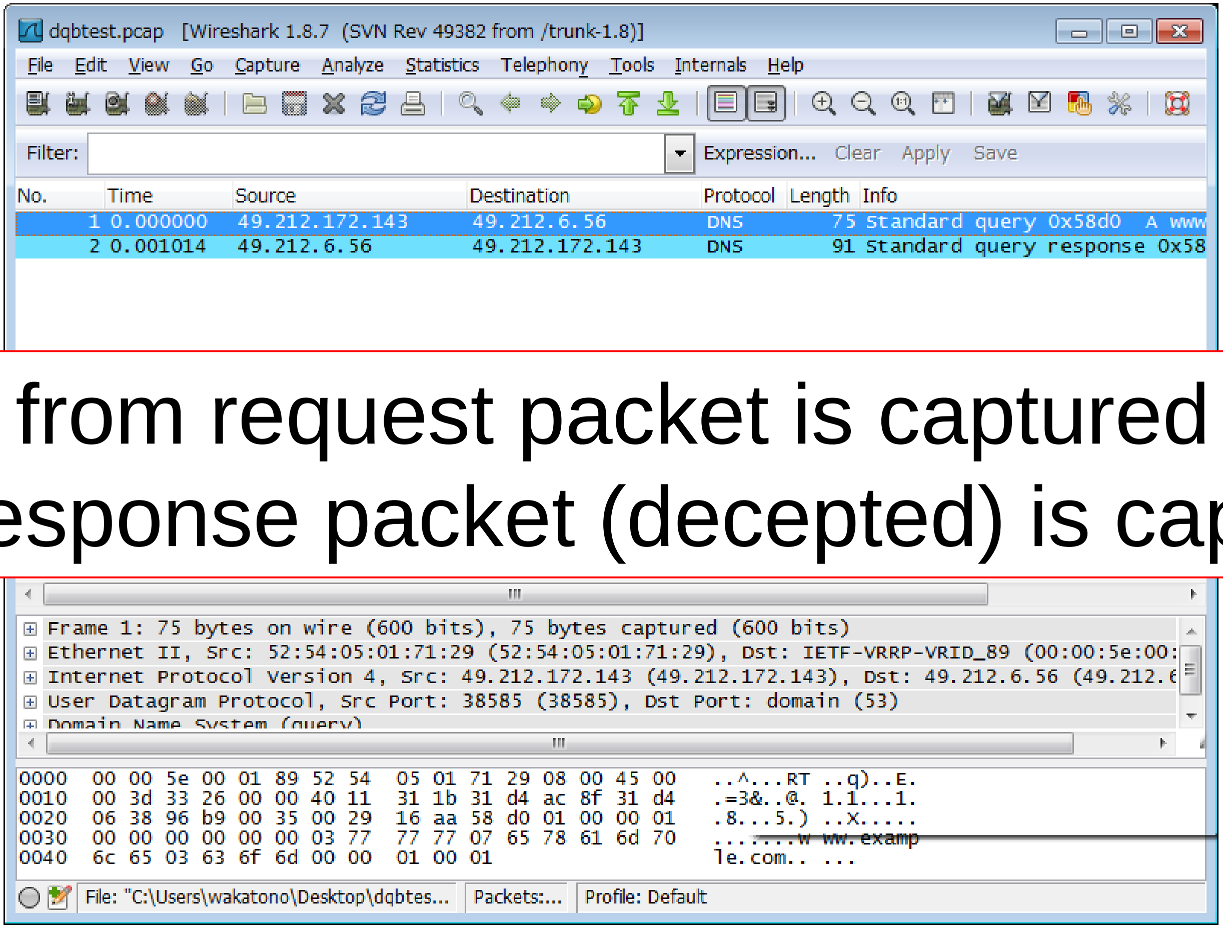
If there is not DICE…



①: what is evil.example.com？
②-2: DNS receives query
③-2: DNS asks other DNS
④-2: Other DNS responses “192.168.1.1”
⑤-1: DNS response “192.168.1.1”
⑥-1: Access to “Real” evil.example.com
⑦-1: Malicious contents is downloaded by client☹

Proof of Concept:

