


БЕСПЛАТНЫЙ ТЕСТ

ПЕРЕД ПОКУПКОЙ



VoiceXpert



**ГАРНИТУРЫ
ДЛЯ ОФИСОВ
И КОЛЛ-ЦЕНТРОВ**



**TRY
BEFORE
YOU BUY**



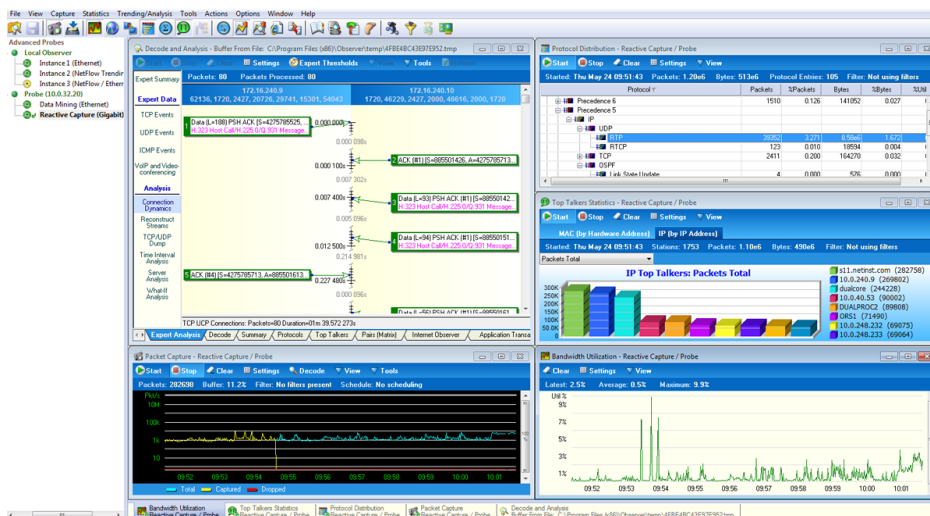
**ОБОРУДОВАНИЕ ДЛЯ
ВИДЕОКОНФЕРЕНЦИЙ**

Реклама, ООО "КаталогСервис"

ПОСМОТРЕТЬ ОБОРУДОВАНИЕ >>

<https://voicexpert.ru/?erid=2SDnjdrJhAY>

Wireshark фильтр по IP, по порту, по протоколу, по MAC



Любой анализатор протоколов должен иметь возможность не только захватить трафик, но и помочь эффективно его проанализировать. Основное отличие коммерческого анализатора протоколов от бесплатного (https://networkguru.ru/5_nedostatkov_wireshark/) – наличие встроенной экспертной системы, которая позволит быстро разобрать буфер по сервисам или типам ошибок. Что позволит существенно ускорить время локализации проблемы и работать с уже отсортированной и предварительно оцененной для вас информацией. Тут можно обратить внимание на решения от VIAVI Solutions под названием Observer или на ClearSight Analyzer от компании Netscout.

В случае если не выделяют бюджет, а проблемы есть, то остается запастись терпением и кофе и установить себе Wireshark (<https://networkguru.ru/wireshark-besplatno-skachat-instrukcii-na-russkom/>). В сетях передачи данных на скоростях 1 Гбит/сек и выше буфер захвата трафика заполняется мгновенно и на выходе получается достаточно большой массив данных. Этот массив данных, понимая взаимодействие между различными устройствами в сети можно отфильтровать по разным параметрам. Для этого Wireshark имеет несколько возможностей:

- Цветовая кодировка ошибочных пакетов — можно настроить под себя. Пакеты, которые несут в себе ошибку, будут выделены в буфере специальным цветом.
- Фильтр через строку фильтрации. Вы имеете большой опыт в работе с Wireshark и протоколами и можете ввести фильтр самостоятельно. Большой выбор фильтров можно найти здесь (<http://www.wireshark.org/docs/dfref/>).
- Выделение любой области в пакете, правый клик мыши и «Применить как фильтр». Метод для начинающих: очень удобно, так как не надо ломать голову.

ПОДПИШИТЕСЬ НА РАССЫЛКУ!

☐ - Я даю своё согласие на обработку

моих персональных данных на условиях и для целей, определенных Политикой конфиденциальности - Я принимаю условия Пользовательского соглашения и даю своё согласие на обработку моих персональных данных на условиях и для целей, определенных Политикой конфиденциальности -

Подписаться

ЗАКАЖИТЕ КОНСУЛЬТАЦИЮ!

