Wireshark starten. Als ersten Schritt die Netzwerkkarte bestimmen, deren Verkehr protokolliert werden soll. Hier LAN-Verbindung. Die beiden darüber genannten Adapter gehören zu VMware.



Anschließend auf Start klicken und das Protokollieren beginnt. Wenn nicht viel Verkehr ist, kann man die gewünschte IP-Adresse im Protokollfenster sehen und man klickt Stop zum Anhalten und schaut nach, was gelaufen ist. Ein Ausschnitt von meinem Rechner. IP-Adressen, die mit 192.168.\*.\* beginnen, sind aus dem lokalen Netz.

2*LAII-Verbindung [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]					
Elle Edit View Go Capture Analyze Statistics Telephony Tools Internals Help					
0	۲	📕 🖩 🖉 🗎 🗶 🥰 🛛 🔍	🍬 🔶 🔷 🔁 🛛		Q. 🖾   👪 🗹 🔞 %   💢
Filter: Expression Clear Apply Save					
No.		Time Source	Destination	Protocol Ler	ngth (Info
	7	8 30.89237100(Asustekc_5d:88:ba	Broadcast	ARP	42 who has 192.168.0.9? Tell 192.168.0.3
	7	9 31.89077700(AsustekC_5d:88:ba	Broadcast	ARP	42 who has 192.168.0.9? Tell 192.168.0.3
	8	0 36.51305200(192.168.0.3	144.76.88.213	TCP	66 50055-443 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1
	8	1 36.51353800(144.76.88.213	192.168.0.3	TCP	66 443→50055 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_F
	8	2 36.51360700(192.168.0.3	144.76.88.213	TCP	54 50055→443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
	8	3 36.51417600(192.168.0.3	144.76.88.213	TLSv1.2	571 Client Hello
	8	4 36.51450600(144.76.88.213	192.168.0.3	TCP	60 443→50055 [ACK] Seq=1 Ack=518 Win=15680 Len=0
	8	5 36.72991300(144.76.88.213	192.168.0.3	TLSV1.2	191 Server Hello, Change Cipher Spec, Encrypted Handshake Message
	8	6 36.73322000(192.168.0.3	144.76.88.213	TLSV1.2	105 Change Cipher Spec, Hello Request, Hello Request
	8	7 36.73360900(144.76.88.213	192.168.0.3	TCP	60 443→50055 [ACK] Seq=138 Ack=569 Win=15680 Len=0
	8	8 36.73586900(192.168.0.3	144.76.88.213	TLSV1.2	847 Application Data
	8	9 36.73620700(144.76.88.213	192.168.0.3	TCP	60 443→50055 [ACK] Seq=138 Ack=1362 Win=17280 Len=0
	9	0 37.03358600(144.76.88.213	192.168.0.3	TLSV1.2	462 Application Data, Application Data, Application Data, Applicatic
	9	1 37.23624400(144.76.88.213	192.168.0.3	TLSv1.2	462 [TCP Retransmission] Application Data, Application Data, Applica
	9	2 37.23633200(192.168.0.3	144.76.88.213	TCP	66 50055→443 [ACK] Seq=1362 Ack=546 Win=66048 Len=0 SLE=138 SRE=54€
	9	3 37.23666400(144.76.88.213	192.168.0.3	TLSV1.2	88 Application Data
	9	4 37.44838300(192.168.0.3	144.76.88.213	TCP	54 50055→443 [ACK] Seq=1362 Ack=580 Win=66048 Len=0
	9	5 37.72137200(192.168.0.3	144.76.88.213	TLSV1.2	969 Application Data
	9	6 37.72188900(144.76.88.213	192.168.0.3	TCP	60 443→50055 [ACK] Seq=580 Ack=2277 Win=19136 Len=0
	9	7 38.06214300(144.76.88.213	192.168.0.3	TLSV1.2	416 Application Data, Application Data, Application Data, Applicatic
	9	8 38.27722600(192.168.0.3	144.76.88.213	TCP	54 50055→443 [ACK] Seq=2277 Ack=942 Win=65792 Len=0
	9	9 38.27764700(144.76.88.213	192.168.0.3	TLSV1.2	88 Application Data
	10	0 38.47995400(192.168.0.3	144.76.88.213	TCP	54 50055→443 [ACK] Seq=2277 Ack=976 Win=65792 Len=0
	10	1 39.21029700(192.168.0.99	224.0.2.3	IGMPV2	60 Membership Report group 224.0.2.3
	10	2 40.37952700(AsustekC_5d:88:ba	Broadcast	ARP	42 who has 192.168.0.101? Tell 192.168.0.3
	10	3 40.38022500(BrotherI_a3:58:e4	AsustekC_5d:88:ba	ARP	60 192.168.0.101 is at 00:1b:a9:a3:58:e4
	10	4 40.38025200(192.168.0.3	192.168.0.101	SNMP	120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.
	10	5 40.38395200(192.168.0.101	192.168.0.3	SNMP	123 get-response 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1

Die IP-Adresse 144.76.88.213 ist übrigens club.computerwissen.de