About
1ms



dqbtest.pcap [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

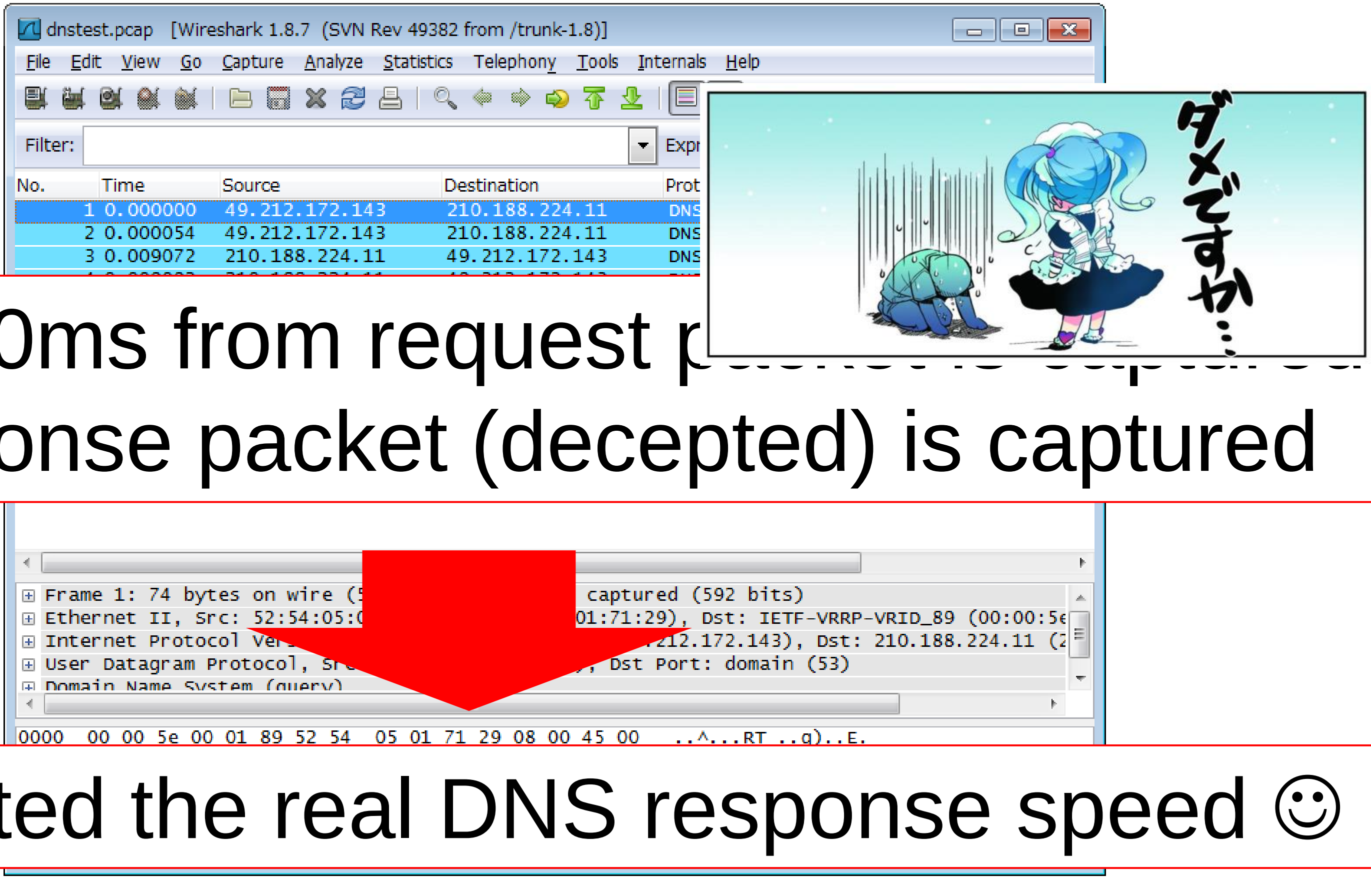
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	49.212.172.143	49.212.6.56	DNS	75	Standard query 0x58d0 A www
2	0.001014	49.212.6.56	49.212.172.143	DNS	91	Standard query response 0x58

1ms from request packet is captured
to response packet (decepted) is captured

```
⊞ Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
⊞ Ethernet II, Src: 52:54:05:01:71:29 (52:54:05:01:71:29), Dst: IETF-VRRP-VRID_89 (00:00:5e:00:
⊞ Internet Protocol Version 4, Src: 49.212.172.143 (49.212.172.143), Dst: 49.212.6.56 (49.212.6
⊞ User Datagram Protocol, Src Port: 38585 (38585), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0000   00 00 5e 00 01 89 52 54  05 01 71 29 08 00 45 00   ..^...RT ..q)..E.
0010   00 3d 33 26 00 00 40 11  31 1b 31 d4 ac 8f 31 d4   .=3&..@. 1.1...1.
0020   06 38 96 b9 00 35 00 29  16 aa 58 d0 01 00 00 01   .8...5.) ..X.....
0030   00 00 00 00 00 00 03 77  77 77 07 65 78 61 6d 70   .......w ww.examp
0040   6c 65 03 63 6f 6d 00 00  01 00 01                  le.com.. ...
```

Normal Request/Response


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expr
ダメですか…

dnstest.pcap [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

```
No.    Time        Source           Destination      Prot
     1 0.000000    49.212.172.143   210.188.224.11   DNS
     2 0.000054    49.212.172.143   210.188.224.11   DNS
     3 0.009072    210.188.224.11   49.212.172.143   DNS
```

