

Lista 2 – Redes de computadores I

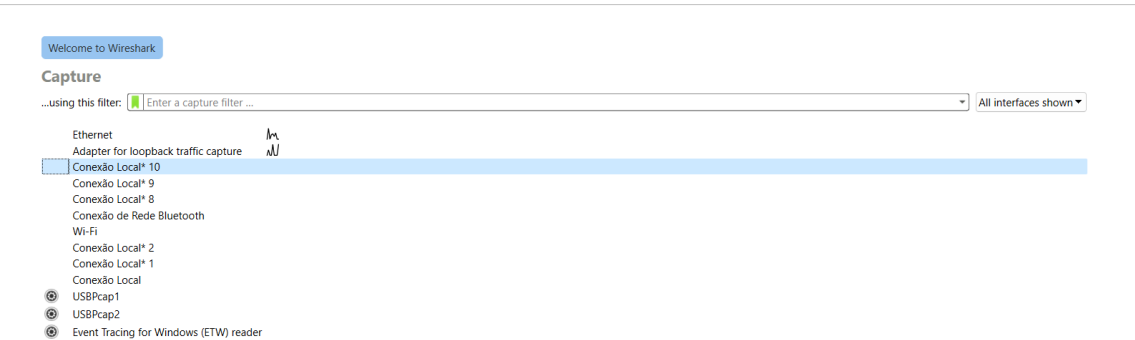
Felipe Campolina

1)

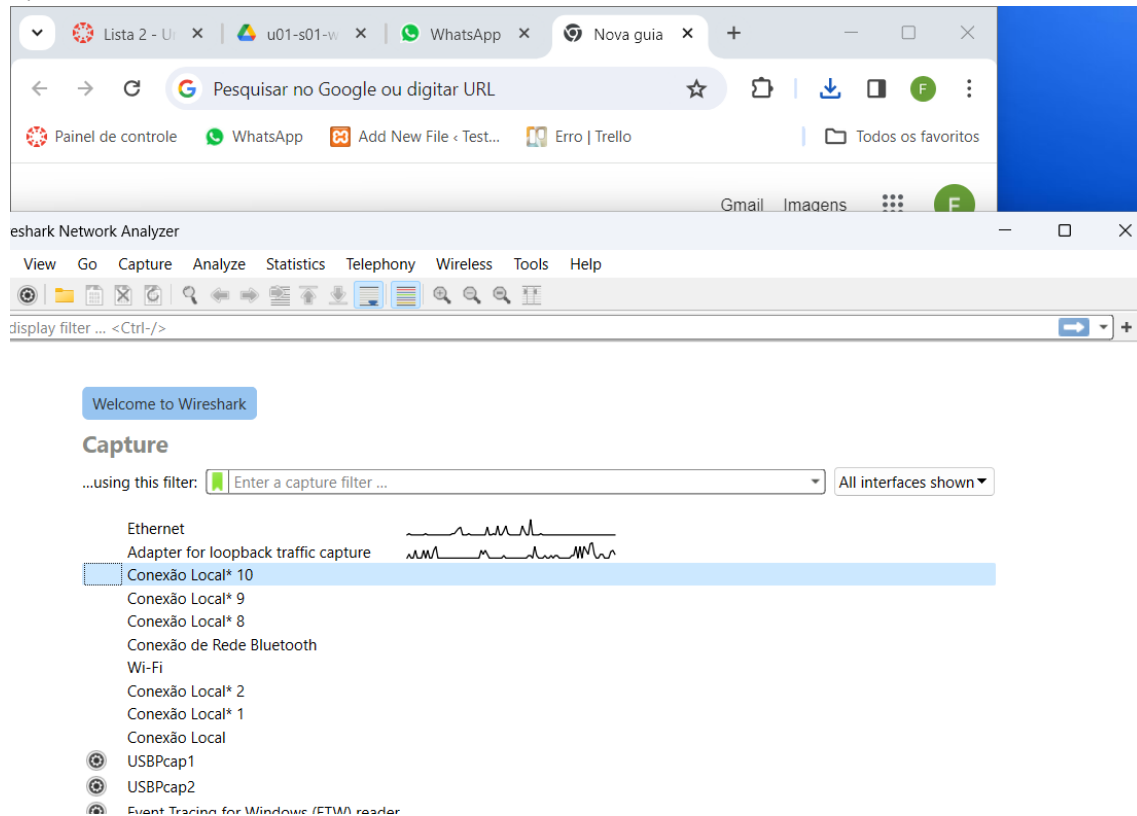
```
Adaptador Ethernet Ethernet:

Sufixo DNS específico de conexão. . . . . : tendawifi.com
Endereço IPv6 de link local . . . . . : fe80::f12a:fae8:1042:2b69%14
Endereço IPv4. . . . . : 192.168.5.67
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : 192.168.5.1
```

