



STEAM Works Artifact

KSIA

김동현

www.facebook.com/digitalisx





김동현 / 19

[학력 사항]

2014. 03 - 현재 : 함지고등학교 재학

[주요 활동]

영남권 정보보호영재교육원 2기 우수 장학생

CSTEC 차세대 핵심보안 전문인력 특별과정 수료

교육청 발명영재교육원 특허출원 과정 수료

한국정보보호학회 동계학술대회 발표

한국학생IT연합(KSIA) 운영사무국원

교내 정보동아리 "ICT" 부장



Pas Peur



ISIS used PS4 for attack!



Your Instant Game Collection

YEAR ONE



1 Year. 64 Games.
\$49.99



*Active PlayStation Plus Membership required to access free content. *Game offerings change each month and availability of game download periods vary.

Just enjoy game? – No!



Play Station Network – PSN

게임 및 DLC 판매

각종 커뮤니케이션 기능 제공



PLAYSTATION®
Network



현실은 ... 해커들의 놀이터



Forbes / Tech

The Little Black Book of Billionaire Secrets

NOV 14, 2015 @ 06:17 PM 671,649 VIEWS

How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks [Updated]

Correction: *It has not been confirmed, as originally written, that a console was found as a result of specific Belgian terror raids. Minister Jambon was speaking about tactics he knows ISIS to be using generally.*

Following [Friday night's terrorist attacks in Paris](#) which killed at least 127 people and left more than 300 injured, authorities are discovering just how the massacre was planned. And it may involve the most popular gaming console in the world, [Sony's PlayStation 4](#).

The hunt for those responsible (eight terrorists were killed Saturday night, but accomplices may still be at large) led to a number of raids in nearby Brussels. Belgian federal home affairs minister [Jan Jambon](#) has said outright that the PS4 is used by ISIS agents to communicate, and was selected due to the fact that it's notoriously hard to monitor. "PlayStation 4 is even more difficult to keep track of than WhatsApp," he said.

When the new generation of consoles launched, there were concerns that they would be too light on privacy, with peripherals like [Microsoft](#) MSFT +0.57%'s Kinect and PlayStation's Camera possibly having the ability to spy on users if say, the government wanted a window into your living room.

While the idea is certainly Orwellian, it's the non-peripheral based communication on consoles which may provide terrorists a channel to effectively converse with one another. The comparatively low-tech system may offer a more secure means of



Bomb blueprint



Information





Why they use Game?



1. 다소 허술한 영역



PLAYSTATION®
Network

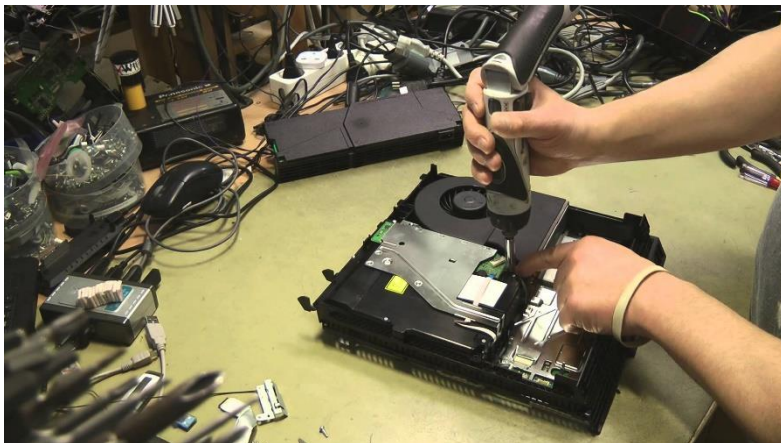


XBOX LIVE





2. 보안 기술



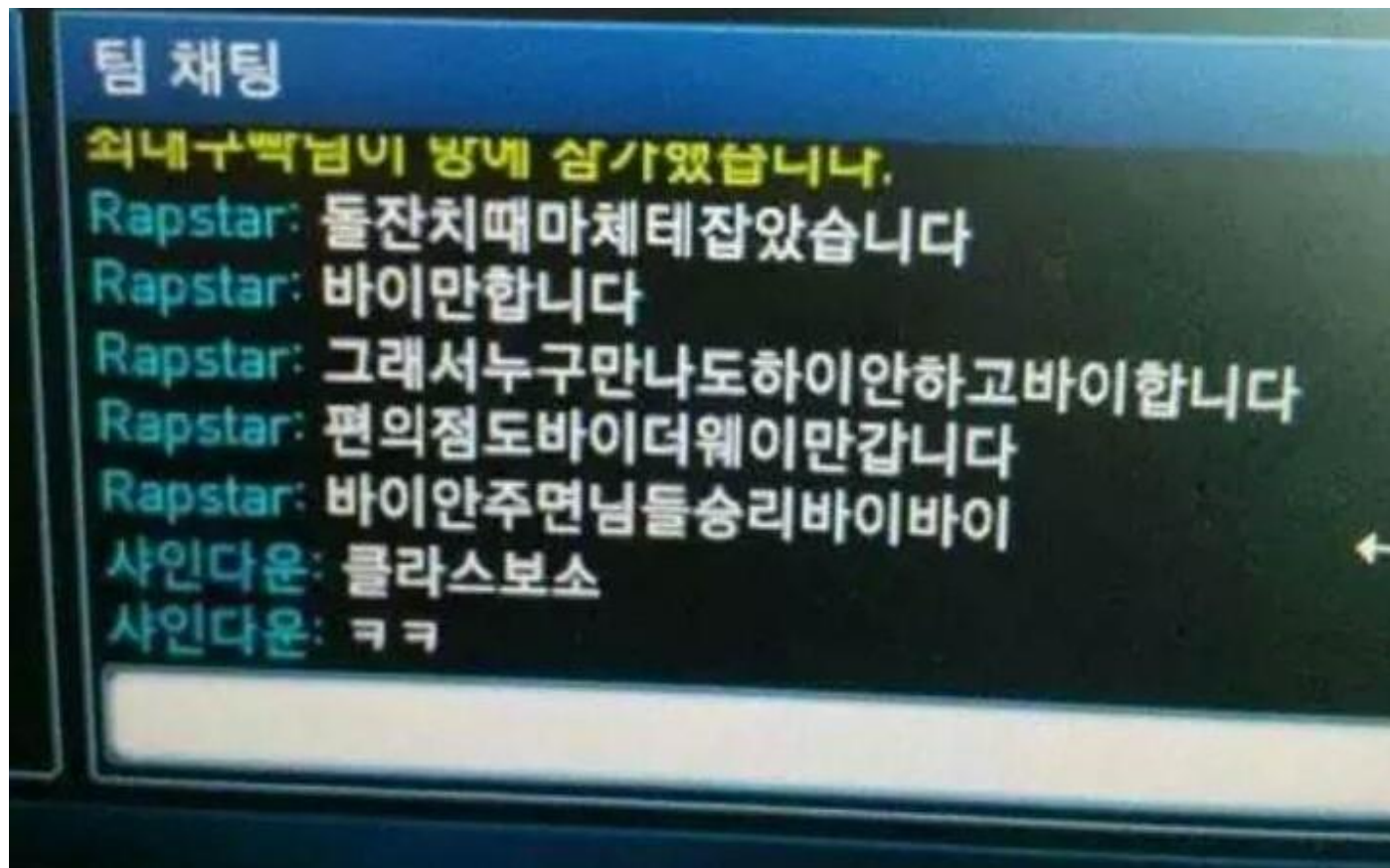
User : Comfortable

Hacker : WTF?





3. 특유의 생태계





요점

- 게임 플랫폼의 커뮤니케이션 기능을 이용한 범죄 확산.
- 도 - 감청에는 제약이 존재.
- 사건 발생시 특유의 생태계로 인해 추적 및 수사가 힘들.
- 해외의 경우 수사 협조에 상당한 시간이 소모.
- 각 생태계에 대한 지식 보유 및 증거 수집 능력 필요.

