1. Начало
2. Сбор соединений сниффером за один час
3. Вывод списка соединений отдельным файлом (список А) в папку для хранения трафика до обработки (директория А)
4. Проверка по счетчику первый ли список идет на обработку в текущей рабочей сессии
5. Если да – с конца списка отобрать все соединения за последние 5 минут, отрезать их и вывести отдельным файлом (список В) в папку для хранения пятиминуток (директория В)
6. Если нет – добавить с предыдущего файла последние 5 минут (список В) к списку А, таким образом при их объединении назовем полученный список – С
7. Очищаем директорию В от уже использованного списка В с целью сохранения свободного пространства памяти
8. Берем список С и выполняем для него п. 5
9. Удаляем из рассматриваемого списка (А или С) все соединения, где адрес отправителя – наша ЭВМ
10. Переходим к рассмотрению каждого соединения в списке
11. Проверяем по количеству пакетов

11.1) Если не прошел – проверяем последнее ли это соединение, если нет, то очередное соединение переходит в п.10

11.2) удаляем в любом случае это соединение как не прошедшее отбор

11.3) если список не пуст, то переход к п.14, если пуст, то к п.23

1. Если прошел – оставляем соединение в списке
2. Проверяем есть ли очередное соединение, если да, то очередное переходит в п.10, иначе переходим к п.14
3. Отобранные соединения сортируем по адресам отправителей и располагаем в хронологическом порядке для каждого адреса отправителя
4. После выполнения п. 14, наш список А (или С) приобретает вид разбитого на подсписки, где каждый подсписок это набор соединений по каждому уникальному IP адресу, расположенных по хронологии. Начинаем рассматривать каждый такой подсписок по отдельности (подсписок D)
5. Для каждого соединения в D вычисляем параметры Т, T”. А для первого соединения в таком подсписке – T’, затем и для него T”
6. После проведения п. 16, каждый D закидываем в поле данных для работы нейронного газа
7. Получаем изображение
8. Сопоставляем изображение и плоскость, определяющую параметры сканирования -пороговая («красная») плоскость
9. Есть ли касание, пересечение границ плоскости кластерами
10. Если да – сохранение данного подсписка D отдельным файлом (файл E) и его изображения в папку для подозрительного трафика (директория E)
11. Есть ли очередной D
12. Сохраняем список А (или С) по состоянию на п. 16 включительно, а если в списке нет соединений, прошедших п. 11, то по состоянию на п. 9 включительно и перемещаем его в папку для обработанного трафика (директория F)
13. Анализ и принятие решения на отнесение трафика к сканирующему
14. конец