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

Воронеж – 2023

Введение

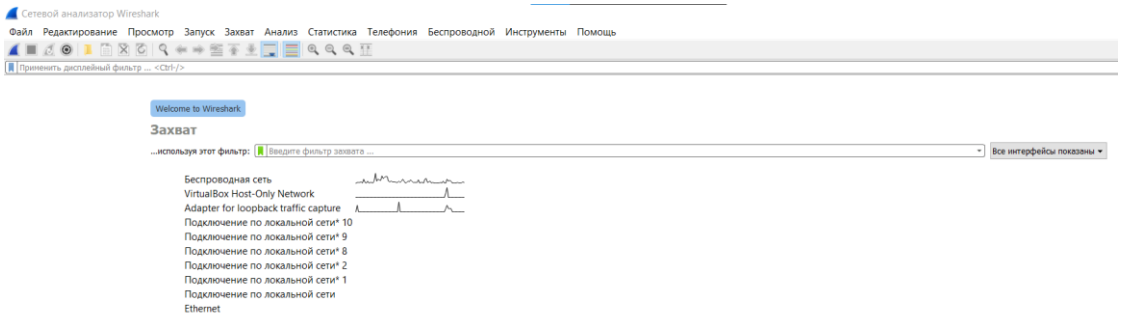
Цель работы: отследить и проанализировать трафик приложений, общающихся с сервером по протоколу HTTP

Порядок выполнения:

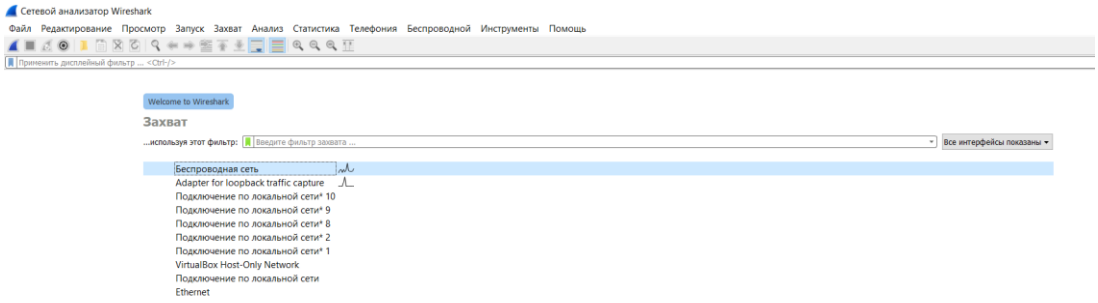
1. Установить программу
2. Выбрать тип сети
3. Запустить анализ
4. Добавить фильтр
5. Начать серфинг в интернете
6. Изучить кадры Http в данных, захваченных программой Wireshark. Сопоставить результаты

Основная часть

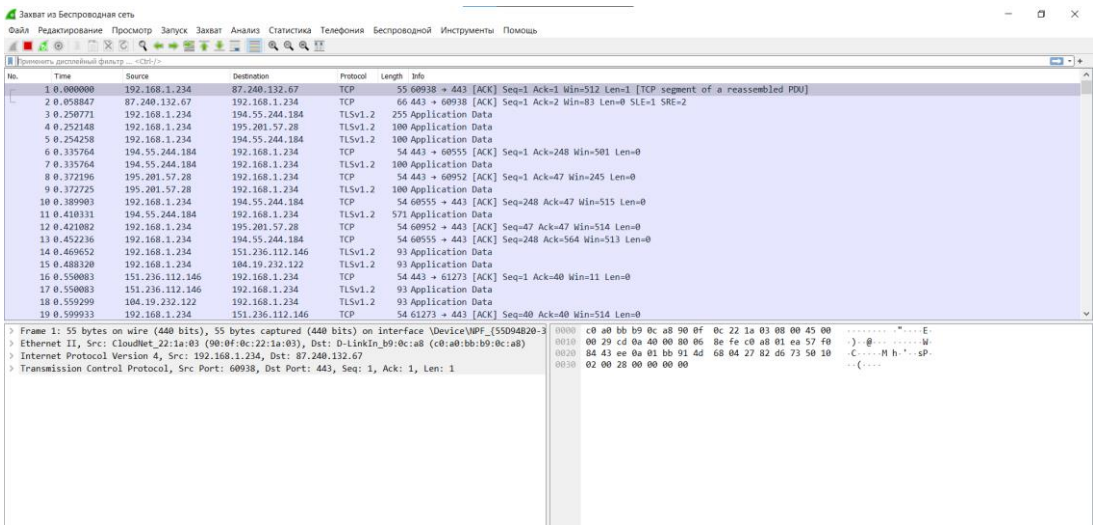
1. Установили программу:



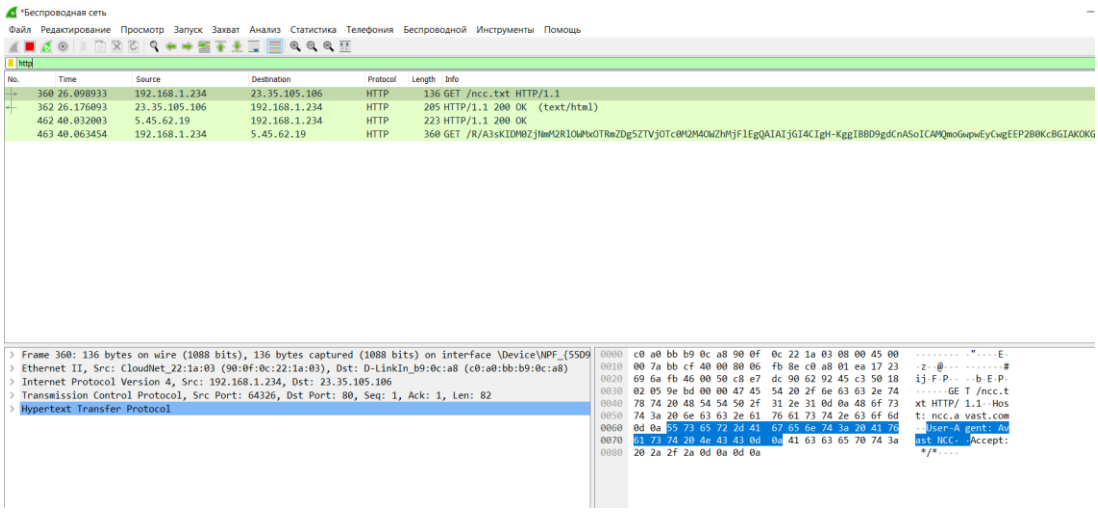
2. Выбираем тип сети:



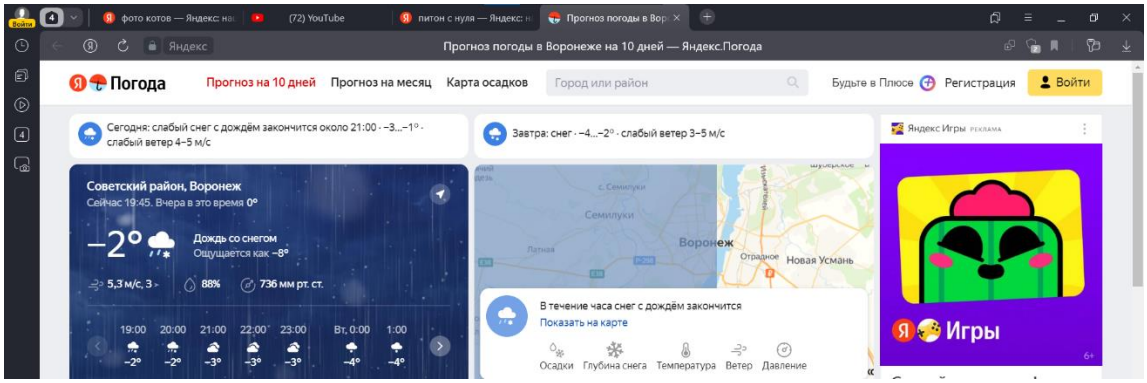
3. Запускаем анализ:

