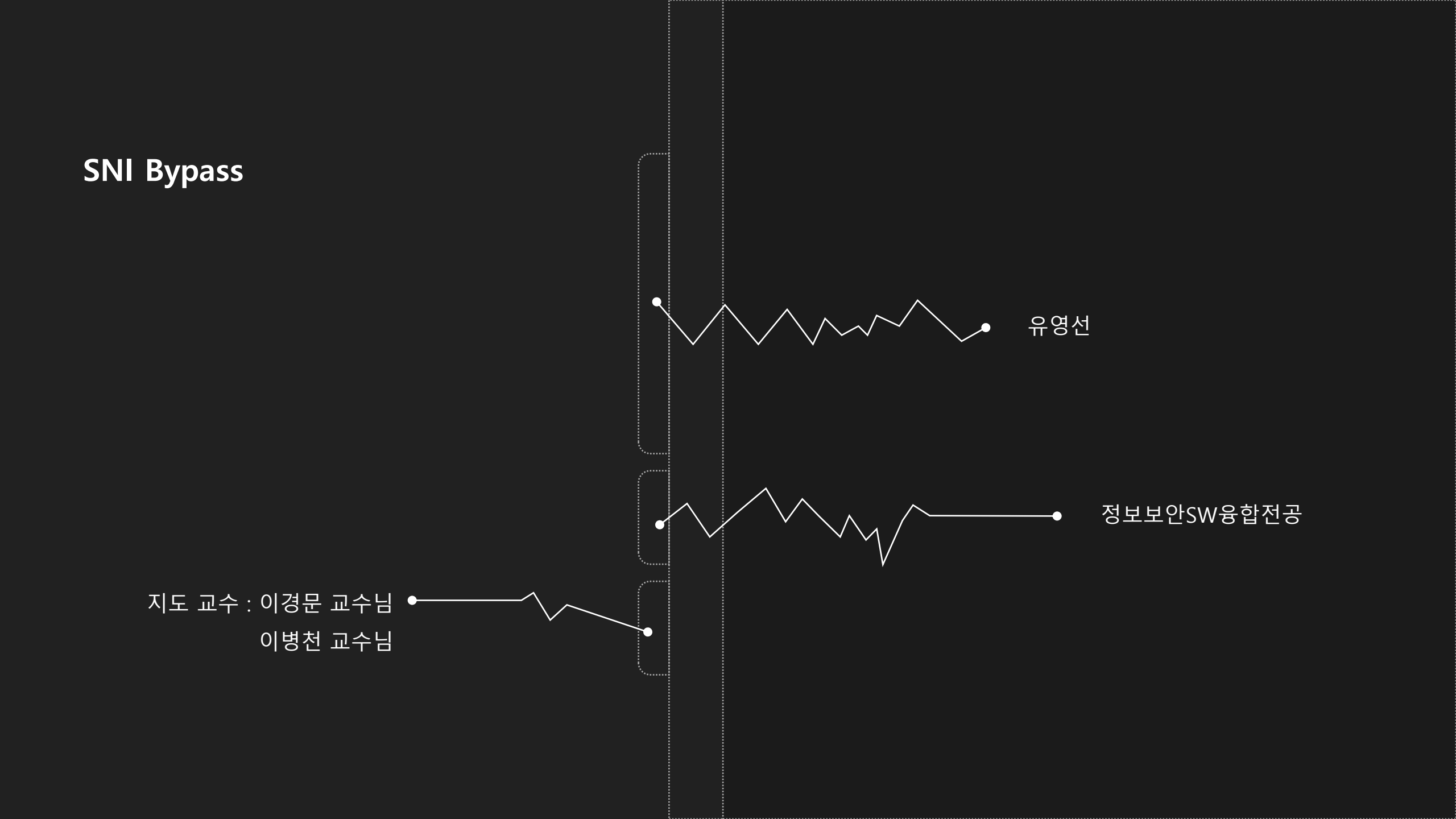
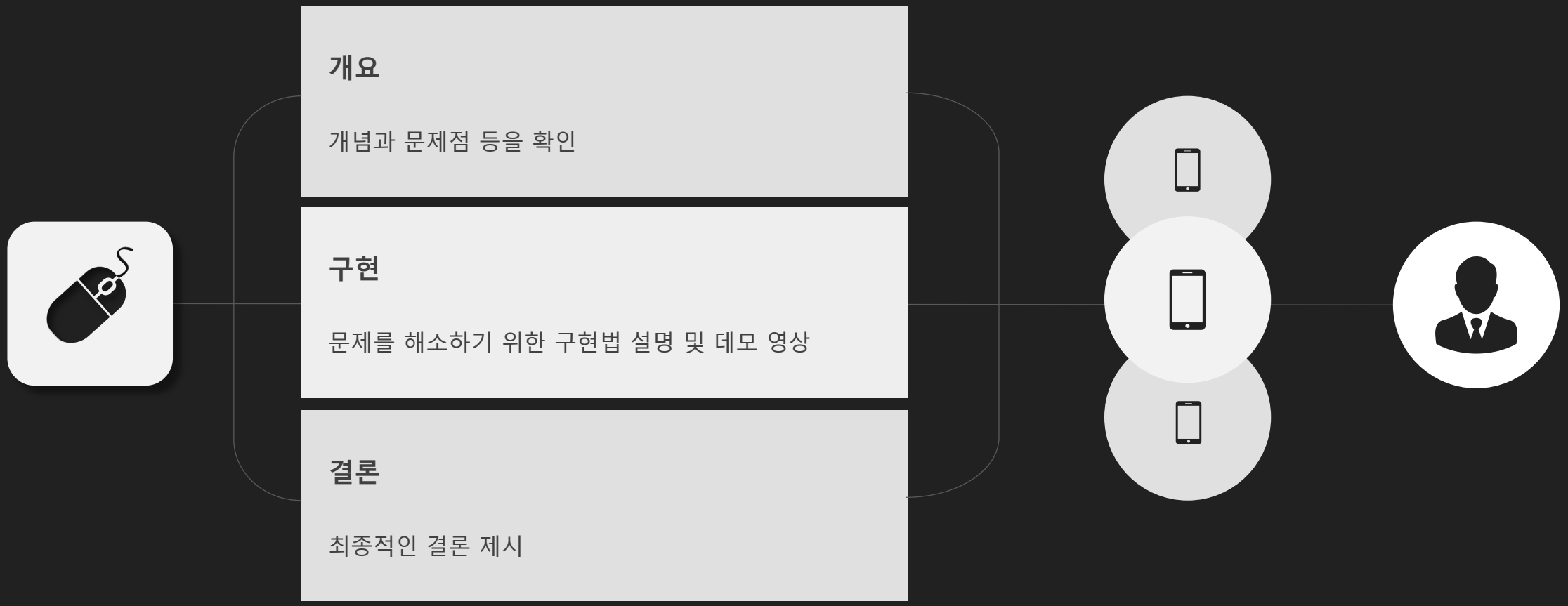
SNI Bypass