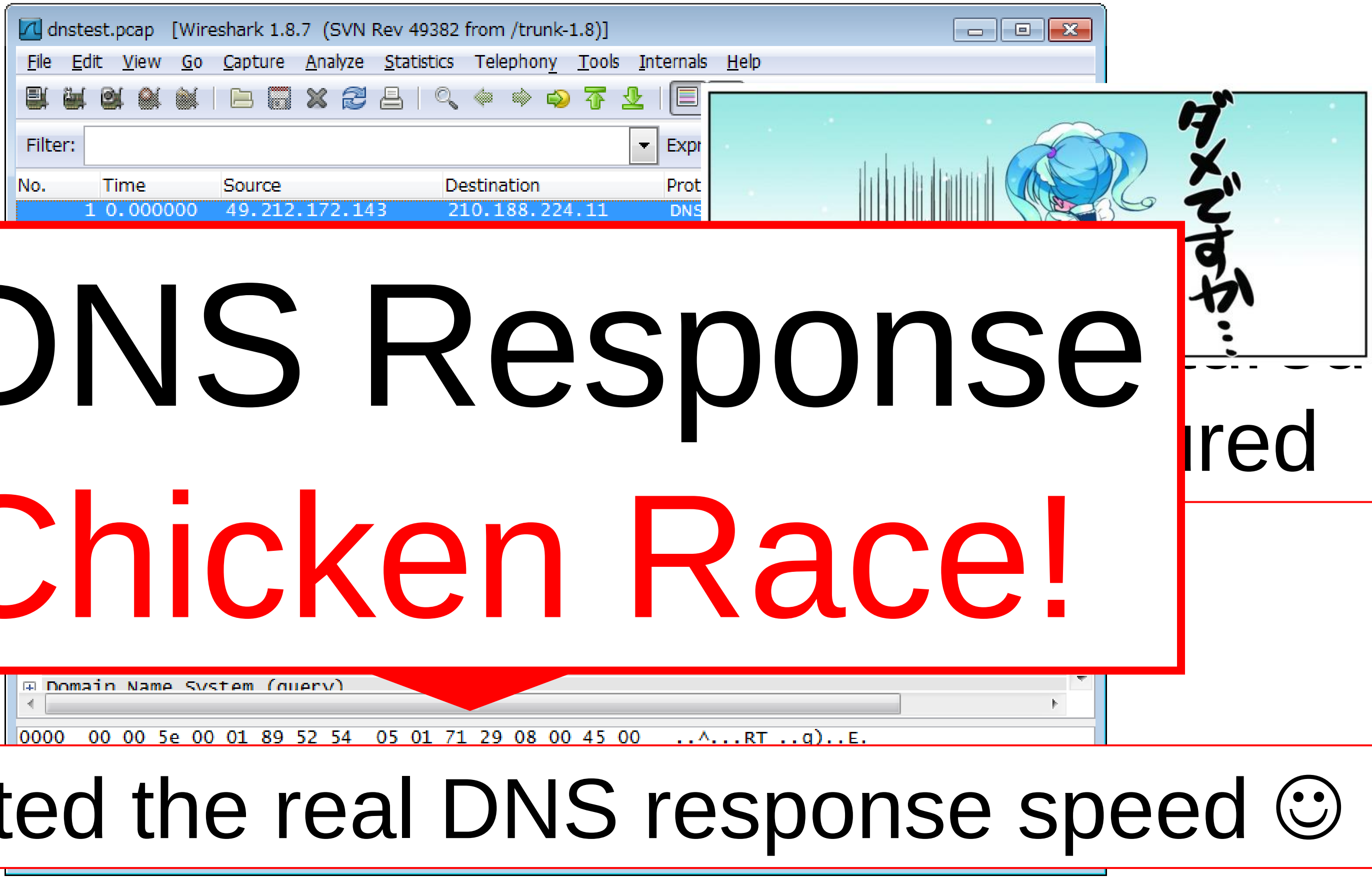
```
⊞ Frame 1: 74 bytes on wire (5            captured (592 bits)
⊞ Ethernet II, Src: 52:54:05:0           01:71:29), Dst: IETF-VRRP-VRID_89 (00:00:5e
⊞ Internet Protocol Ver                  .212.172.143), Dst: 210.188.224.11 (2
⊞ User Datagram Protocol, Sr              ), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0000   00 00 5e 00 01 89 52 54  05 01 71 29 08 00 45 00   ..^...RT ..q)..E.
```

about 10ms from request p
to response packet (decepted) is captured

I defeated the real DNS response speed ☺

Normal Request/Response



dnstest.pcap [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

No.	Time	Source	Destination	Prot
1	0.000000	49.212.172.143	210.188.224.11	DNS

```
⊞ Domain Name System (query)
0000  00 00 5e 00 01 89 52 54  05 01 71 29 08 00 45 00   ..^...RT ..q)..E.
```

about

to res ured

DNS Response

Chicken Race!