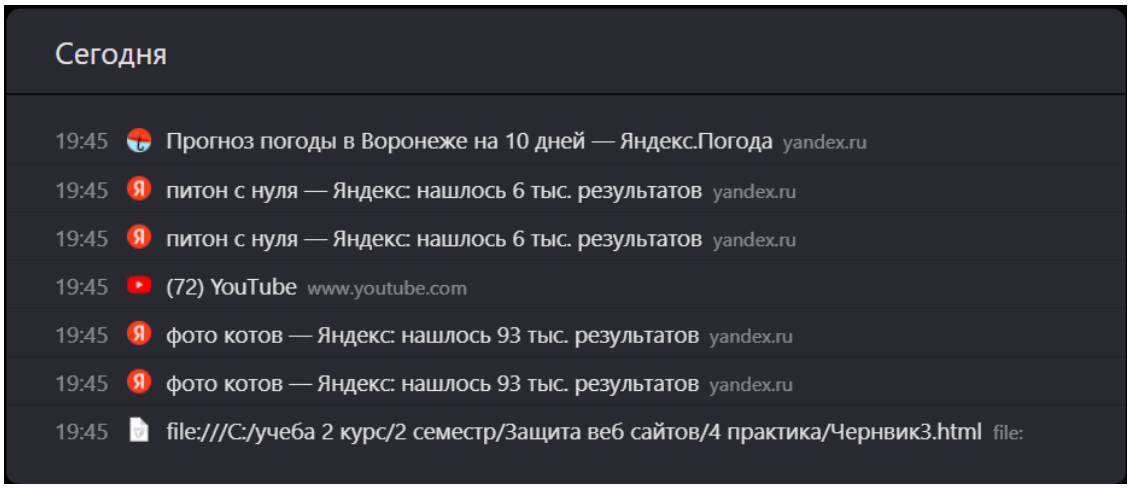


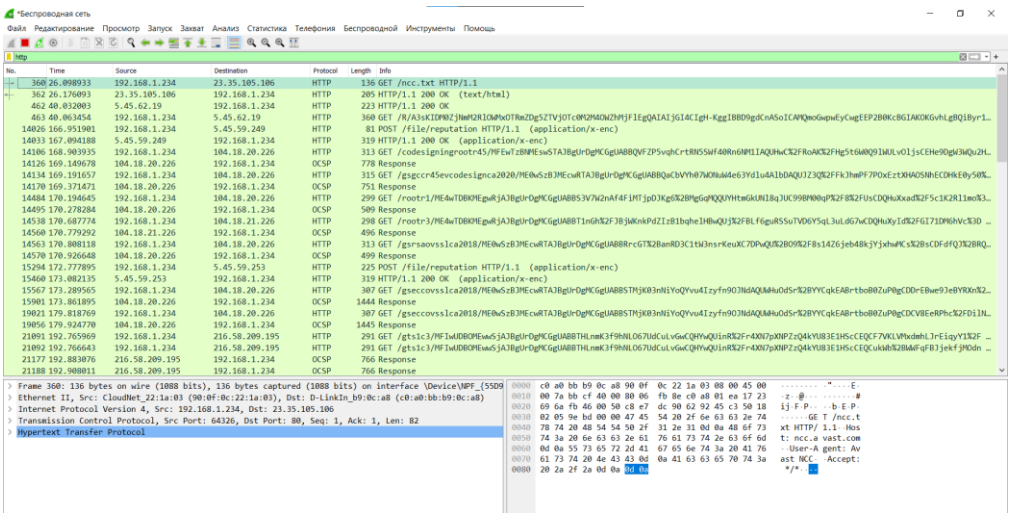
4. Добавляем фильтр:

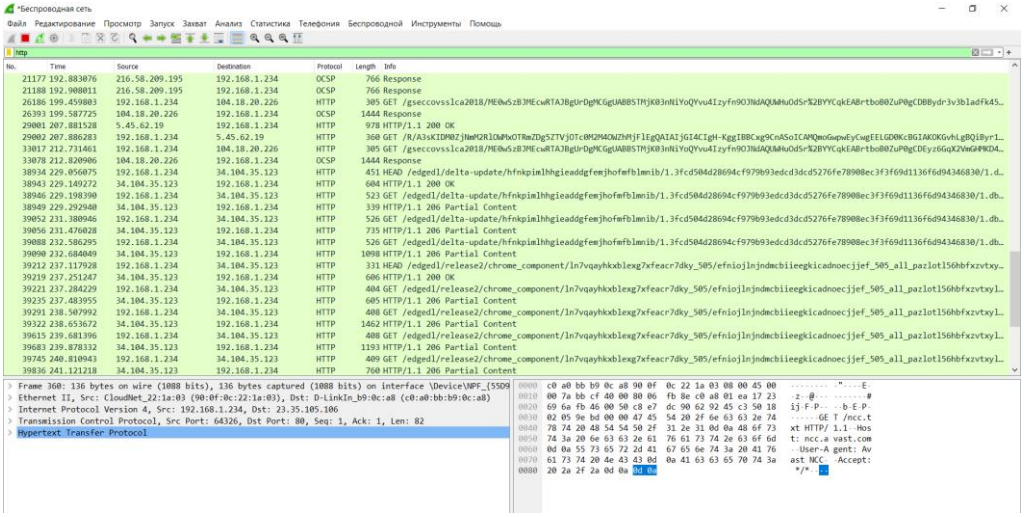


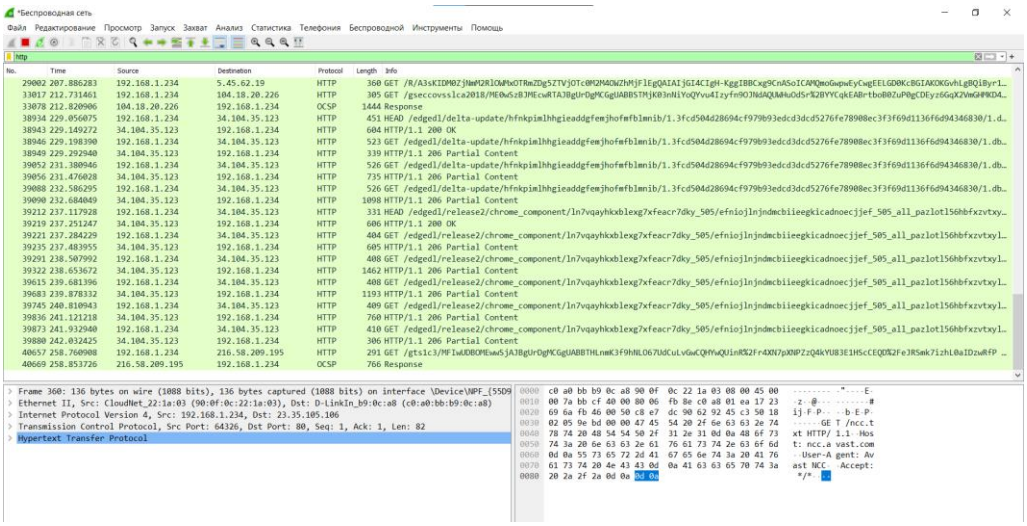
5. Начинаем серфинг в интернете:



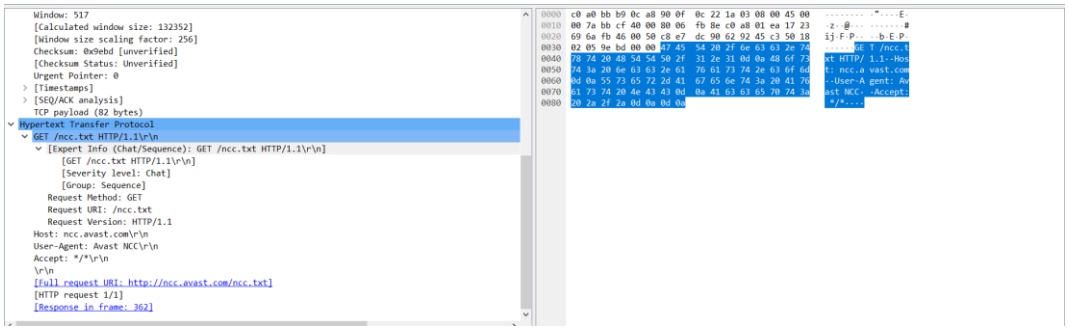


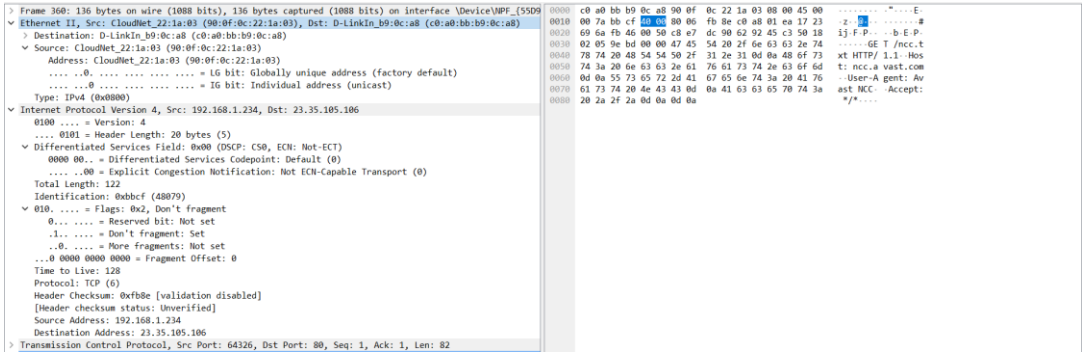

*Беспроводная сеть
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
http
No. Time Source Destination Protocol Length Info
360 26.098933 192.168.1.234 23.35.105.106 HTTP 136 GET /ncc.txt HTTP/1.1
362 26.176093 23.35.105.106 192.168.1.234 HTTP 205 HTTP/1.1 200 OK (text/html)
462 40.032003 5.45.62.19 192.168.1.234 HTTP 223 HTTP/1.1 200 OK
463 40.063454 192.168.1.234 5.45.62.19 HTTP 360 GET /R/A3sKIDM0ZjNmM2RlOWMxOTRmZDg5ZTVjOTc0M2M4OWZhMjFlEgQAIAIjGI4CIgH-KggIBBD9gdCnASoICAMQmoGwpwEyCwgEEP2B0KcBGIAKOKGvhLgBQiByr1…
14026 166.951901 192.168.1.234 5.45.59.249 HTTP 81 POST /file/reputation HTTP/1.1 (application/x-enc)
14033 167.094188 5.45.59.249 192.168.1.234 HTTP 319 HTTP/1.1 200 OK (application/x-enc)
14106 168.903935 192.168.1.234 104.18.20.226 HTTP 313 GET /codesigningrootr45/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQVF2P5vqhCrtRN5SWf40Rn6NM1IAQUHwC%2FRoAK%2FHg5t6W0Q9lWULvOljsCEHe9OgW3WQu2H…
14126 169.149678 104.18.20.226 192.168.1.234 OCSP 778 Response
14134 169.191657 192.168.1.234 104.18.20.226 HTTP 315 GET /gsgccr45evcodesignca2020/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBQaCbVYh07WXNuW4e63Ydlu4AlbDAQUJ3Q%2FFk3hmPF7POxEztXHAO5NhECDHkE0y50%…
14170 169.371471 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/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCDQHuXxad%2F5c1K2Rl1mo%3…
14495 170.278284 104.18.20.226 192.168.1.234 OCSP 509 Response
14538 170.687774 192.168.1.234 104.18.21.226 HTTP 298 GET /rootr3/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBT1nGh%2FJBjWKnkPdZIzB1bqhelHBwQUj%2FBLf6guRSSuTVD6Y5qL3uLdG7wCDQHuXyId%2FGI71DM6hVc%3D …
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 /gsr1aovssl1ca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBRrcGT%2Bam8D3Cit%3nsrKeuXC7DPwQU%2BO9%2F8s14Z6jeb48kjYjxhwMC%3D%2BCDFdfQ3%2BRQ…