목차

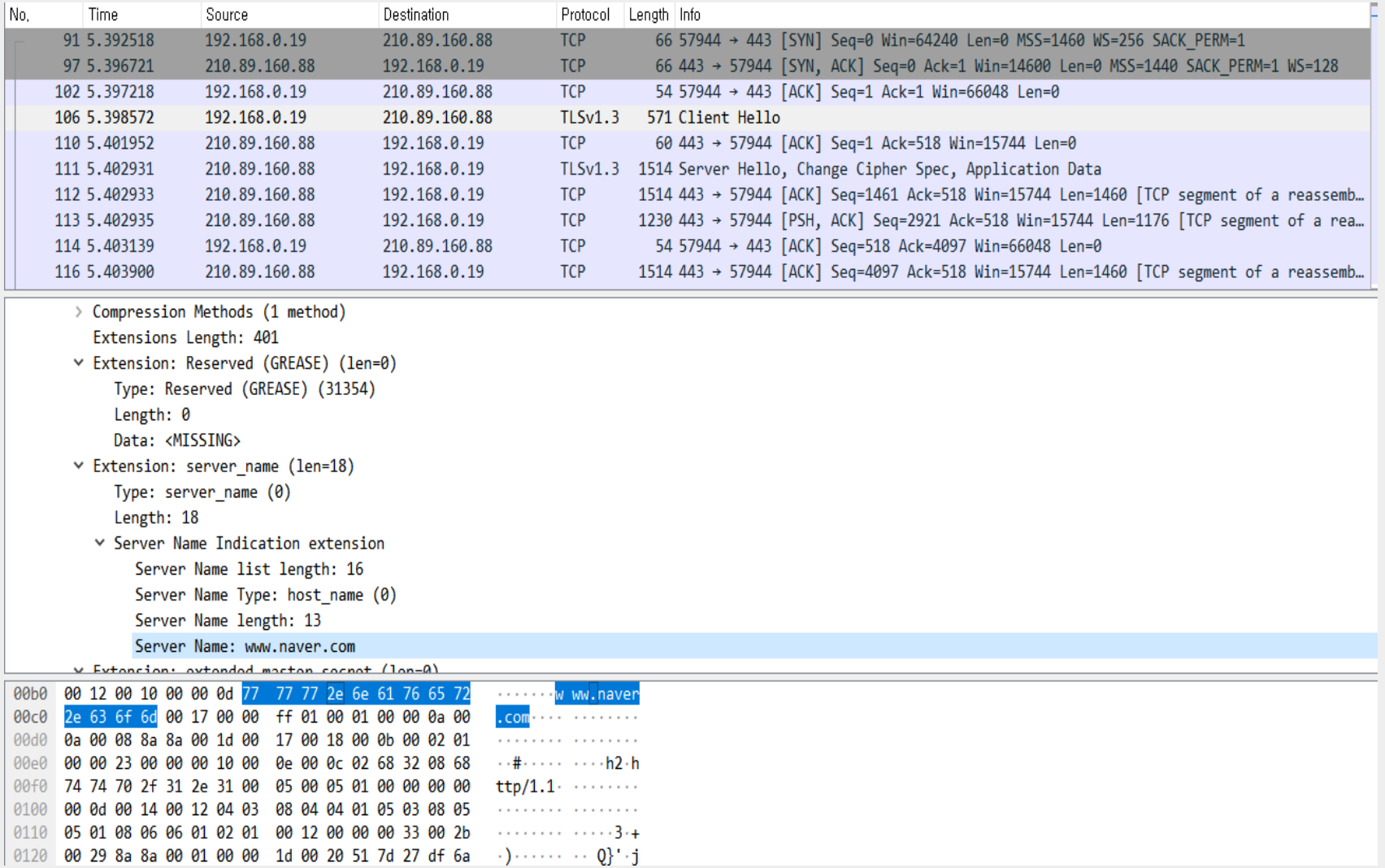


PROCESS 1

개요

SNI Field

- HTTPS 통신을 할 때 Handshake 과정 중 Client Hello 패킷의 Extension인 server_name을 가리킵니다.
- 해당 필드에 호스트 이름(Example. naver.com)이 들어갑니다.