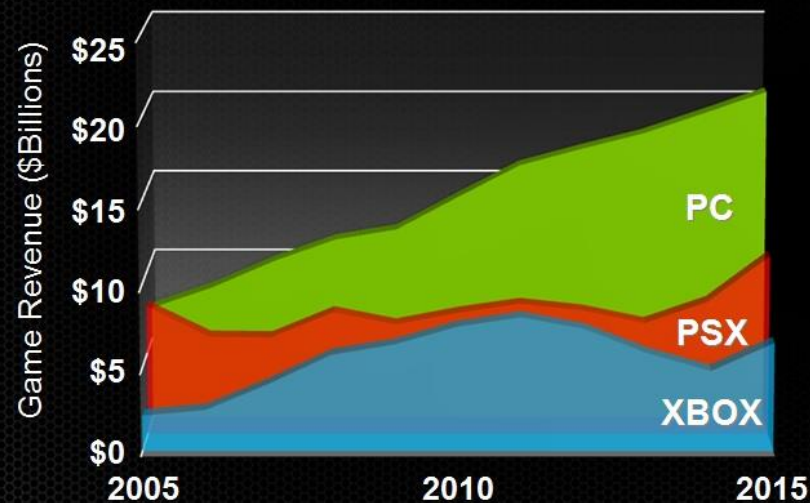


많은 종류와 비싼 가격 ...



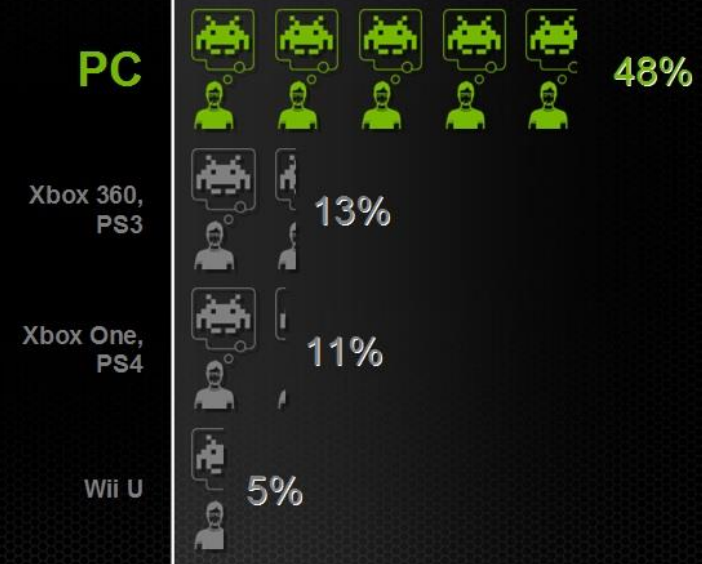
PC – MOST IMPORTANT GAMING PLATFORM

GAMING SOFTWARE REVENUE



Source: DFC

DEVELOPERS WORKING ON GAMING PLATFORMS



Source: 2013 GDC Survey



Driven by Digital Distribution & Transactions



Source: DFC Intelligence



Ultimate Platform



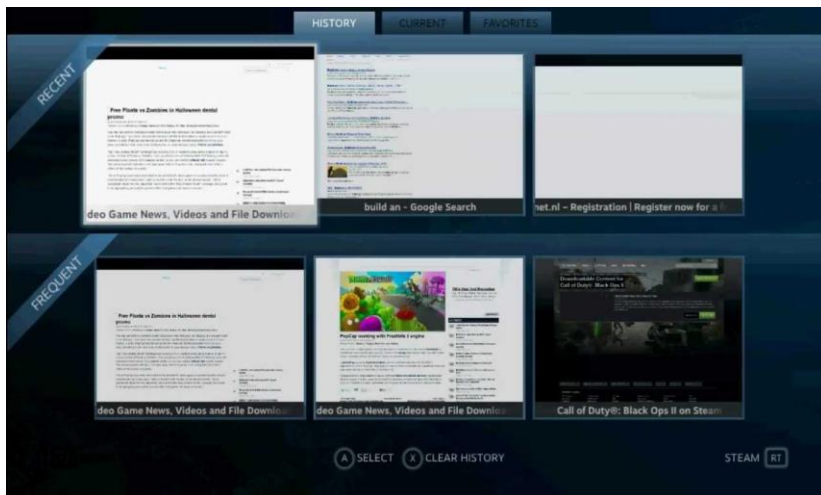
Steam

- Developed by Valve Corporation
- ESD (Electronic Software Distribution)
- DRM (Digital Rights Management)
- 4,500개 이상 의 게임 판매 (인디 – AAA)
- 사용자 1억 명 돌파 (2014년 기준)









Screenshot, Video Live Stream



Movie, Music Web, Community







[전체](#) [이미지](#) [뉴스](#) [동영상](#) [더보기 ▼](#) [검색 도구](#)

검색결과 약 167,000개 (0.45초)

관련검색: [digital forensic ppt](#) [digital forensic conference](#) [digital forensic tool](#)
[digital forensic challenge](#) [digital forensic news](#)


steam digital forensic에 대한 학술자료 

... framework of distributed agent-based network **forensics** ... - [Wei](#) - 15회 인용
... agent-based real time network intrusion **forensics** ... - [Ren](#) - 31회 인용
... for establishing provenance of timestamps in **digital** ... - [Schatz](#) - 37회 인용