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 307 GET /gseccovsslca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBSTMjK03nNiYoQYvu4Izyfn9OJNdAQUkHuOdSr%2BYYCqkEABrtboB0ZuP0gCDCDrEBwe9JeBYRXn%2…
15901 173.861895 104.18.20.226 192.168.1.234 OCSP 1444 Response
19021 179.818769 192.168.1.234 104.18.20.226 HTTP 307 GET /gseccovsslca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBSTMjK03nNiYoQYvu4Izyfn9OJNdAQUkHuOdSr%2BYYCqkEABrtboB0ZuP0gCDCV8EeRPhc%2FDiINL…
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 /gts1c3/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBTHLnmK3f9hNLO67UdCuLvGwCQHYwQUinR%2Fr4XN7pXNPZzQ4kYU83E1HScCEQCF7VKLVMxdmhLJrEiqyY1%2F …
21092 192.766643 192.168.1.234 216.58.209.195 HTTP 291 GET /gts1c3/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBTHLnmK3f9hNLO67UdCuLvGwCQHYwQUinR%2Fr4XN7pXNPZzQ4kYU83E1HScCEQCukWb%2BWAFqFBIjekfjMOdn …
21177 192.883076 216.58.209.195 192.168.1.234 OCSP 766 Response
21188 192.908011 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 \Device\NPF_{55D9
Ethernet II, Src: CloudNet_22:1a:03 (90:0f:0c:22:1a:03), Dst: D-LinkIn_b9:0c:a8 (c0: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
0000 c0 a0 bb b9 0c a8 90 0f 0c 22 1a 03 08 00 45 00 ·····"····E·
0010 00 7a bb cf 40 00 80 06 fb 8e c0 a8 01 ea 17 23 ·z··@····· ·····#
0020 69 6a fb 46 00 50 c8 e7 dc 90 62 92 45 c3 50 18 ij·F·P···· ··b·E·P·
0030 02 05 9e bd 00 00 47 45 54 20 2f 6e 63 63 2e 74 ····· GE T /ncc.t
0040 78 74 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 xt HTTP/ 1.1··Hos
0050 74 3a 20 6e 63 63 2e 61 76 61 73 74 2e 63 6f 6d t: ncc.a vast.com
0060 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 41 76 ··User-A gent: Av
0070 61 73 74 20 4e 43 43 0d 0a 41 63 63 65 70 74 3a ast NCC· ·Accept:
0080 20 2a 2f 2a 0d 0a */*· ·

