

컴퓨터공학 All in One


C/C++ 문법, 자료구조 및 심화 프로젝트 (나동빈)
제 77강 - 패킷 변조를 통한 게임 서버 공격

패킷 변조를 통한 게임 서버 공격

게임 서버/클라이언트 구축하기

① cd {특정한 폴더}

② git clone <https://github.com/ndb796/CPP-Server-And-CSharp.Net-Client-Network-Gomoku-Game.git>

 명령 프롬프트

```
Microsoft Windows [Version 10.0.17134.523]  
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\나동빈>cd C:\Game
```

```
C:\Game>git clone https://github.com/ndb796/CPP-Server-And-CSharp.Net-Client-Network-Gomoku-Game.git  
Cloning into 'CPP-Server-And-CSharp.Net-Client-Network-Gomoku-Game'...
```

```
remote: Enumerating objects: 36, done.
```

```
remote: Counting objects: 100% (36/36), done.
```

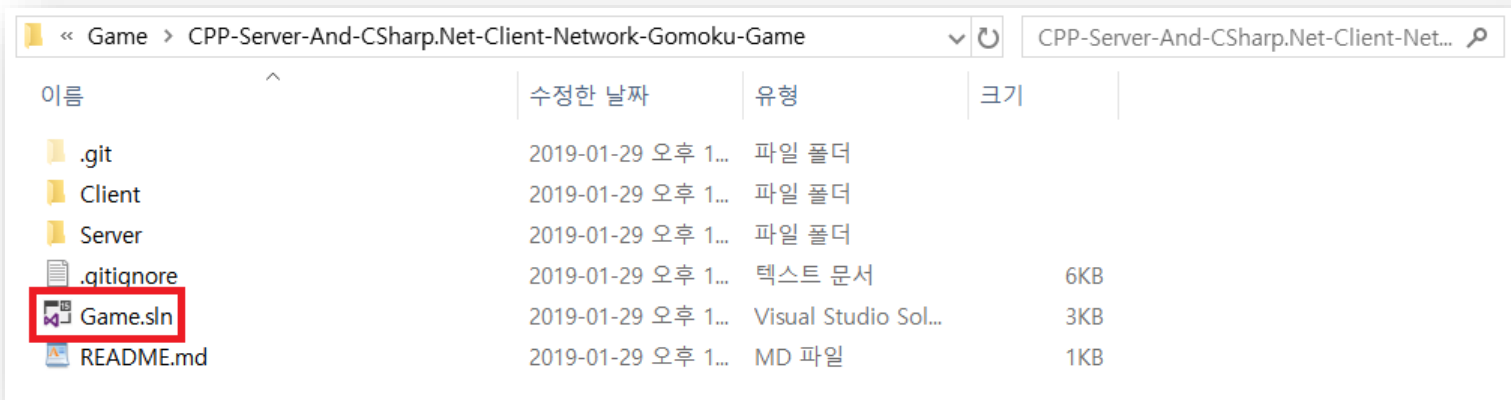
```
remote: Compressing objects: 100% (28/28), done.
```

```
remote: Total 36 (delta 11), reused 29 (delta 8), pack-reused 0
```

```
Unpacking objects: 100% (36/36), done.
```

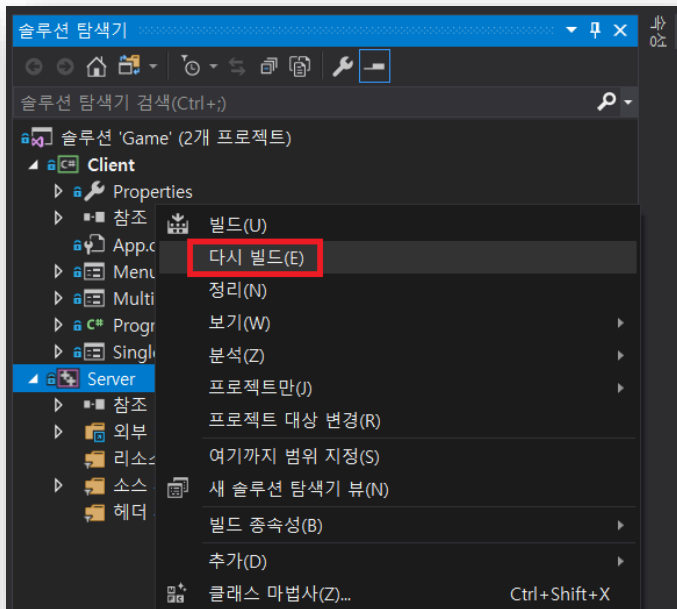
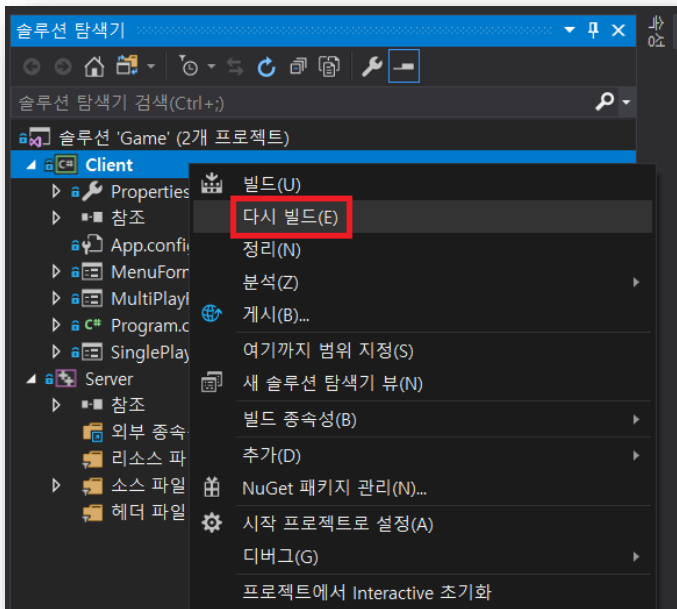
패킷 변조를 통한 게임 서버 공격