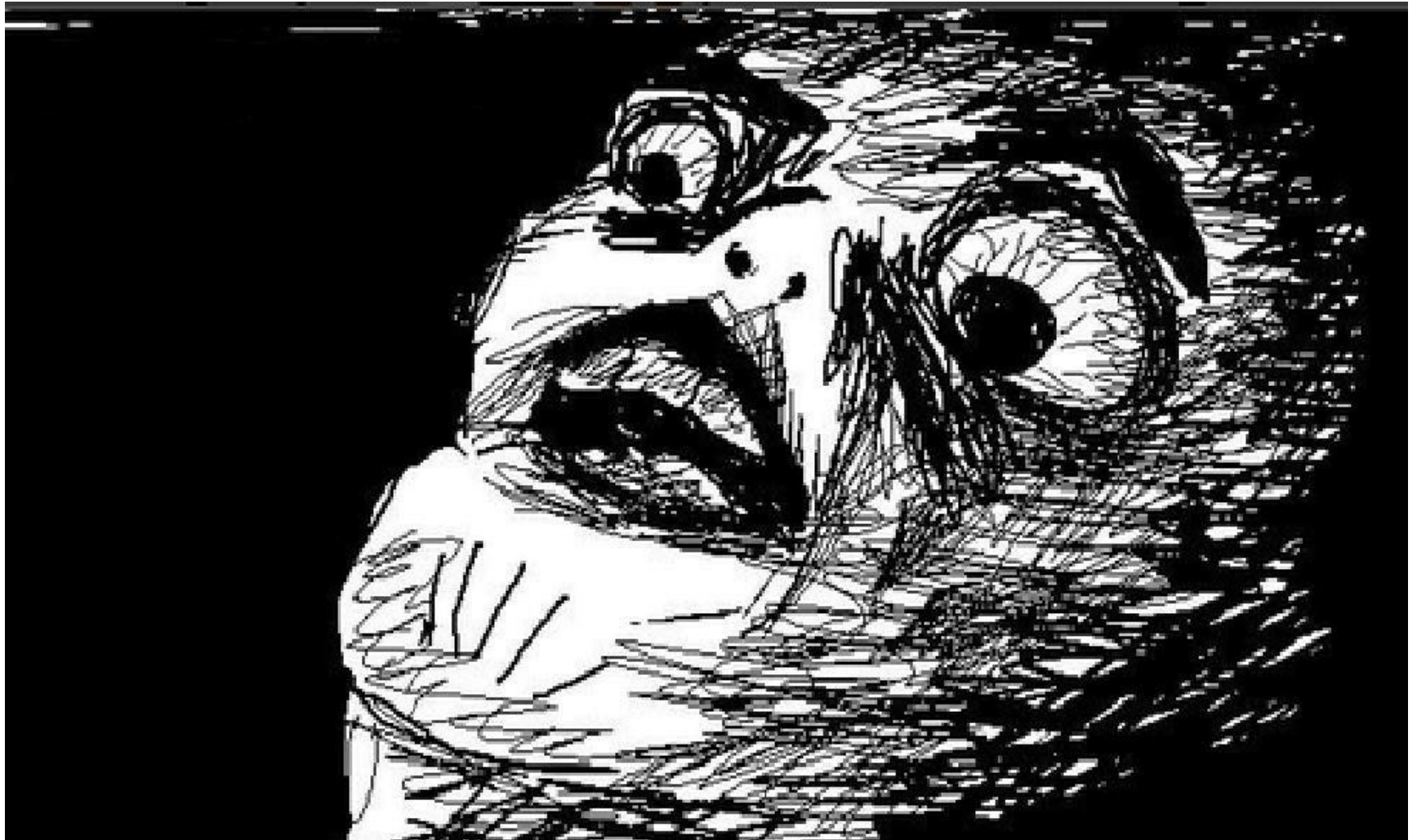
Steam Forensic Artifacts 

[tdforensics.blogspot.com/](#) ▼ [이 페이지 번역하기](#)
2014. 1. 20. - Steam forensics could help with setting up time lines or verifying that our
.... I am a Computer and Digital Forensics major at Champlain College.
이 페이지를 16. 4. 1에 방문했습니다.

Steam app for iOS and Android - Digital Forensics Forums ...



[www.forensicfocus.com/Forums/viewtopic/t=10410/](#) ▼ [이 페이지 번역하기](#)
2013. 3. 20. - 댓글 6 - 작성자 3
This is a fork that has been added into the Steam app on iOS or Android. I am









Artifact #1 – Login User

The image shows the Steam login page. At the top, there is a dark blue header with the Steam logo (a white robot head) and the word "STEAM" in white. To the right of the logo are links: "상점", "커뮤니티", "정보", and "지원". Below the header is a navigation bar with several buttons: "특집 항목", "게임", "소프트웨어", "하드웨어", "동영상", "뉴스", and "나의 맞춤 검색". The main content area is divided into two columns. The left column is titled "로그인" (Login) and "Steam 계정으로 로그인" (Login with Steam account). It contains two input fields: "Steam 계정 이름" (Steam account name) and "비밀번호" (Password). Below these fields is a "로그인" (Login) button. The right column is titled "만들기" (Create) and "새 무료 계정" (New free account). It contains a paragraph of text: "자유롭게 참가하고 쉽게 이용할 수 있습니다. Steam 계정을 만들어 PC 그리고 Mac 게이머들을 위한 선두적인 디지털 솔루션인 Steam을 이용해 보세요." (You can participate freely and use it easily. Create a Steam account to use the leading digital solution for PC and Mac gamers, Steam. Try it out.) Below this text is a "Steam 가입" (Join Steam) button.



 config.vdf	2016-04-03 오후...	VDF 파일	5KB
 DialogConfig.vdf	2016-04-03 오후...	VDF 파일	8KB
 loginusers.vdf	2016-04-03 오후...	VDF 파일	1KB
 SteamAppData.vdf	2016-04-03 오후...	VDF 파일	1KB

File Location

C:\Program Files(x86)\Steam\config\loginusers.vdf

PC에 설치된 스팀 클라이언트를 통해 로그인 하였던
사용자의 Profile Link, ID 및 Username 정보



.VDF?



VDF Format Used by Valve Software
Installation Script, Configuration Script



How to Open?



Source SDK



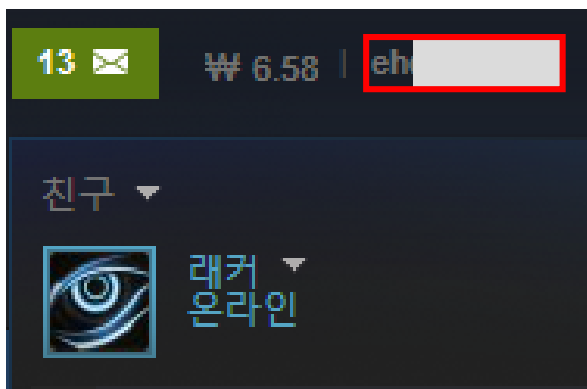
Text Editor



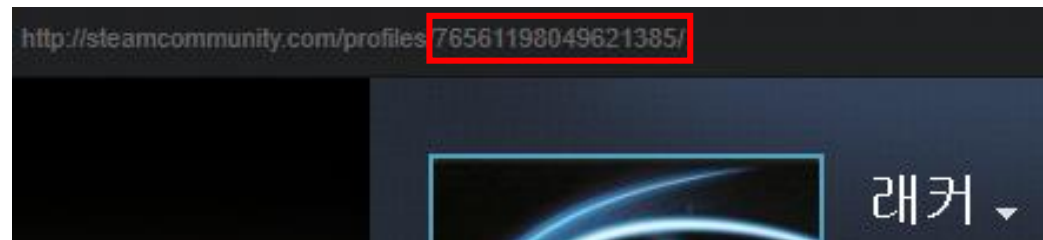
```
"users"
{
  "76561198049621385"
  {
    "AccountName"      "eh"
    "PersonaName"      "래커"
    "RememberPassword" "0"
    "Timestamp"        "1459657901"
  }
}
```

Profile Link

User ID



User ID



Profile Link



STEAM

STORE **NEW COMMUNITY** NEWS ABOUT SUPPORT STATS
FRIENDS PROFILE **GAME HUBS** DISCUSSIONS WORKSHOP GREENLIGHT

Install Steam Login | language

Search players and groups

STEAM COMMUNITY HUBS

Community Hubs showcase the activity of the Steam Community at large. Here you can discover, download, and create new game content and share it with millions of other gamers.

109,680,277 Community Content Contributions | 389,250 Players In-Game | 3,071,633 Players Online

Dota 2

917,584
COMMUNITY CONTRIBUTIONS
[VIEW ALL](#)

Log in to the Steam Community to view your games list and find more Hubs to browse

[SIGN IN](#) or [JOIN STEAM](#)

New to Steam?
Join Steam for free and purchase full retail versions of games delivered straight to your desktop, complete with automatic updates and in-game community features. Best of all, it's free. [Learn More.](#)

Find a Specific Game Hub

Artifact #2 – Group & Friends



이름	수정된 날짜	유형
 localconfig.vdf	2016-04-05 오전...	VDF 파일

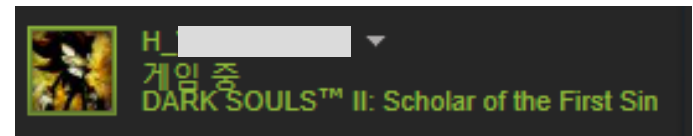
File Location

C:\Program Files (x86)\Steam\userdata\[Usernum]\config

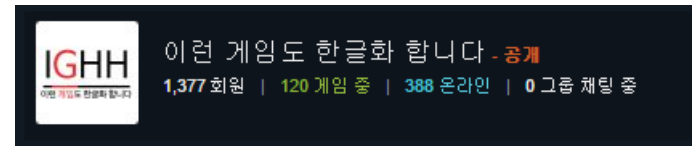
클라이언트로 로그인 하였던 사용자의 친구 목록 및
소속된 그룹의 이름 및 태그가 포함됨