I defeated the real DNS response speed ☺

Name Resolution Step Summary Decepted by DICE

- 1. DNS Request is sent by client
- 2. Decepted DNS Response is sent to client by DICE
- 3. Real DNS Response is sent by DNS Cache

Name Resolution Step Summary Decepted by DICE

- 1. DNS Request is sent by client
- 2. Decepted DNS Response is sent to

One Request for Two Response!

- 3. Real DNS Re s sent by DNS Cache

Omitted

Real DNS response too slow?

- Slow (most case of oversea)
  - e.g. Tokyo – San Francisco
    - Round trip: 18,000km
  - Speed of Light: 300,000km/s
  - At least, about 60msec is required as a time between IP packet round trip - Traffic initiated from Tokyo to San Francisco and Response sent from San Francisco to Tokyo reaches to traffic initiator(in Tokyo)

To develop like DICE

- Use Linux Socket API（～GbE）
  - – In fact, GbE wirespeed capture is too hard for (old) Socket API(!)

- Use Intel DPDK（～10GbE）
  - – DPDK is used for various development of NW appliance
    - e.g. Lagopas (SDN Switch implementation by NTT and IIJ)

DICE Deployment principle

- 1st: Understand your network topology
- 2nd: Identify DNS server(or Server to Decept) and Gateway to internet
- 3rd: Place the appropriate DICE unit

DICE Practical Deployment in DNS

- 1st: Understand your network topology
- 2nd: Identify Top DNS “Cache” server
  - And NW Switch that DNS “Cache” Server is connected
- 3rd: Place the DICE unit near the Top DNS “Cache server”
  - And change configuration of the NW switch above.

Protocol Deception – Joyful and Useful Decepting Technology

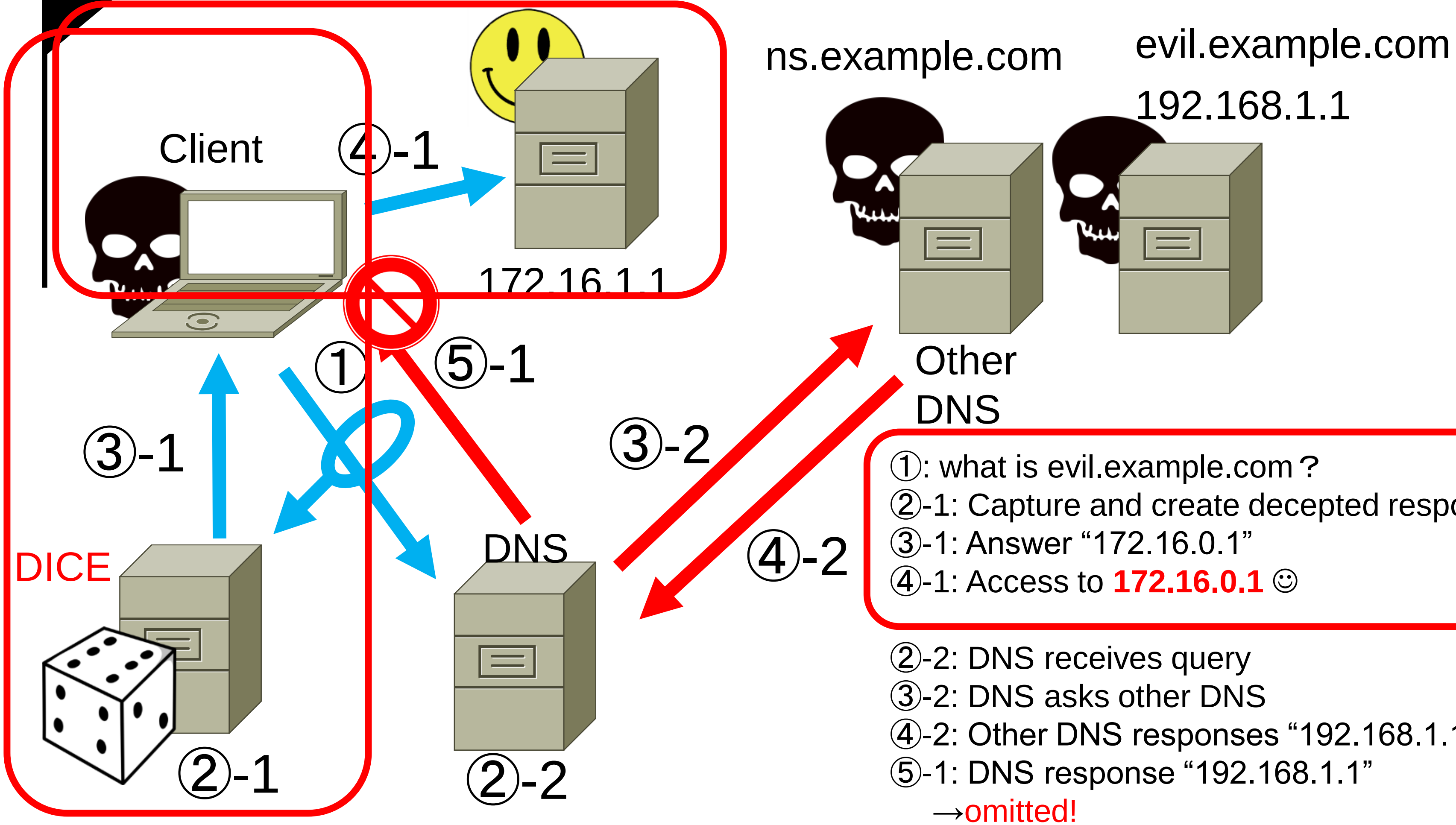
Plain Text Communications without sign can be decepted easily ☺

