U D P D E L A Y

U D P P A C K E T D E L A Y

정보보안융합s/w
김경수

UDP Protocol

1

I N D E X

UDP Protocol

UDP는 TCP에서 제공하는 reliabile connection, seqence check 를 제공하지않는 Protocol

TCP보다 부하가 적다는 장점이 있으며 UDP사용시
위와같은 단점들에 대해 필요 시 따로 처리를 해줘야 한다.

01

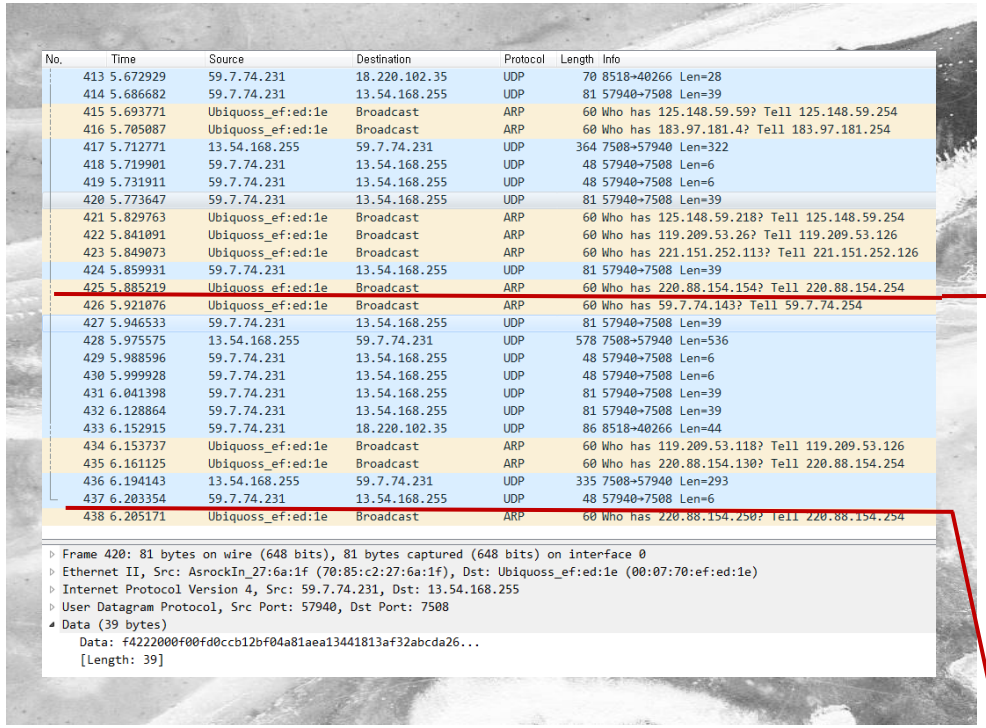
UDP 사용 이유

UDP는 TCP보다 적은 오버헤드로 빠른 속도를 제공하기
때문에 게임 조작에 대한 높은 반응성을 가진다.

때문에 FPS 같은 게임들은 높은 반응 시간을 요구하는
게임들은 패킷의 손실보다 빠른 전송을 해야 하며
때문에 UDP 로 전송할 DATA를 작성하게 된다.

01

게임내에서 패킷



No.	Time	Source	Destination	Protocol	Length	Info
413	5.672929	59.7.74.231	18.220.102.35	UDP	70	8518→40266 Len=28
414	5.686682	59.7.74.231	13.54.168.255	UDP	81	57940→7508 Len=39
415	5.693771	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 125.148.59.59? Tell 125.148.59.254
416	5.705087	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 183.97.181.4? Tell 183.97.181.254
417	5.712771	13.54.168.255	59.7.74.231	UDP	364	7508→57940 Len=322
418	5.719901	59.7.74.231	13.54.168.255	UDP	48	57940→7508 Len=6
419	5.731911	59.7.74.231	13.54.168.255	UDP	48	57940→7508 Len=6
420	5.773647	59.7.74.231	13.54.168.255	UDP	81	57940→7508 Len=39
421	5.829763	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 125.148.59.218? Tell 125.148.59.254
422	5.841091	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 119.209.53.26? Tell 119.209.53.126
423	5.849073	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 221.151.252.113? Tell 221.151.252.126
424	5.859931	59.7.74.231	13.54.168.255	UDP	81	57940→7508 Len=39
425	5.885219	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 220.88.154.154? Tell 220.88.154.254
426	5.921076	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 59.7.74.143? Tell 59.7.74.254
427	5.946533	59.7.74.231	13.54.168.255	UDP	81	57940→7508 Len=39
428	5.975575	13.54.168.255	59.7.74.231	UDP	578	7508→57940 Len=536
429	5.988596	59.7.74.231	13.54.168.255	UDP	48	57940→7508 Len=6
430	5.999928	59.7.74.231	13.54.168.255	UDP	48	57940→7508 Len=6
431	6.041398	59.7.74.231	13.54.168.255	UDP	81	57940→7508 Len=39
432	6.128864	59.7.74.231	13.54.168.255	UDP	81	57940→7508 Len=39
433	6.152915	59.7.74.231	18.220.102.35	UDP	86	8518→40266 Len=44
434	6.153737	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 119.209.53.118? Tell 119.209.53.126
435	6.161125	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 220.88.154.130? Tell 220.88.154.254
436	6.194143	13.54.168.255	59.7.74.231	UDP	335	7508→57940 Len=293
437	6.203354	59.7.74.231	13.54.168.255	UDP	48	57940→7508 Len=6
438	6.205171	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 220.88.154.250? Tell 220.88.154.254