프로젝트 열기



패킷 변조를 통한 게임 서버 공격

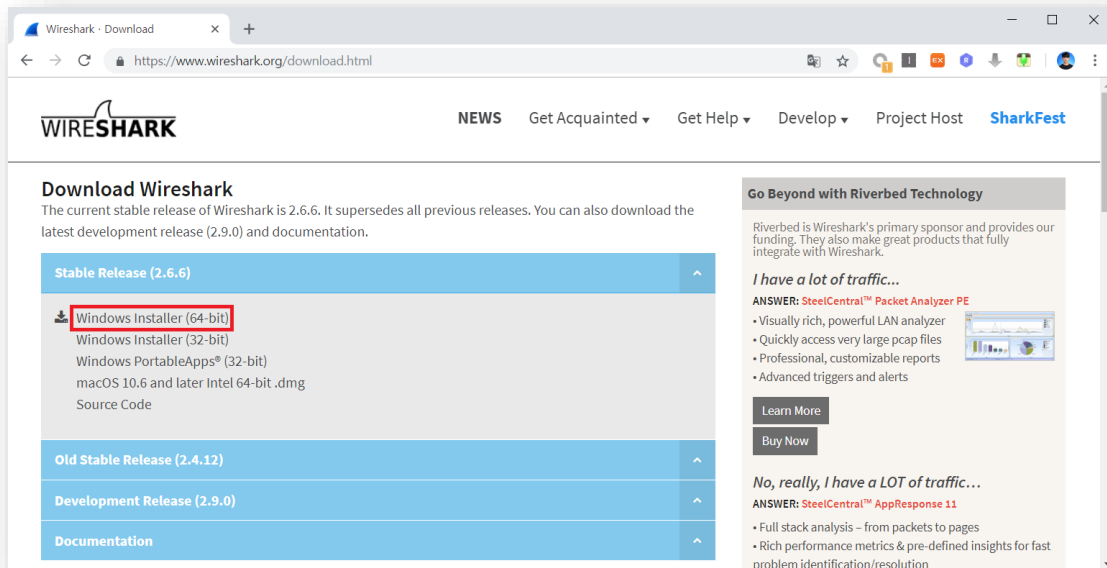
클라이언트 및 서버 프로그램 빌드하기



패킷 변조를 통한 게임 서버 공격

패킷 분석을 위한 와이어샤크 설치하기

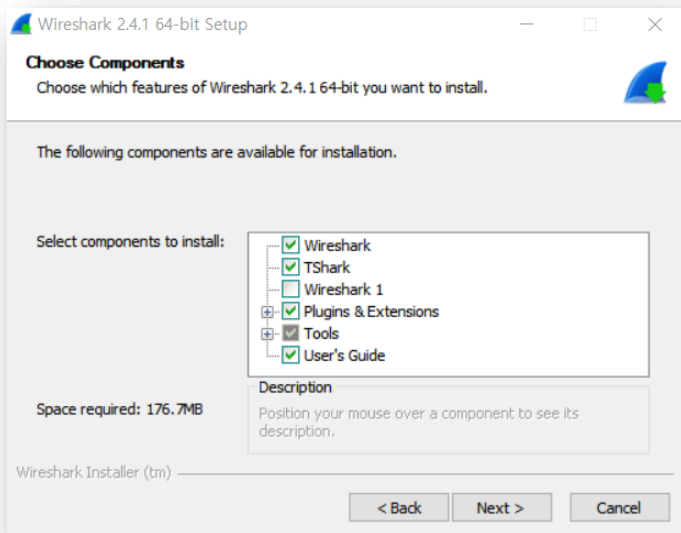
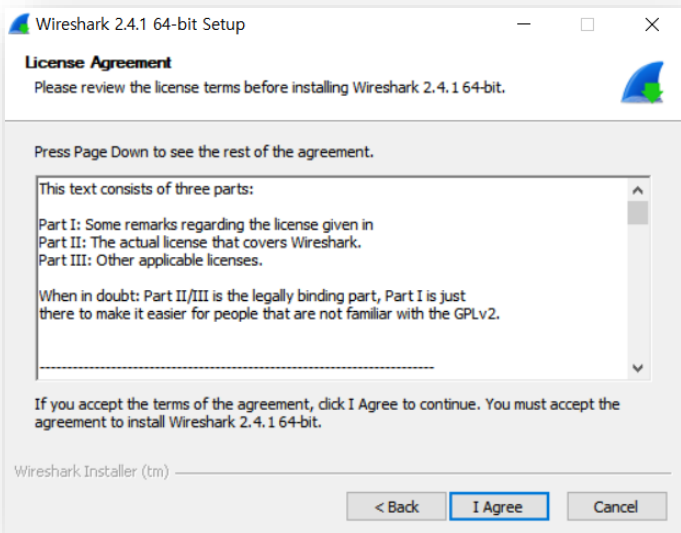
와이어샤크 다운로드: <https://www.wireshark.org/download.html>



The screenshot shows the Wireshark website's download page. The browser's address bar displays <https://www.wireshark.org/download.html>. The page features the Wireshark logo and navigation links: NEWS, Get Acquainted, Get Help, Develop, Project Host, and SharkFest. The main content area is titled "Download Wireshark" and states that the current stable release is 2.6.6, which supersedes all previous releases. It also mentions the latest development release (2.9.0) and documentation. A list of download options is provided, with "Windows Installer (64-bit)" highlighted by a red box. Other options include Windows Installer (32-bit), Windows PortableApps® (32-bit), macOS 10.6 and later Intel 64-bit .dmg, and Source Code. Below this list, there are links for "Old Stable Release (2.4.12)", "Development Release (2.9.0)", and "Documentation". On the right side of the page, there is a section titled "Go Beyond with Riverbed Technology" which mentions Riverbed as Wireshark's primary sponsor. It includes a quote from a user: "I have a lot of traffic..." and provides an answer: "ANSWER: SteelCentral™ Packet Analyzer PE". It lists several features: "Visually rich, powerful LAN analyzer", "Quickly access very large pcap files", "Professional, customizable reports", and "Advanced triggers and alerts". There are buttons for "Learn More" and "Buy Now". At the bottom of this section, it says "No, really, I have a LOT of traffic..." and provides another answer: "ANSWER: SteelCentral™ AppResponse 11". It lists more features: "Full stack analysis – from packets to pages" and "Rich performance metrics & pre-defined insights for fast problem identification/resolution".

