МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Обнаружение сетевого P2P-трафика

Курсовую работу выполнил студент 4 курса 431 группы
специальности 10.05.01 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Стаин Роман Игоревич
Научный руководитель доцент, к.ю.н.
Алексей Владимирович Гортинский

P2P-сети используются для обмена файлами и распространения контента, в том числе нелегального. Это может приводить к нарушению авторских прав и угрожать безопасности пользователей, так как в P2P-сетях часто распространяются вирусы и другие вредоносные программы. Пользователей таких сетей практически невозможно контролировать, поэтому необходимы способы обнаружения и идентификации P2P-трафика.

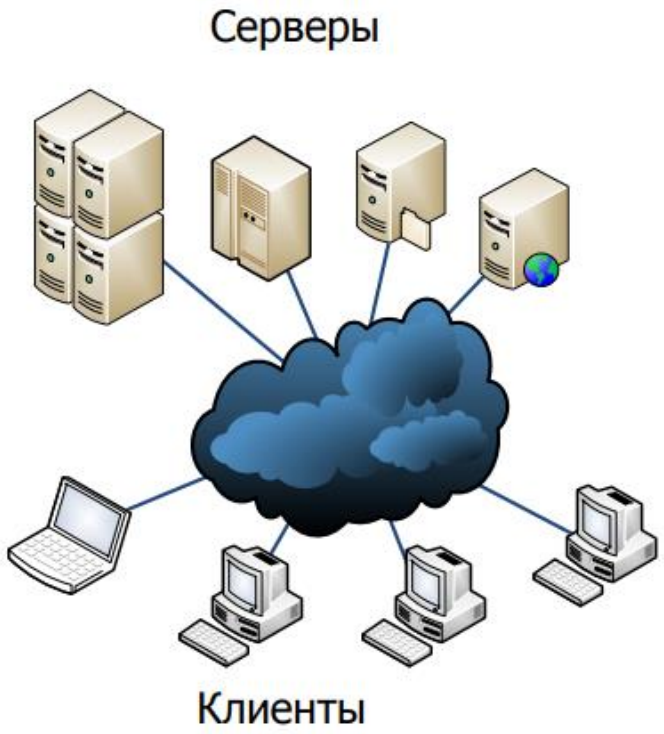
Целью данной работы является изучение и обнаружение общих и частных, позволяющих идентифицировать конкретные протоколы, признаков P2P-трафика.

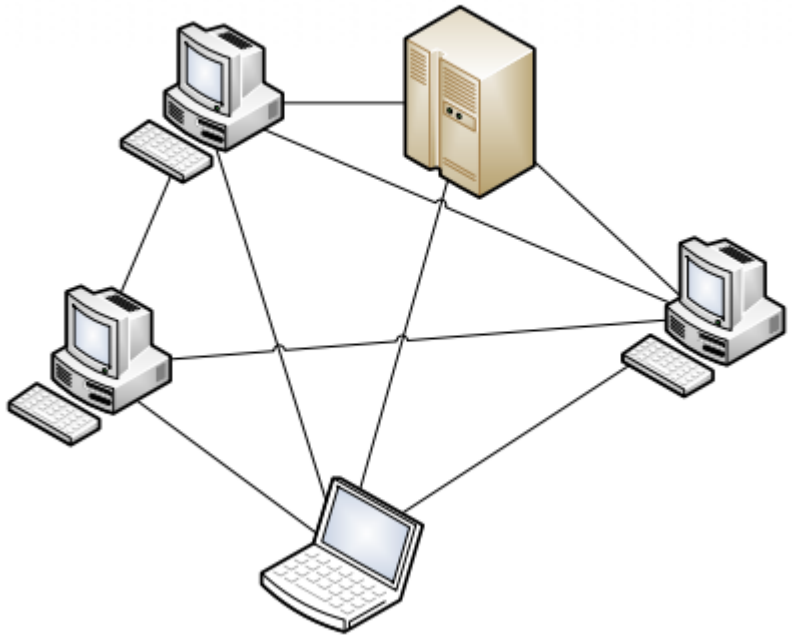
Задачи исследования:

- Изучение архитектуры и общих принципов работы P2P-сети.
- Исследование общих признаков P2P-трафика.
- Исследование признаков некоторых P2P-протоколов.
- Рассмотрение протоколов и приложений, схожих по поведению с P2P.
- Разработка программы, способной перехватывать TCP/UDP-трафик и обнаруживать и идентифицировать P2P-трафик.

Архитектура P2P-сети

P2P (**p**eer-**to**-**p**eer) — одноранговая, децентрализованная или пиринговая сеть. Это распределённая архитектура приложения, которая разделяет задачи между узлами (peer).