PROCESS 1 개요

[딜라이트닷넷] 저작권보호냐, 기본권 침해냐… 도마 오른 'https' 차단

이형두 기자 2018.05.04 09:51:18

[IT전문 블로그 미디어=딜라이트닷넷] 웹툰 등 콘텐츠 불법복제물 사이트를 막기 위한 정부 정책이 도마에 올랐다. 정부가 지난 2일 기존 URL 차단방식으로 차단이 어려웠던 보안 프로토콜(https) 사이트를 SNI(Server Name Indication) 필드 차단, DNS(Domain Name System) 서버 차단 방식까지 동원해 막겠다고 밝히면서다.

반대 측은 불법사이트 규제에는 동의하지만, 중국처럼 인터넷 검열이 강화된다는 점에서 반발하고 있다. 트위터를 비롯한 각종 인터넷 커뮤니티에서는 향후 민간인 감시, 사찰 목적으로 악용돼 기본권 침해 가능성이 우려된다는 점도 지적했다. 청와대 청원 게시판에는 차단 계획을 철회하라는 내용의 게시글이 올라왔다. 3일 기준 5000명 이상이 청원에 동의했다.

진보네트워크 오병일 정책활동가는 "불법여부가 명확하지 않은 상태에서 행정기관이 해외 사이트 차단을 진행하는 것은 기본적으로 검열"이라며 "타인의 저작물이라도 공정이용범위 내에서 활용되는 경우나, 불법과 합법 콘텐츠가 공존하는 경우가 있는데도 모든 콘텐츠에 접근이 차단되는 것은 문제"라고 말했다.

이어 "결국 지적재산권이라는 것도 사적인 재산권의 하나, 권리의 균형이 필요하다"며 "이용자의 표현의 자유나 기본권도 함께 보장이 돼야하는데, 과도하게 한쪽에 치우친 정책들이 이뤄지고 있다"고 덧붙였다.

반면 찬성 측은 새 방식이 현행 방식과 원리적으로 크게 다르지 않아 기본권 침해가 가중되는 것은 아니라는 입장이다. 실제로 새 방식 역시 제3자가 서버(홈페이지)와 클라이언트(사용자) 간 통신 내용을 들여다보고 특정 사이트 접속 여부를 확인한다는 점에서 큰 결은 같다.

웹툰인사이트 이세인 대표는 "이번 정부 조치를 러시아, 중국 등지에서 이뤄지는 일괄 접속 차단과 같은 것으로 혼동해 생기는 오해"라며 "성인사이트 등에 미칠 파급력을 우려하는 것으로 추정되며, 정상적인 콘텐츠 유통에는 문제가 없다"고 일축했다.

현행 차단 방식은 ISP(Internet Service Provider)가 이용자의 일반 페이지(http) 접속 패킷을 들여다보고 분석해 차단한다. 사이트 주소가 블랙리스트와 일치하면 접속차단사이트(warning.or.kr)로 접속을 유도한다.

TOP

접속 막힌 불법사이트.. SNI 필드 차단이 뭔가요?

강일용 | 2019-02-13 | 언어 선택 | Google 번역에서 제공

[IT동아 강일용 기자] 정부가 더 강력한 불법사이트 차단 기술을 적용함에 따라 음란물, 폭력, 마약 등 불법 정보를 담은 해외 유해사이트 접근이 원천 차단됐다. 방송통신위원회는 12일 "불법음란물, 불법도박 등 불법 정보를 유통하는 해외 인터넷 사이트를 우회해서 접속하는 것을 막기위해 접속 차단 기능을 고도화했다"고 밝혔다.

11일 이후 국내 이동통신 3사를 이용 중인 사용자는 정부가 불법으로 지정한 해외 홈페이지에 접속하더라도 '연결할 수 없음'이라는 표시가 뜨게 되었다. 때문에 일각에선 표현의 자유를 위축시키고 정부가 인터넷 감청과 검열을 시도하는 것이라는 비판이 제기되고 있다.

차단에 이용된 기술은 원래 보안 취약점?

이번 접속차단에 활용된 기술은 'SNI(Server Name Indication) 필드' 차단이다. SNI는 실제 홈페이지(IP주소)는 하나이지만 여러 주소(URL)로 접속할 수 있도록 홈페이지를 구성할 때 홈페이지 보안 인증서가 사용자에게 제대로 전달되지 않는 문제를 해결하기 위해 만든 기술이다.