If DNS Response is decepted successfully…

- Connection can be intercepted as you like

- Malicious request parameter(s) can be obtained easily and effectively

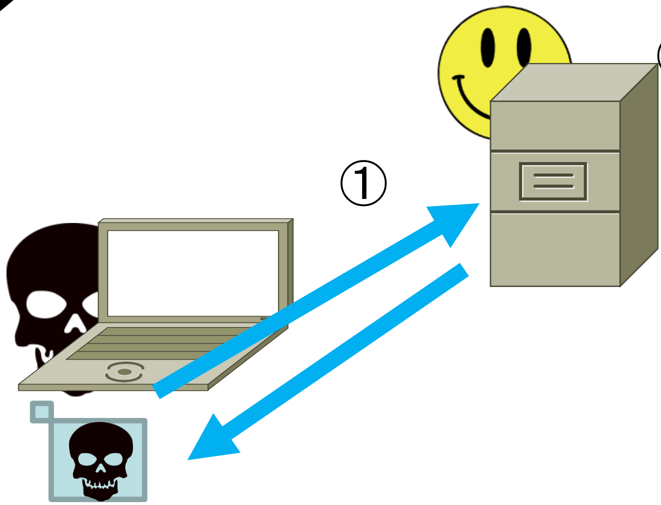
Connection can be intercepted as you like



①: what is evil.example.com？
②-1: Capture and create decepted response
③-1: Answer “172.16.0.1”
④-1: Access to **172.16.0.1** ☺

②-2: DNS receives query
③-2: DNS asks other DNS
④-2: Other DNS responses “192.168.1.1”
⑤-1: DNS response “192.168.1.1”
→omitted!

Malicious request parameter(s) can be obtained easily(1/2)



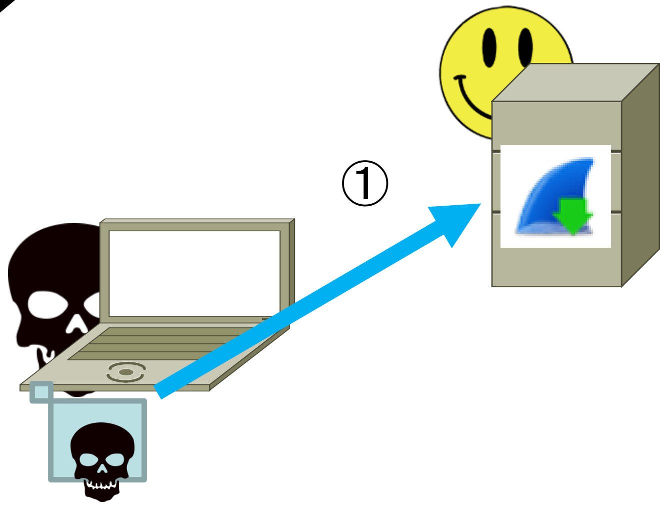
⓪ AliasMatch ^/ //var/www/html/fault.html

② logged parameter(s) is recorded in the leaded host
e.g. 172.16.0.2 - - [22/Jul/2016:13:21:24 +0900] "GET /cc.php?init=succeed&target=inhouse&..." 200 36 "-" "-"

① send request to “evil.example.com”
e.g. Access to URL
http://evil.example.com/cc.php?init=succeed&target=inhouse&...

② logged parameter(s) is recorded in the leaded host
172.16.0.2 - - [22/Jul/2016:13:21:24 +0900] "GET /cc.php?init=succeed&target=inhouse&..." 200 36 "-" "-"

Malicious request parameter(s) can be obtained easily(2/2)



⓪ AliasMatch ^/ //var/www/html/fault.html
(Apache2 configuration)

② Packet data including POST data is available

① send request to “evil.example.com” by POST method
e.g. Access to URL by POST method http://evil.example.com/cc.php
POST init=succeed, target=inhouse&...