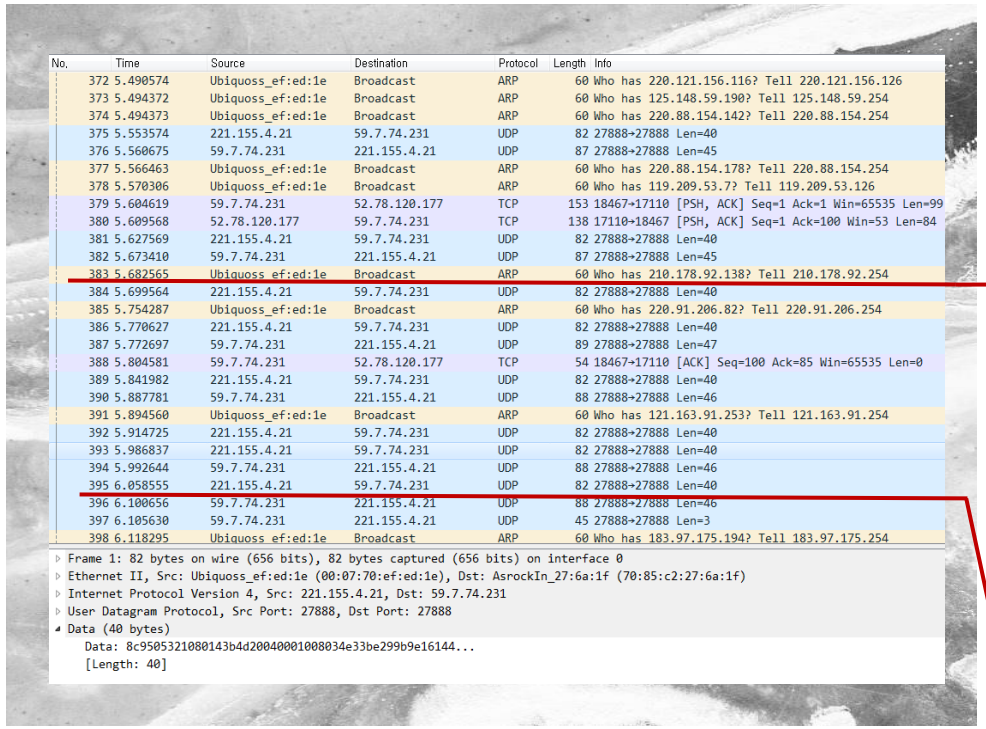
```
▷ Frame 420: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▷ Ethernet II, Src: AsrockIn_27:6a:1f (70:85:c2:27:6a:1f), Dst: Ubiquoss_ef:ed:1e (00:07:70:ef:ed:1e)
▷ Internet Protocol Version 4, Src: 59.7.74.231, Dst: 13.54.168.255
▷ User Datagram Protocol, Src Port: 57940, Dst Port: 7508
◢ Data (39 bytes)
    Data: f4222000f00fd0ccb12bf04a81aea13441813af32abcda26...
    [Length: 39]
```