Методы обнаружения P2P-трафика без анализа полезной нагрузки

1. Анализ портов
2. TCP/UDP-эвристика
3. IP/Port-эвристика
4. Пороговый метод идентификации BitTorrent

Эвристические предположения

TCP/UDP-эвристика:

Если пара адресов использует одновременно TCP и UDP, то эти адреса считаются как P2P.

IP/Port-эвристика:

Факт, что при обращении к паре <dst_ip, dst_port> количество адресов источников практически совпадает с количеством портов источников, характеризует P2P-деятельность.

Пороговый метод идентификации BitTorrent

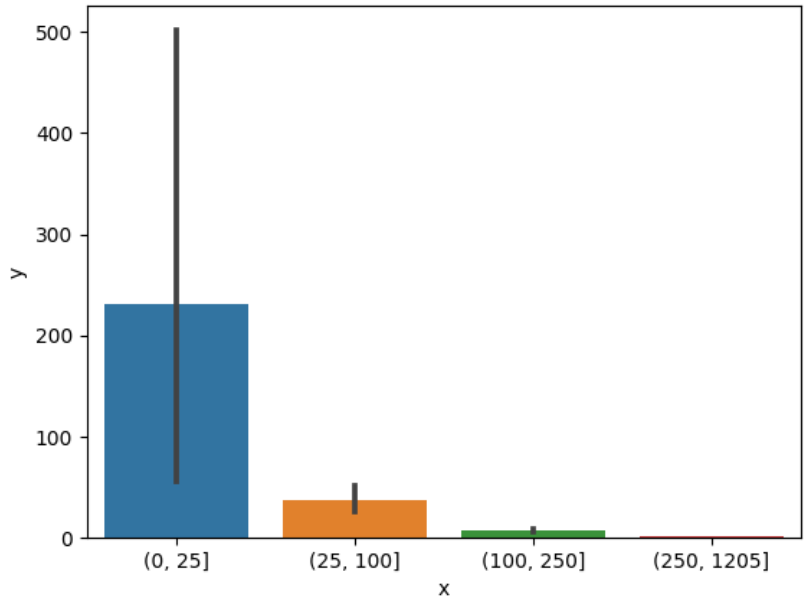
Каждые 30 секунд рассчитываются специальные метрики, которые сравниваются с пороговыми значениями, чтобы определить, является ли хост пиром BitTorrent.

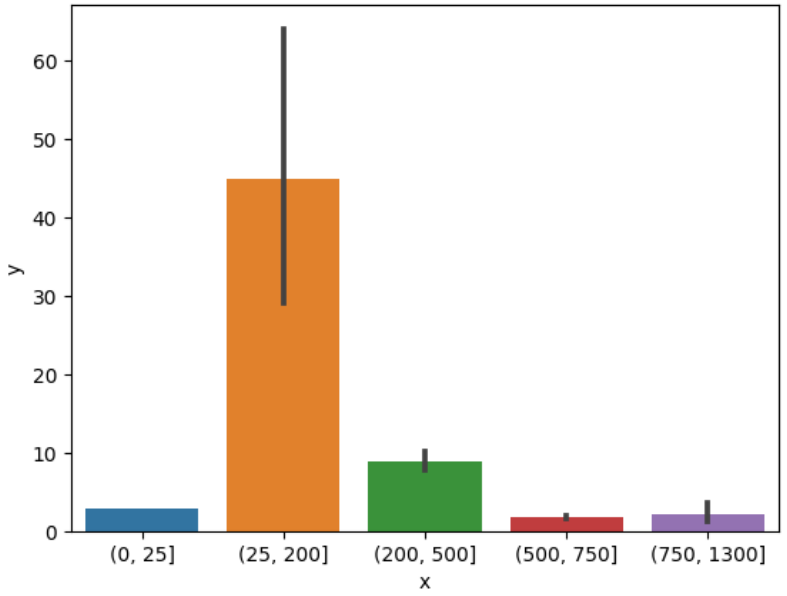
1. Число подключений к хосту C.
2. Коэффициент активной передачи $R_{AT} = \frac{AT}{C}$.
3. Двусторонние передачи данных $BiAT$.
4. Коэффициент изменений отношений $R_{RC} = \frac{RC}{AT}$.

Исключения

Поведение некоторых легальных протоколов, например, SMTP, POP, DNS, NTP может быть схожим с поведением P2P-протоколов.

Также игры и вредоносные программы имеют уникальное поведение и номера портов, что усложняет обработку исключений.





Идентификация P2P-трафика

Адреса могут быть отнесены к некоторому P2P-протоколу исходя из:

1. Номера порта.
2. Анализа полезной нагрузки.
3. Порогового метода идентификации BitTorrent.