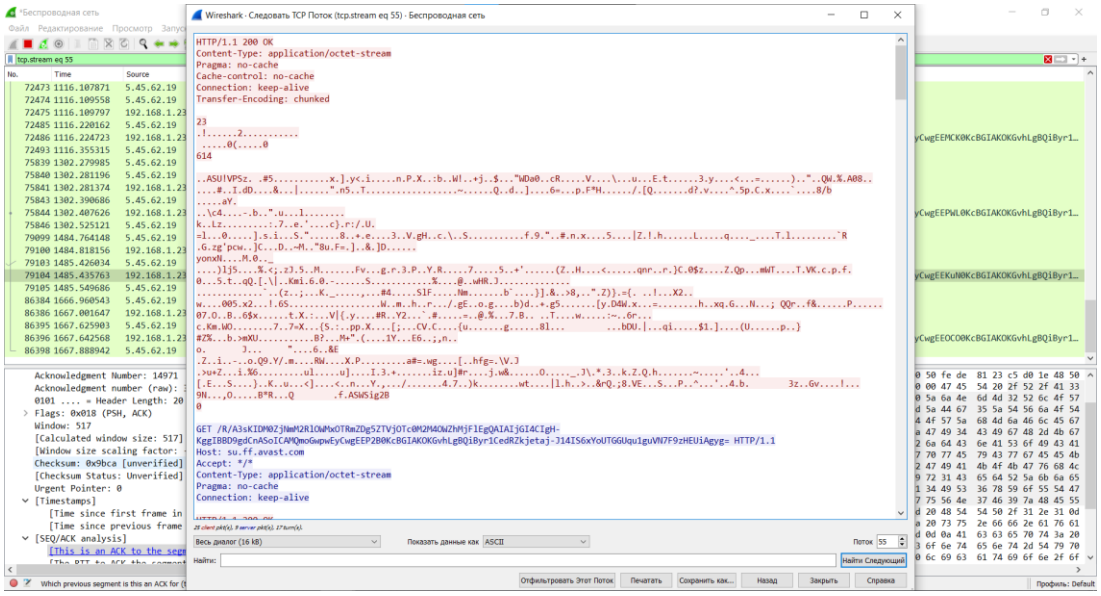

*Беспроводная сеть
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
http
No. Time Source Destination Protocol Length Info
21177 192.883076 216.58.209.195 192.168.1.234 OCSP 766 Response
21188 192.908011 216.58.209.195 192.168.1.234 OCSP 766 Response
26186 199.459803 192.168.1.234 104.18.20.226 HTTP 305 GET /gseccovsslca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBSTMjK03nNiYoQYvu4Izyfn9OJNdAQUkHuOdSr%2BYYCqkEABrtboB0ZuP0gCDBBydr3v3bladFk45…
26393 199.587725 104.18.20.226 192.168.1.234 OCSP 1444 Response
29001 207.881528 5.45.62.19 192.168.1.234 HTTP 978 HTTP/1.1 200 OK
29002 207.886283 192.168.1.234 5.45.62.19 HTTP 360 GET /R/A3sKIDM0ZjNmM2RlOWMxOTRmZDg5ZTVjOTc0M2M4OWZhMjFlEgQAIAIjGI4CIgH-KggIBBCxg9CnASoICAMQmoGwpwEyCwgEELGD0KcBGIAKOKGvhLgBQiByr1…
33017 212.731461 192.168.1.234 104.18.20.226 HTTP 305 GET /gseccovsslca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBSTMjK03nNiYoQYvu4Izyfn9OJNdAQUkHuOdSr%2BYYCqkEABrtboB0ZuP0gCDEyz6GqX2VmGHPKD4…
33078 212.820906 104.18.20.226 192.168.1.234 OCSP 1444 Response
38934 229.056075 192.168.1.234 34.104.35.123 HTTP 451 HEAD /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.d…
38943 229.149272 34.104.35.123 192.168.1.234 HTTP 604 HTTP/1.1 200 OK
38946 229.198390 192.168.1.234 34.104.35.123 HTTP 523 GET /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.db…
38949 229.292940 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 /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.db…
39056 231.476028 34.104.35.123 192.168.1.234 HTTP 735 HTTP/1.1 206 Partial Content
39088 232.586295 192.168.1.234 34.104.35.123 HTTP 526 GET /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.db…
39090 232.684049 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 /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxy…
39219 237.251247 34.104.35.123 192.168.1.234 HTTP 606 HTTP/1.1 200 OK
39221 237.284229 192.168.1.234 34.104.35.123 HTTP 404 GET /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
39235 237.483955 34.104.35.123 192.168.1.234 HTTP 605 HTTP/1.1 206 Partial Content
39291 238.507992 192.168.1.234 34.104.35.123 HTTP 408 GET /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
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 /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
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 /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
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 \Device\NPF_{55D9
Ethernet II, Src: CloudNet_22:1a:03 (90:0f:0c:22:1a:03), Dst: D-LinkIn_b9:0c:a8 (c0: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
0000 c0 a0 bb b9 0c a8 90 0f 0c 22 1a 03 08 00 45 00 ·····"····E·
0010 00 7a bb cf 40 00 80 06 fb 8e c0 a8 01 ea 17 23 ·z··@····· ·····#
0020 69 6a fb 46 00 50 c8 e7 dc 90 62 92 45 c3 50 18 ij·F·P···· ··b·E·P·
0030 02 05 9e bd 00 00 47 45 54 20 2f 6e 63 63 2e 74 ····· GE T /ncc.t
0040 78 74 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 xt HTTP/ 1.1··Hos
0050 74 3a 20 6e 63 63 2e 61 76 61 73 74 2e 63 6f 6d t: ncc.a vast.com
0060 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 41 76 ··User-A gent: Av
0070 61 73 74 20 4e 43 43 0d 0a 41 63 63 65 70 74 3a ast NCC· ·Accept:
0080 20 2a 2f 2a 0d 0a */*· ·