Ubiquoss_ef:ed:1e	Broadcast	ARP	60 Who has 59.7.74.143? Tel
59.7.74.231	13.54.168.255	UDP	81 57940→7508 Len=39
13.54.168.255	59.7.74.231	UDP	578 7508→57940 Len=536
59.7.74.231	13.54.168.255	UDP	48 57940→7508 Len=6
59.7.74.231	13.54.168.255	UDP	48 57940→7508 Len=6
59.7.74.231	13.54.168.255	UDP	81 57940→7508 Len=39
59.7.74.231	13.54.168.255	UDP	81 57940→7508 Len=39
59.7.74.231	18.220.102.35	UDP	86 8518→40266 Len=44
Ubiquoss_ef:ed:1e	Broadcast	ARP	60 Who has 119.209.53.118?
Ubiquoss_ef:ed:1e	Broadcast	ARP	60 Who has 220.88.154.130?
13.54.168.255	59.7.74.231	UDP	335 7508→57940 Len=293
59.7.74.231	13.54.168.255	UDP	48 57940→7508 Len=6

배틀 그라운드

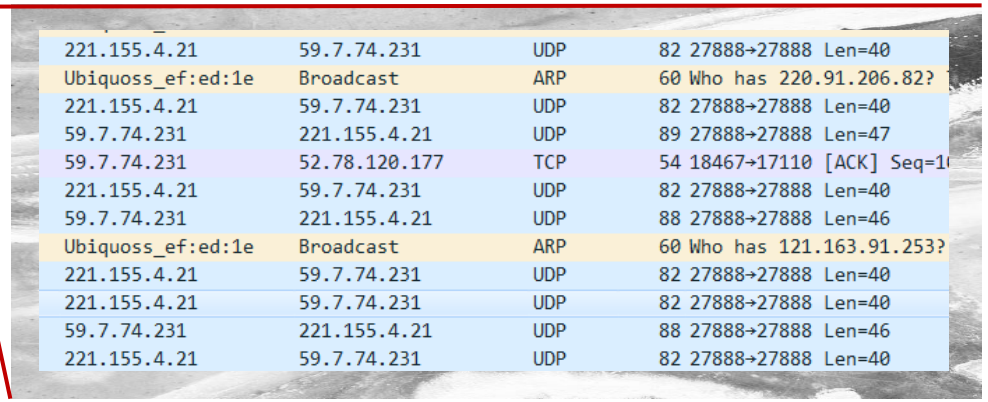
01

게임내에서 패킷



No.	Time	Source	Destination	Protocol	Length	Info
372	5.490574	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 220.121.156.116? Tell 220.121.156.126
373	5.494372	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 125.148.59.190? Tell 125.148.59.254
374	5.494373	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 220.88.154.142? Tell 220.88.154.254
375	5.553574	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
376	5.560675	59.7.74.231	221.155.4.21	UDP	87	27888→27888 Len=45
377	5.566463	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 220.88.154.178? Tell 220.88.154.254
378	5.570306	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 119.209.53.7? Tell 119.209.53.126
379	5.604619	59.7.74.231	52.78.120.177	TCP	153	18467→17110 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=99
380	5.609568	52.78.120.177	59.7.74.231	TCP	138	17110→18467 [PSH, ACK] Seq=1 Ack=100 Win=53 Len=84
381	5.627569	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
382	5.673410	59.7.74.231	221.155.4.21	UDP	87	27888→27888 Len=45
383	5.682565	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 210.178.92.138? Tell 210.178.92.254
384	5.699564	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
385	5.754287	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 220.91.206.82? Tell 220.91.206.254
386	5.770627	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
387	5.772697	59.7.74.231	221.155.4.21	UDP	89	27888→27888 Len=47
388	5.804581	59.7.74.231	52.78.120.177	TCP	54	18467→17110 [ACK] Seq=100 Ack=85 Win=65535 Len=0
389	5.841982	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
390	5.887781	59.7.74.231	221.155.4.21	UDP	88	27888→27888 Len=46
391	5.894560	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 121.163.91.253? Tell 121.163.91.254
392	5.914725	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
393	5.986837	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
394	5.992644	59.7.74.231	221.155.4.21	UDP	88	27888→27888 Len=46
395	6.058555	221.155.4.21	59.7.74.231	UDP	82	27888→27888 Len=40
396	6.100656	59.7.74.231	221.155.4.21	UDP	88	27888→27888 Len=46
397	6.105630	59.7.74.231	221.155.4.21	UDP	45	27888→27888 Len=3
398	6.118295	Ubiquoss_ef:ed:1e	Broadcast	ARP	60	Who has 183.97.175.194? Tell 183.97.175.254

```
▷ Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▷ Ethernet II, Src: Ubiquoss_ef:ed:1e (00:07:70:ef:ed:1e), Dst: AsrockIn_27:6a:1f (70:85:c2:27:6a:1f)
▷ Internet Protocol Version 4, Src: 221.155.4.21, Dst: 59.7.74.231
▷ User Datagram Protocol, Src Port: 27888, Dst Port: 27888
◢ Data (40 bytes)
    Data: 8c9505321080143b4d20040001008034e33be299b9e16144...
    [Length: 40]
```