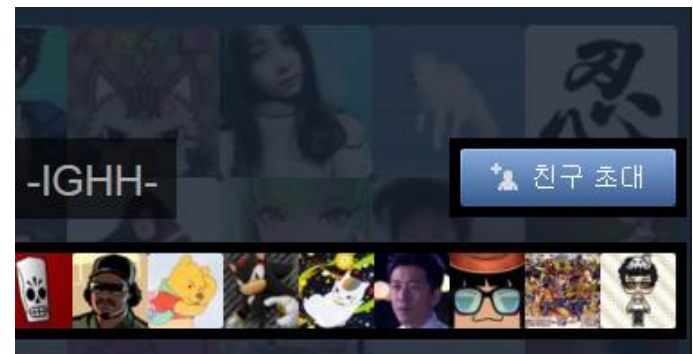
```
{
  "name" "H_ "
  "NameHistory"
  {
    "0" "H_ "
  }
  "avatar" "b46cd0eea0679130e9da9f748b7281763c7a57fa"
}
"104582147"
{
  "name" " "
  "NameHistory"
  {
    "0" " "
  }
  "avatar" "9e54b5dbde1278a8f474561462bdbb98a618eb96"
}
"122003789"
{
  "name" " "
  "NameHistory"
  {
    "0" " "
  }
}
"103582791434744753"
{
  "name" "이런 게임도 한글화 합니다"
  "tag" "- IGHH -"
  "avatar" "2d0f5d091ca67268a26f16cb1419db448416e7d3"
}
"103582791438104253"
{
  "name" " "
  "tag" " "
  "avatar" "0d5045e249dfbae1ce31f81fa1120c8ab7998b98"
}
```



Friends Name / History



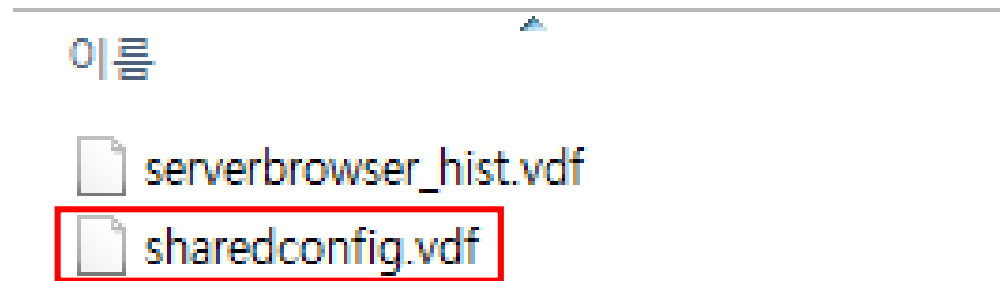
Group Name



Group Tag



Artifact #3 – Site Artifact



File Location

C:\Program Files (x86)\Steam\userdata\[Usernum]\7\remote

Big Picture 모드로 실행하여 접속한 사이트 및
즐거찾기로 지정한 사이트의 목록



```
"UserRoamingConfigStore"
{
  "Web"
  {
    "WebFav0_URL"      "https://www.google.com/"
    "WebFav0_Name"     "Google"
    "WebFav1_URL"      "http://www.youtube.com/"
    "WebFav1_Name"     "YouTube"
    "WebFav2_URL"      "http://www.twitter.com/"
    "WebFav2_Name"     "Twitter"
    "WebFav3_URL"      "http://www.facebook.com/"
    "WebFav3_Name"     "Facebook"
    "WebFav4_URL"      "http://www.reddit.com/"
    "WebFav4_Name"     "Reddit"
```

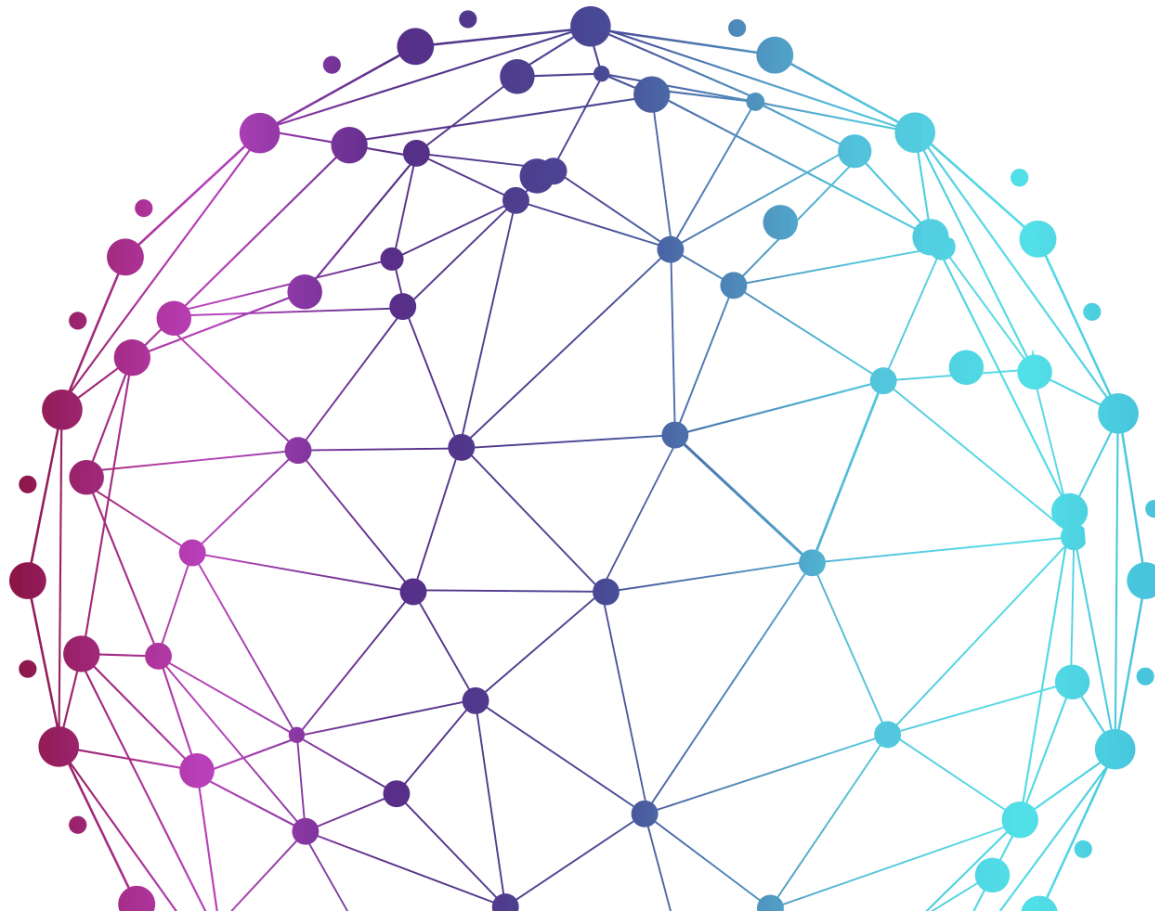
기본 지정된
즐거찾기 목록

```
"WebRecent0_URL"      "http://steamcommunity.com/id/ehdgus9549/inventory/"
"WebRecent0_Name"     "Steam 커뮤니티 :: 래커 :: 소지 항목"
"WebFrequent0_URL"    "http://steamcommunity.com/id/ehdgus9549/inventory/"
"WebFrequent0_Name"   "Steam 커뮤니티 :: 래커 :: 소지 항목"
"WebFrequent0_Access" "10"
"WebRecent1_URL"      "http://www.youtube.com/"
"WebRecent1_Name"     "YouTube"
```