*Беспроводная сеть
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
http
No. Time Source Destination Protocol Length Info
29002 207.886283 192.168.1.234 5.45.62.19 HTTP 360 GET /R/A3sKIDM0ZjNmM2RlOWMxOTRmZDg5ZTVjOTc0M2M4OWZhMjFlEgQAIAIjGI4CIgH-KggIBBCxg9CnASoICAMQmoGwpwEyCwgEELGD0KcBGIAKOKGvhLgBQiByr1…
33017 212.731461 192.168.1.234 104.18.20.226 HTTP 305 GET /gseccovsslca2018/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBSTMjK03nNiYoQYvu4Izyfn9OJNdAQUkHuOdSr%2BYYCqkEABrtboB0ZuP0gCDEyz6GqX2VmGHPKD4…
33078 212.820906 104.18.20.226 192.168.1.234 OCSP 1444 Response
38934 229.056075 192.168.1.234 34.104.35.123 HTTP 451 HEAD /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.d…
38943 229.149272 34.104.35.123 192.168.1.234 HTTP 604 HTTP/1.1 200 OK
38946 229.198390 192.168.1.234 34.104.35.123 HTTP 523 GET /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.db…
38949 229.292940 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 /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.db…
39056 231.476028 34.104.35.123 192.168.1.234 HTTP 735 HTTP/1.1 206 Partial Content
39088 232.586295 192.168.1.234 34.104.35.123 HTTP 526 GET /edgedl/delta-update/hfnkpimlhhgieaddgfemjhofmfblmnib/1.3fcd504d28694cf979b93edcd3dcd5276fe78908ec3f3f69d1136f6d94346830/1.db…
39090 232.684049 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 /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxy…
39219 237.251247 34.104.35.123 192.168.1.234 HTTP 606 HTTP/1.1 200 OK
39221 237.284229 192.168.1.234 34.104.35.123 HTTP 404 GET /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
39235 237.483955 34.104.35.123 192.168.1.234 HTTP 605 HTTP/1.1 206 Partial Content
39291 238.507992 192.168.1.234 34.104.35.123 HTTP 408 GET /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
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 /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
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 /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
39836 241.121218 34.104.35.123 192.168.1.234 HTTP 760 HTTP/1.1 206 Partial Content
39873 241.932940 192.168.1.234 34.104.35.123 HTTP 410 GET /edgedl/release2/chrome_component/ln7vqayhkxblexg7xfeacr7dky_505/efniojlnjndmcbiieegkicadnoecjjef_505_all_pazlot156hbfxzvtxyl…
39880 242.032425 34.104.35.123 192.168.1.234 HTTP 306 HTTP/1.1 206 Partial Content
40657 258.760908 192.168.1.234 216.58.209.195 HTTP 291 GET /gts1c3/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBTHLnmK3f9hNLO67UdCuLvGwCQHYwQUinR%2Fr4XN7pXNPZzQ4kYU83E1HScCEQD%2Fe3RSmk7izhL0aIDzwRfP …
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 \Device\NPF_{55D9
Ethernet II, Src: CloudNet_22:1a:03 (90:0f:0c:22:1a:03), Dst: D-LinkIn_b9:0c:a8 (c0: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
0000 c0 a0 bb b9 0c a8 90 0f 0c 22 1a 03 08 00 45 00 ·····"····E·
0010 00 7a bb cf 40 00 80 06 fb 8e c0 a8 01 ea 17 23 ·z··@····· ·····#
0020 69 6a fb 46 00 50 c8 e7 dc 90 62 92 45 c3 50 18 ij·F·P···· ··b·E·P·
0030 02 05 9e bd 00 00 47 45 54 20 2f 6e 63 63 2e 74 ····· GE T /ncc.t
0040 78 74 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 xt HTTP/ 1.1··Hos
0050 74 3a 20 6e 63 63 2e 61 76 61 73 74 2e 63 6f 6d t: ncc.a vast.com
0060 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 41 76 ··User-A gent: Av
0070 61 73 74 20 4e 43 43 0d 0a 41 63 63 65 70 74 3a ast NCC· ·Accept:
0080 20 2a 2f 2a 0d 0a */*· ·

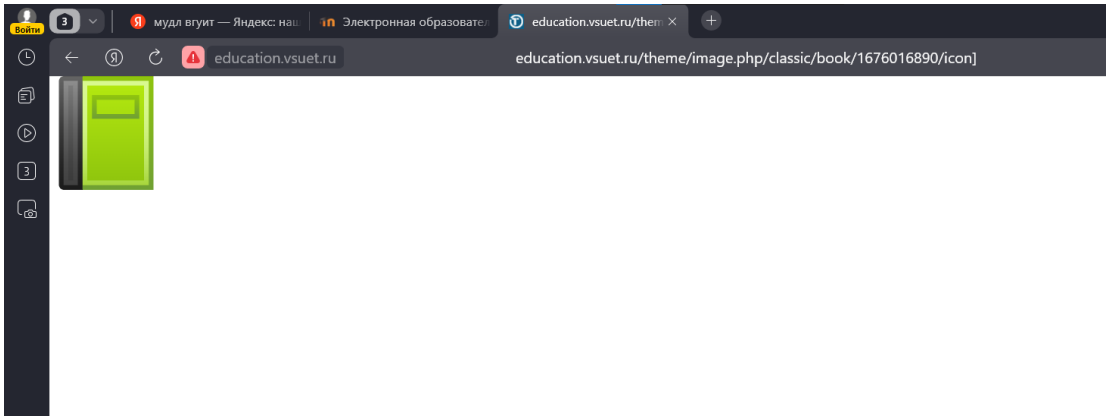
6. Изучить кадры Http в данных, захваченных программой Wireshark. Сопоставить результаты:

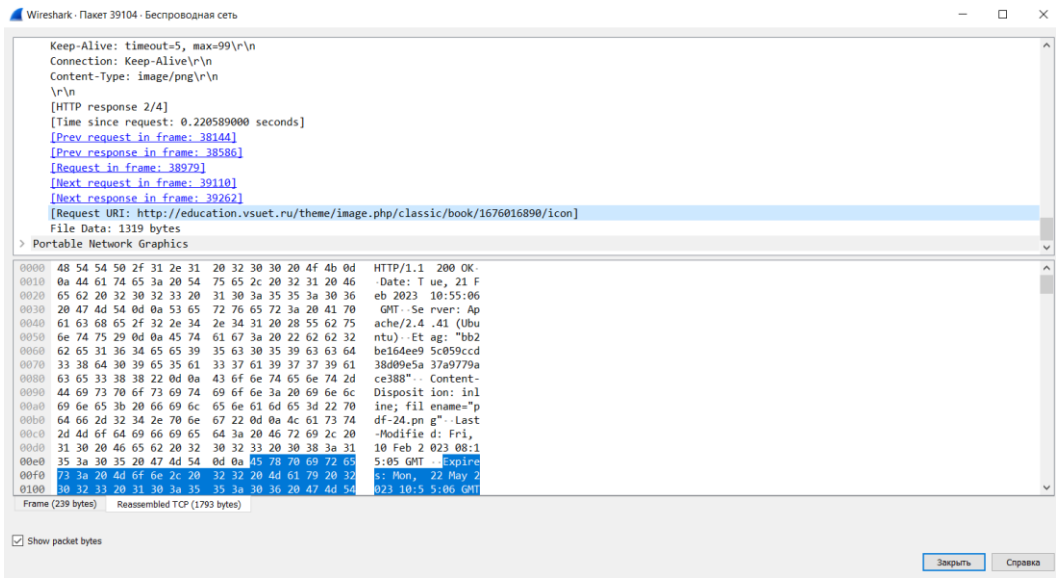


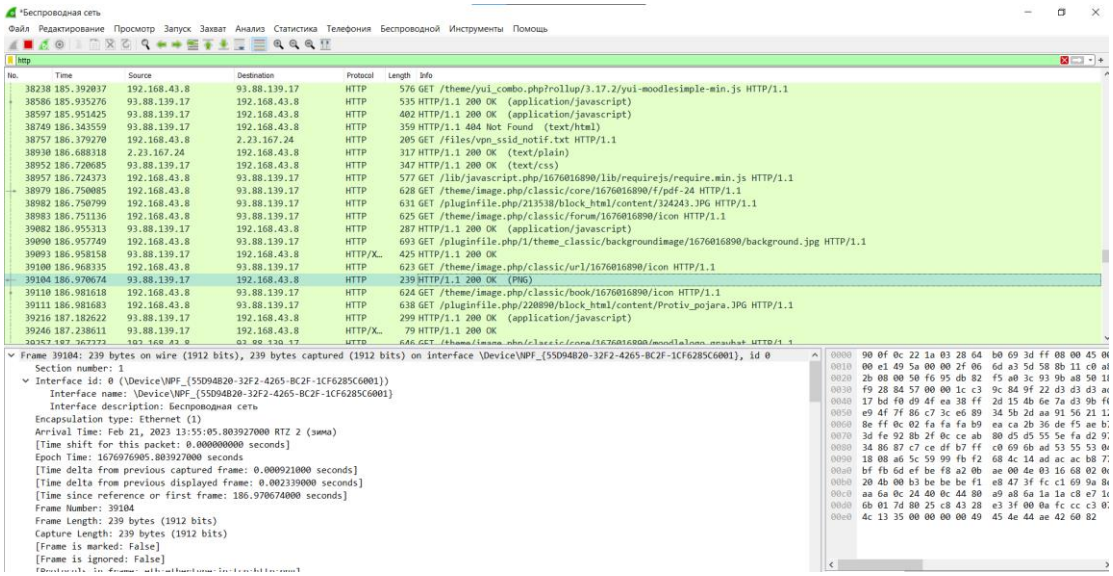




7. Сделаем захват файлов с сайта moodle.







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.