패킷 변조를 통한 게임 서버 공격

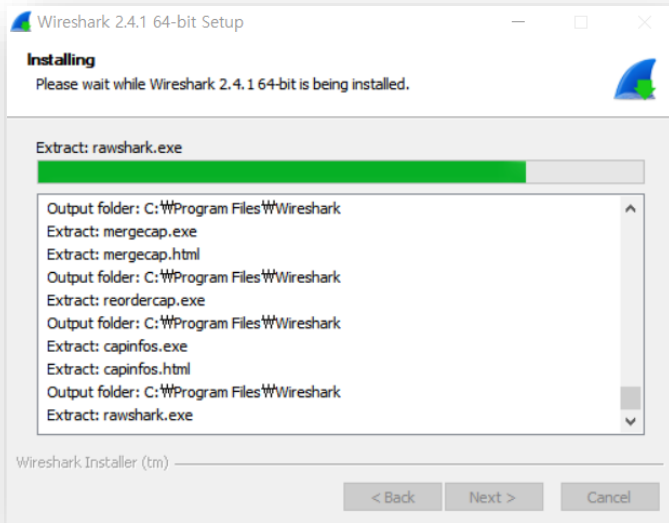
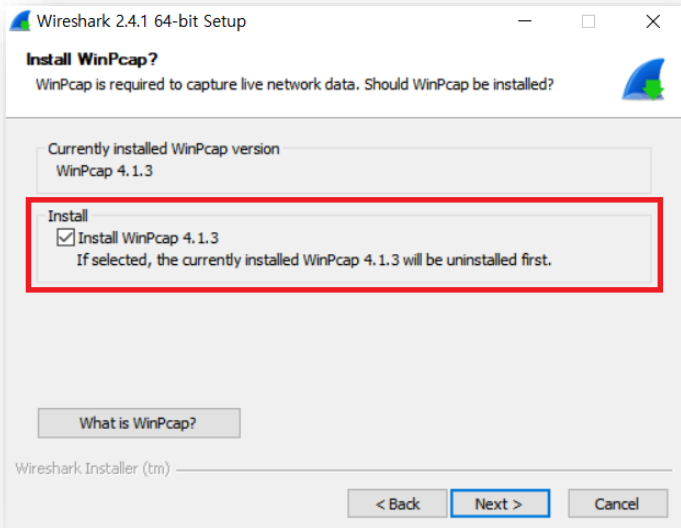
패킷 분석을 위한 와이어샤크 설치하기



패킷 변조를 통한 게임 서버 공격

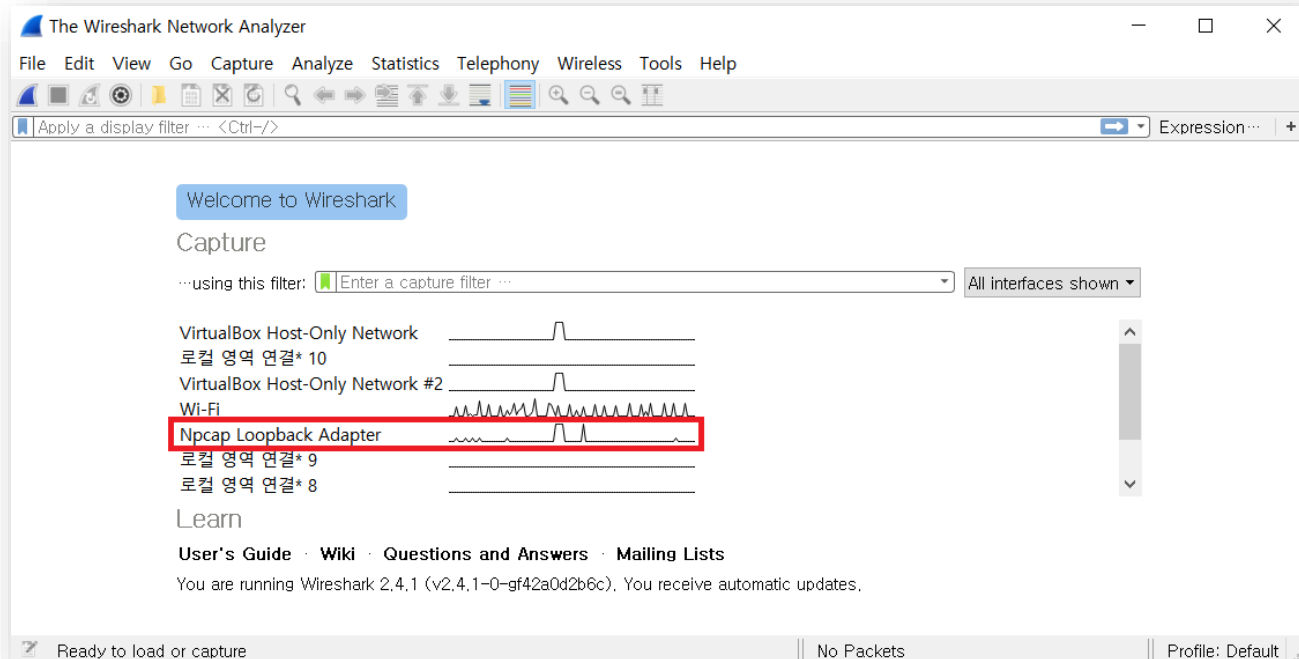
패킷 분석을 위한 와이어샤크 설치하기

- 처음 설치하는 경우 WinPcap을 설치합니다.