Normally, these info are not recorded in Web Server log

②detail: Packet data including POST parameter data is available
 packet capture works always but capture really works only when malicious communication is identified effectively

DICE Applications, Issues, and future

In fact, DICE is the grand design to interfare various of communications between victims and attackers

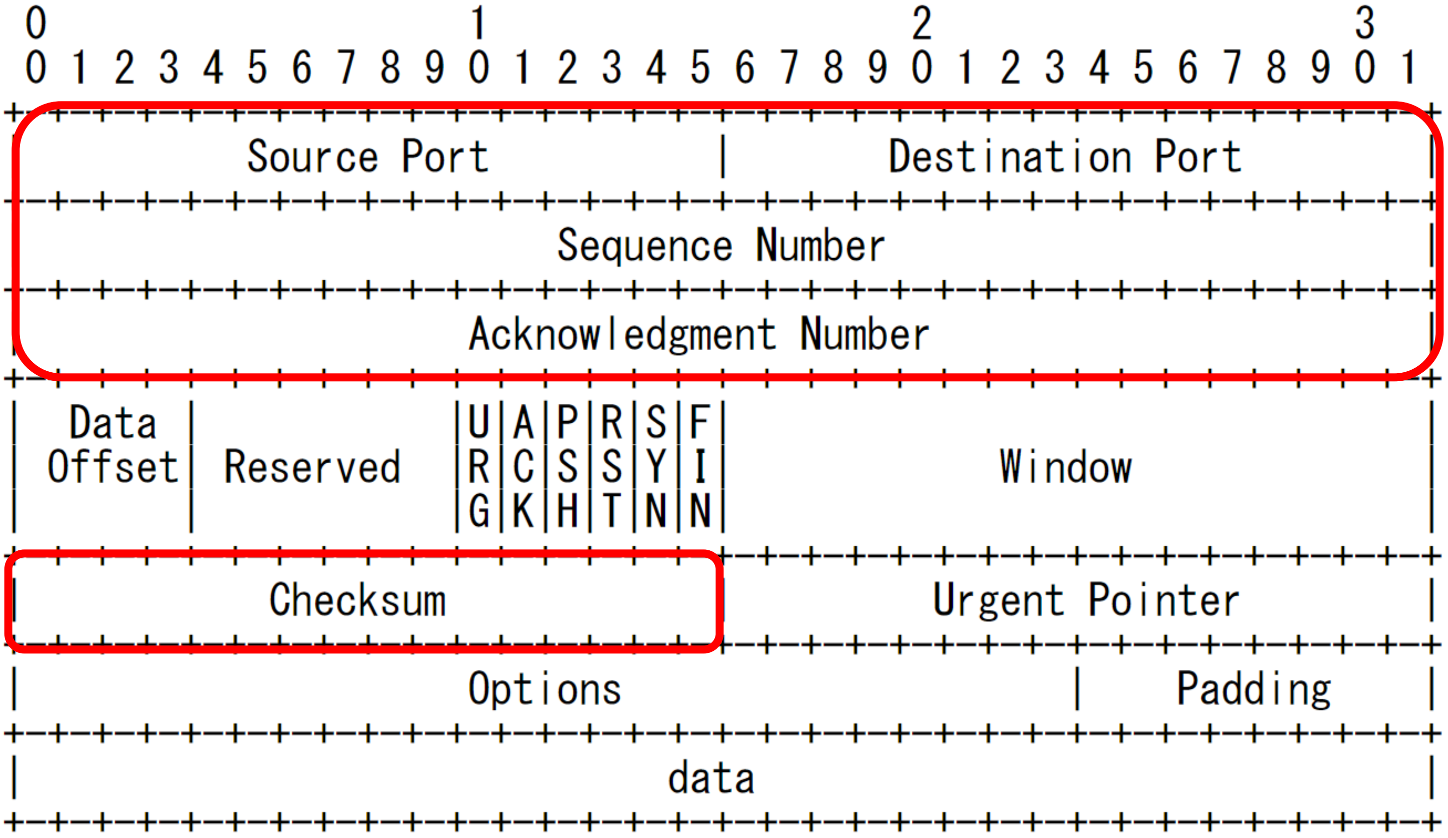
Applications:
1st step→DNS deception,
2nd step→TCP deception

TCP deception is easy to implement(except on performance)

TCP 3way handshake Response
- easily Deceptable Protocol Response

- Normal TCP Response of Connection Initiation can be decepted easily
  - – Signed and/or encrypted Packet (e.g. IPsec) is hard to be decepted.
- Applicable to various of deception
  - – After Decepted, connection is “hijacked” ☺
  - – After Connection Decepted, we can decept interaction to enemies by using Hijacked connection ☺

TCP Connection Interaction
- easily Deceptable Protocol Response



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Reference: RFC793 TRANSMISSION CONTROL PROTOCOL

I want to terminate malicious connection to specific “client(s)”