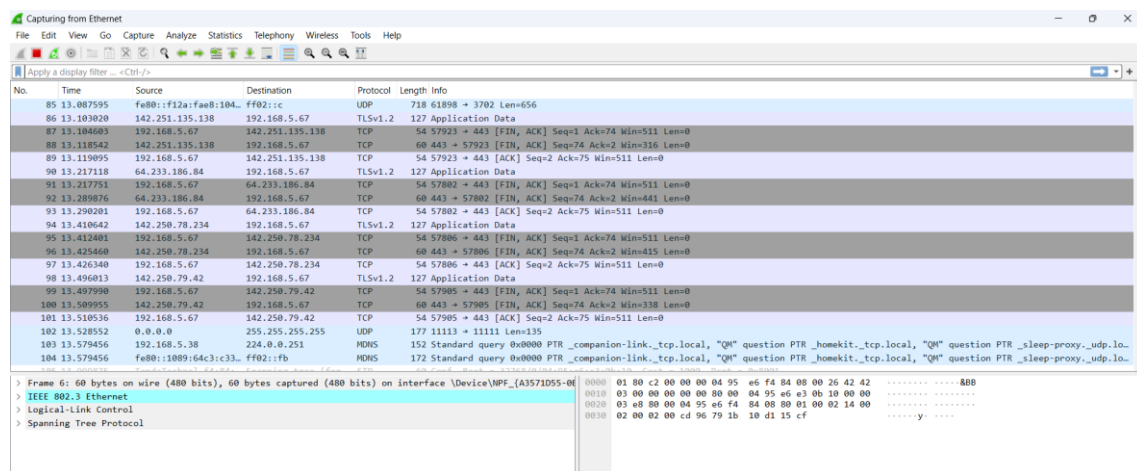
2)



3)



4)



5)

No.	Time	Source	Destination	Protocol	Length	Info
4	0.875738	152.255.32.42	192.168.5.67	TCP	66	443 → 57991 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
15	4.504318	142.250.79.3	192.168.5.67	TCP	66	443 → 57991 [ACK] Seq=1 Ack=2 Win=269 Len=0 SLE=1 SRE=2
16	4.642373	4.1.82.186	192.168.5.67	TCP	60	443 → 57962 [ACK] Seq=1 Ack=79 Win=63747 Len=0
17	4.642373	4.1.82.186	192.168.5.67	TCP	60	443 → 57962 [ACK] Seq=1 Ack=951 Win=63747 Len=0
18	4.642373	4.1.82.186	192.168.5.67	TLsv1.2	189	Application Data
19	4.642373	4.1.82.186	192.168.5.67	TLsv1.2	197	Application Data
20	4.642373	4.1.82.186	192.168.5.67	TLsv1.2	114	Application Data
35	7.904458	20.42.73.27	192.168.5.67	TCP	60	443 → 58038 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	9.384967	162.159.136.234	192.168.5.67	TCP	60	443 → 54188 [ACK] Seq=1 Ack=55 Win=7 Len=0
49	9.510650	162.159.136.234	192.168.5.67	TLsv1.2	86	Application Data
54	9.727438	142.250.79.174	192.168.5.67	TCP	66	443 → 57788 [ACK] Seq=1 Ack=2 Win=2710 Len=0 SLE=1 SRE=2
60	10.582840	142.250.79.163	192.168.5.67	TCP	66	443 → 57913 [ACK] Seq=1 Ack=2 Win=289 Len=0 SLE=1 SRE=2
64	11.171283	142.251.135.65	192.168.5.67	TLsv1.2	127	Application Data
66	11.189296	142.251.135.65	192.168.5.67	TCP	60	443 → 57789 [FIN, ACK] Seq=74 Ack=2 Win=316 Len=0
68	11.346881	142.251.135.78	192.168.5.67	TLsv1.2	127	Application Data
70	11.360886	142.251.135.78	192.168.5.67	TCP	60	443 → 57785 [FIN, ACK] Seq=74 Ack=2 Win=371 Len=0
76	12.009629	40.71.11.167	192.168.5.67	TCP	66	443 → 58222 [ACK] Seq=1 Ack=2 Win=16386 Len=0 SLE=1 SRE=2
77	12.342124	142.251.135.74	192.168.5.67	TLsv1.2	127	Application Data
79	12.354915	142.251.135.74	192.168.5.67	TCP	60	443 → 57922 [FIN, ACK] Seq=74 Ack=2 Win=273 Len=0
83	12.574005	142.250.78.206	192.168.5.67	TCP	66	443 → 57792 [ACK] Seq=1 Ack=2 Win=4751 Len=0 SLE=1 SRE=2