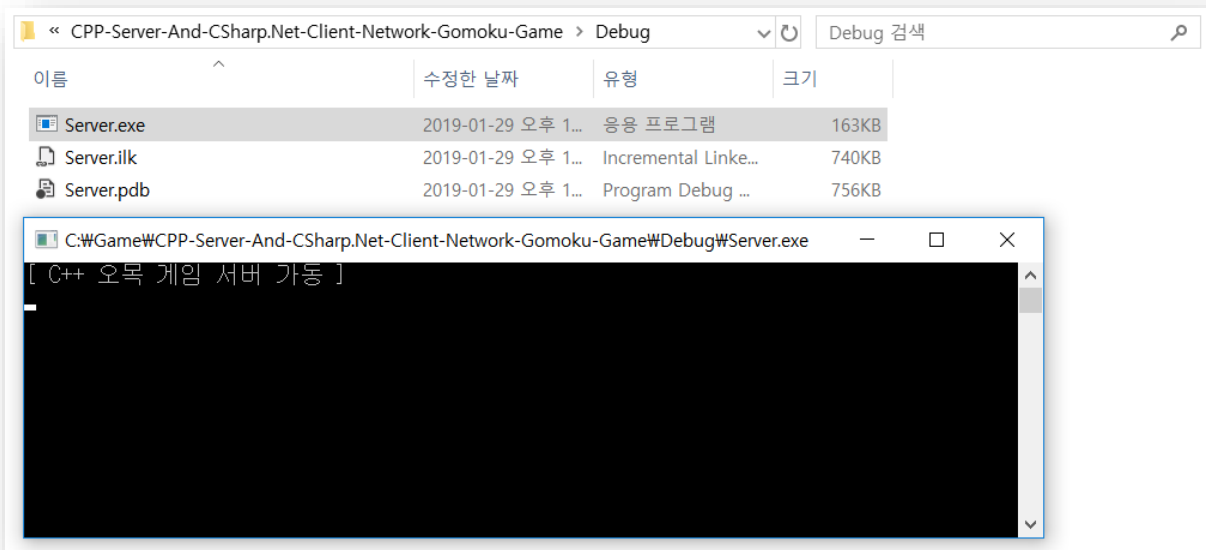
패킷 변조를 통한 게임 서버 공격

루프백(Loopback) 드라이버 찾기: 컴퓨터 시스템에 따라 어댑터 이름이 다를 수 있음



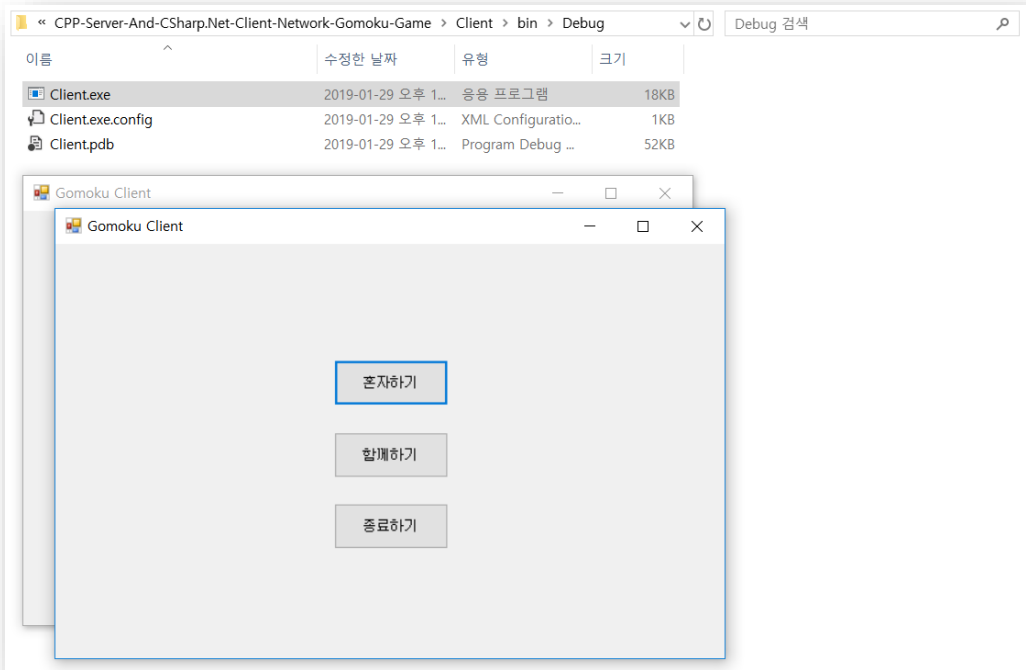
패킷 변조를 통한 게임 서버 공격

서버 프로그램 구동하기



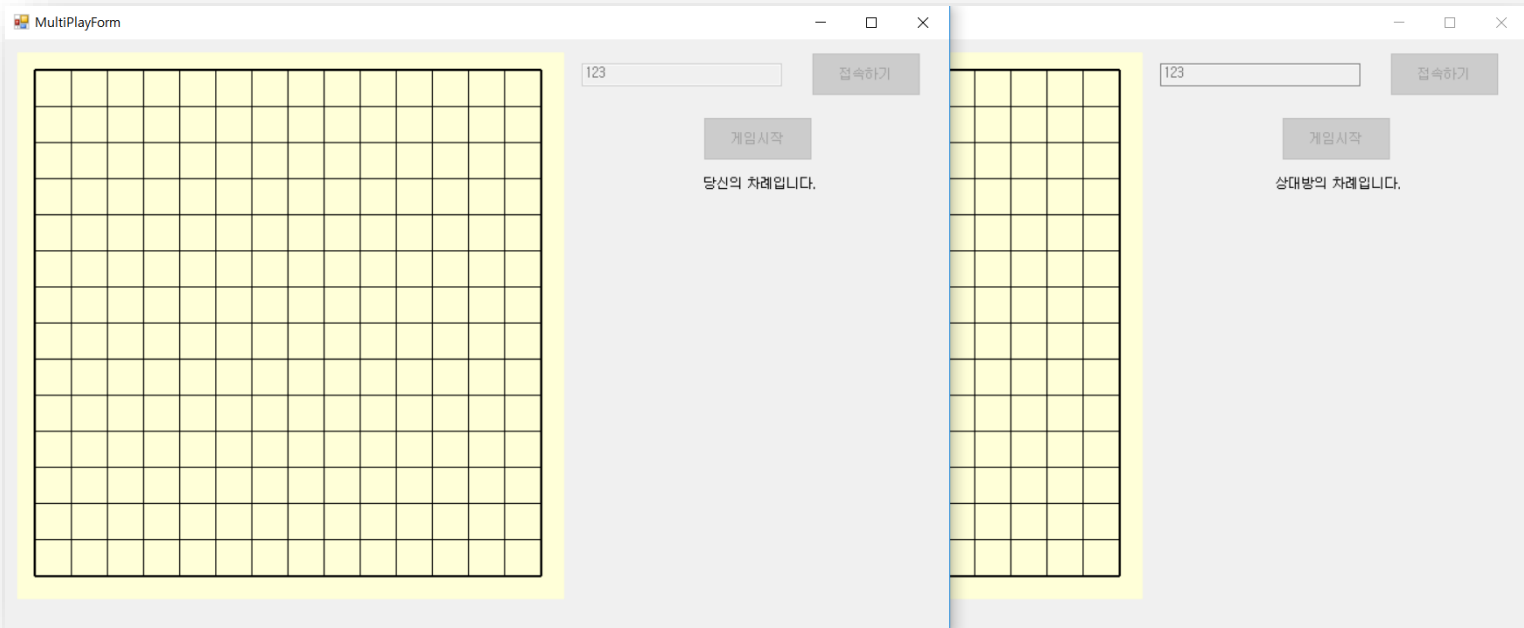
패킷 변조를 통한 게임 서버 공격

클라이언트 프로그램 구동하기



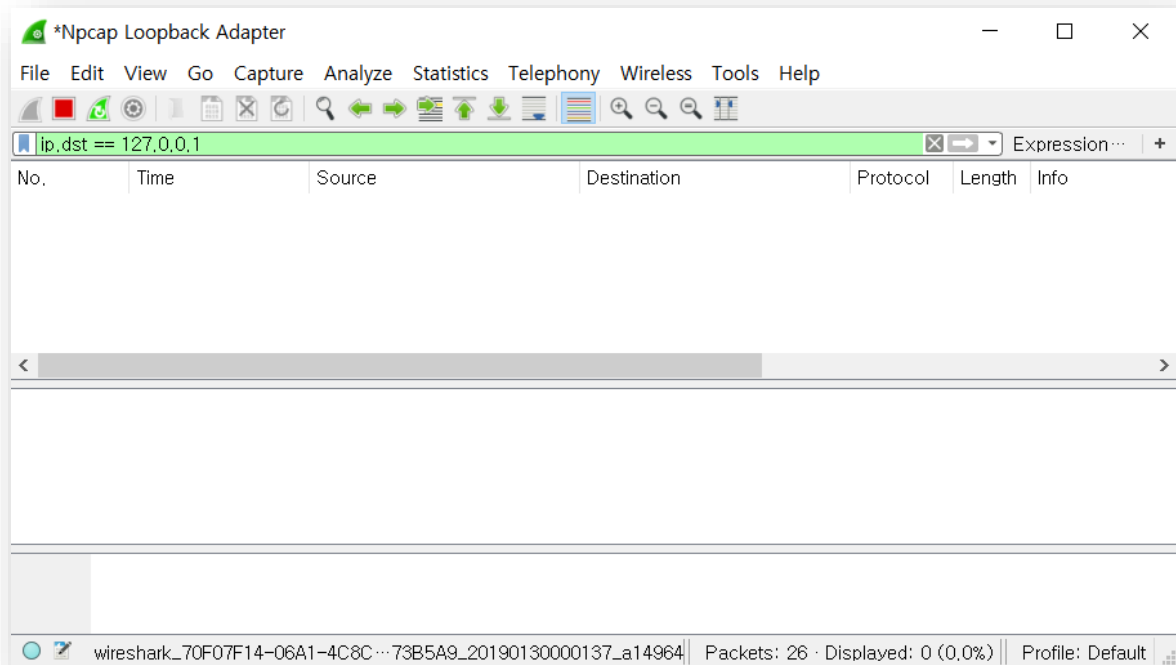
패킷 변조를 통한 게임 서버 공격

클라이언트 프로그램 구동하기



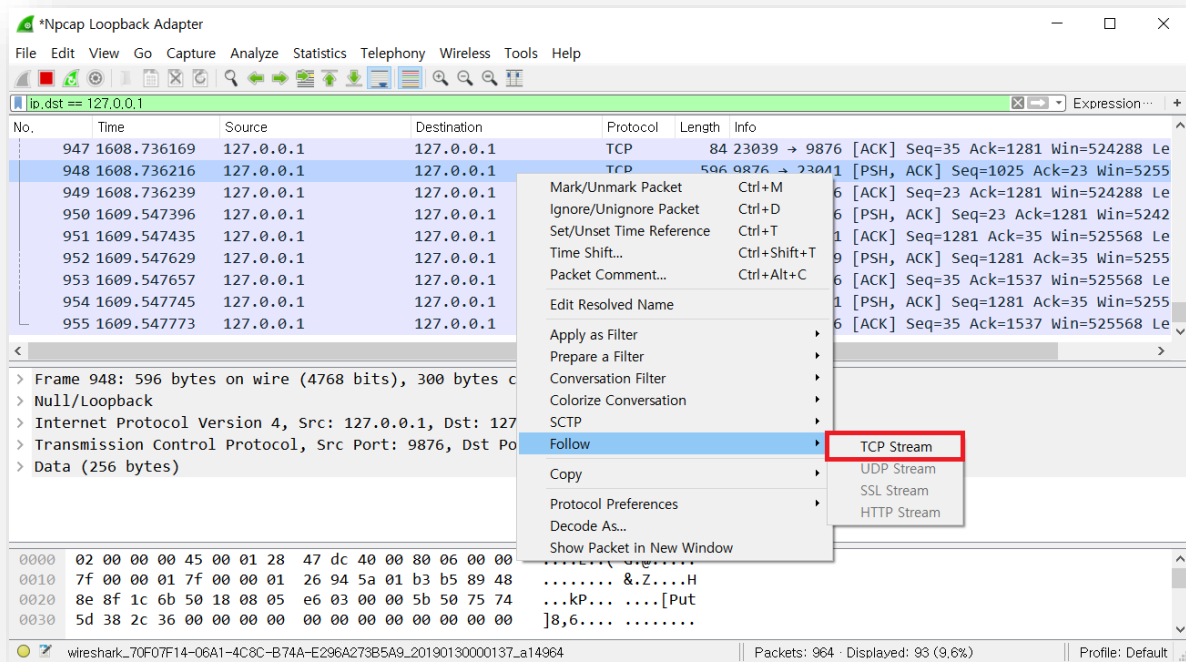
패킷 변조를 통한 게임 서버 공격

루프백 주소(127.0.0.1)로 필터링 수행하기



패킷 변조를 통한 게임 서버 공격

게임 플레이 이후에 생성되는 패킷의 [TCP Stream] 확인하기



The screenshot shows the Npcap Loopback Adapter interface. The packet list displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
947	1608.736169	127.0.0.1	127.0.0.1	TCP	84	23039 → 9876 [ACK] Seq=35 Ack=1281 Win=524288 Le
