

## 2 Monitoring von Sockets)

1)

139 Sockets sind offen.

2)

UDP hat keinen State, TCP schon.

UDP verwendet nie einen Remote Port

3)

Established: represents an open connection, data received can be delivered to the user. The normal state for the data transfer phase of the connection.

Listening: represents waiting for a connection request from any remote TCP and port.






















Close Wait: represents waiting for a connection termination request from the local user.

Time Wait: represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request.

4)

28 Listening States + 46 UDP

5)

	RiotClientServ...	2180	TCP	49999	127.0.0.1	50710	127.0.0.1	Established
	chrome.exe	7072	TCP	50373	192.168.1.5	443	https 141.37.20.51	bbbsrv4.htwg-kon... Established
	Discord.exe	4480	TCP	50388	192.168.1.5	443	https 162.159.135.234	Established
	chrome.exe	7072	TCP	50547	192.168.1.5	443	https 141.37.20.51	bbbsrv4.htwg-kon... Established
	Spotify.exe	8524	TCP	50560	192.168.1.5	443	https 35.186.224.25	25.224.186.35.bc.g... Established
	chrome.exe	7072	TCP	50577	192.168.1.5	443	https 141.37.20.27	feproxysrv1.htwg-... Established
	Discord.exe	4480	TCP	50605	192.168.1.5	443	https 162.159.138.232	Established
	Spotify.exe	8524	TCP	50643	192.168.1.5	443	https 151.101.114.248	Established
	chrome.exe	7072	TCP	50648	192.168.1.5	443	https 141.37.20.51	bbbsrv4.htwg-kon... Established
	chrome.exe	7072	TCP	50651	192.168.1.5	443	https 216.58.206.14	fra16s20-in-f14.1e... Established
	chrome.exe	7072	TCP	50685	192.168.1.5	443	https 172.217.22.14	fra16s14-in-f14.1e... Established
	chrome.exe	7072	TCP	50686	192.168.1.5	443	https 216.58.212.138	ams15s21-in-f10.1... Established
	chrome.exe	7072	TCP	50692	192.168.1.5	443	https 108.177.127.189	Established
	chrome.exe	7072	TCP	50695	192.168.1.5	443	https 172.217.18.99	zrh04s05-in-f99.1e... Established
	RiotClientServ...	2180	TCP	50702	192.168.1.5	443	https 162.247.243.239	Established
	chrome.exe	7072	TCP	50704	192.168.1.5	443	https 172.217.23.132	fra16s18-in-f132.1... Established
	GameBarPrese...	8528	TCP	50705	192.168.1.5	443	https 40.67.188.15	Established
	LeagueClient...	7732	TCP	50708	192.168.1.5	443	https 104.19.222.81	Established
	LeagueClient...	7732	TCP	50710	127.0.0.1	49999	127.0.0.1	Established
	RiotClientServ...	2180	TCP	50713	192.168.1.5	443	https 2.17.45.152	a2-17-45-152.depl... Established
	chrome.exe	7072	TCP	50714	192.168.1.5	443	https 172.217.23.131	fra16s18-in-f3.1e1... Established

21 neue Establishes

6)

Um sich selbst zu pingen (lokale IP-Adresse)

Die meisten agieren über 80 und 443.  
Spotify einmal über 4070 (tripe)  
LeagueClient über 2099 (H.255.0 Annex G Signalling)  
RiotClientService über 5223 (HP Virtual Management Group)  
chrome einmal über 5228 (Reserved Netflow/IPFIX/sFlow)

### 3 Details über die Kommunikationspartner ihres PCs)

241	2.123980	199.212.0.46	192.168.1.5	TCP	60 43 → 55403 [ACK] Seq=1 Ack=21 Win=29440 Len=0
242	2.124867	199.212.0.46	192.168.1.5	TCP	392 43 → 55403 [PSH, ACK] Seq=1 Ack=21 Win=29440 Len=338 [TCP segment of a reassembled PDU]
243	2.126003	199.212.0.46	192.168.1.5	TCP	1514 43 → 55403 [ACK] Seq=339 Ack=21 Win=29440 Len=1460 [TCP segment of a reassembled PDU]
244	2.126020	192.168.1.5	199.212.0.46	TCP	54 55403 → 43 [ACK] Seq=21 Ack=1799 Win=262656 Len=0
245	2.126401	199.212.0.46	192.168.1.5	WHOIS	1091 Answer: n + 34.212.119.245
246	2.126417	192.168.1.5	199.212.0.46	TCP	54 55403 → 43 [ACK] Seq=21 Ack=2837 Win=261632 Len=0
247	2.126483	192.168.1.5	199.212.0.46	TCP	54 55403 → 43 [FIN, ACK] Seq=21 Ack=2837 Win=261632 Len=0

### WHOIS and TCP

2)

Order	IP Address	Status	Country	Network Name	Owner Name	From IP	To IP	CIDR	Allocated	Contact Name	Address	Postal Code	Email	Abuse Email	Abuse Contact	Phone	Fax	Whois Source
1	178.250.2.146	Succeed	France	CRITEO-EURO...	Criteo Europe L...	178.250.0.0	178.250.3.255	178.250.0.0/22	Yes	Criteo Networ...	Criteo, 32 Rue ...		ripe@criteo.com		noc@criteo.com			RIPE NCC
2	205.185.216.42	Succeed	USA - Texas	HIGHWINDS-A...	Highwinds Net...	205.185.216.0	205.185.216.255	205.185.216.0/24	Yes	Highwinds Net...	2021 McKinne...	75201	neteng@stack...	abuse@hwng...		+1-469-899-57...		ARIN
3	216.58.206.1	Succeed	USA - California	GOOGLE	Google LLC	216.58.192.0	216.58.223.255	216.58.192.0/19	Yes	Google LLC	1600 Amphith...	94043	arin-contact@...	network-abuse...		+1-650-253-00...		ARIN
4	217.79.188.54	Succeed	Germany	FASTIT-DE-DU...	ADITION techn...	217.79.188.0	217.79.188.63	217.79.188.0/26	Yes	Marcus Schlue...	ADITION techn...		info@adition.c...	abuse@myloc...	abuse@myloc...	+49 761 88147 ...	+49 761 88147 ...	RIPE NCC
5	144.76.223.73	Succeed	Germany	HETZNER-fsn1...	Hetzner Online...	144.76.223.64	144.76.223.95	144.76.223.64/27	Yes	Hetzner Online...	Hetzner Online...		ripe@hetzner.c...	abuse@hetzne...	abuse@hetzne...	+49 9831 505-0	+49 9831 505-3	RIPE NCC
6	88.198.47.102	Succeed	Germany	HETZNER-RZ...	Hetzner Online...	88.198.32.0	88.198.63.255	88.198.32.0/19	Yes	Hetzner Online...	Hetzner Online...		ripe@hetzner.c...	abuse@hetzne...	abuse@hetzne...	+49 9831 505-0	+49 9831 505-3	RIPE NCC
7	91.215.100.40	Succeed	Germany	DE-INFONLINE...	INFOnline Gm...	91.215.100.0	91.215.103.255	91.215.100.0/22	Yes	Steffen Passm...	INFOnline Gm...		spassmann@i...	abuse@infonli...	abuse@infonli...	+49 228 41029 ...		RIPE NCC
8	148.251.64.134	Succeed	Germany	GUNDI-ELECT...	G+J Electronic ...	148.251.64.134	148.251.64.134	148.251.64.134...	Yes	Anne Steinmetz	G+J Electronic ...		steinmetz.ame...		abuse@hetzne...	+494037037384		RIPE NCC
9	54.220.3.30	Succeed	USA - Washing...	AMAZO-ZDUB4	Amazon.com, ...	54.220.0.0	54.220.255.255	54.220.0.0/16	Yes	Amazon.com, ...	Amazon Web ...	98108-1226	amzn-noc-con...	abuse@amazo...		+1-206-266-40...		ARIN

Order	IP Address	Status	Country	Network Name	Owner Name	From IP	To IP
1	141.37.20.24	Succeed	Germany	FH-KN	Hochschule K...	141.37.0.0	141.37.255.255
2	141.37.20.17	Succeed	Germany	FH-KN	Hochschule K...	141.37.0.0	141.37.255.255

inetnum: 141.37.0.0 - 141.37.255.255  
netname: FH-KN  
country: DE  
admin-c: HKTW1-RIPE  
tech-c: HKTW1-RIPE  
org: ORG-HKTW1-RIPE  
status: LEGACY  
remarks: \*\*\*\*\*  
remarks: \* DEFAULT ABUSE CONTACT: abuse@htwg-konstanz.de \*  
remarks: \*\*\*\*\*  
mnt-by: BELWUE-MNT  
mnt-by: RIPE-NCC-LEGACY-MNT  
created: 2002-04-25T09:54:38Z  
last-modified: 2016-04-14T08:23:18Z  
source: RIPE  
sponsoring-org: ORG-BA9-RIPE  
  
organisation: ORG-HKTW1-RIPE  
org-name: Hochschule Konstanz Technik, Wirtschaft und Gestaltung  
org-type: OTHER  
address: Brauneggerstr. 55  
address: 78462 Konstanz, Germany  
e-mail: netzwerk@htwg-konstanz.de  
admin-c: HKTW1-RIPE  
tech-c: HKTW1-RIPE  
abuse-c: HKTW1-RIPE

mnt-ref: BELWUE-MNT  
mnt-by: BELWUE-MNT  
created: 2015-06-17T14:46:25Z  
last-modified: 2015-06-18T11:34:36Z  
source: RIPE

role: Hochschule Konstanz Technik, Wirtschaft und Gestaltung  
address: Brauneggerstr. 55  
address: 78462 Konstanz, Germany  
e-mail: netzwerk@htwg-konstanz.de  
admin-c: MS3208-RIPE  
tech-c: MS3208-RIPE  
nic-hdl: HKTW1-RIPE  
abuse-mailbox: abuse@htwg-konstanz.de  
mnt-by: BELWUE-MNT  
created: 2015-06-17T14:46:25Z  
last-modified: 2015-06-18T11:34:36Z  
source: RIPE

% Information related to '141.37.0.0/16AS553'

route: 141.37.0.0/16  
descr: FH-KONSTANZ  
origin: AS553  
mnt-by: BELWUE-MNT  
created: 1970-01-01T00:00:00Z  
last-modified: 2001-09-22T09:32:38Z  
source: RIPE

% This query was served by the RIPE Database Query Service version 1.98 (HEREFORD)

4)

21 neue Sockets

5)

65535 TCP-Ports+ 65535 UDP-Ports

6)

443 (https)

7)

Julien Bailhache  
Amazon Data Services Limited Ireland  
Google LLC  
Marcus Schlueter  
Steffen Passmann  
Hetzner Online GmbH  
Akamai Technologies  
viel Amazon

Bei Naver:  
IP Manager von Naver  
Akamai Technologies