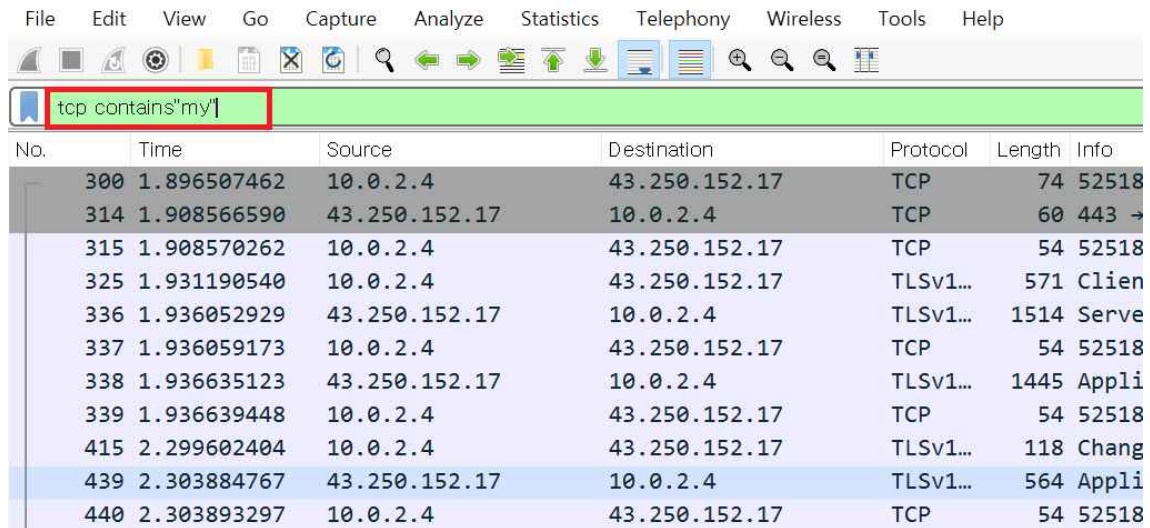


PART 1

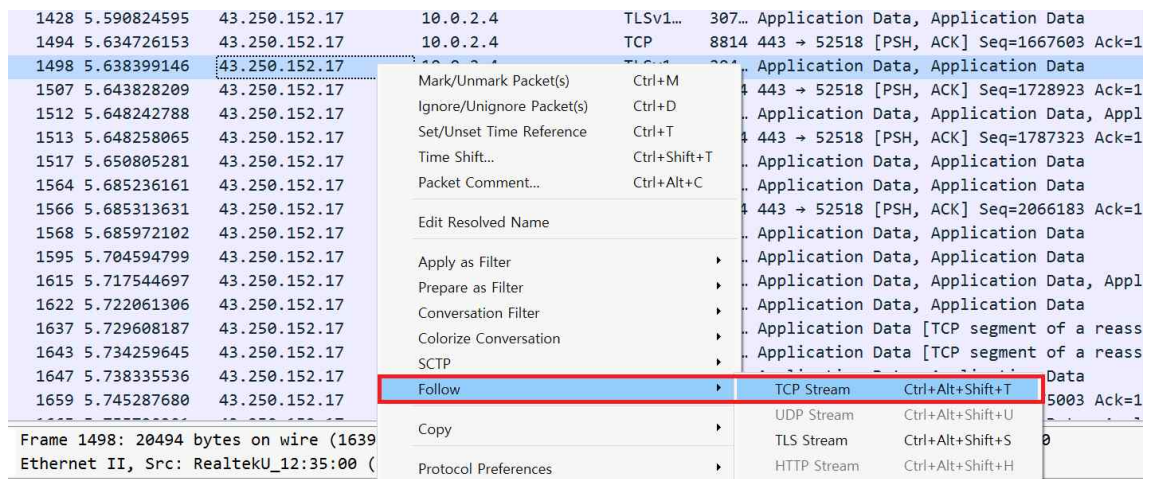
1. 패킷 분석(와이어샤크) 프로그램을 사용하여 원하는 내용이 포함된 패킷 그룹을 얻을 수 있다.



