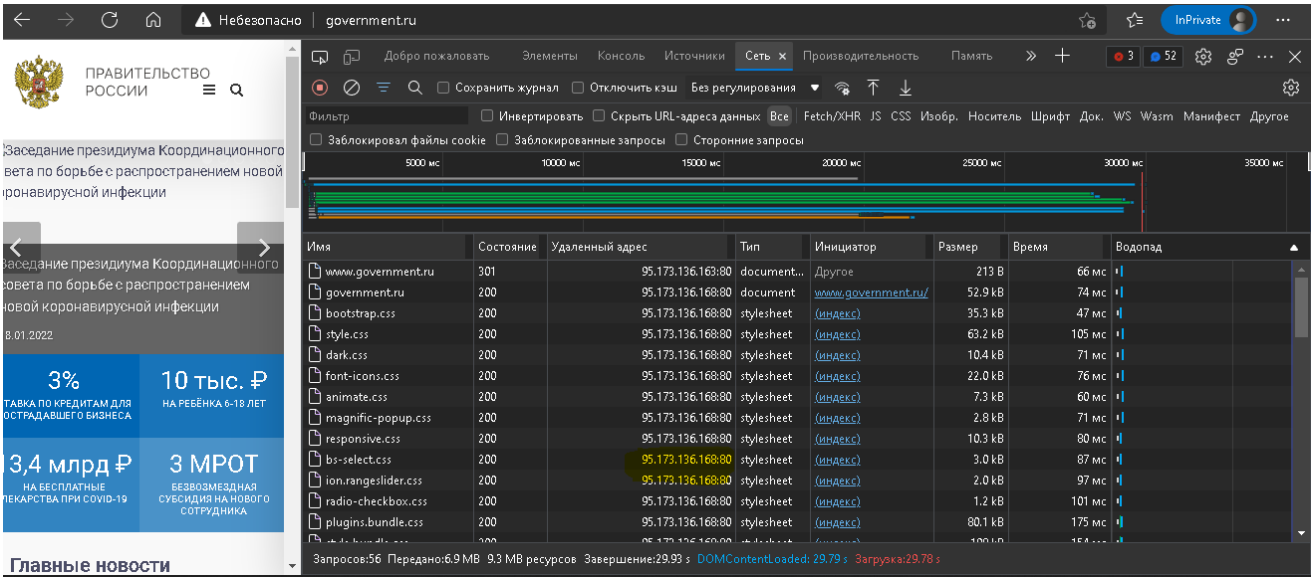
1. Работа в Wireshark.

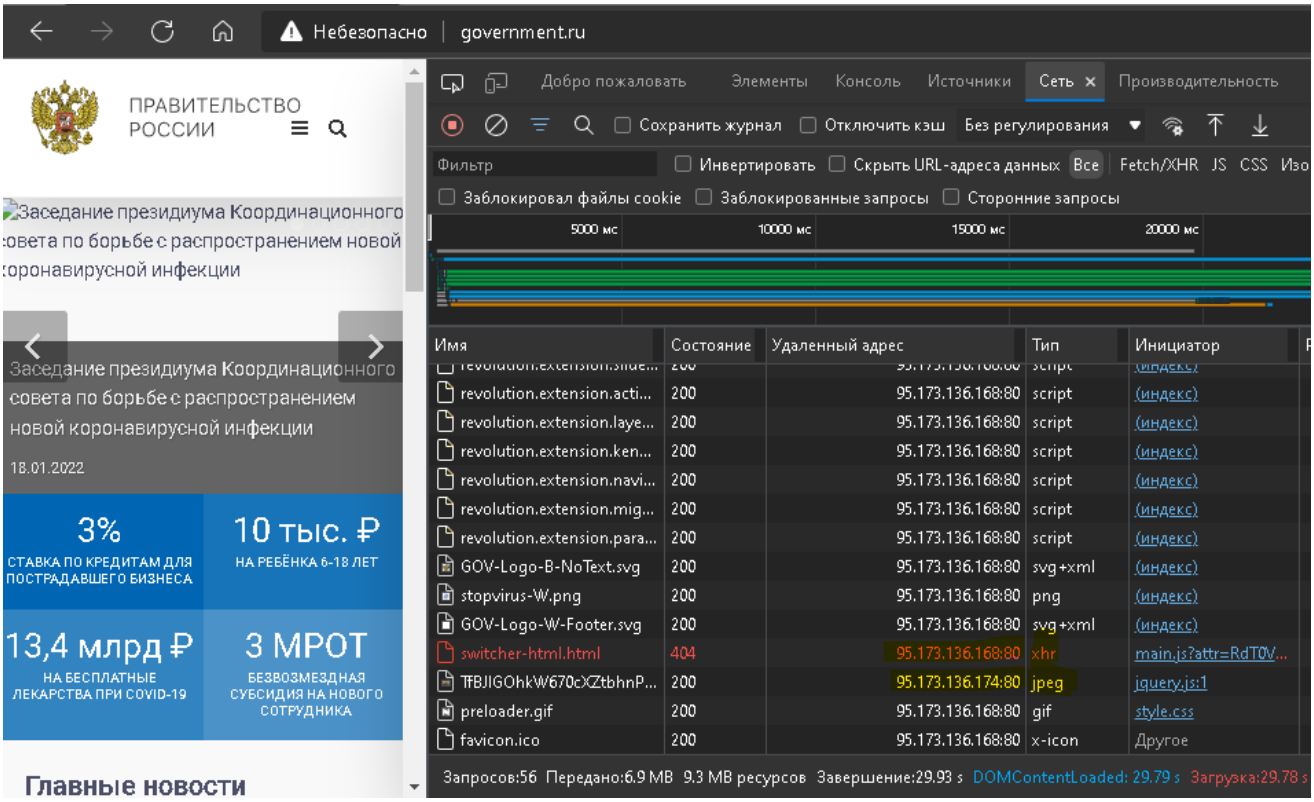
-- Запустить Wireshark, выбрать любой веб-сайт, определить IP-адрес сервера, отфильтровать в Wireshark трафик по этому IP-адресу. Набрать адрес сервера в строке браузера. Сколько TCP-соединений было открыто и почему.
Потренироваться с фильтрованием. (Попробовать пофильтровать другие протоколы, например icmp ssh ospf в приложенном pcap файле)