948	1608.736216	127.0.0.1	127.0.0.1	TCP	596	9876 → 23041 [PSH, ACK] Seq=1025 Ack=23 Win=5255
949	1608.736239	127.0.0.1	127.0.0.1			6 [ACK] Seq=23 Ack=1281 Win=524288 Le
950	1609.547396	127.0.0.1	127.0.0.1			6 [PSH, ACK] Seq=23 Ack=1281 Win=5242
951	1609.547435	127.0.0.1	127.0.0.1			1 [ACK] Seq=1281 Ack=35 Win=525568 Le
952	1609.547629	127.0.0.1	127.0.0.1			9 [PSH, ACK] Seq=1281 Ack=35 Win=5255
953	1609.547657	127.0.0.1	127.0.0.1			6 [ACK] Seq=35 Ack=1537 Win=525568 Le
954	1609.547745	127.0.0.1	127.0.0.1			1 [PSH, ACK] Seq=1281 Ack=35 Win=5255
955	1609.547773	127.0.0.1	127.0.0.1			6 [ACK] Seq=35 Ack=1537 Win=525568 Le

The context menu for packet 948 is open, showing the following options:

- Mark/Unmark Packet (Ctrl+M)
- Ignore/Unignore Packet (Ctrl+D)
- Set/Unset Time Reference (Ctrl+T)
- Time Shift... (Ctrl+Shift+T)
- Packet Comment... (Ctrl+Alt+C)
- Edit Resolved Name
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow (highlighted)
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

The 'Follow' option is highlighted, and a sub-menu is open showing the following options:

- TCP Stream (highlighted)
- UDP Stream
- SSL Stream
- HTTP Stream

The packet details pane shows the following information:

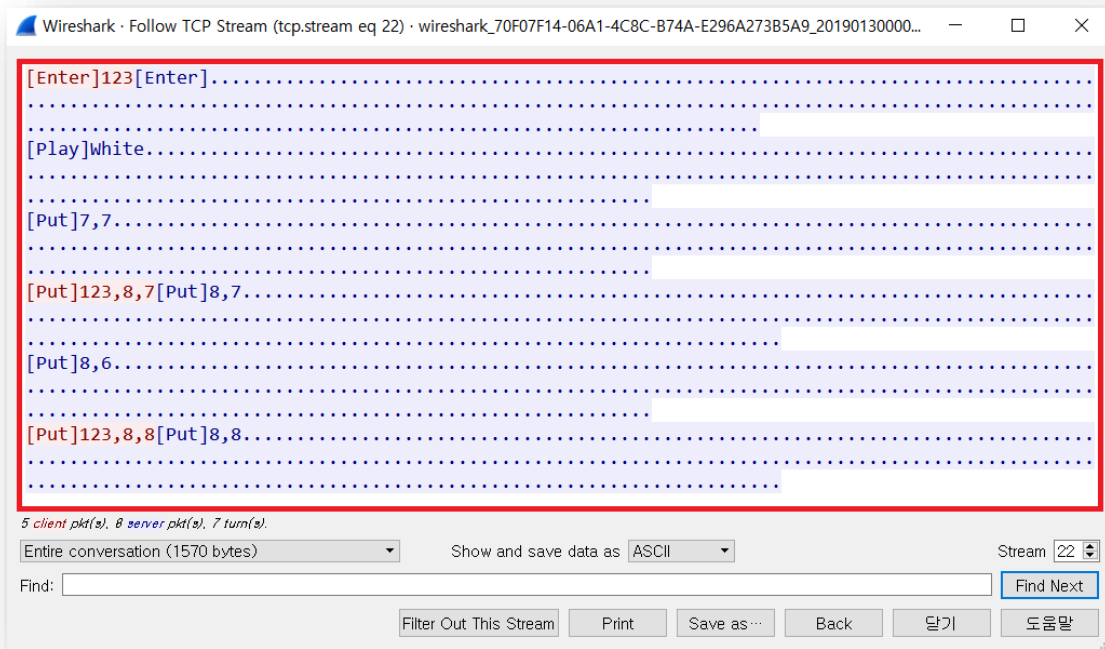
- Frame 948: 596 bytes on wire (4768 bits), 300 bytes captured (2400 bits) on interface
- Null/Loopback
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 9876, Dst Port: 23041
- Data (256 bytes)