Бесплатно проконсультируем по подбору и применению решений для NPM, APM и др!

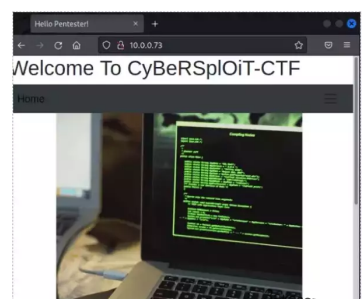
☐ - Я даю своё согласие на обработку

моих персональных данных на условиях и для целей, определенных Политикой конфиденциальности - Я принимаю условия Пользовательского соглашения и даю своё согласие на обработку моих персональных данных на условиях и для целей, определенных Политикой конфиденциальности -

Заказать консультацию!

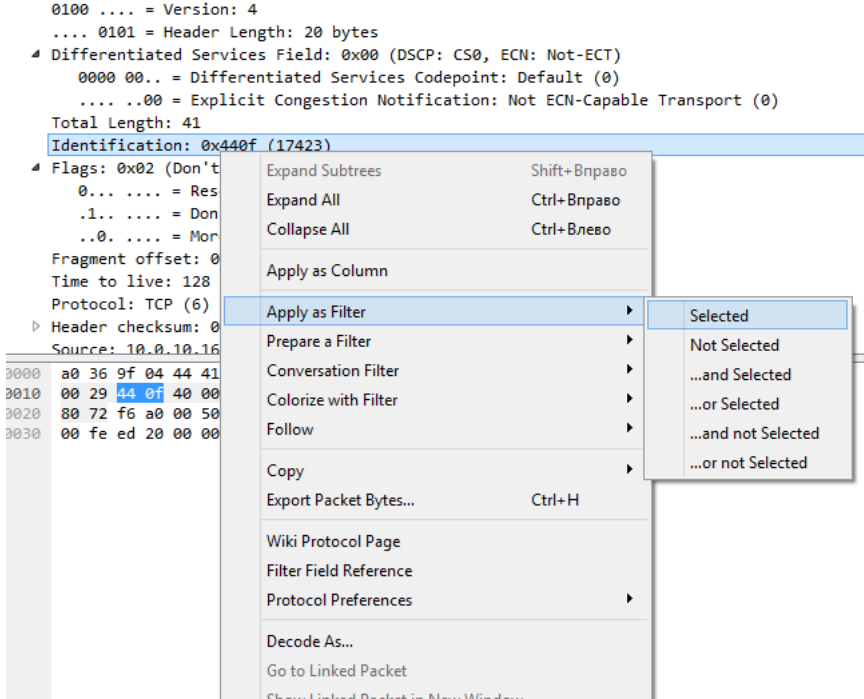
Свежие материалы

Как использовать ChatGPT для пентеста



[\(/pentest-s-chatgpt/\)](/pentest-s-chatgpt/)

ЗВОНОК



Атака NUIT (Near Ultrasound Inaudible Trojan)



(/ataka-nuit-near-ultrasound-inaudible-trojan/)

NGFW: Современные технологии защиты сетей



(/ngfw/)

Какие основные фильтры существуют для отображения трафика?

Wireshark фильтр по протоколу

Достаточно в строке фильтра ввести название протокола и нажать ввод. На экране останутся пакеты, которые относятся к искомому протоколу. Таким образом, фильтр выглядит:

http

No.	Time	Source	Destination	Protocol	Length	Info
4658	46.901361	10.0.10.163	185.72.231.16	HTTP	1025	GET /iei9c/jiy/ah5/img.gif?s=cnews_attn.201012281833
4659	46.905405	185.72.231.16	10.0.10.163	HTTP	360	HTTP/1.1 200 OK (GIF89a)
4660	46.931856	10.0.10.163	185.72.231.44	HTTP	514	GET /code?pid=746&gid=2&oin=1&rid=317977169 HTTP/1.1
4663	46.944510	185.72.231.44	10.0.10.163	HTTP	779	HTTP/1.1 200 OK (text/javascript)
4666	46.972003	10.0.10.163	185.72.231.44	HTTP	514	GET /code?pid=748&gid=2&oin=1&rid=964060966 HTTP/1.1
4667	46.972028	10.0.10.163	185.72.231.16	HTTP	1028	GET /7ej9rjky9naw/img.gif?s=cnews_attn.201012281835
4668	46.975802	185.72.231.16	10.0.10.163	HTTP	360	HTTP/1.1 200 OK (GIF89a)
4671	46.976946	185.72.231.44	10.0.10.163	HTTP	778	HTTP/1.1 200 OK (text/javascript)
4683	47.105669	10.0.10.163	88.212.196.124	HTTP	470	GET /hit?44.3;rs1920*1080*24;uhttpX3A/www.cnews.ru
4687	47.109408	88.212.196.124	10.0.10.163	HTTP	415	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
4694	47.179310	10.0.10.163	185.72.231.64	HTTP	1006	GET /p4.gif?r=&width=1920&height=1080&hash=&rn=0.1081
4699	47.183036	185.72.231.64	10.0.10.163	HTTP	289	HTTP/1.1 200 OK (GIF89a)

Frame 4746: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface 0

Ethernet II, Src: IntelCor_04:44:41 (a0:36:9f:04:44:41), Dst: LcfHefe_75:78:2b (28:d2:45:75:78:2b)

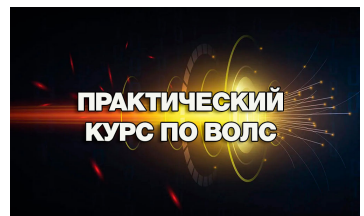
Internet Protocol Version 4, Src: 185.72.231.16, Dst: 10.0.10.163

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49319 (49319), Seq: 1452, Ack: 5801, Len: 306

Hypertext Transfer Protocol

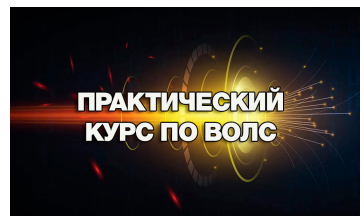
CompuServe GIF, Version: GIF89a

Практический курс по ВОЛС. Вебинар 2



(/prakticheskij-kurs-po-vols-vebinar-2/)

Практический курс по ВОЛС. Вебинар 1



(/prakticheskij-kurs-po-rabote-s-vols-ot-nashego-partnyora-svyazkomplekt-2022/)

Если буфер захвата необходимо отфильтровать по нескольким протоколам, то необходимо перечислить все желаемые протоколы и разделить их знаком ||. Например:

arp || http || icmp

No.	Time	Source	Destination	Protocol	Length	Info
4784	47.724691	10.0.10.163	80.68.246.17	HTTP	612	POST /comme
4798	47.729719	80.68.241.196	10.0.10.163	HTTP	775	HTTP/1.1 20
4805	47.731588	80.68.241.196	10.0.10.163	HTTP	1203	HTTP/1.1 20
4807	47.733443	80.68.246.17	10.0.10.163	HTTP	604	HTTP/1.1 20
4808	47.744336	AsustekC_45:f2:7f	Broadcast	ARP	60	Who has 10.
4814	47.780299	10.0.10.163	80.68.241.196	HTTP	839	GET /mrtest
4815	47.781436	10.0.10.163	80.68.241.196	HTTP	839	GET /mrtest
4825	47.787448	80.68.241.196	10.0.10.163	HTTP	1164	HTTP/1.1 20
4828	47.789453	80.68.241.196	10.0.10.163	HTTP	332	HTTP/1.1 20
4831	47.804046	10.0.10.163	80.68.241.196	HTTP	839	GET /mrtest
4839	47.812563	80.68.241.196	10.0.10.163	HTTP	439	HTTP/1.1 20
4863	47.948589	IntelCor_04:44:41	Broadcast	ARP	60	Who has 10.

