

## 1. Работа в Wireshark.

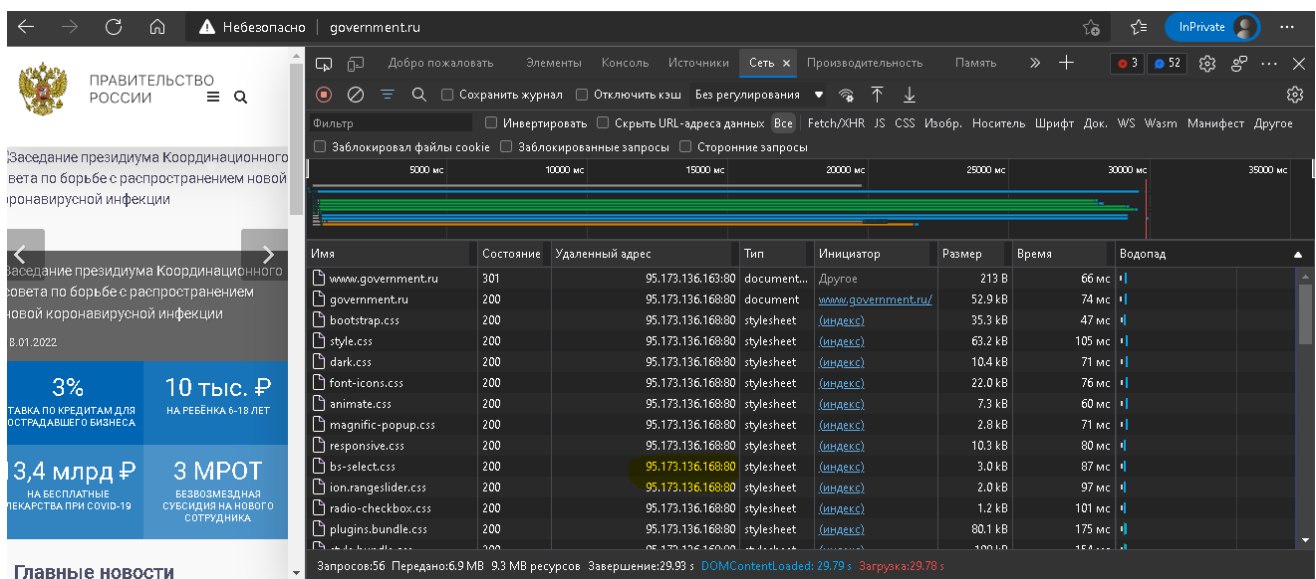
– Запустить Wireshark, выбрать любой веб-сайт, определить IP-адрес сервера, отфильтровать в Wireshark трафик по этому IP-адресу. Набрать адрес сервера в строке браузера. Сколько TCP-соединений было открыто и почему.

Потренироваться с фильтрованием. (Попробовать пофильтровать другие протоколы, например icmp ssh ospf в приложенном pcap файле)

12 соединений:

Process Name	Process ID	Protocol	Local Port	Local Port	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:



ПРАВИТЕЛЬСТВО РОССИИ

Заседание президиума Координационного совета по борьбе с распространением новой коронавирусной инфекции

Заседание президиума Координационного совета по борьбе с распространением новой коронавирусной инфекции

18.01.2022

3% СТАВКА ПО КРЕДИТАМ ДЛЯ ПОСТРАДАВШЕГО БИЗНЕСА

10 тыс. ₽ НА РЕБЕНКА 6-18 ЛЕТ

13,4 млрд ₽ НА БЕСПЛАТНЫЕ ЛЕКАРСТВА ПРИ COVID-19

3 МРОТ БЕЗВОЗМЕЗДНАЯ СУБСИДИЯ НА НОВОГО СОТРУДНИКА

Главные новости

Имя	Состояние	Удаленный адрес	Тип	Инициатор
revolution.extension.zip...	200	95.173.136.168:80	script	(индекс)
revolution.extension.acti...	200	95.173.136.168:80	script	(индекс)
revolution.extension.laye...	200	95.173.136.168:80	script	(индекс)
revolution.extension.ken...	200	95.173.136.168:80	script	(индекс)
revolution.extension.navi...	200	95.173.136.168:80	script	(индекс)
revolution.extension.mig...	200	95.173.136.168:80	script	(индекс)
revolution.extension.para...	200	95.173.136.168:80	script	(индекс)
GOV-Logo-B-NoText.svg	200	95.173.136.168:80	svg+xml	(индекс)
stopvirus-W.png	200	95.173.136.168:80	png	(индекс)
GOV-Logo-W-Footer.svg	200	95.173.136.168:80	svg+xml	(индекс)
switcher-html.html	404	95.173.136.168:80	xhr	main.js?attr=RdTDV...
ТВJIGOhkW670cXZtbhnp...	200	95.173.136.174:80	jpeg	jquery.js:1
preloader.gif	200	95.173.136.168:80	gif	style.css
favicon.ico	200	95.173.136.168:80	x-icon	Другое

Запросов:56 Передано:6.9 MB 9.3 MB ресурсов Завершение:29.93 s DOMContentLoaded: 29.79 s Загрузка:29.78 s

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

Не совсем не защищенный сайт - интерфейс админки роутера:

No.	Time	Source	Destination	Protocol	Length	Info
144	2.650661	192.168.0.202	192.168.0.1	HTTP/...	354	POST /upnp/control/WANCommonIFC1 HTTP/1.1
4092	17.810701	192.168.0.202	192.168.0.1	HTTP/...	354	POST /upnp/control/WANCommonIFC1 HTTP/1.1
4692	21.927165	192.168.0.202	192.168.0.1	HTTP/...	356	POST /wps_control HTTP/1.1
4768	22.826059	192.168.0.202	192.168.0.1	HTTP	491	POST /asp/GetRandCount.asp HTTP/1.1
4780	22.901006	192.168.0.202	192.168.0.1	HTTP	812	POST /login.cgi HTTP/1.1 (application/x-www-form-urlencoded)
5126	23.646768	192.168.0.202	192.168.0.227	HTTP/...	787	POST /fd8e71fb-e809-4a7c-b314-99e853557251/ HTTP/1.1
6503	32.931890	192.168.0.202	192.168.0.1	HTTP/...	354	POST /upnp/control/WANCommonIFC1 HTTP/1.1

[Prev request in frame: 4768]  
[Response in frame: 4792]  
File Data: 95 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "UserName" = "admin"
- > Form item: "PassWord" = "cm9vdDRI"
- > Form item: "Language" = "russian"
- > Form item: "x.X\_HM-Token" = "5649e80e431a27d10c05a785fde4555c"

Логин передается в открытом виде, пароль - зашифрованный.