Анализ полезной нагрузки

Для идентификации BitTorrent:

1. Минимальная длина полезной нагрузки пакета 20 байт.
2. Байт со значением 19.
3. Следующая за ним строка «BitTorrent protocol».

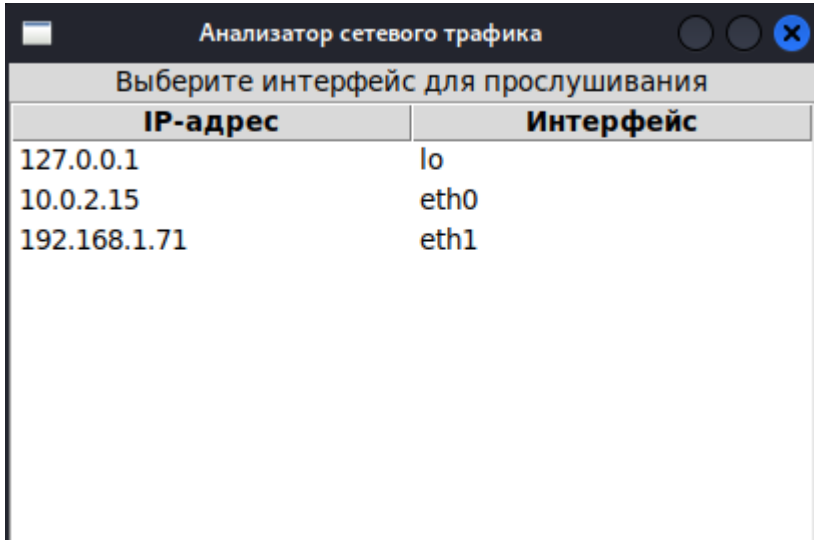
Для идентификации Bitcoin:

1. Минимальная длина полезной нагрузки пакета 20 байт.
2. Порт источника или назначения равен 8333 или 8334.
3. Содержится команда или сообщение, характерное для Bitcoin.