Frame 4746: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface 0

Ethernet II, Src: IntelCor_04:44:41 (a0:36:9f:04:44:41), Dst: LcfHefe_75:78:2b (28:d2:45:75:78:2b)

Internet Protocol Version 4, Src: 185.72.231.16, Dst: 10.0.10.163

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49319 (49319), Seq: 1452, Ack: 5801, Len: 306

Hypertext Transfer Protocol

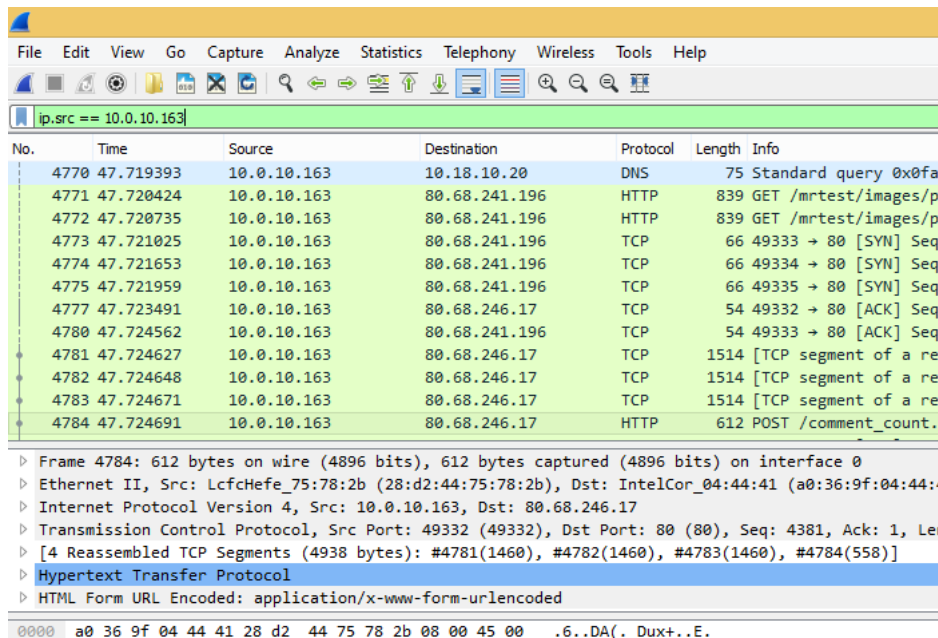
CompuServe GIF, Version: GIF89a

Заказать
звонок

Wireshark фильтр по IP адресу и фильтры по MAC

В зависимости от направления трафика фильтр будет немного отличаться. Например, мы хотим отфильтровать по IP адресу отправителя 50.116.24.50:

`ip.src==10.0.10.163`



No.	Time	Source	Destination	Protocol	Length	Info
4770	47.719393	10.0.10.163	10.18.10.20	DNS	75	Standard query 0x0fa
4771	47.720424	10.0.10.163	80.68.241.196	HTTP	839	GET /mrtest/images/p
4772	47.720735	10.0.10.163	80.68.241.196	HTTP	839	GET /mrtest/images/p
4773	47.721025	10.0.10.163	80.68.241.196	TCP	66	49333 → 80 [SYN] Seq
4774	47.721653	10.0.10.163	80.68.241.196	TCP	66	49334 → 80 [SYN] Seq
4775	47.721959	10.0.10.163	80.68.241.196	TCP	66	49335 → 80 [SYN] Seq
4777	47.723491	10.0.10.163	80.68.246.17	TCP	54	49332 → 80 [ACK] Seq
4780	47.724562	10.0.10.163	80.68.241.196	TCP	54	49333 → 80 [ACK] Seq
4781	47.724627	10.0.10.163	80.68.246.17	TCP	1514	[TCP segment of a re
4782	47.724648	10.0.10.163	80.68.246.17	TCP	1514	[TCP segment of a re
4783	47.724671	10.0.10.163	80.68.246.17	TCP	1514	[TCP segment of a re
4784	47.724691	10.0.10.163	80.68.246.17	HTTP	612	POST /comment_count.

Frame 4784: 612 bytes on wire (4896 bits), 612 bytes captured (4896 bits) on interface 0
Ethernet II, Src: LcfcHefe_75:78:2b (28:d2:44:75:78:2b), Dst: IntelCor_04:44:41 (a0:36:9f:04:44:..)
Internet Protocol Version 4, Src: 10.0.10.163, Dst: 80.68.246.17
Transmission Control Protocol, Src Port: 49332 (49332), Dst Port: 80 (80), Seq: 4381, Ack: 1, Len
[4 Reassembled TCP Segments (4938 bytes): #4781(1460), #4782(1460), #4783(1460), #4784(558)]
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded

0000 a0 36 9f 04 44 41 28 d2 44 75 78 2b 08 00 45 00 .6..DA(. Dux+..E.