6)

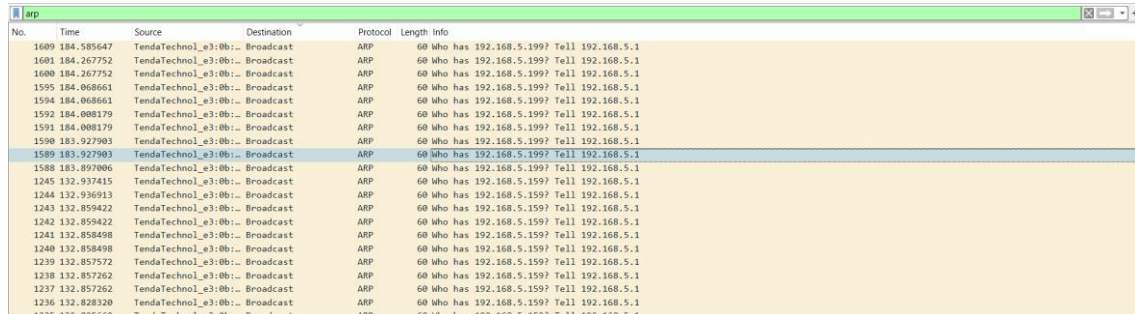
No.	Time	Source	Destination	Protocol	Length	Info
21170	303.237459	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21165	302.228005	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21161	301.214522	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21158	300.193875	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21146	299.177725	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21132	298.165559	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21125	297.140936	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21102	296.125232	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21053	295.115745	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21035	294.095242	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21023	293.086200	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
21015	292.079635	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20997	291.060311	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20979	290.052216	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20949	289.045259	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20944	288.028858	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20940	287.016903	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20936	286.005306	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20929	284.994009	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...
20924	283.982007	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=...

7) Se quisermos simplificar a expressão, podemos remover redundâncias e simplificar a estrutura. No entanto, a simplificação pode depender do contexto específico e dos requisitos do sistema. Uma possível simplificação seria remover a parte relacionada ao endereço IP de destino, assumindo que não é necessário verificar o destino na expressão

8) Se você usarmos o filtro "icmp" em um contexto de análise de tráfego de rede ou em ferramentas que suportam filtragem de pacotes, isso geralmente implica que você está interessado em todos os pacotes que utilizam o protocolo ICMP

No.	Time	Source	Destination	Protocol	Length	Info
20613	275.885518	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=64 (reply in 20614)
20610	274.876226	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=64 (reply in 20611)
20605	273.864593	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (reply in 20606)
1715	200.373179	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 1716)
1710	199.359100	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 1711)
1707	198.344115	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 1708)
1703	197.326062	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 1704)
1432	156.032742	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 1433)
1428	155.017881	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 1429)
1423	153.998602	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 1425)
1418	152.984043	192.168.5.67	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=64 (reply in 1419)
31662	359.101361	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=106/27136, ttl=56 (request in 31661)
31649	358.008097	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=105/26880, ttl=56 (request in 31648)
31643	357.065974	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=104/26624, ttl=56 (request in 31642)
31640	356.053247	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=103/26368, ttl=56 (request in 31639)
31626	355.034878	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=102/26112, ttl=56 (request in 31625)
31605	354.015408	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=101/25856, ttl=56 (request in 31603)
31586	352.999543	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=100/25600, ttl=56 (request in 31585)
31580	351.985686	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=99/25344, ttl=56 (request in 31579)
31572	350.965508	8.8.8.8	192.168.5.67	ICMP	74	Echo (ping) reply id=0x0001, seq=98/25088, ttl=56 (request in 31571)