자주 방문한,
최근 방문한 사이트

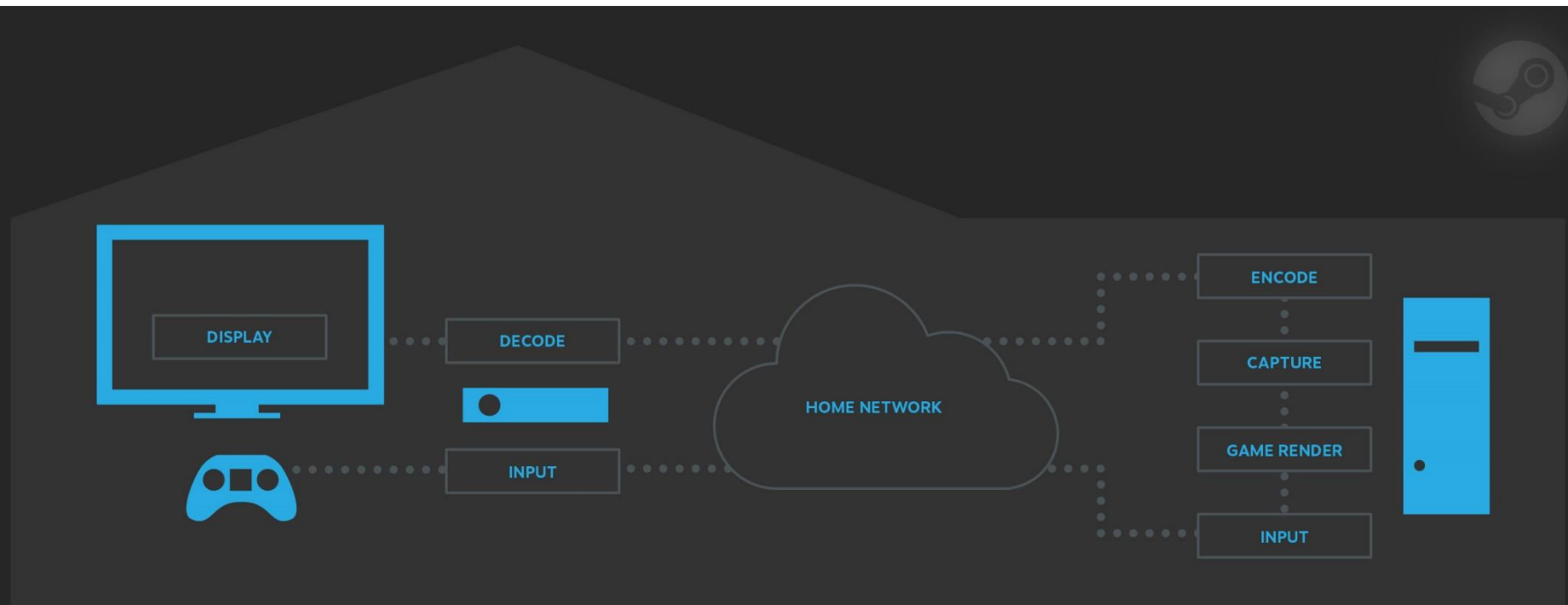


Artifact #4 – Streaming History



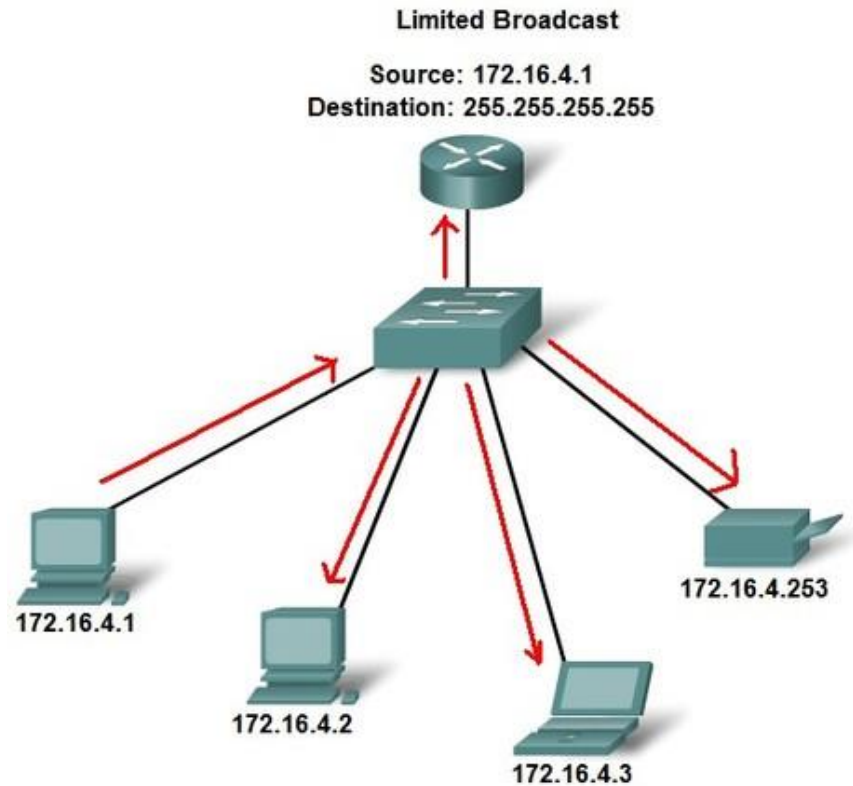


Streaming Service





Use Broadcast





appinfo_log.txt	2016-04-03 오후...	텍스트 문서	19KB
bootstrap_log.txt	2016-04-03 오후...	텍스트 문서	33KB
cloud_log.txt	2016-04-03 오후...	텍스트 문서	3KB
configstore_log.txt	2016-03-26 오후...	텍스트 문서	14KB
connection_log.txt	2016-04-03 오후...	텍스트 문서	3KB
content_log.txt	2016-04-03 오후...	텍스트 문서	13KB
librarysharing_log.txt	2016-04-03 오후...	텍스트 문서	1KB
parental_log.txt	2016-04-03 오후...	텍스트 문서	1KB
remote_connections.txt	2016-04-03 오후...	텍스트 문서	1KB
stats_log.txt	2016-04-03 오후...	텍스트 문서	3KB
workshop_log.txt	2016-04-03 오후...	텍스트 문서	1KB

File Location

C:\Program Files(x86)\Steam\log\remote_connections.txt

게임 스트리밍 연결을 위한 네트워크 기록 (상대방 IP, PC 명)



```
[2016-04-02 14:12:29] Loaded client id: 12343341285548209263  
[2016-04-02 14:12:29] Listening for broadcast on: 27036  
[2016-04-02 14:12:29] Listening for connections on: 127.0.0.1:27036
```

None-Connect

```
[2016-04-03 13:31:41] Generated client id: 12356010471690929350  
[2016-04-03 13:31:41] Listening for broadcast on: 27036  
[2016-04-03 13:31:41] Listening for connections on: 127.0.0.1:27036  
[2016-04-03 21:06:50] Received broadcast message from client 12343341285548209263 (MSDN-PC):   
[2016-04-03 21:06:50] Received discovery message from client 12343341285548209263  
[2016-04-03 21:06:53] Received discovery message from client 12343341285548209263  
[2016-04-03 21:06:54] Connecting to remote: 0x15d   
[2016-04-03 21:06:54] Received broadcast message from client 12343341285548209263 (MSDN-PC):   
[2016-04-03 21:06:54] Connected to remote client: 0x15d  
[2016-04-03 21:06:59] Received discovery message from client 12343341285548209263  
[2016-04-03 21:07:09] Received broadcast message from client 12343341285548209263 (MSDN-PC): 
```

Success Connect



Artifact #5 – Contents Download














Main Game



Mod

New World



 appinfo_log.txt	2016-04-03 오후...	텍스트 문서	19KB
 bootstrap_log.txt	2016-04-03 오후...	텍스트 문서	33KB
 cloud_log.txt	2016-04-03 오후...	텍스트 문서	3KB
 configstore_log.txt	2016-03-26 오후...	텍스트 문서	14KB
 connection_log.txt	2016-04-03 오후...	텍스트 문서	3KB
 content_log.txt	2016-04-03 오후...	텍스트 문서	13KB
 librarysharing_log.txt	2016-04-03 오후...	텍스트 문서	1KB
 parental_log.txt	2016-04-03 오후...	텍스트 문서	1KB
 remote_connections.txt	2016-04-03 오후...	텍스트 문서	1KB
 stats_log.txt	2016-04-03 오후...	텍스트 문서	3KB
 workshop_log.txt	2016-04-03 오후...	텍스트 문서	1KB

File Location

C:\Program Files(x86)\Steam\log

게임 다운로드 기록, 업데이트 기록, Workshop 이용 기록



Content_log.txt

```
[2016-04-03 20:30:25] AppID 105600 state changed : Update Required,
[2016-04-03 20:30:25] Scheduler update appID 105600: Priority First, legacy=no, restore="",
timeSinceLastPlayed=71443083, appDisableSecondsRemaining=0
[2016-04-03 20:30:25] AppID 105600 state changed : Update Required,Update Running,
[2016-04-03 20:30:25] AppID 105600 update changed : Running,
[2016-04-03 20:30:25] AppID 105600 update changed : Running,Reconfiguring,
[2016-04-03 20:30:25] Download system icon for AppID 105600 to C:\Program Files (x86)
\Steam\steam\games\aa4ce7b163832f35ffcbf560ca40974bccd5d4cd5.ico
[2016-04-03 20:30:25] Created download interface of type 'CS' (1) to host valve39.cs.steampowered.com (
valve39.cs.steampowered.com)
[2016-04-03 20:30:25] Created download interface of type 'CS' (1) to host valve41.cs.steampowered.com (
valve41.cs.steampowered.com)
[2016-04-03 20:30:25] Created download interface of type 'CS' (1) to host valve40.cs.steampowered.com (
valve40.cs.steampowered.com)
[2016-04-03 20:30:25] HTTP (CS,110) - valve41.cs.steampowered.com (valve41.cs.steampowered.com):
OpenConnection - Success!
[2016-04-03 20:30:25] HTTP (CS,108) - valve39.cs.steampowered.com (valve39.cs.steampowered.com):
OpenConnection - Success!
[2016-04-03 20:30:25] HTTP (CS,109) - valve40.cs.steampowered.com (valve40.cs.steampowered.com):
OpenConnection - Success!
[2016-04-03 20:30:25] HTTP (CS,110) - valve41.cs.steampowered.com (valve41.cs.steampowered.com):
AuthenticateDepotID (105601) - Success!
[2016-04-03 20:30:26] HTTP (CS,110) - valve41.cs.steampowered.com (valve41.cs.steampowered.com):
/depot/105601/manifest/4187789340605599532/5 - received 200 (OK) HTTP response
[2016-04-03 20:30:26] AppID 105600 update changed : Running,
[2016-04-03 20:30:26] AppID 105600 update changed : Running,Validating,
[2016-04-03 20:30:26] AppID 105600 update changed : Running,
[2016-04-03 20:30:26] AppID 105600 update changed : Running,Preallocating,
[2016-04-03 20:30:27] AppID 105600 update changed : Running,
[2016-04-03 20:30:27] AppID 105600 update started : download 0/83890656, store 0/0, reuse 0/0, stage
0/103873023
[2016-04-03 20:30:27] AppID 105600 state changed : Update Required,Update Running,Update Started,
[2016-04-03 20:30:27] AppID 105600 update changed : Running,Downloading,
[2016-04-03 20:30:27] AppID 105600 update changed : Running,Downloading,Staging,
[2016-04-03 20:30:27] HTTP (CS,108) - valve39.cs.steampowered.com (valve39.cs.steampowered.com):
AuthenticateDepotID (105601) - Success!
[2016-04-03 20:30:27] HTTP (CS,109) - valve40.cs.steampowered.com (valve40.cs.steampowered.com):
AuthenticateDepotID (105601) - Success!
[2016-04-03 20:30:27] Scheduler update appID 105600: Priority Last, legacy=no, restore="",
```




APP ID?

The screenshot shows the SteamDB website. At the top is a navigation bar with links: Apps, Packages, Sales, Calculator, Forum, Stats, and Other. There is also a search bar and a 'Sign In' button. Below the navigation bar is a large black banner with the text 'Welcome to the Steam Database!'. Underneath the banner, there is a paragraph of text explaining the tool's purpose and providing links to a FAQ and forums. At the bottom, there are two tables: 'Most Played Games' and 'Currently on Sale'.

Welcome to the Steam Database!

This tool was made to give better insight into the applications and packages that [Steam](#) has in its database.

Apps and packages in the database will update the second Steam sends out the update to the Steam client.

Check out our [FAQ](#) if you have any questions about SteamDB, if your question is not listed feel free to make a thread on our [forums](#).

Most Played Games			
	Name	Current Players	Peak Today
	Dota 2	864,057	909,145
	Counter-Strike: GL...	484,748	672,192
	Team Fortress 2	54,060	59,142
	Grand Theft Auto V	49,603	50,172
	Football Manager ...	40,165	60,361
	Tom Clancy's The...	38,160	38,579

Currently on Sale			
	Name	Discount	Price
	HotLead	-51%	\$0.49
	Lup	-51%	\$0.49
	Cultures - Northland	-90%	\$0.79
	Jagged Alliance 2 - Wildfire	-87%	\$0.90
	RoBoRumble	-80%	\$1.19
	The Sun and Moon	-66%	\$2.37

<https://steamdb.info>



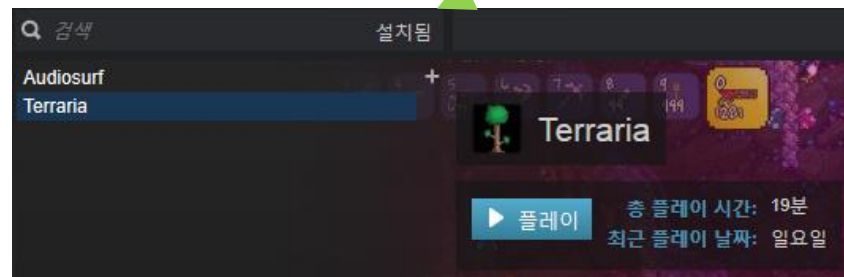
```
[2016-04-03 20:30:25] AppID 105600 state changed : Update Required,  
[2016-04-03 20:30:25] Scheduler update appID 105600: Priority First, legacy=no, restore="",  
timesSinceLastPlayed=71443083, appDisableSecondsRemaining=0  
[2016-04-03 20:30:25] AppID 105600 state changed : Update Required,Update Running,  
[2016-04-03 20:30:25] AppID 105600 update changed : Running,  
[2016-04-03 20:30:25] AppID 105600 update changed : Running,Reconfiguring,  
[2016-04-03 20:30:25] Download system icon for AppID 105600 to C:\Program Files (x86)  
[2016-04-03 20:30:25] Steam\steam\games\04ce7b163832f35ffcbf560ca40974bccd5d4cd5.ico  
[2016-04-03 20:30:25] Created download interface of type 'CS' (1) to host valve39.cs.steampowered.com (valve39.cs.steampowered.com)  
[2016-04-03 20:30:25] Created download interface of type 'CS' (1) to host valve41.cs.steampowered.com (valve41.cs.steampowered.com)  
[2016-04-03 20:30:25] Created download interface of type 'CS' (1) to host valve40.cs.steampowered.com (valve40.cs.steampowered.com)  
[2016-04-03 20:30:25] HTTP (CS,110) - valve41.cs.steampowered.com (valve41.cs.steampowered.com):  
OpenConnection - Success!  
[2016-04-03 20:30:25] HTTP (CS,108) - valve39.cs.steampowered.com (valve39.cs.steampowered.com):  
OpenConnection - Success!  
[2016-04-03 20:30:25] HTTP (CS,109) - valve40.cs.steampowered.com (valve40.cs.steampowered.com):  
OpenConnection - Success!  
[2016-04-03 20:30:25] HTTP (CS,110) - valve41.cs.steampowered.com (valve41.cs.steampowered.com):  
AuthenticateDepotID (105601) - Success!  
[2016-04-03 20:30:26] HTTP (CS,110) - valve41.cs.steampowered.com (valve41.cs.steampowered.com):  
/depot/105601/manifest/41e72e0340c0e50a62326 received 200 (OK) HTTP response  
[2016-04-03 20:30:26] AppID 105600 update changed : Running,  
[2016-04-03 20:30:26] AppID 105600 update changed : Running,Validating,  
[2016-04-03 20:30:26] AppID 105600 update changed : Running,  
[2016-04-03 20:30:26] AppID 105600 update changed : Running,Preallocating,  
[2016-04-03 20:30:27] AppID 105600 update changed : Running,  
[2016-04-03 20:30:27] AppID 105600 update started : download 0/83890656, store 0/0, reuse 0/0, stage  
0/103873023  
[2016-04-03 20:30:27] AppID 105600 state changed : Update Required,Update Running,Update Started,  
[2016-04-03 20:30:27] AppID 105600 update changed : Running,Downloading,  
[2016-04-03 20:30:27] AppID 105600 update changed : Running,Downloading,Staging,  
[2016-04-03 20:30:27] HTTP (CS,108) - valve39.cs.steampowered.com (valve39.cs.steampowered.com):  
AuthenticateDepotID (105601) - Success!  
[2016-04-03 20:30:27] HTTP (CS,109) - valve40.cs.steampowered.com (valve40.cs.steampowered.com):  
AuthenticateDepotID (105601) - Success!  
[2016-04-03 20:30:27] Scheduler update appID 105600: Priority Last, legacy=no, restore="",
```