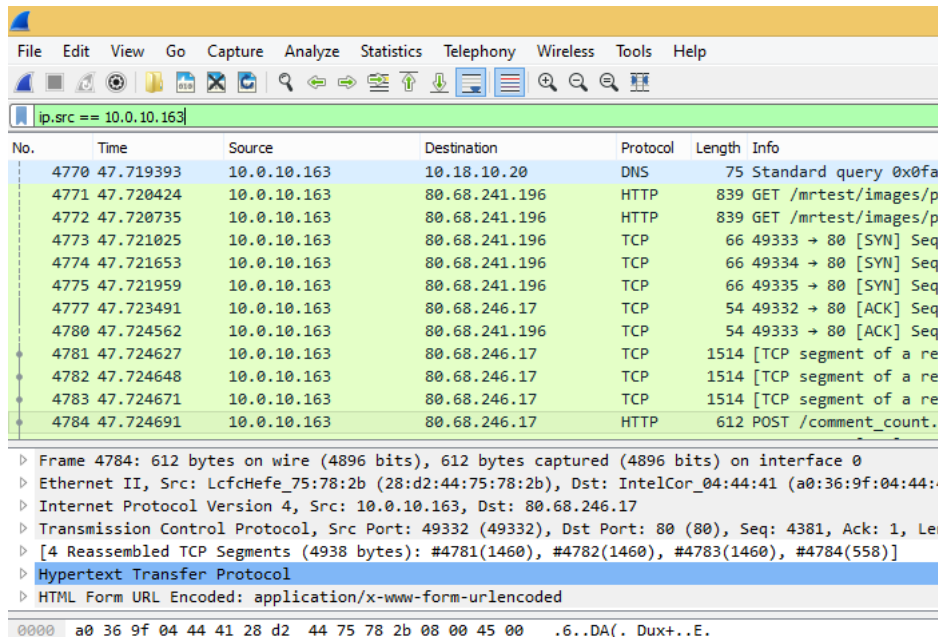
По получателю фильтр будет выглядеть `ip.dst == x.x.x.x`, а если хотим увидеть пакеты в независимости от направления трафика, то достаточно ввести:

`ip.addr==50.116.24.50`

В случае если нам необходимо исключить какой то адрес из поля отбора, то необходимо добавить `!=`.

Пример:

`ip.src!=80.68.246.17`



No.	Time	Source	Destination	Protocol	Length	Info
4770	47.719393	10.0.10.163	10.18.10.20	DNS	75	Standard query 0x0fa
4771	47.720424	10.0.10.163	80.68.241.196	HTTP	839	GET /mrtest/images/p
4772	47.720735	10.0.10.163	80.68.241.196	HTTP	839	GET /mrtest/images/p
4773	47.721025	10.0.10.163	80.68.241.196	TCP	66	49333 → 80 [SYN] Seq
4774	47.721653	10.0.10.163	80.68.241.196	TCP	66	49334 → 80 [SYN] Seq
4775	47.721959	10.0.10.163	80.68.241.196	TCP	66	49335 → 80 [SYN] Seq
4777	47.723491	10.0.10.163	80.68.246.17	TCP	54	49332 → 80 [ACK] Seq
4780	47.724562	10.0.10.163	80.68.241.196	TCP	54	49333 → 80 [ACK] Seq
4781	47.724627	10.0.10.163	80.68.246.17	TCP	1514	[TCP segment of a re
4782	47.724648	10.0.10.163	80.68.246.17	TCP	1514	[TCP segment of a re
4783	47.724671	10.0.10.163	80.68.246.17	TCP	1514	[TCP segment of a re
4784	47.724691	10.0.10.163	80.68.246.17	HTTP	612	POST /comment_count.

Frame 4784: 612 bytes on wire (4896 bits), 612 bytes captured (4896 bits) on interface 0
Ethernet II, Src: LcfcHefe_75:78:2b (28:d2:44:75:78:2b), Dst: IntelCor_04:44:41 (a0:36:9f:04:44:..)
Internet Protocol Version 4, Src: 10.0.10.163, Dst: 80.68.246.17
Transmission Control Protocol, Src Port: 49332 (49332), Dst Port: 80 (80), Seq: 4381, Ack: 1, Len
[4 Reassembled TCP Segments (4938 bytes): #4781(1460), #4782(1460), #4783(1460), #4784(558)]
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded

0000 a0 36 9f 04 44 41 28 d2 44 75 78 2b 08 00 45 00 .6..DA(. Dux+..E.