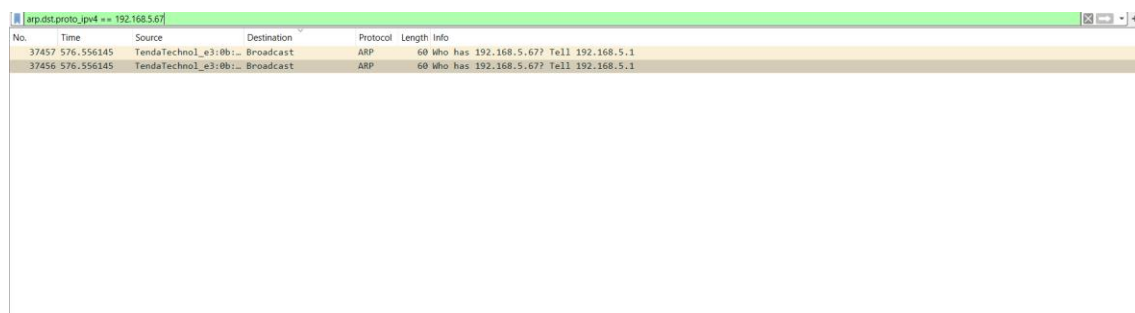
9)



No.	Time	Source	Destination	Protocol	Length	Info
1600	184.855647	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1601	184.267752	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1600	184.267752	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1595	184.068661	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1594	184.068661	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1592	184.088179	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1591	184.088179	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1590	183.927983	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1589	183.927983	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1588	183.897086	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.199? Tell 192.168.5.1
1245	132.937415	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1244	132.936913	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1243	132.859422	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1242	132.859422	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1241	132.858498	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1240	132.858498	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1239	132.857572	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1238	132.857262	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1237	132.857262	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1236	132.828320	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1
1235	132.805669	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.159? Tell 192.168.5.1

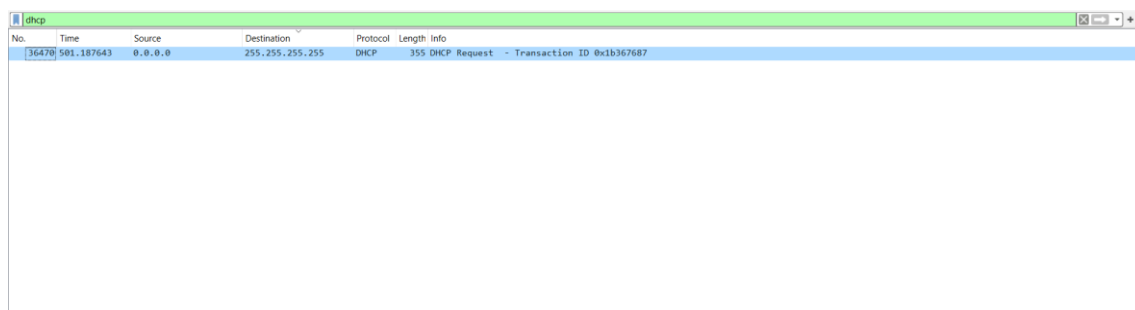
10) O "arp.opcode == 1" é usado para selecionar pacotes ARP Request, enquanto "arp.opcode == 2" é usado para selecionar pacotes ARP Reply. Esses filtros podem ser úteis ao analisar o tráfego da rede para entender as solicitações e respostas ARP, o que é fundamental para a resolução de endereços IP para endereços MAC em uma rede local.

11) Filtraria pacotes ARP em que o endereço IP de destino no cabeçalho ARP seja igual ao valor fornecido em "seu-ip". Essa expressão é útil se você quiser analisar ou capturar apenas os pacotes ARP direcionados a um endereço IP específico.



No.	Time	Source	Destination	Protocol	Length	Info
37457	576.556145	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.67? Tell 192.168.5.1
37456	576.556145	TendaTechno1_e3:0b:1: Broadcast	Broadcast	ARP	60	60 who has 192.168.5.67? Tell 192.168.5.1

12) A expressão "dhcp" irá incluir todos os pacotes que utilizam o protocolo DHCP, o que pode incluir mensagens DHCP Discover, Offer, Request, Acknowledge, e assim por diante. Essas mensagens são usadas para alocar e renovar configurações de IP automaticamente em redes locais. Usar esse filtro pode ser útil para analisar o tráfego DHCP em uma rede específica, monitorar a alocação de endereços IP ou diagnosticar problemas relacionados à configuração dinâmica de hosts.



No.	Time	Source	Destination	Protocol	Length	Info
36470	501.187643	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0x1b367687

13) A expressão "icmpv6" irá incluir todos os pacotes que utilizam o ICMPv6. Isso pode abranger diversas mensagens ICMPv6, como pacotes de echo request e echo reply (semelhantes ao ICMP no IPv4), mensagens de erro, mensagens de redirecionamento, e assim por diante.