<TLS 1.2와 TLS 1.3의 차이점 출처:클라우드플레어>

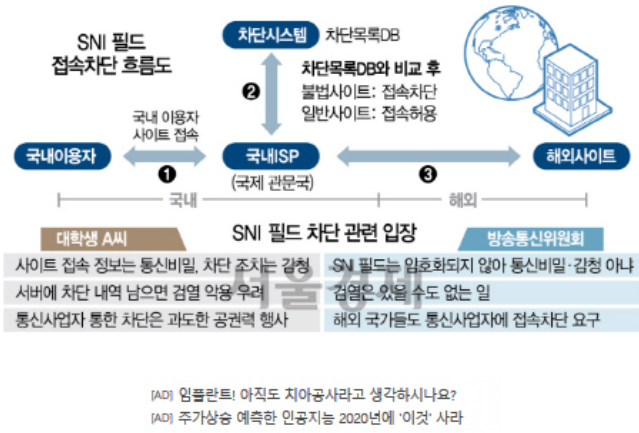
[단독]'불법사이트 차단 조치' 위헌 심판 받는다

방통위 도박·음란물 사이트 차단 조치
인터넷 감청·검열 논란 휩싸여
"이용자 접속정보 일일이 확인
침해의 최소성 차원서 과도해"
대학생 헌법소원에 심판 절차 착수
앞서 청와대 국민청원도 27만 달해

조권형 기자 2019-08-12 17:12:06 | 사회일반

인터넷 감청·검열 논란에 휩싸였던 방송통신위원회의 도박·음란물 등 해외 불법사이트 접속차단 조치가 헌법재판소의 판단을 받게 됐다. 앞서 이 조치에 반대하는 청와대 청원글이 27만여명의 동의를 받으면서 방통위원장이 소통 미숙에 대해 사과했지만 해당 조치는 철회되지 않았다.

12일 법조계에 따르면 헌법재판소는 대학생 A씨가 지난 2월11일부터 시행된 방통위의 '불법정보 유통 해외 인터넷사이트 접속차단 기능 고도화 조치'에 대해 청구한 헌법소원 심판 절차에 착수했다. 헌법재판소는 이 사건의 국선대리인으로 헌법재판관 출신인 이공현 법무법인 지평 대표변호사를 선정했다. 방통위는 이 사건과 관련해 현재에 답변서를 냈고 이에 대해 A씨가 이 대표변호사를 통해 답변서를 내는 식으로 절차가 진행되고 있다.

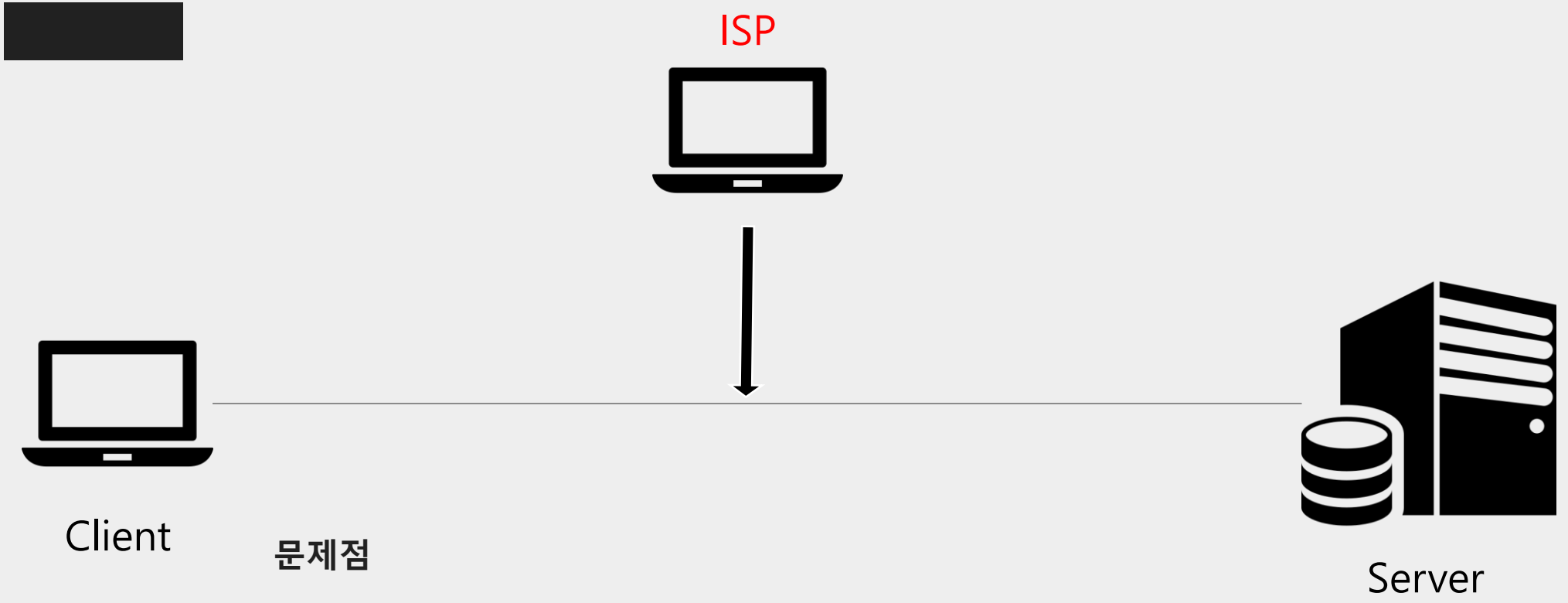


[AD] 임플란트! 아직도 치아공사라고 생각하시나요?
[AD] 주가상승 예측한 인공지능 2020년에 '이것' 사라

이번 헌법소원의 쟁점은 개인의 사이트 접속정보가 드러나는 방통위의 조치가 통신비밀 감청 등에 해당하는지 여부다. 이 헌법 소원은 방통위가 불법사이트 보안접속(https) 차단에 사용하는 '서버네임인디케이션(SNI) 필드 방식'을 겨냥하고 있다. 이 방식은 인터넷 이용자가 사이트 주소를 입력해 서버에 접속할 때 SNI 필드 영역에 노출되는 서버 네임을 이용한다. 서버 네임이 방송통신심의위원회에서 심의·의결한 불법사이트 목록과 일치하면 접속을 차단해 사이트 화면을 암전(black out) 상태로 만든다. 기존 인터넷주소(URL) 차단과 도메인네임서버(DNS) 차단을 우회하는 이용자들을 차단하려는 목적이다.