221.155.4.21	59.7.74.231	UDP	82 27888→27888 Len=40
Ubiquoss_ef:ed:1e	Broadcast	ARP	60 Who has 220.91.206.82?
221.155.4.21	59.7.74.231	UDP	82 27888→27888 Len=40
59.7.74.231	221.155.4.21	UDP	89 27888→27888 Len=47
59.7.74.231	52.78.120.177	TCP	54 18467→17110 [ACK] Seq=1
221.155.4.21	59.7.74.231	UDP	82 27888→27888 Len=40
59.7.74.231	221.155.4.21	UDP	88 27888→27888 Len=46
Ubiquoss_ef:ed:1e	Broadcast	ARP	60 Who has 121.163.91.253?
221.155.4.21	59.7.74.231	UDP	82 27888→27888 Len=40
221.155.4.21	59.7.74.231	UDP	82 27888→27888 Len=40
59.7.74.231	221.155.4.21	UDP	88 27888→27888 Len=46
221.155.4.21	59.7.74.231	UDP	82 27888→27888 Len=40

서든 어택

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

INDEX

응답 지연 현상

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

02

지연 현상의 원인

데이터 전송시 연결을 맺고 있는 유저나 서버에게 정보를 요청하고 받는 응답시간이 길어지는 경우가 생깁니다.

원인으로는 회선의 트래픽 문제, 라우팅 경로 문제 등이 있습니다.

02

지연 현상의 결과

데이터의 응답이 지연될수록 정보를 수신하고,
받은 데이터를 기준으로 상태를 갱신을 하는 속도가
느려지게 됩니다.

브라우저창을 통해 인터넷 접속이 느려지거나,
로그인 속도가 느려지는 현상등을 확인할 수 있습니다.