12 соединений:

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Sent Bytes
msedge.exe	13068	TCP	24862		192.168.0.202	80	http	95.173.136.163		Established	
msedge.exe	13068	TCP	24864		192.168.0.202	80	http	95.173.136.168		Established	
msedge.exe	13068	TCP	24866		192.168.0.202	80	http	95.173.136.168		Established	
msedge.exe	13068	TCP	24867		192.168.0.202	80	http	95.173.136.168		Established	
msedge.exe	13068	TCP	24868		192.168.0.202	80	http	95.173.136.168		Established	
msedge.exe	13068	TCP	24869		192.168.0.202	80	http	95.173.136.168		Established	
msedge.exe	13068	TCP	24870		192.168.0.202	80	http	95.173.136.168		Established	
msedge.exe	13068	TCP	24874		192.168.0.202	80	http	95.173.136.174		Established	
msedge.exe	13068	TCP	24875		192.168.0.202	80	http	95.173.136.174		Established	
msedge.exe	13068	TCP	24876		192.168.0.202	80	http	95.173.136.174		Established	
msedge.exe	13068	TCP	24877		192.168.0.202	80	http	95.173.136.174		Established	
msedge.exe	13068	TCP	24878		192.168.0.202	80	http	95.173.136.174		Syn-Sent	

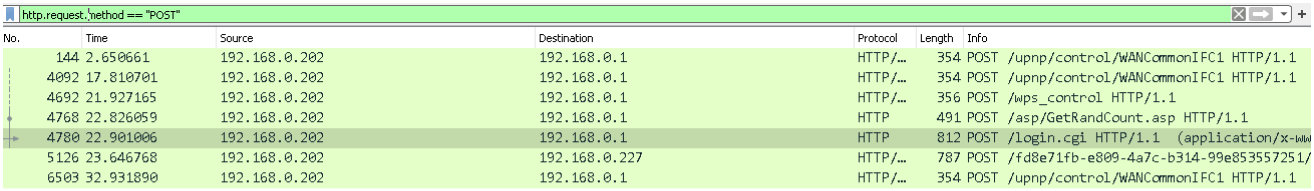
Потому что идет загрузка контента, не только с сайта government.ru:

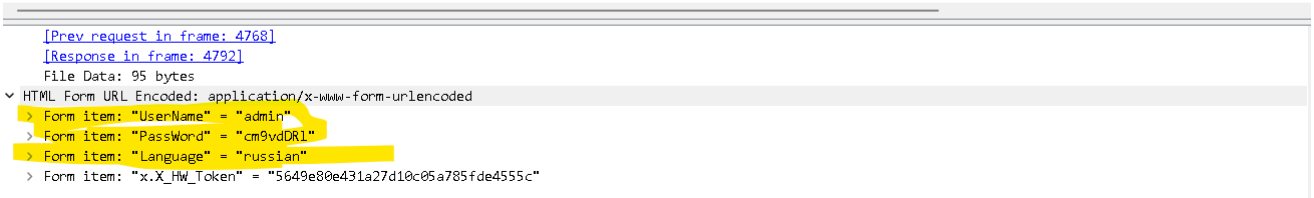




-- Найти незашифрованный сайт, где можно вбить какие-либо аутентификационные данные (логин/пароль). Перехватить их в шарке.

Не совсем не защищенный сайт - интерфес админки роутера:





Логин передается в открытом виде, пароль - зашифрованный.