PROCESS 1

개요



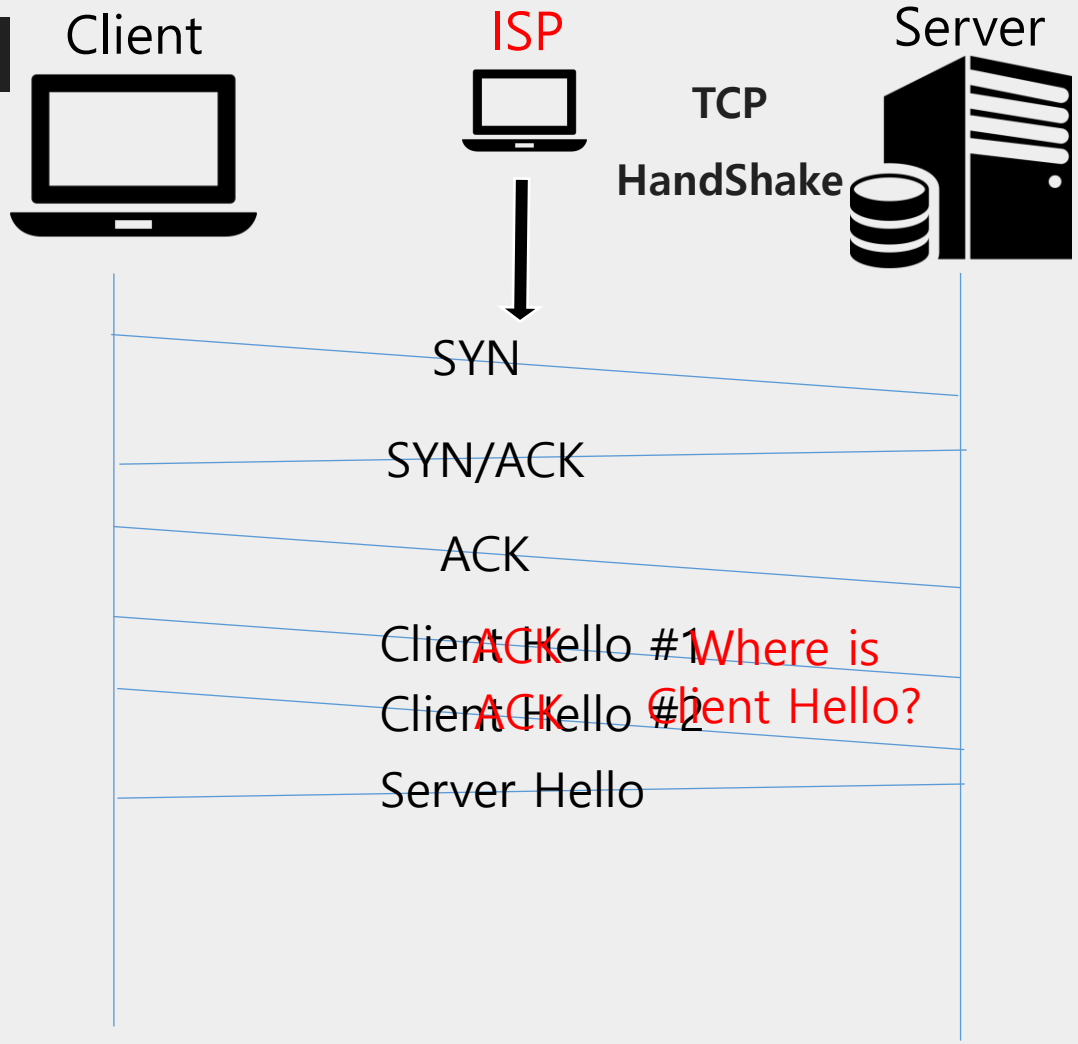
문제점

- Client와 Server 사이의 패킷을 확인해서 SNI Field를 확인후 호스트 이름을 보고 유해사이트일 경우 모두 차단합니다.