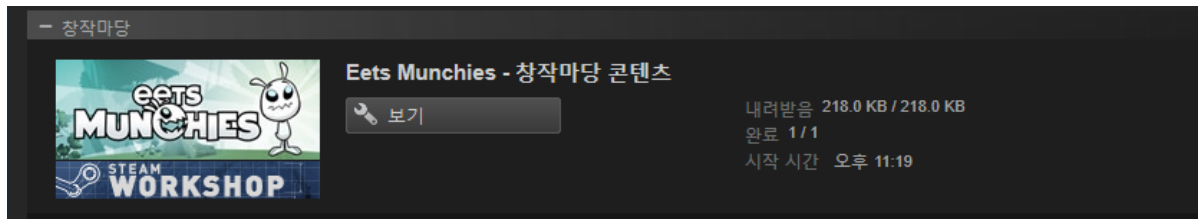
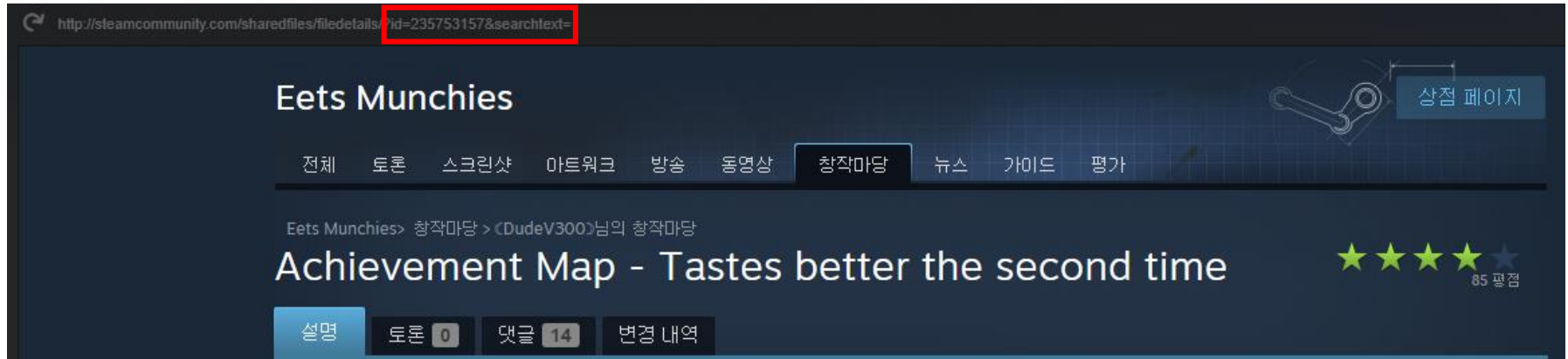
Terraria	
App ID	105600
App Type	Game
Name	Terraria
Developer	● Re-Logic
Publisher	● Re-Logic
Supported Systems	STEAMPLAY
Last Record Update	21 days ago (March 15, 2016 - 23:26:23 UTC)
Last Change Number	1826540
Release Date	May 16, 2011 (5 years ago)

APP ID : 105600

Terraria



Installed!



Installed!

```
[2016-04-05 23:05:45] [AppID 214550] Loaded workshop items in "C:\Program Files (x86)\Steam\steamapps\workshop" (0 installed, 0 needed)
[2016-04-05 23:06:07] [AppID 214550] Starting Workshop download job
[2016-04-05 23:06:07] [AppID 214550] Finished Workshop download job : No Error
[2016-04-05 23:19:17] [AppID 214550] Subscribed to item 235753157
```