No.	Time	Source	Destination	Protocol	Length	Info
300	1.896507462	10.0.2.4	43.250.152.17	TCP	74	52518
314	1.908566590	43.250.152.17	10.0.2.4	TCP	60	443 →
315	1.908570262	10.0.2.4	43.250.152.17	TCP	54	52518
325	1.931190540	10.0.2.4	43.250.152.17	TLSv1...	571	Clie...
336	1.936052929	43.250.152.17	10.0.2.4	TLSv1...	1514	Serve...
337	1.936059173	10.0.2.4	43.250.152.17	TCP	54	52518
338	1.936635123	43.250.152.17	10.0.2.4	TLSv1...	1445	Appli...
339	1.936639448	10.0.2.4	43.250.152.17	TCP	54	52518
415	2.299602404	10.0.2.4	43.250.152.17	TLSv1...	118	Chang...
439	2.303884767	43.250.152.17	10.0.2.4	TLSv1...	564	Appli...
440	2.303893297	10.0.2.4	43.250.152.17	TCP	54	52518

(그림 1-1) contains 명령어를 사용하여 원하는 단어 “my” 를 검색할 수 있다.

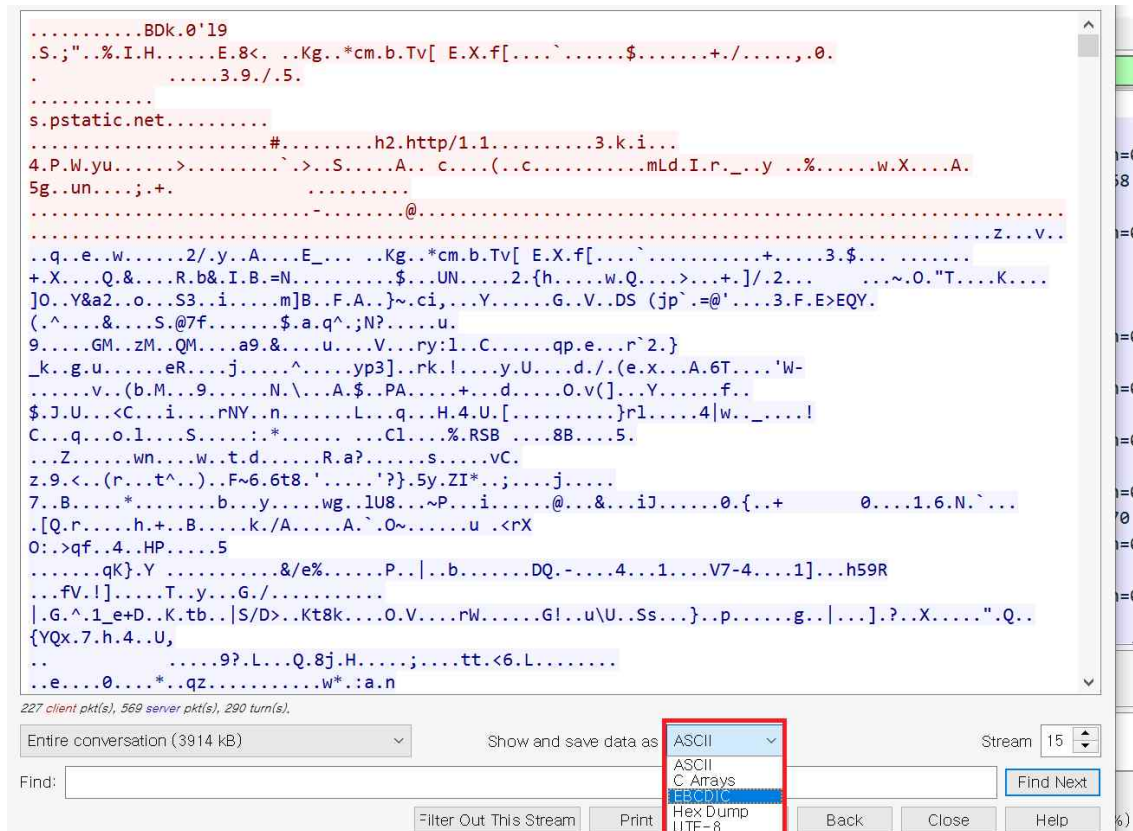
2. 관련된 패킷을 결합하여 논리적인 내용을 추출한다.