PROCESS

1

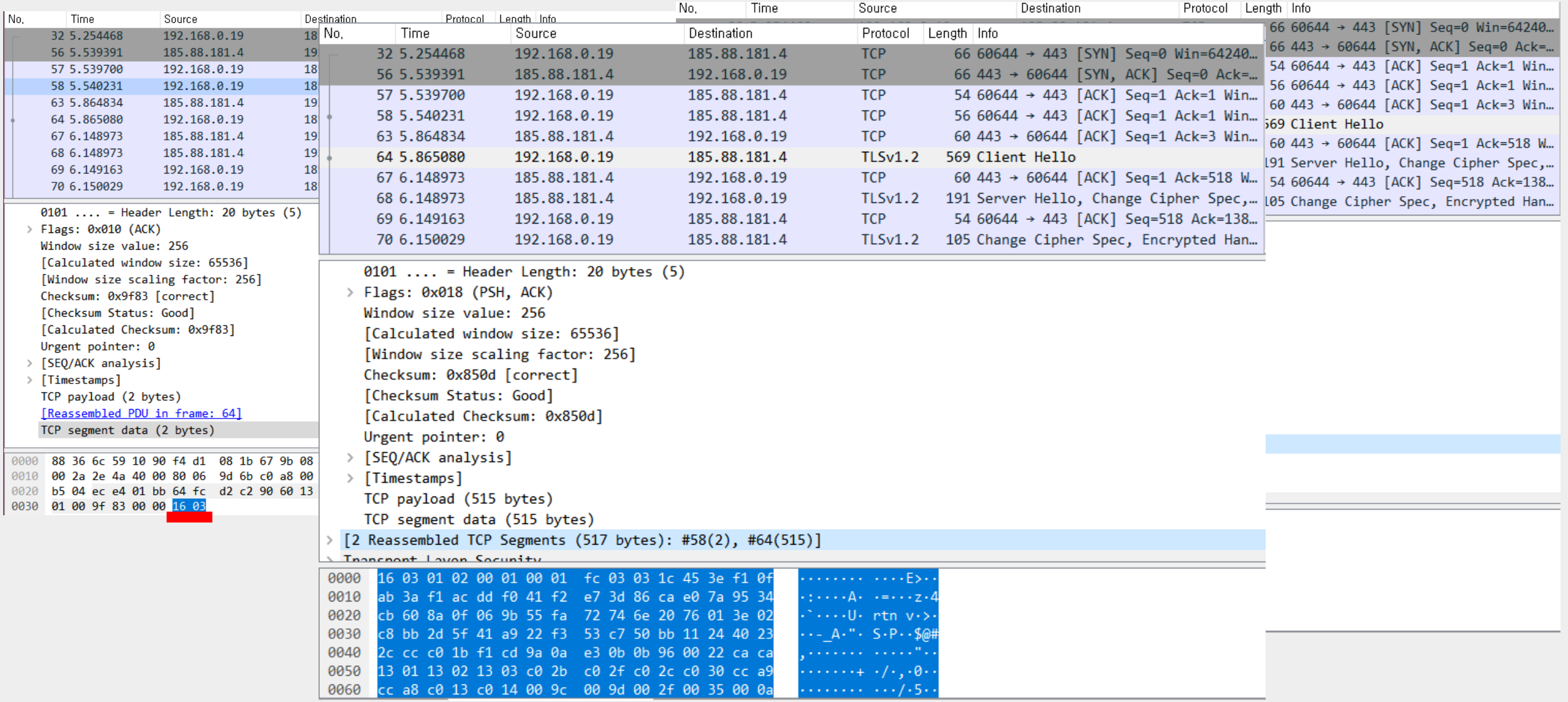
개요



SNI 차단은 SNI Field가 존재하는
Client Hello 패킷을 분할하여
전송하는 방식으로 구현되어 있으며
Sniper, GoodbyeDPI, Unicorn 등의
상용 프로그램도 같은 원리입니다.

그 중 Sniper가 Client Hello 패킷을
분할하는 모습을 소개하고자 합니다.

PROCESS 1 개요



No.	Time	Source	Destination	Protocol	Length	Info
32	5.254468	192.168.0.19	185.88.181.4	TCP	66	60644 → 443 [SYN] Seq=0 Win=64240…
56	5.539391	185.88.181.4	192.168.0.19	TCP	66	443 → 60644 [SYN, ACK] Seq=0 Ack=…
57	5.539700	192.168.0.19	185.88.181.4	TCP	54	60644 → 443 [ACK] Seq=1 Ack=1 Win…
58	5.540231	192.168.0.19	185.88.181.4	TCP	56	60644 → 443 [ACK] Seq=1 Ack=1 Win…
63	5.864834	185.88.181.4	192.168.0.19	TCP	60	443 → 60644 [ACK] Seq=1 Ack=3 Win…
64	5.865080	192.168.0.19	185.88.181.4	TLSv1.2	569	Client Hello
67	6.148973	185.88.181.4	192.168.0.19	TCP	60	443 → 60644 [ACK] Seq=1 Ack=518 W…
68	6.148973	185.88.181.4	192.168.0.19	TLSv1.2	191	Server Hello, Change Cipher Spec,…
69	6.149163	192.168.0.19	185.88.181.4	TCP	54	60644 → 443 [ACK] Seq=518 Ack=138…
70	6.150029	192.168.0.19	185.88.181.4	TLSv1.2	105	Change Cipher Spec, Encrypted Han…