3

UDP Delay

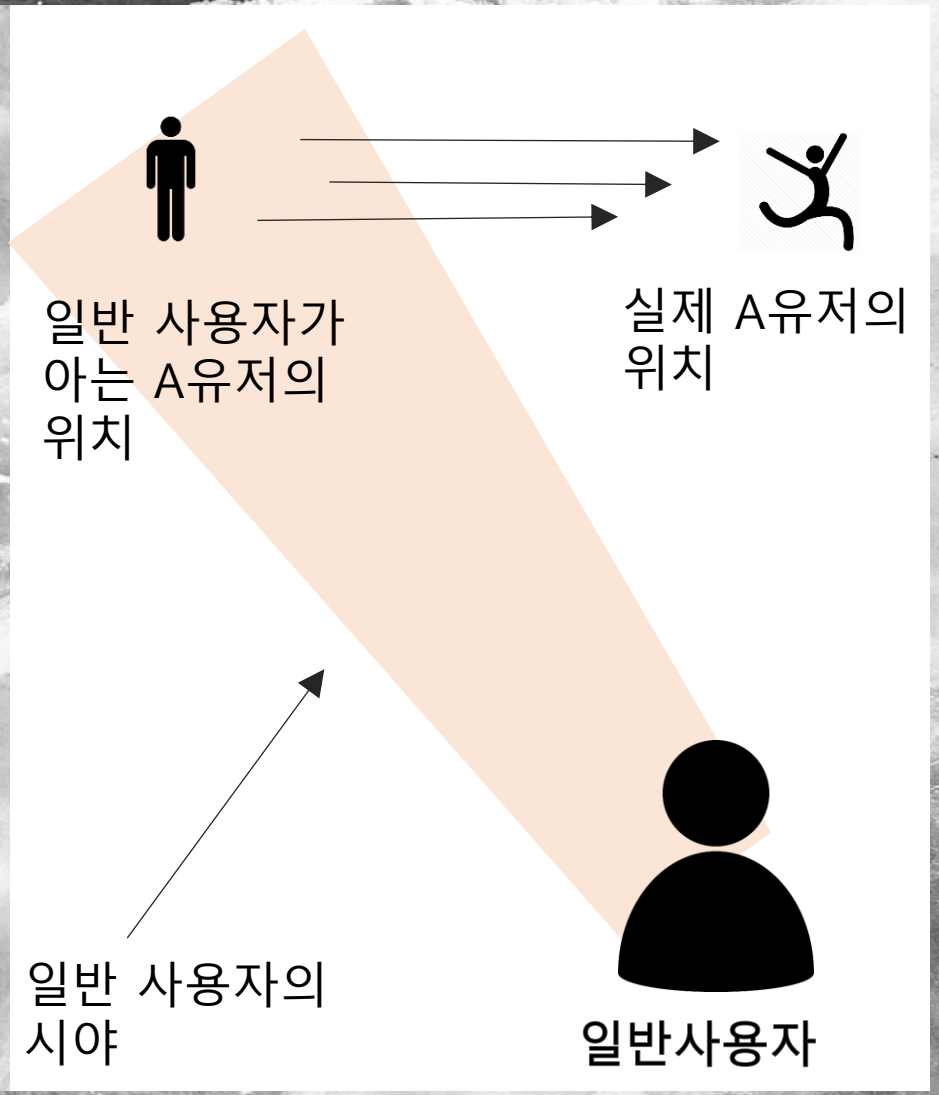
I N D E X

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

UDP Delay

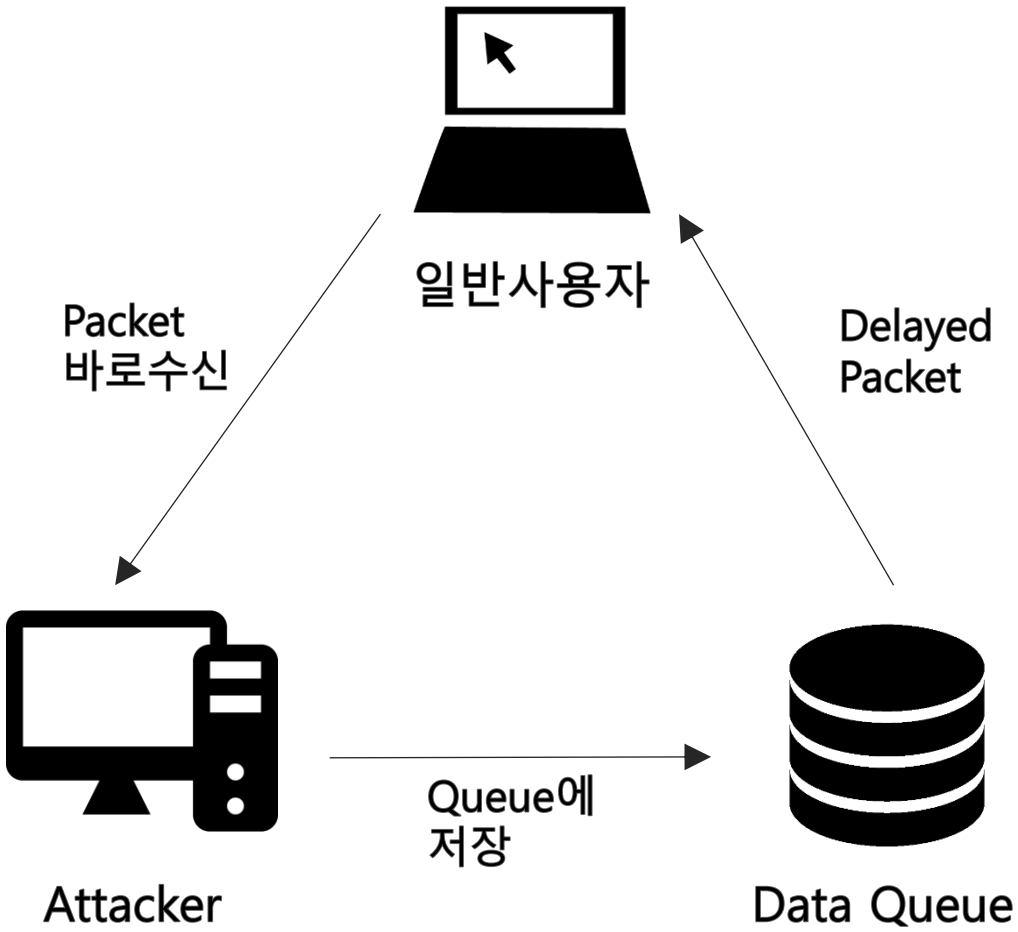
중간의 손실이 발생해도 상관없는 **UDP**의 특성에 **Attacker**의 정보를 늦게 전송하는 방법입니다.

일반 사용자는 **Attacker**의 정보가 수신되지 않아 **Attacker**의 위치와 같은 정보를 알 수 없게 됩니다.



Delay 방식

일반사용자에게 보내는
Attacker의 **UDP Packet**을
저장해 놓았다가
원하는 지연시간 이후
일반 사용자에게 전송합니다.



시 연 영 상

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

감 사 합 니 다 .

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY