



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

Факультет управления и информатики в технологических системах
Кафедра информационной безопасности
Направление подготовки (специальность) 10.05.03 Информационная
безопасность автоматизированных систем

Отчет

по практической работе №1

Выполнил студент гр. УБ-11

Долгих Е.И.

Проверил:
Денисенко В.В

Введение

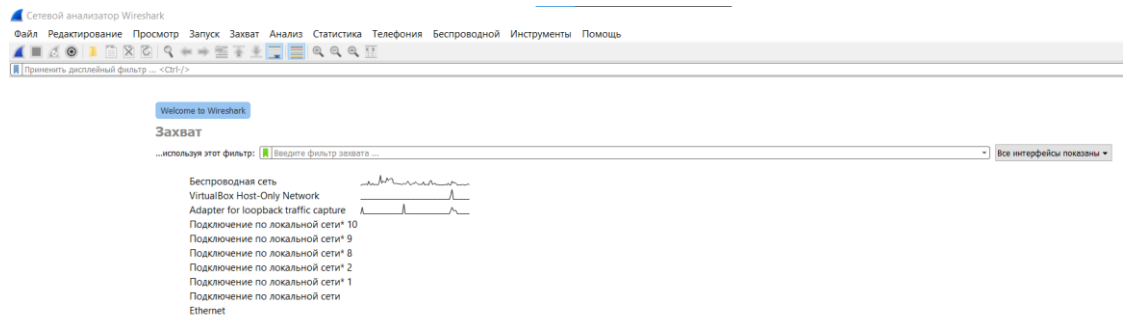
Цель работы: отследить и проанализировать трафик приложений, общающихся с сервером по протоколу HTTP

Порядок выполнения:

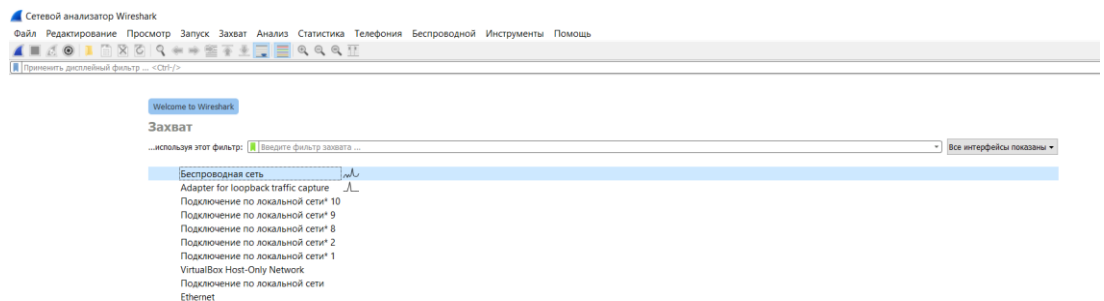
1. Установить программу
 2. Выбрать тип сети
 3. Запустить анализ
 4. Добавить фильтр
 5. Начать серфинг в интернете
 6. Изучить кадры Http в данных, захваченных программой Wireshark.
- Сопоставить результаты

Основная часть

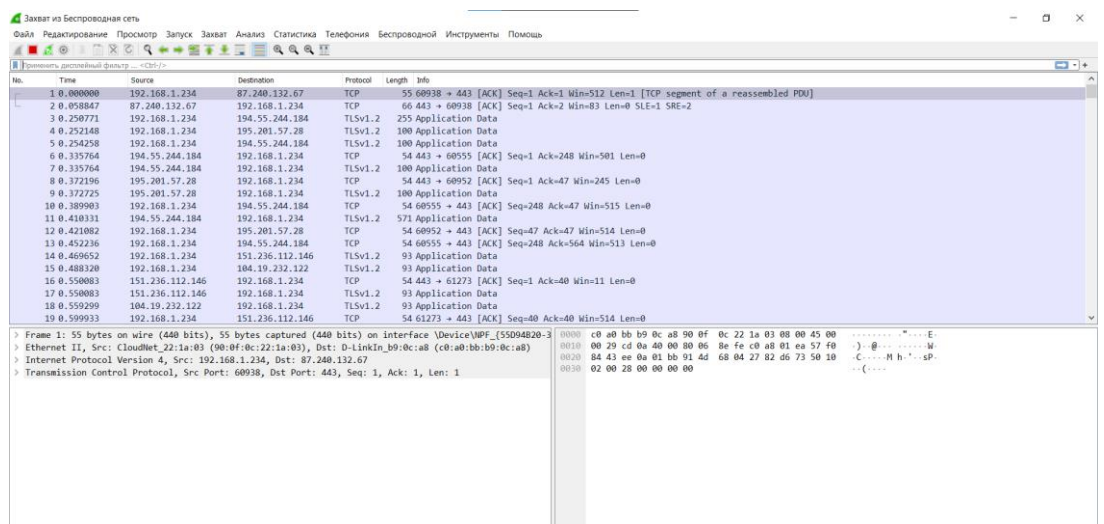
1. Установили программу:



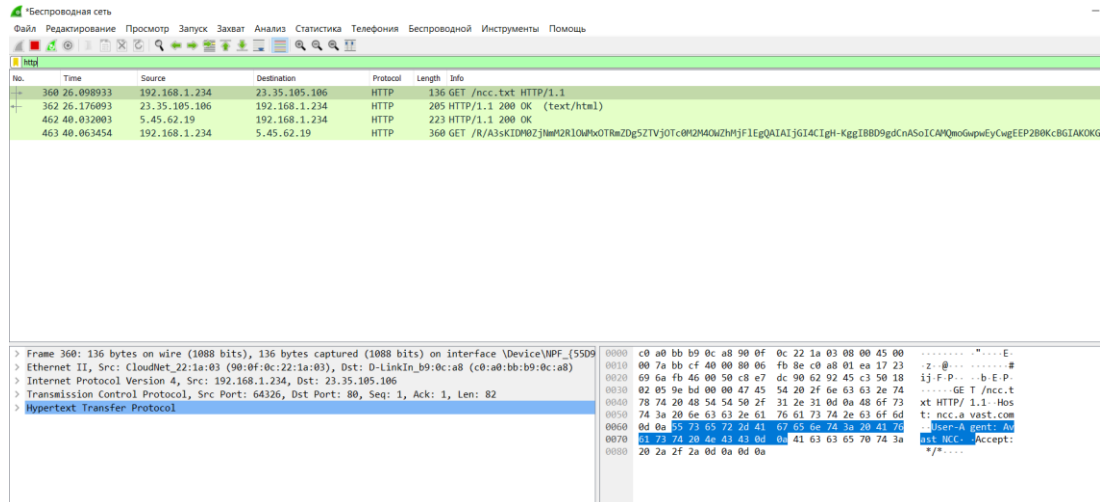
2. Выбираем тип сети:



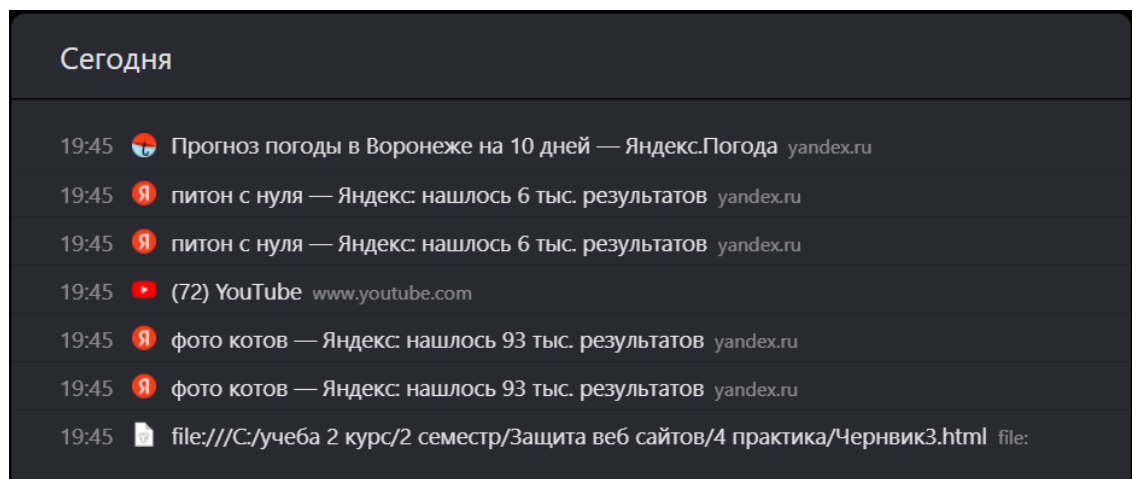
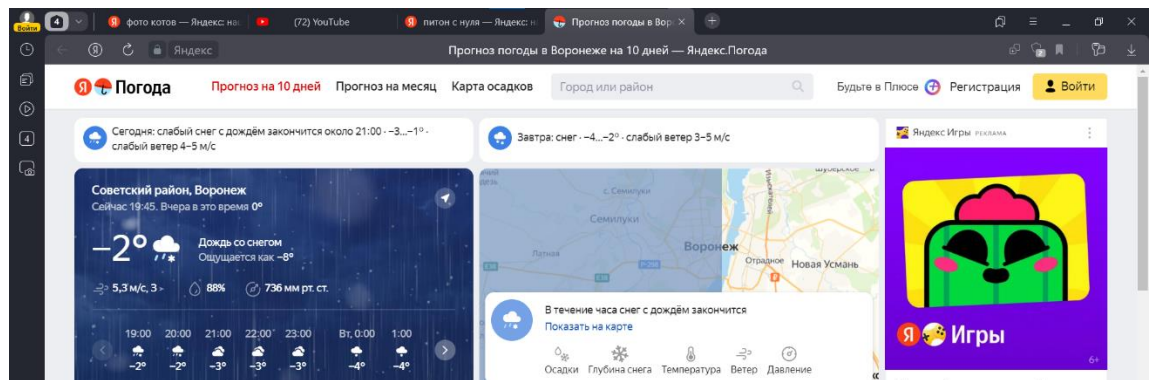
3. Запускаем анализ:



4. Добавляем фильтр:



5. Начинаем серфинг в интернете:



Беспроводная сеть

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

No.	Time	Source	Destination	Protocol	Length	Info
368	26.998933	192.168.1.234	23.35.105.106	HTTP	136	GET /ncc.txt HTTP/1.1
362	26.170991	23.35.105.106	192.168.1.234	HTTP	205	HTTP/1.1 200 OK (text/html)
462	40.832083	5.45.62.19	192.168.1.234	HTTP	223	HTTP/1.1 200 OK
463	40.963454	192.168.1.234	5.45.62.19	HTTP	368	GET /R/AsKIDP02jWmZK10MhOTRmZg52TVJOTc0PQ4M2MhJf1EgQAI2jG14CIgH-KggIB8DgCnA50ICAPQn0bupdyCugEEL2B0KcBGIAK0KXvHlgRQ1Byr1..
14026	166.951901	192.168.1.234	5.45.62.19	HTTP	81	POST /file/reputation HTTP/1.1 (application/x-enc)
14033	167.094188	5.45.62.19	192.168.1.234	HTTP	339	HTTP/1.1 200 OK (application/x-enc)
14106	168.903935	192.168.1.234	104.18.20.226	HTTP	313	GET /codesigningroot45/PwFwZBMEu5A3J8gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
14126	169.149678	104.18.20.226	192.168.1.234	OCSP	778	Response
14134	169.151657	192.168.1.234	104.18.20.226	HTTP	315	GET /gsecovssica2018/PEu5c83PecurTA3gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
14170	169.374741	104.18.20.226	192.168.1.234	OCSP	751	Response
14484	170.194645	192.168.1.234	104.18.20.226	HTTP	299	GET /rootr1/NE4wTD80Eg6A3J8gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
14495	170.272884	104.18.20.226	192.168.1.234	OCSP	589	Response
14538	170.687774	192.168.1.234	104.18.21.226	HTTP	298	GET /rootr1/NE4wTD80Eg6A3J8gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
14560	170.779292	104.18.21.226	192.168.1.234	OCSP	496	Response
14563	170.808118	192.168.1.234	104.18.20.226	HTTP	313	GET /gsecovssica2018/PEu5c83PecurTA3gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
14570	170.926648	104.18.20.226	192.168.1.234	OCSP	499	Response
15294	172.777895	192.168.1.234	5.45.59.253	HTTP	225	POST /file/reputation HTTP/1.1 (application/x-enc)
15460	173.082135	5.45.59.253	192.168.1.234	HTTP	319	HTTP/1.1 200 OK (application/x-enc)
15567	173.289565	192.168.1.234	104.18.20.226	HTTP	387	GET /gsecovssica2018/PEu5c83PecurTA3gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
15981	173.861895	104.18.20.226	192.168.1.234	OCSP	1444	Response
15981	170.818769	192.168.1.234	104.18.20.226	HTTP	387	GET /gsecovssica2018/PEu5c83PecurTA3gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
19056	179.924770	104.18.20.226	192.168.1.234	OCSP	1445	Response
21091	192.765969	192.168.1.234	216.58.209.195	HTTP	291	GET /gtsic1/NE4wTD80Eg6A3J8gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
21092	192.766643	192.168.1.234	216.58.209.195	HTTP	291	GET /gtsic1/NE4wTD80Eg6A3J8gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
21177	192.883076	216.58.209.195	192.168.1.234	OCSP	766	Response
21188	192.908911	216.58.209.195	192.168.1.234	OCSP	766	Response

> Frame 360: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface DeviceVMPF_55009
 > Ethernet II, Src: CloudNet_22:1a:03 (90:0f:0c:22:1a:03), Dst: D-LinkIn_b9:0c:a8 (c8:a0:bb:b9:0c:a8)
 > Internet Protocol Version 4, Src: 192.168.1.234, Dst: 23.35.105.106
 > Transmission Control Protocol, Src Port: 64326, Dst Port: 80, Seq: 1, Ack: 1, Len: 82
 > Hypertext Transfer Protocol

Беспроводная сеть

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

No.	Time	Source	Destination	Protocol	Length	Info
21177	192.883076	216.58.209.195	192.168.1.234	OCSP	766	Response
21188	192.908911	216.58.209.195	192.168.1.234	OCSP	766	Response
26186	195.459883	192.168.1.234	104.18.20.226	HTTP	305	GET /gsecovssica2018/PEu5c83PecurTA3gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
26393	195.587725	104.18.20.226	192.168.1.234	OCSP	1444	Response
29081	207.881288	5.45.62.19	192.168.1.234	HTTP	978	HTTP/1.1 200 OK
29082	207.886281	192.168.1.234	5.45.62.19	HTTP	368	GET /R/AsKIDP02jWmZK10MhOTRmZg52TVJOTc0PQ4M2MhJf1EgQAI2jG14CIgH-KggIB8DgCnA50ICAPQn0bupdyCugEEL2B0KcBGIAK0KXvHlgRQ1Byr1..
33017	212.731461	192.168.1.234	104.18.20.226	HTTP	305	GET /gsecovssica2018/PEu5c83PecurTA3gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
33078	212.820986	104.18.20.226	192.168.1.234	OCSP	1444	Response
38934	229.956875	192.168.1.234	34.104.35.123	HTTP	451	HEAD /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
38946	229.193890	192.168.1.234	34.104.35.123	HTTP	523	GET /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
38949	229.292480	34.104.35.123	192.168.1.234	HTTP	339	HTTP/1.1 206 Partial Content
39052	231.380946	192.168.1.234	34.104.35.123	HTTP	526	GET /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
39056	231.476028	34.104.35.123	192.168.1.234	HTTP	735	HTTP/1.1 206 Partial Content
39088	232.580295	192.168.1.234	34.104.35.123	HTTP	526	GET /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
39090	232.680449	34.104.35.123	192.168.1.234	HTTP	1098	HTTP/1.1 206 Partial Content
39212	237.117928	192.168.1.234	34.104.35.123	HTTP	331	HEAD /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39219	237.251247	34.104.35.123	192.168.1.234	HTTP	606	HTTP/1.1 200 OK
39221	237.284220	192.168.1.234	34.104.35.123	HTTP	404	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39225	237.483955	34.104.35.123	192.168.1.234	HTTP	605	HTTP/1.1 206 Partial Content
39221	238.507992	192.168.1.234	34.104.35.123	HTTP	408	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39322	238.653672	34.104.35.123	192.168.1.234	HTTP	1462	HTTP/1.1 206 Partial Content
39615	239.681396	192.168.1.234	34.104.35.123	HTTP	408	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39683	239.878332	34.104.35.123	192.168.1.234	HTTP	1193	HTTP/1.1 206 Partial Content
39745	240.810943	192.168.1.234	34.104.35.123	HTTP	409	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39836	241.121218	34.104.35.123	192.168.1.234	HTTP	760	HTTP/1.1 206 Partial Content

> Frame 360: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface DeviceVMPF_55009
 > Ethernet II, Src: CloudNet_22:1a:03 (90:0f:0c:22:1a:03), Dst: D-LinkIn_b9:0c:a8 (c8:a0:bb:b9:0c:a8)
 > Internet Protocol Version 4, Src: 192.168.1.234, Dst: 23.35.105.106
 > Transmission Control Protocol, Src Port: 64326, Dst Port: 80, Seq: 1, Ack: 1, Len: 82
 > Hypertext Transfer Protocol

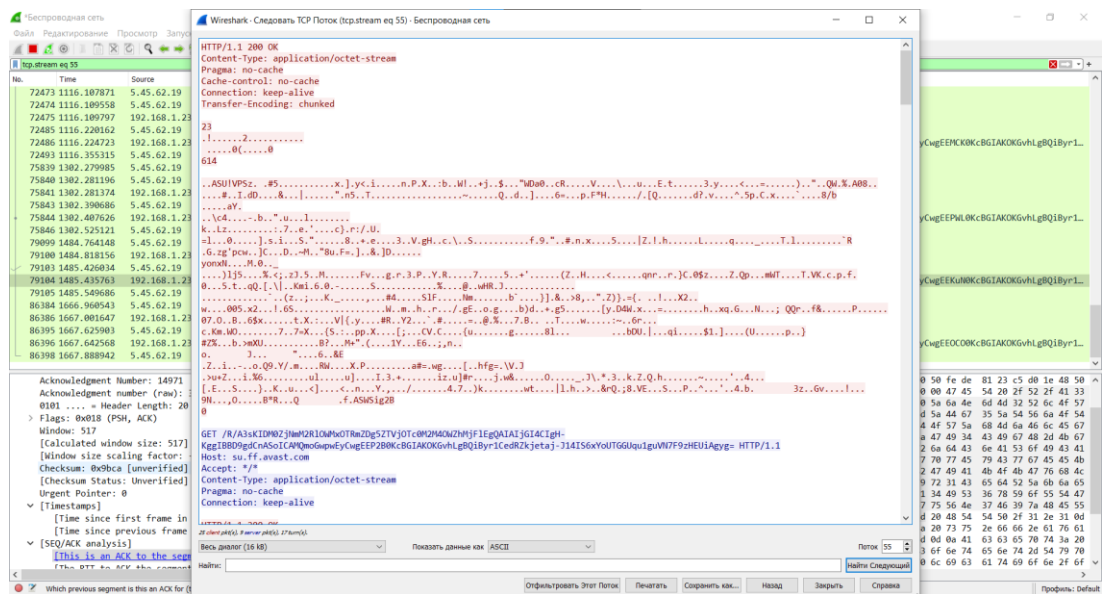
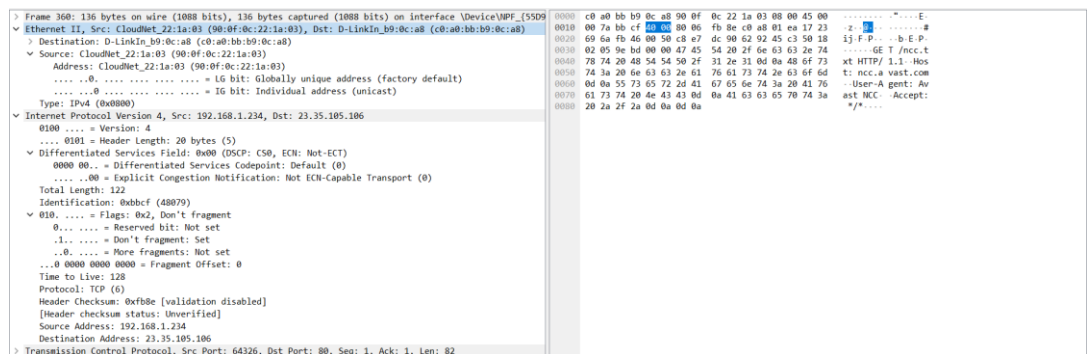
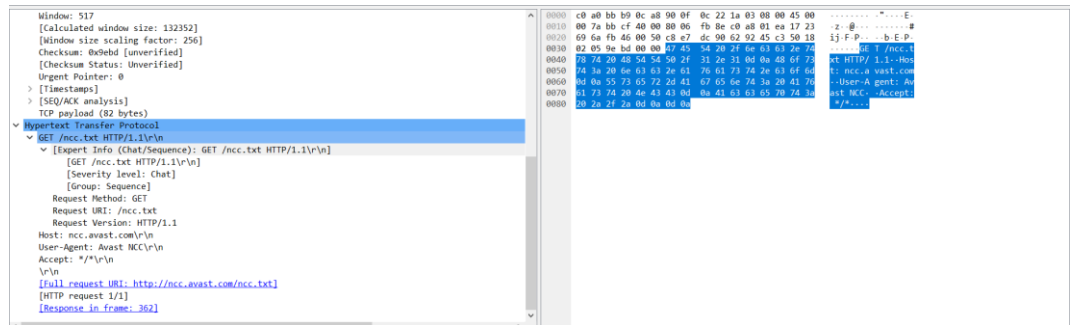
Беспроводная сеть

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

No.	Time	Source	Destination	Protocol	Length	Info
29082	207.886281	192.168.1.234	5.45.62.19	HTTP	368	GET /R/AsKIDP02jWmZK10MhOTRmZg52TVJOTc0PQ4M2MhJf1EgQAI2jG14CIgH-KggIB8DgCnA50ICAPQn0bupdyCugEEL2B0KcBGIAK0KXvHlgRQ1Byr1..
33017	212.731461	192.168.1.234	104.18.20.226	HTTP	305	GET /gsecovssica2018/PEu5c83PecurTA3gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
33078	212.820986	104.18.20.226	192.168.1.234	OCSP	1444	Response
38934	229.956875	192.168.1.234	34.104.35.123	HTTP	451	HEAD /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
38943	229.149272	34.104.35.123	192.168.1.234	HTTP	604	HTTP/1.1 200 OK
38946	229.193890	192.168.1.234	34.104.35.123	HTTP	523	GET /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
38949	229.292480	34.104.35.123	192.168.1.234	HTTP	339	HTTP/1.1 206 Partial Content
39052	231.380946	192.168.1.234	34.104.35.123	HTTP	526	GET /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
39056	231.476028	34.104.35.123	192.168.1.234	HTTP	735	HTTP/1.1 206 Partial Content
39088	232.580295	192.168.1.234	34.104.35.123	HTTP	526	GET /edged/delta-update/fnkpialhgieaddfemjofefb1mb/1.3fc450428694c-f97893edcd3dc45276fe78908ec3f3f69d1136f6d94346830/1..
39090	232.680449	34.104.35.123	192.168.1.234	HTTP	1098	HTTP/1.1 206 Partial Content
39212	237.117928	192.168.1.234	34.104.35.123	HTTP	331	HEAD /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39219	237.251247	34.104.35.123	192.168.1.234	HTTP	606	HTTP/1.1 200 OK
39221	237.284220	192.168.1.234	34.104.35.123	HTTP	404	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39225	237.483955	34.104.35.123	192.168.1.234	HTTP	605	HTTP/1.1 206 Partial Content
39221	238.507992	192.168.1.234	34.104.35.123	HTTP	408	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39322	238.653672	34.104.35.123	192.168.1.234	HTTP	1462	HTTP/1.1 206 Partial Content
39615	239.681396	192.168.1.234	34.104.35.123	HTTP	408	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39683	239.878332	34.104.35.123	192.168.1.234	HTTP	1193	HTTP/1.1 206 Partial Content
39745	240.810943	192.168.1.234	34.104.35.123	HTTP	409	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39836	241.121218	34.104.35.123	192.168.1.234	HTTP	760	HTTP/1.1 206 Partial Content
39873	241.932040	192.168.1.234	34.104.35.123	HTTP	410	GET /edged/release2/chrome_component/In7vayhkbxleg7xfear7dky_505/efniojInjndmchieegkicadnoecjef_505_all_pazlot156bbfzvrtxy..
39880	242.032425	34.104.35.123	192.168.1.234	HTTP	306	HTTP/1.1 206 Partial Content
40657	258.760988	192.168.1.234	216.58.209.195	HTTP	291	GET /gtsic1/NE4wTD80Eg6A3J8gIrDgPcGgUAB8THK03nHLYoQvuu4Izyfn903M4Mu0d5rS2BYVCkEABrtb08ZUPgDey6G6QW4P4D4..
40669	258.853726	216.58.209.195	192.168.1.234	OCSP	766	Response

> Frame 360: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface DeviceVMPF_55009
 > Ethernet II, Src: CloudNet_22:1a:03 (90:0f:0c:22:1a:03), Dst: D-LinkIn_b9:0c:a8 (c8:a0:bb:b9:0c:a8)
 > Internet Protocol Version 4, Src: 192.168.1.234, Dst: 23.35.105.106
 > Transmission Control Protocol, Src Port: 64326, Dst Port: 80, Seq: 1, Ack: 1, Len: 82
 > Hypertext Transfer Protocol

6. Изучить кадры Http в данных, захваченных программой Wireshark. Сопоставить результаты:



Вывод

Установили программу Wireshark. Отследили и проанализировали трафик приложений. Изучили кадры в данных, захваченных программой Wireshark, сопоставить результаты. Ознакомились с гипертекстовым протоколом HTTP, научились производить анализ HTTP-трафика, с помощью программы WireShark.