1428	5.590824595	43.250.152.17	10.0.2.4	TLSv1...	307...	Application Data, Application Data
1494	5.634726153	43.250.152.17	10.0.2.4	TCP	8814	443 → 52518 [PSH, ACK] Seq=1667603 Ack=1
1498	5.638399146	43.250.152.17	10.0.2.4	TCP	54	52518
1507	5.643828209	43.250.152.17	10.0.2.4	TCP	54	52518
1512	5.648242788	43.250.152.17	10.0.2.4	TCP	54	52518
1513	5.648258065	43.250.152.17	10.0.2.4	TCP	54	52518
1517	5.650805281	43.250.152.17	10.0.2.4	TCP	54	52518
1564	5.685236161	43.250.152.17	10.0.2.4	TCP	54	52518
1566	5.685313631	43.250.152.17	10.0.2.4	TCP	54	52518
1568	5.685972102	43.250.152.17	10.0.2.4	TCP	54	52518
1595	5.704594799	43.250.152.17	10.0.2.4	TCP	54	52518
1615	5.717544697	43.250.152.17	10.0.2.4	TCP	54	52518
1622	5.722061306	43.250.152.17	10.0.2.4	TCP	54	52518
1637	5.729608187	43.250.152.17	10.0.2.4	TCP	54	52518
1643	5.734259645	43.250.152.17	10.0.2.4	TCP	54	52518
1647	5.738335536	43.250.152.17	10.0.2.4	TCP	54	52518
1659	5.745287680	43.250.152.17	10.0.2.4	TCP	54	52518

(그림 1-2) 패킷의 내용을 볼 수 있다.

3. 추출된 내용의 의미를 파악하기 위해 다양한 인코딩을 적용해 본다.



그림(1-3) 알지 못하는 내용들이 있으므로 다른 문자로 인코딩

PART II

1. Diffie-Hellman을 통한 키 공유 절차

가. Alice는 충분히 큰 소수 p 와 적당한 g 를 하나씩 정한다.(단, $g < p$)

나. Alice는 무작위로 정수 a 를 하나 고른다. (단, $a < p$)

다. Alice는 $A = g^a \bmod p$ 를 구한다.

라. Alice는 p, g, A 를 Bob에게 전달한다.

마. Bob은 무작위로 정수 b 를 하나 고른다. (단, $b < p$)

바. Bob은 $B = g^b \bmod p$ 를 구한다.

사. Bob은 Alice에게 B 를 전달한다.

$K = (g^a)^b \bmod p = (g^b)^a \bmod p$ 임을 이용해

A 와 B 는 서로 공유하는 비밀키 K 를 가질 수 있다.

2. 간단한 예제

$p = 11$, $g = 2$ 이라고 하고 $a = 3$ 이라고 할 때

Alice의 $A = 2^3 \bmod 11$ 이므로 $A = 8$ 이다.

Bob은 Alice가 보내준 $p = 11$, $g = 2$, $A = 8$ 을 통해 B 를 구한다.($b=7$ 로 선택)

$B = 2^7 \bmod 11 = 7$ 이므로 $B = 7$ 이다.

A 는 B 한테서 7을, B 는 A 한테서 8을 받았다.

A 는 B 한테 받은 7로 계산하면 $K = 7^3 \bmod 11$ 이라는 식을 구할 수 있다.

식을 계산하면 $K = 2$ 가 된다.

B 는 A 한테 받은 8로 계산하면 $K = 8^7 \bmod 11$ 이라는 식을 구할 수 있다.

식을 계산하면 $K = 2$ 가 된다.

이러한 계산을 통해서 A 와 B 가 서로 공유하는 K 를 구할 수 있다.

3. 참고 자료

<https://tramamte.github.io/2018/07/20/diffie-hellman/>

— 블로그 Awesome Patrick