The packet bytes pane shows the following data:

```
0000  02 00 00 00 45 00 01 28 47 dc 40 00 80 06 00 00
0010  7f 00 00 01 7f 00 00 01 26 94 5a 01 b3 b5 89 48
0020  8e 8f 1c 6b 50 18 08 05 e6 03 00 00 5b 50 75 74
0030  5d 38 2c 36 00 00 00 00 00 00 00 00 00 00 00 00
      ...&Z...H
      ...kP...[Put
      ]8,6....
```

패킷 변조를 통한 게임 서버 공격

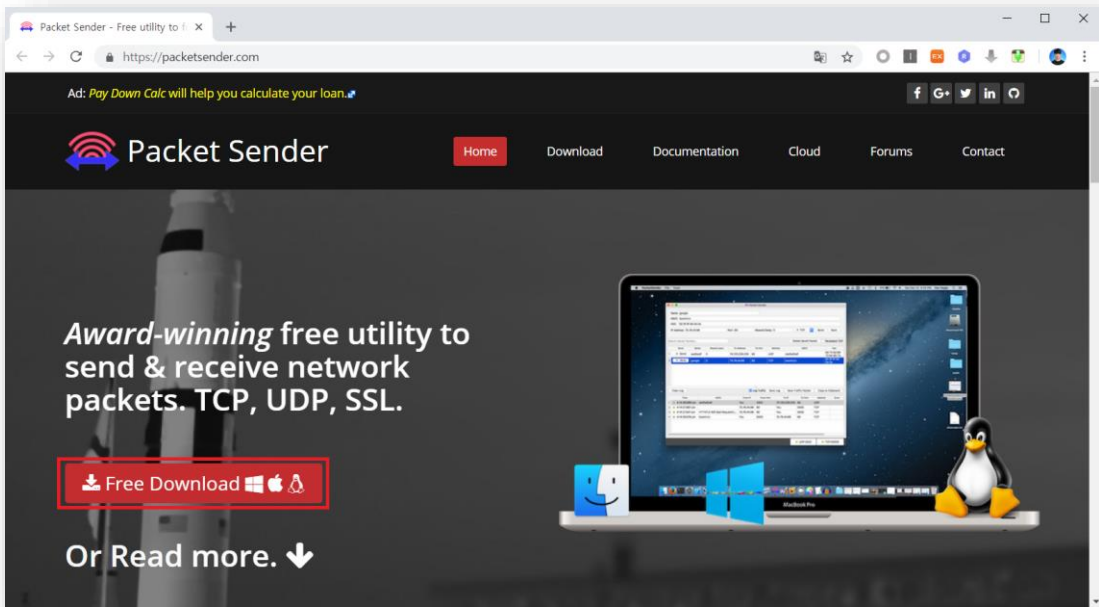
서버와 주고 받은 패킷 데이터 확인하기



패킷 변조를 통한 게임 서버 공격

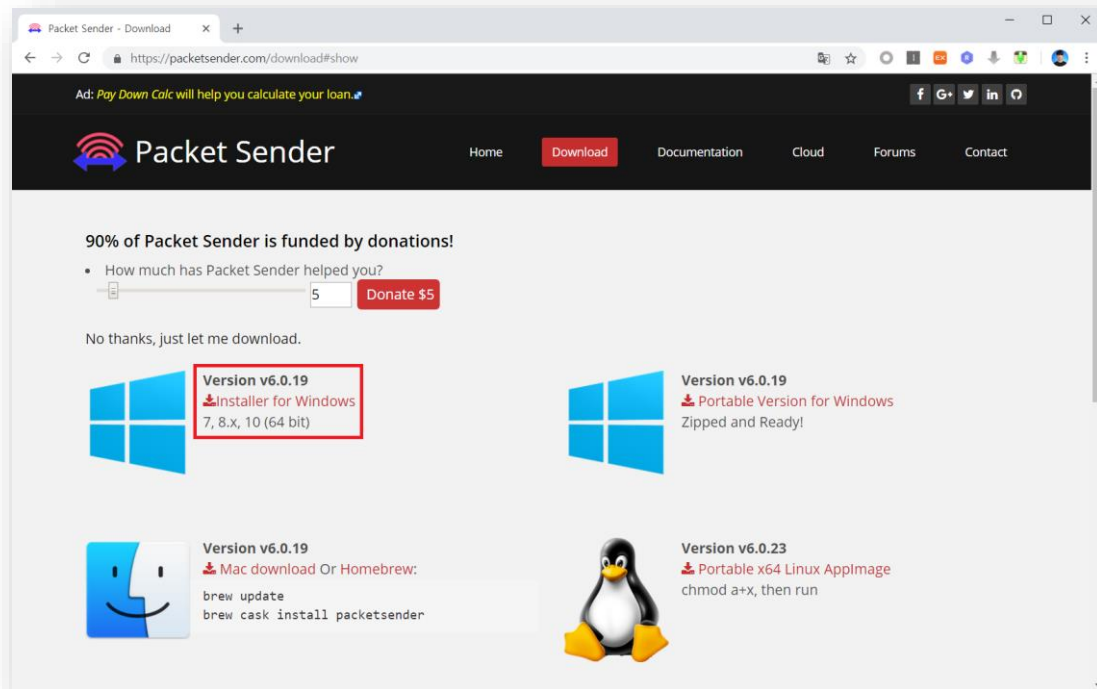
패킷 전송기(Packet Sender) 설치하기

- <https://packetsender.com/>



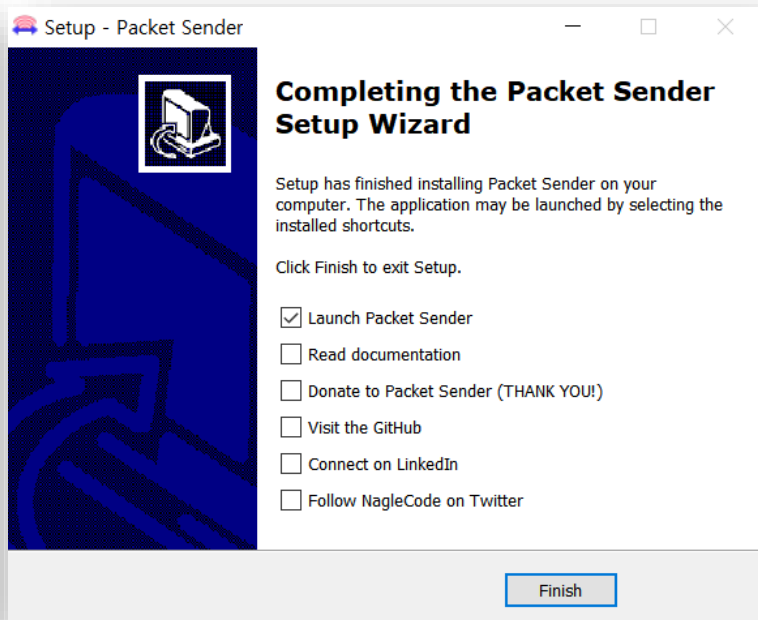
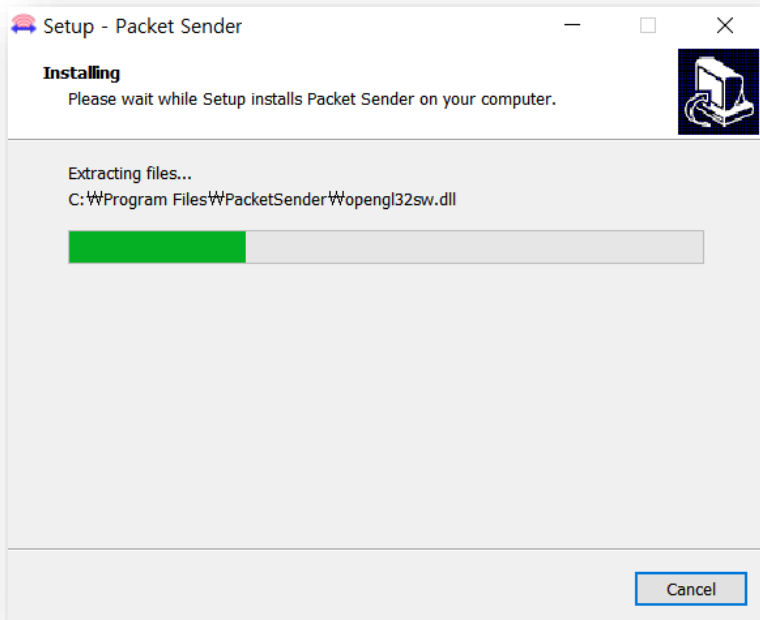
패킷 번조를 통한 게임 서버 공격

패킷 전송기(Packet Sender) 설치하기



패킷 변조를 통한 게임 서버 공격

패킷 전송기(Packet Sender) 설치하기



패킷 변조를 통한 게임 서버 공격

패킷 전송기 실행하기

Packet Sender - IPs: 172.16.100.192, 169.254.151.25, 192.168.99.1, 192.168.56.1, fe80::39ff:2931:fb63:38b...

File Tools Multicast Help

Name

ASCII

HEX

Address

Port

Resend Delay

TCP

Send

Save

Search Saved Packets...

Delete Saved Packet

☐ Persistent TCP

Send	Name	Resend (sec)	To Address	To Port	Method	ASCII	Hex