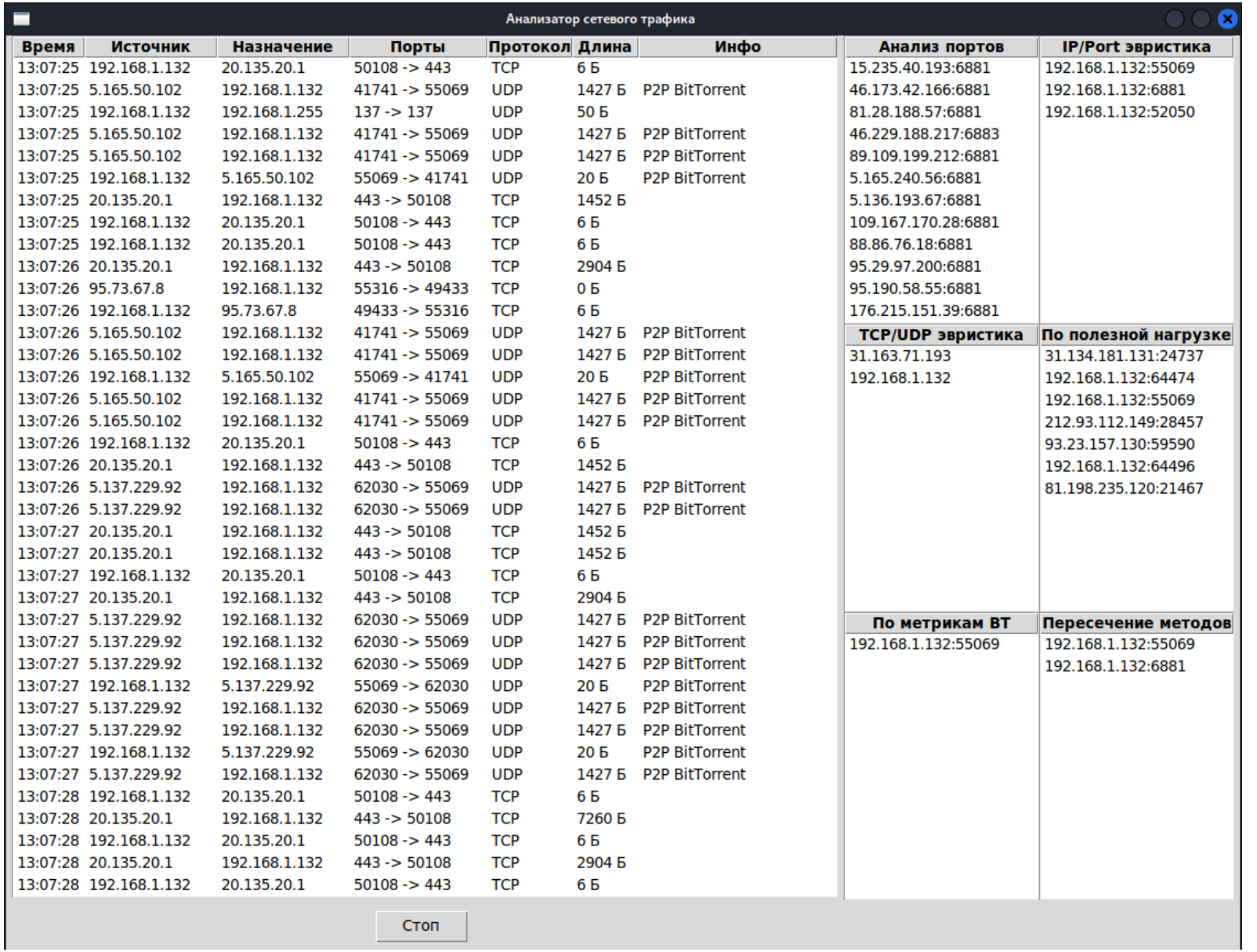
Описание программы

В данной работе был разработан сниффер или анализатор сетевого трафика, который перехватывает TCP/UDP-трафик и анализирует его на наличие P2P-деятельности.

При запуске программы предлагается выбор сетевого интерфейса, который будет прослушиваться:



Далее открывается основное окно программы:



Заключение

В данной работе были рассмотрены теоретические сведения о технологии P2P, в частности, характерное поведение P2P-трафика и признаки некоторых протоколов.

В практической части была реализована программа — сниффер или анализатор сетевого трафика на языке Python, которая позволяет перехватывать TCP и UDP трафик и анализировать его на присутствие P2P-активности, а также определять некоторые протоколы и приложения. Были реализованы методы анализа портов, обнаружения TCP/UDP- и IP/Port-эвристики, анализ полезной нагрузки для BitTorrent и Bitcoin и пороговый метод сравнения характерных метрик BitTorrent.

Список использованных источников

1. P2P (Peer-to-Peer) [Электронный ресурс]. — URL: https://web.archive.org/web/20171205204322/http://ru.bmstu.wiki/P2P_(Peer-to-Peer) (Дата обращения 19.05.2023). Загл. с экр. Яз. рус.

2. P2P [Электронный ресурс]. — URL: https://glebradchenko.susu.ru/courses/bachelor/odp/2013/SUSU_Distr_11_P2P.pdf (Дата обращения 14.05.2023). Загл. с экр. Яз. рус.

3. Bhatia, M. Multi-level p2p traffic classification using heuristic and statisticalbased techniques: A hybrid approach / M. Bhatia, V. Sharma, P. Singh, M. Masud // Symmetry. — 12 2020. — Vol. 12. — P. 2117.

4. Karagiannis, T. A longitudinal study of p2p traffic classification / T. Karagiannis,

K. Papagiannaki, M. Faloutsos // Proc. of 14th IEEE International Symposium

on Modeling, Analysis, and Simulation. — 2005.

5. Karagiannis, T. BLINC: multilevel traffic classification in the dark / T. Karagiannis, K. Papagiannaki, M. Faloutsos. — 2005. — Pp. 229–240.

6. Karagiannis, T. Transport layer identification of P2P traffic / T. Karagiannis,

A. Broido, M. Faloutsos, K. C. Claffy. — 2004. — Pp. 121–134.

7. Ngiwlay, W. Bittorrent peer identification based on behaviors of a choke algorithm / W. Ngiwlay, C. Intanagonwiwat, Y. Teng-amnuay // Association for

Computing Machinery. — 2008.

8. Бредихин, С. В.Диагностика p2p-АКТИВНОСТИ на основе анализа потоков netflow / С. В. Бредихин, Н. Г. Щербакова // Проблемы информатики. — 2012. — № 1. — С. 40–51.
9. Desclaux, F. Vanilla skype part 1 / F. Desclaux, K. Kortchinsky // Proc of RECON2006. — 2006.
10. BitTorrentSpecification - TheoryOrg. [Электронный ресурс]. — URL: https://wiki.theory.org/BitTorrentSpecification (Дата обращения 19.05.2023). Загл. с экр. Яз. англ.
11. Protocol documentation - Bitcoin Wiki. [Электронный ресурс]. — URL: https://en.bitcoin.it/wiki/Protocol_documentation (Дата обращения 19.05.2023). Загл. с экр. Яз. англ.

Спасибо за внимание!