Если мы анализируем трафик внутри локальной сети и знаем MAC адрес пользователя, то можно указать в качестве фильтра Wireshark его MAC адрес, например:

`eth.addr == AA:BB:CC:DD:EE:FF`

Wireshark фильтр по номеру порта

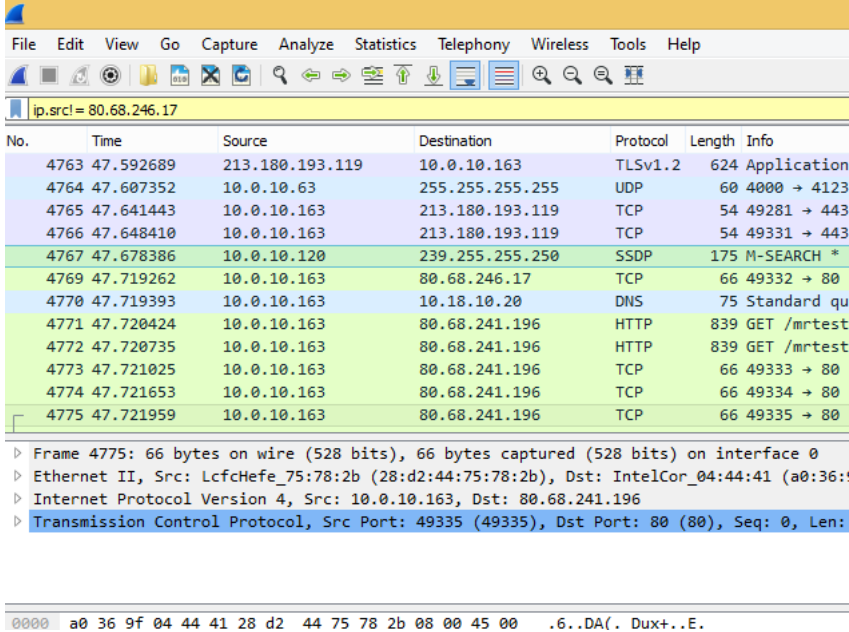
При анализе трафика мы можем настроить фильтр по номеру порта, по которому осуществляет передачу трафика тот или иной протокол. Номера всех зарегистрированных портов можно узнать [здесь](http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml).

(<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>) Пример:

`ftp.port==21`

Так же как и с адресами IP и MAC мы можем отдельно фильтровать по портам получения или отправления **tcp.srcport** и **tcp.dstport**. Кроме указания номеров портов Wireshark дает отличную возможность отфильтровать буфер по флагам в TCP протоколе. Например, если мы хотим увидеть TCP пакеты с флагом SYN (установление соединения между устройствами), то вводим в строке поиска:

`tcp.flags.syn`



Популярные фильтры

В таблице ниже приведены наиболее популярные фильтры для отображения содержимого буфера захвата:

Фильтр для отображения	Описание	Пример написания
eth.addr	MAC адрес отправителя или получателя	eth.addr == 00:1a:6b:ce:fc:bb
eth.src	MAC-адрес оправителя	eth.src == 00:1a:6b:ce:fc:bb
eth.dst	MAC-адрес получателя	eth.dst == 00:1a:6b:ce:fc:bb
arp.dst.hw_mac	Протокол ARP – MAC адрес получателя	arp.dst.hw_mac == 00:1a:6b:ce:fc:bb
arp.dst.proto_ipv4	Протокол ARP – IP адрес версии 4 получателя	arp.dst.proto_ipv4 == 10.10.10.10
arp.src.hw_mac	Протокол ARP – MAC адрес отправителя	arp.src.hw_mac == 00:1a:6b:ce:fc:bb
arp.src.proto_ipv4	Протокол ARP – IP адрес версии 4 отправителя	arp.src.proto_ipv4 == 10.10.10.10
vlan.id	Идентификатор VLAN	vlan.id == 16
ip.addr	IP адрес версии 4 получателя или отправителя	ip.addr == 10.10.10.10
ip.dst	IP адрес версии 4 получателя	ip.addr == 10.10.10.10
ip.src	IP адрес версии 4 отправителя	ip.src == 10.10.10.10
ip.proto	IP protocol (decimal)	ip.proto == 1
ipv6.addr	IP адрес версии 6 получателя или отправителя	ipv6.addr == 2001::5
ipv6.src	IP адрес версии 6 отправителя	ipv6.addr == 2001::5
ipv6.dst	IP адрес версии 6 получателя	ipv6.dst == 2001::5
tcp.port	TCP порт получателя или отправителя	tcp.port == 20
tcp.dstport	TCP порт получателя	tcp.dstport == 80
tcp.srcport	TCP порт отправителя	tcp.srcport == 60234
udp.port	UDP порт получателя или отправителя	udp.port == 513
udp.dstport	UDP порт получателя	udp.dstport == 513
udp.srcport	UDP порт отправителя	udp.srcport == 40000
vtp.vlan_info.vlan_name	Имя VLAN	vtp.vlan_info.vlan_name == TEST
bgp.originator_id	Идентификатор BGP (Адрес IPv4)	bgp.originator_id == 192.168.10.15