------	------	--------------	------------	---------	--------	-------	-----

Clear Log (0)

☒ Log Traffic

Save Log

Save Traffic Packet

Copy to Clipboard

Time	From IP	From Port	To IP	To Port	Method	Error
------	---------	-----------	-------	---------	--------	-------

<

>

UDP:54579

TCP:22917

SSL:22918

패킷 변조를 통한 게임 서버 공격

전송 결과 확인하기

Packet Sender - IPs: 172.16.100.192, 169.254.151.25, 192.168.99.1, 192.168.56.1, fe80::39ff:2931:fb63:38b7%ethernet_32775, fe80::51f0:...

File Tools Multicast Help

Name

ASCII

HEX

Address Port Resend Delay TCP

Search Saved Packets,...

☐ Persistent TCP

Send	Name	Resend (sec)	To Address	To Port	Method	ASCII	Hex
1	👉 00:44:33.998	127.0.0.1	9876	You	23246	TCP	
2	👉 00:44:33.497	127.0.0.1	9876	You	23246	TCP	
3	👉 00:44:33.495	You	23246	127.0.0.1	9876	TCP	[Put]123,10,10 5b 50 75 74 5d 31 32 33 2c 31 30 2c 31 30

Clear Log (3) ☒ Log Traffic

👉 UDP:53013 👉 TCP:23024 👉 SSL:23025

패킷 변조를 통한 게임 서버 공격

다양한 공격 벡터

- 서버에서 클라이언트의 인증을 수행하지 않고 있음.
- 따라서 부적절한 인가 문제를 해결하지 않으면 다른 사용자의 권한을 악용할 수 있음.