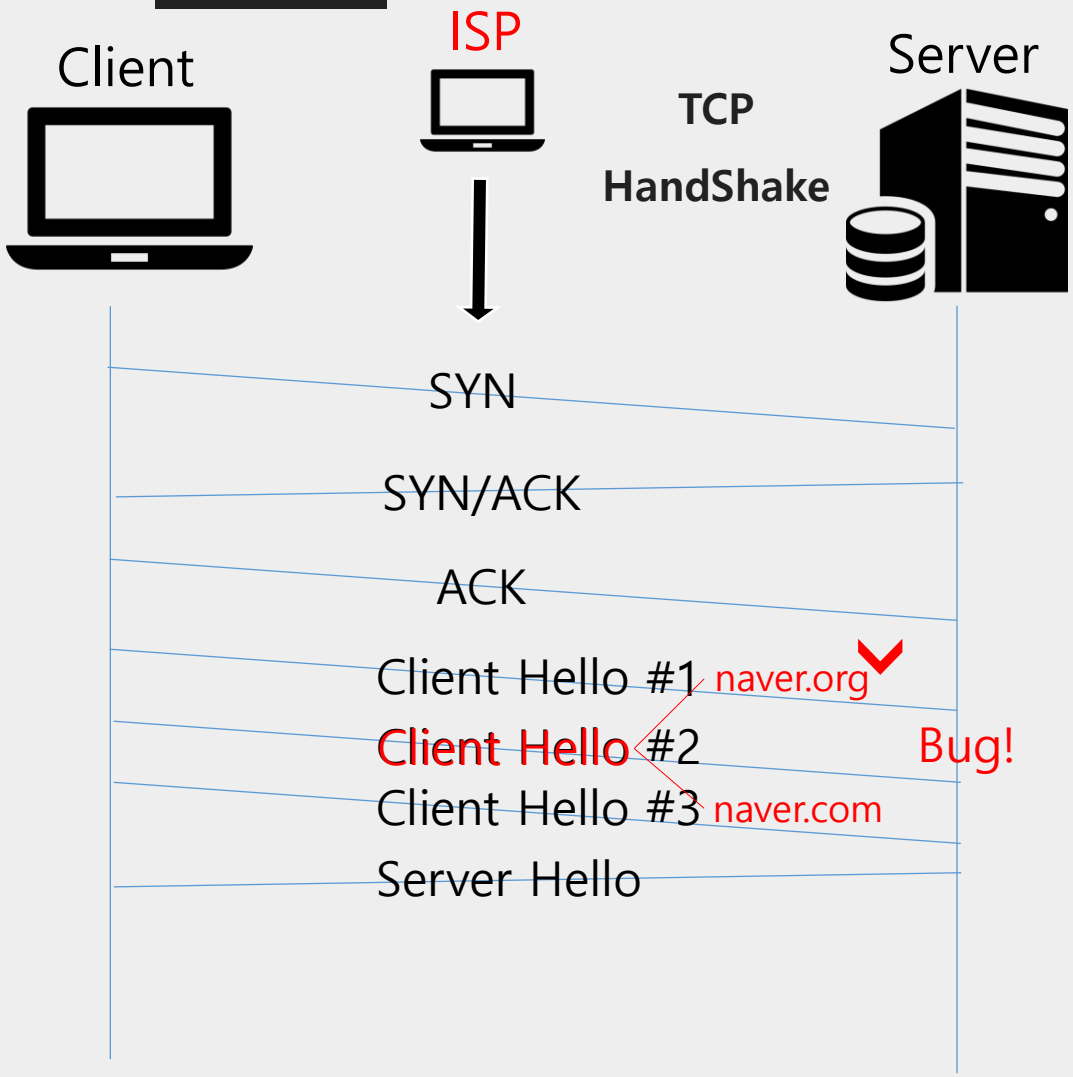
```
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0x9f83 [correct]
    [Checksum Status: Good]
    [Calculated Checksum: 0x9f83]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (2 bytes)
    [Reassembled PDU in frame: 64]
    TCP segment data (2 bytes)
```

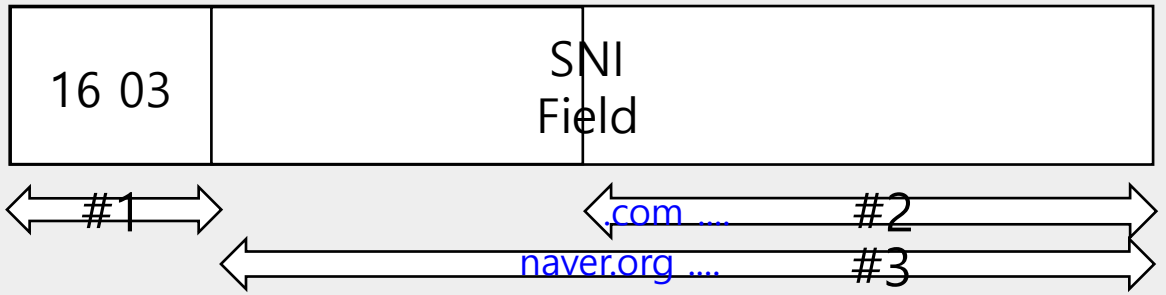
```
0000  88 36 6c 59 10 90 f4 d1  08 1b 67 9b 08
0010  00 2a 2e 4a 40 00 80 06  9d 6b c0 a8 00
0020  b5 04 ec e4 01 bb 64 fc  d2 c2 90 60 13
0030  01 00 9f 83 00 00 16 03
```

```
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0x850d [correct]
    [Checksum Status: Good]
    [Calculated Checksum: 0x850d]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (515 bytes)
    TCP segment data (515 bytes)
> [2 Reassembled TCP Segments (517 bytes): #58(2), #64(515)]
```

```
0000  16 03 01 02 00 01 00 01  fc 03 03 1c 45 3e f1 0f   ···· ···· ····E>··
0010  ab 3a f1 ac dd f0 41 f2  e7 3d 86 ca e0 7a 95 34   ·:···· A· ·=···z·4
0020  cb 60 8a 0f 06 9b 55 fa  72 74 6e 20 76 01 3e 02   ·`···· U· rtn v·>·
0030  c8 bb 2d 5f 41 a9 22 f3  53 c7 50 bb 11 24 40 23   ··-_A·"· S·P··$@#
0040  2c cc c0 1b f1 cd 9a 0a  e3 0b 0b 96 00 22 ca ca   ,····· ···· ····"··
0050  13 01 13 02 13 03 c0 2b  c0 2f c0 2c c0 30 cc a9   ·····+ ·/·,·0··
0060  cc a8 c0 13 c0 14 00 9c  00 9d 00 2f 00 35 00 0a   ···· ···· ···/·5··
```