bgp.next_hop	Следующий хоп BGP (Адрес IPv4)	bgp.next_hop == 192.168.10.15
rip.ip	RIP IPv4 address	rip.ip == 200.0.2.0
ospf.advrouter	Идентификатор маршрутизатора по протоколу OSPF	ospf.advrouter == 192.168.170.8
eigrp.as	Номер автономной системы EIGRP	eigrp.as == 100
hsrp.virt_ip	Виртуальный IP адрес по протоколу HSRP	hsrp.virt_ip == 192.168.23.250
vrrp.ip_addr	Виртуальный IP адрес по протоколу VRRP	vrrp.ip_addr == 192.168.23.250
wlan.addr	MAC адрес отправителя или получателя Wi-Fi	wlan.addr == 00:1a:6b:ce:fc:bb
wlan.sa	MAC-адрес оправителя Wi-Fi	wlan.sa == 00:1a:6b:ce:fc:bb
wlan.da	MAC-адрес получателя Wi-Fi	wlan.da == 00:1a:6b:ce:fc:bb

А какие фильтры чаще всего используете в своей работе вы?

Всегда на связи, Игорь Панов (<https://networkguru.ru/contact/>)

См. также:

- Как настроить фильтры для захвата трафика в WireShark? Примеры! (https://networkguru.ru/kak_nastroit_filtru_dlya_zahvata_trafika/)
- Диагностика сети и приложений с помощью OptiView XG (<https://networkguru.ru/diagnostika-seti-i-prilozheniy-s-pomoshchiu-optiview-xg/>)
- Что такое Network Performance Monitoring (NPM)? (https://networkguru.ru/chto_takoe_network_performance_monitoring/)

<https://vk.com/share.php?url=https%3A%2F%2Fnetworkguru.ru%2Fwireshark-filtr-po-ip-portu-protokolu-mac%2F&title=%D0%9F%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D0%B5%20%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D1%8B%20Wireshark>
<https://connect.ok.ru/offer?url=https%3A%2F%2Fnetworkguru.ru%2Fwireshark-filtr-po-ip-portu-protokolu-mac%2F&title=%D0%9F%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D0%B5%20%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D1%8B%20Wireshark>
<https://pinterest.com/pin/create/button/?url=https%3A%2F%2Fnetworkguru.ru%2Fwireshark-filtr-po-ip-portu-protokolu-mac%2F&media=https%3A%2F%2Fskomplekt.com%2Fcatalog%2Fview%2Ftheme-wireshark>
<https://twitter.com/intent/tweet?text=%D0%9F%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D0%B5%20%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D1%8B%20Wireshark>
<https://viber://forward?text=%D0%9F%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D0%B5%20%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D1%8B%20Wireshark>
<https://api.whatsapp.com/send?text=%D0%9F%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D0%B5%20%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D1%8B%20Wireshark>
https://web.skype.com/share?url=https%3A%2F%2Fnetworkguru.ru%2Fwireshark-filtr-po-ip-portu-protokolu-mac%2F&utm_source=share2
<https://t.me/share/url?url=https%3A%2F%2Fnetworkguru.ru%2Fwireshark-filtr-po-ip-portu-protokolu-mac%2F&text=%D0%9F%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D0%B5%20%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D1%8B%20Wireshark>

Комментарии

Тут пока ничего нет, но Вы можете быть первым!

Авторизуйтесь для этого