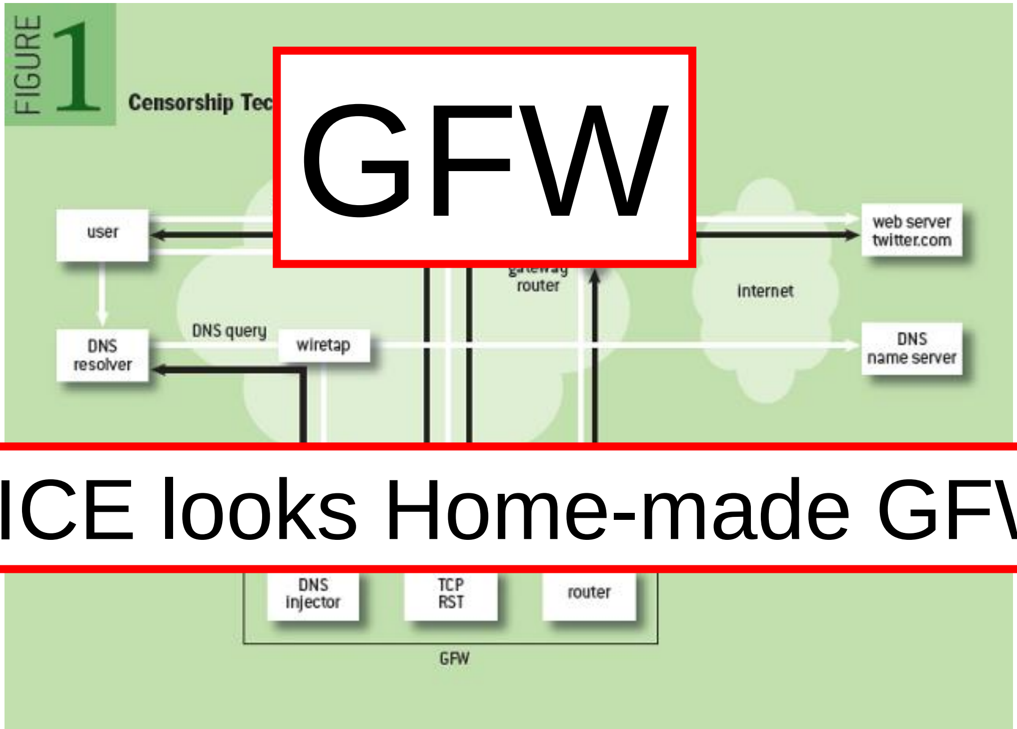
- RST packet may be filtered(and connection is still alive ☹)
  - Many IPS have function of sending RST packet(and may be filtered).

- ACK, SYN+ACK packet of Connection initiation state to proper port must not be filtered ☺
  - If filtered every packet, that computer turned to useless object ☺

Protocol Condition
Easy to Decept

- Fields to be used for relation between request and response is identified from request easily
  - In case of DNS: (Transaction) ID only
- There is “No” signed field ☺
  - Other Challenge ☹
- Fulfill the General Requirement of MITM

DICE basic concept is similar to…



GFW

DICE looks Home-made GFW

Figure From “Splinternet Behind the Great Firewall of China”
http://queue.acm.org/detail.cfm?id=2405036

Issues: Protocol Difficult to Decept

- Fields to be used for relation between request and response cannot be identified from request easily

- There is “Signed” field ☺
  - Sigh…☹

- Adaptive Payload(e.g. Result of Application Processing is included in headers and/or payloads and difficult to guess or calculate)

Copyright by wakatono

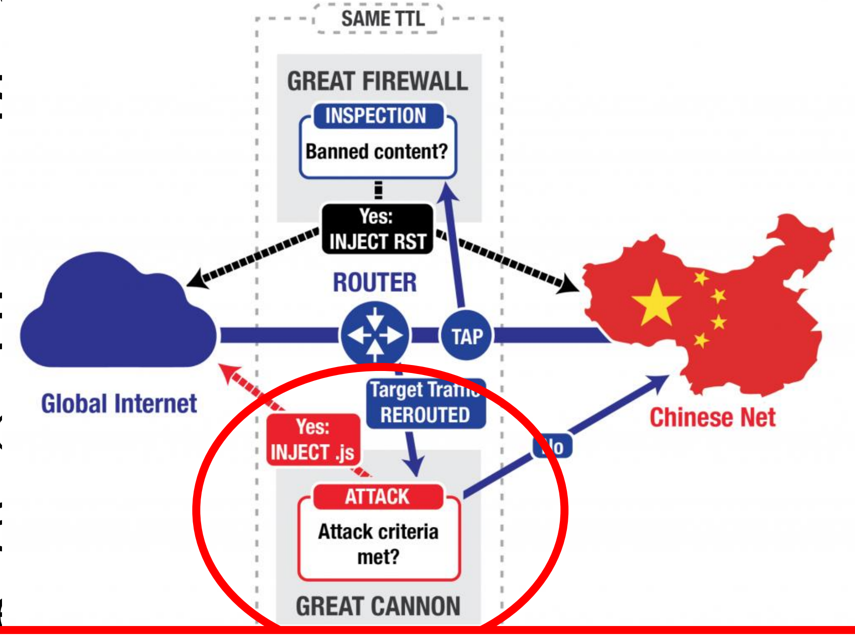
Issues: LIMITATION!