PROCESS 2 구현

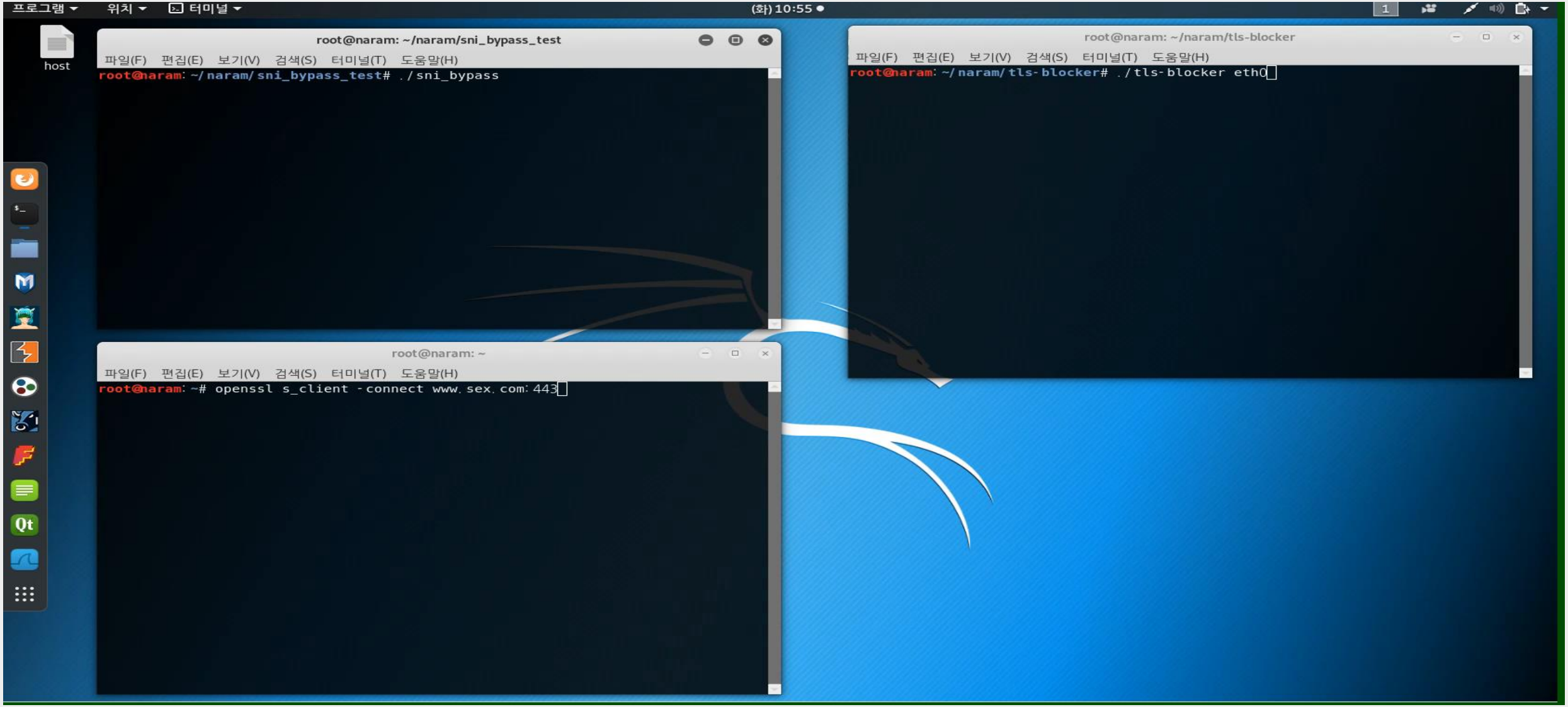




상용화된 프로그램은 #1을 보내고 #3을 보내는 방식인데 분할되는 영역을 랜덤하게 조절해서 보내는 경우도 있습니다. 프로젝트 내에서는 #1을 보내고 #2를 보낸 후 #3을 보냅니다. #2 영역이 중첩되었어도 Server는 제대로 인식합니다.

#1과 #2만 보낼 경우 Server에서 #1을 받고 #1의 다음 내용을 달라고 요청하고(ACK), 그 내용이 #3이며 전송하지 않을 경우 TCP에서 TCP Retransmission으로 #3을 전송합니다.

PROCESS 2 구현


프로그램
위치
터미널
(화) 10:55
host
root@naram: ~/naram/sni_bypass_test
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@naram: ~/naram/sni_bypass_test# ./sni_bypass
root@naram: ~/naram/tls-blocker
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@naram: ~/naram/tls-blocker# ./tls-blocker eth0
root@naram: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@naram: ~# openssl s_client -connect www.sex.com:443

PROCESS

3

결론

- TCP Payload의 중첩된 영역을 처리하지 못하는 버그를 이용한 방식입니다.
  제대로 Reassemble할 경우 해당 버그를 사용할 수 없습니다.

- Server Name Field를 확인한 후에 RST 패킷이 MITM 방식으로 들어오므로 RST 패킷을
  우회하거나 Server Name Field를 인식하지 못하는 방식으로 추가 보완이 필요합니다.

- Server Name Field가 평문이어서 생긴 문제이므로 근본적인 수정 없이
  확실한 우회는 어렵습니다. (ESNI, VPN 등의 차선책 존재)

Q&A

감사합니다