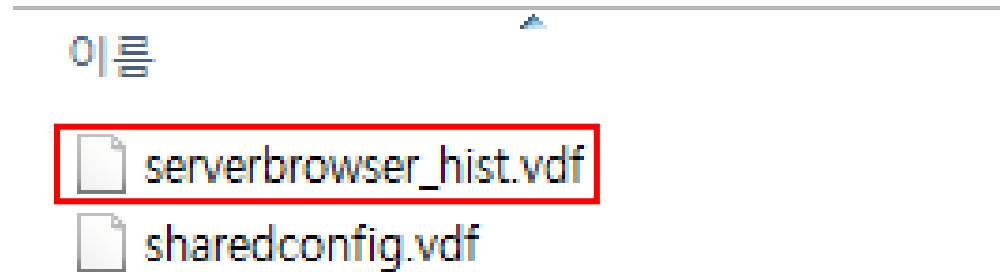
APP ID : 214550

Item : 235753157



Artifact #6 – Connect server History





File Location

C:\Program Files(x86)\Steam\userdata\[Usernum]\7

게임 내 서버 접속 기록, IP 및 즐겨 찾기 서버 IP

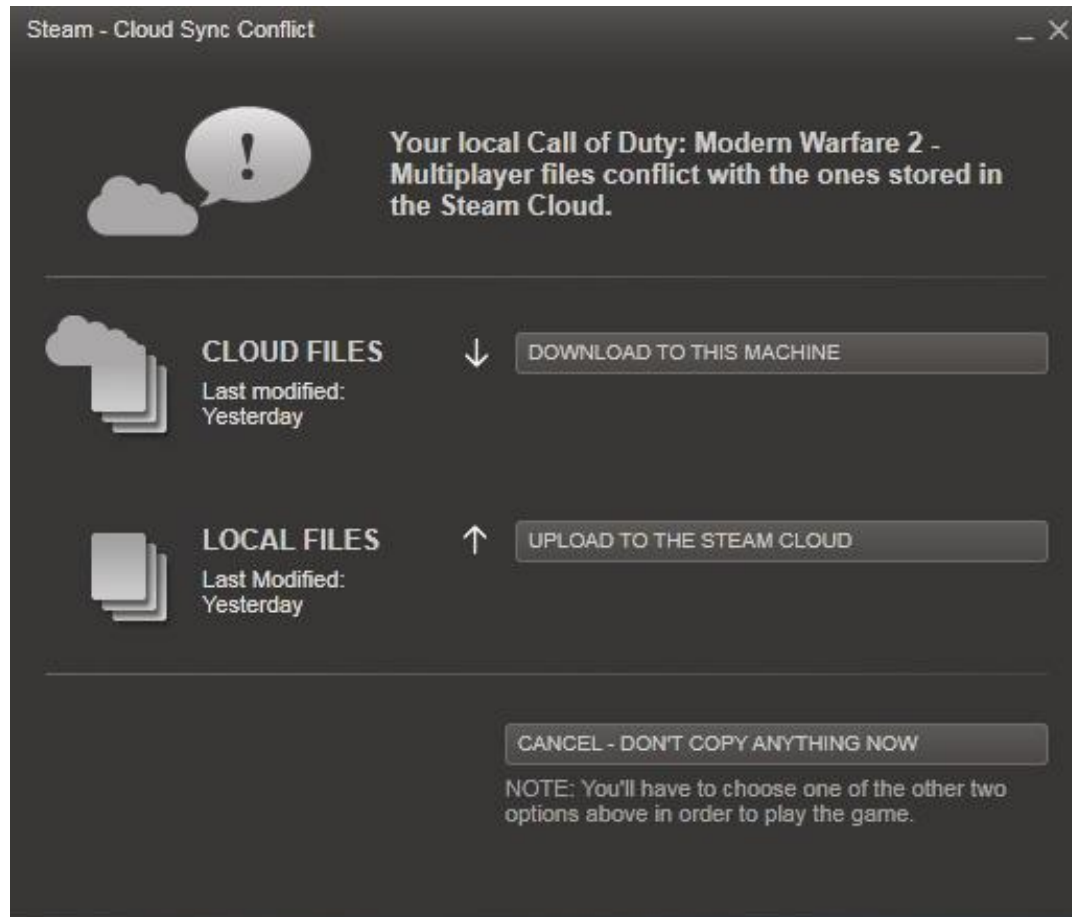


Favorite Server

```
"Filters"
{
  "Favorites"
  {
    "1"
    {
      "name"      "14.35.19.192:27015"
      "address"    "14.35.19.192:27015"
      "LastPlayed" "1358486572"
      "appid"      "0"
      "accountid"  "0"
    }
    "2"
    {
      "name"      "121.143.109.99:27016"
      "address"    "121.143.109.99:27016"
      "LastPlayed" "1358495778"
      "appid"      "0"
      "accountid"  "0"
    }
    "3"
    {
      "name"      "221.153.224.42:4860"
      "address"    "221.153.224.42:4860"
      "LastPlayed" "1358489479"
      "appid"      "0"
      "accountid"  "0"
    }
    "4"
    {
      "name"      "119.196.47.96:27016"
      "address"    "119.196.47.96:27016"
      "LastPlayed" "1368887677"
      "appid"      "0"
      "accountid"  "0"
    }
  }
}
```












Connect History

```
"history"
{
  "1"
  {
    "name"      "14.35.19.192:27015"
    "address"    "14.35.19.192:27015"
    "LastPlayed" "1358486572"
    "appid"      "0"
    "accountid"  "0"
  }
  "2"
  {
    "name"      "121.143.109.99:27016"
    "address"    "121.143.109.99:27016"
    "LastPlayed" "1358495778"
    "appid"      "0"
    "accountid"  "0"
  }
  "4"
  {
    "name"      "119.196.47.96:27016"
    "address"    "119.196.47.96:27016"
    "LastPlayed" "1368887677"
    "appid"      "0"
    "accountid"  "0"
  }
  "5"
  {
    "name"      "220.125.78.20:27015"
    "address"    "220.125.78.20:27015"
    "LastPlayed" "1368939187"
    "appid"      "0"
    "accountid"  "0"
  }
}
```



Artifact #7 – Cloud System



 appinfo_log.txt	2016-04-03 오후...	텍스트 문서	19KB
 bootstrap_log.txt	2016-04-03 오후...	텍스트 문서	33KB
 cloud_log.txt	2016-04-03 오후...	텍스트 문서	3KB
 configstore_log.txt	2016-03-26 오후...	텍스트 문서	14KB
 connection_log.txt	2016-04-03 오후...	텍스트 문서	3KB
 content_log.txt	2016-04-03 오후...	텍스트 문서	13KB
 librarysharing_log.txt	2016-04-03 오후...	텍스트 문서	1KB
 parental_log.txt	2016-04-03 오후...	텍스트 문서	1KB
 remote_connections.txt	2016-04-03 오후...	텍스트 문서	1KB
 stats_log.txt	2016-04-03 오후...	텍스트 문서	3KB
 workshop_log.txt	2016-04-03 오후...	텍스트 문서	1KB

File Location

C:\WProgram Files(x86)\WSteam\Wlog

게임의 Save File 및 Profile을 동기화 및 업로드한 기록



```
[2016-04-03 21:06:36] [AppID 72850] File is in sync My Games/Skyrim/Saves/Save 11 - ashhr 02.53.59.ess  
[2016-04-03 21:06:36] [AppID 72850] File is in sync My Games/Skyrim/Saves/backup-1_16-23.51.54.ess  
[2016-04-03 21:06:36] [AppID 72850] Eval complete  
[2016-04-03 21:06:36] [AppID 259080] Eval complete
```

Skyrim (SKSE) Steam Cloud Profile & Save File

ashr, 하이엘프, 레벨 23
016.41.55
1/21/2016, 11:32 PM

자동 The Ragged Flagon
자동 The Ratway
자동 Riften
빠른저 The Ragged Flagon
012 backup-1_16-23.51.54
011 스카이림

이여하기
새로시작



Reference

- Playing the Forensics Game (Peter Clemenko)
- Steam Forensic Artifacts (Tod Delaricheliere)
- 해외 자료 : 빈약 ...
- 국내 자료 : 없음 ...

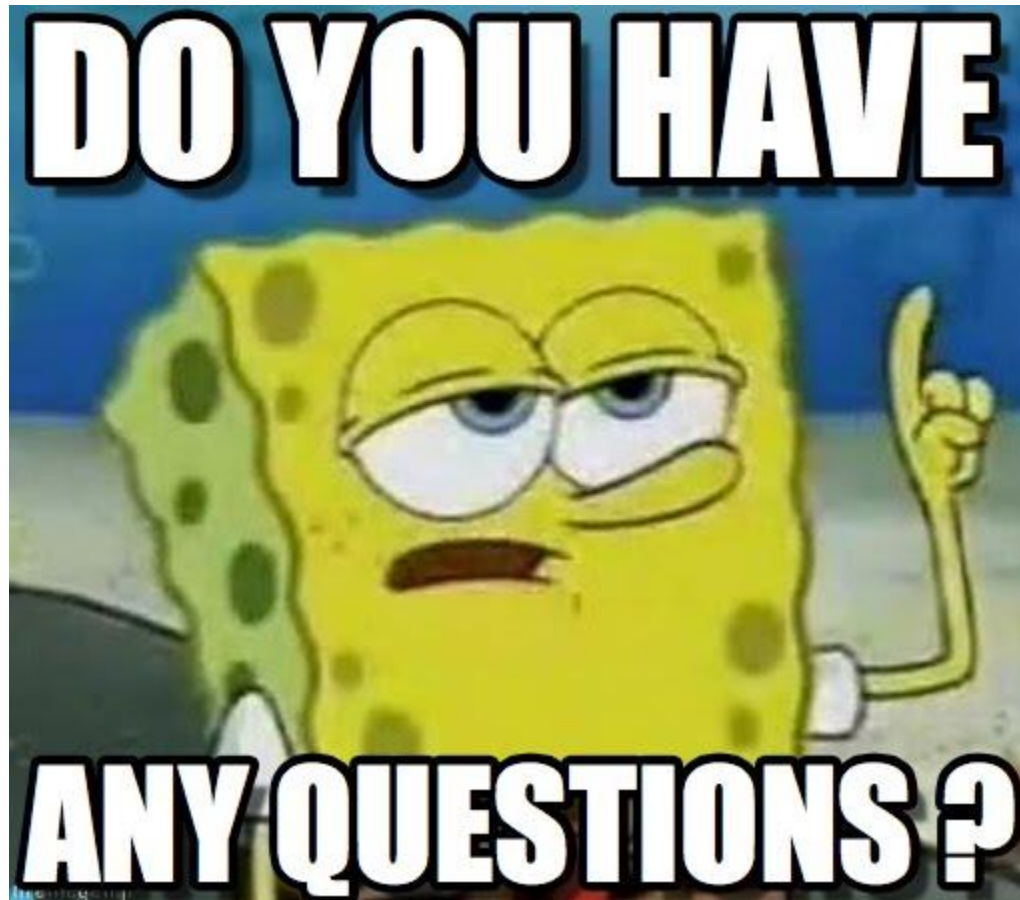


결론

- 로컬 파일에서도 많은 중요한 정보를 수집이 가능.
- 계정 탈취와 관련하여 사회적 공학 기법에 활용 될 수 있음.
- 특정 증거 수집을 위해서는 배경 지식이 필요.
- 계정 내에서 얻을 수 있는 더 많은 중요 정보가 존재함.
- 이러한 게임 플랫폼에서의 증거 수집에 대한 연구 필요.



Q & A





Thank you!