- Of course, this mechanism is not suitable for faking DNS response signed by DNSSEC mechanism.

- RFC7766 allows DNS query via TCP
  - Little a bit complex for decepting DNS response
  - RFC7766 DNS Transport over TCP - Implementation Requirements(March, 2016)
  - Fortunately, there is no implementation yet.

Issues: LIMITATION!

- Of course, this mechanism is not suitable for faking DN ꟷ NSSEC mechanis

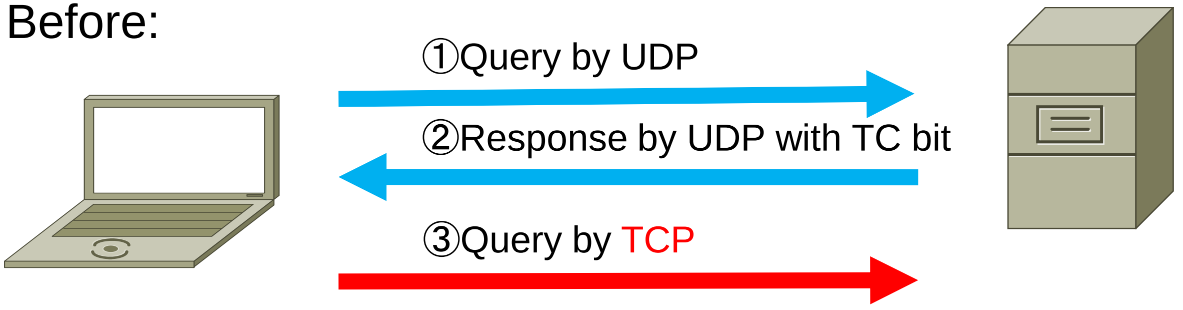


- RFC776 CP
  - Little a l S response
  - RFC776 -
    Impleme h, 2016)
  - Fortu yet.

Like a GREAT CANNON…

RFC7766 Before / After

Before:

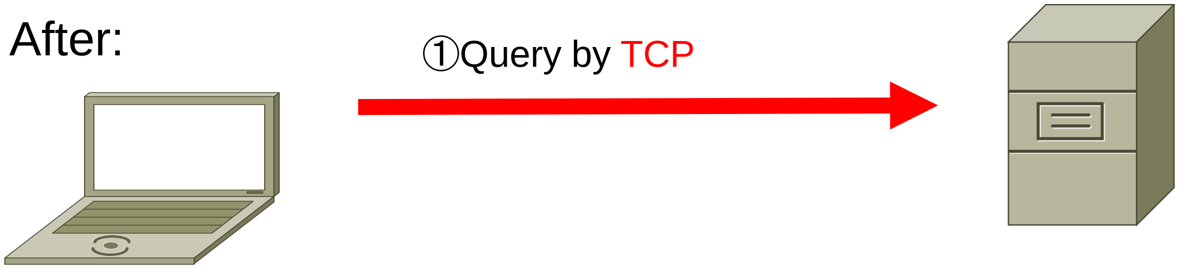


①Query by UDP

②Response by UDP with TC bit

③Query by TCP

After:



①Query by TCP

Future: Current Status of this research

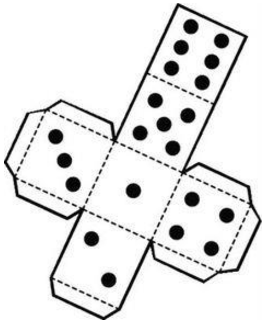
- I developed and deployed the variation of DICE
  - Malicious FQDNs find by other method(s)

- Ideas for more(for example):
  Respond by decepting response related to the request of domain name generated by DGA(Domain Generation Algorithm)

Future: DICE troubles and then stop?

- If DICE stops abnormally, no traffic can be decepted
  - These troubles don’t stop communication to outside

- DICE can be redundant by place same DICE unit to same place on network topology
  - This is effective to reduce load of each DICE unit



Conclusion

Summary of this presentation

Conclusions

- If you understand protocols, you can decept part of TCP/IP and Some Application Procotol easily
- DICE architecture is very simple(you can develop similar system(s) easily)
- Decepting Protocol makes more application to respond some kind of attacks

Thank you!

wakatono@gmail.com
@wakatono(Twitter)
https://www.facebook.com/wakatono
If possible, any questions are welcome via email or Twitter.
Of course, in banquet or any networking time ☺

Special thanks to:
My friends (they are illustrator in Japan)