# Учебный курс
# «ИНФОРМАТИКА»

Преподаватель:

ст. преп. Зуева Екатерина Александровна

# Информационная безопасность

Лекция 13

# Информационная безопасность

1. Основные понятия информационной безопасности.
2. Классификация угроз и атак.
3. Способы и методы защиты информации.
4. Защитные механизмы информационной безопасности.
5. ЭЦП.
6. Физическая защита.
7. Изучение основных функций единого портала государственных услуг www.egov.kz.

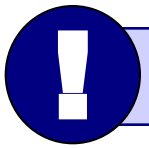
# Объектами авторского права

**… являются**

- **программы** для компьютеров (включая подготовительные материалы, а также звук, графику и видео, которые получаются с помощью программы)
- **базы данных** (данные, специально организованные для поиска и обработки с помощью компьютеров)

**… не являются**

- **алгоритмы и языки программирования**
- **идеи и принципы**, лежащие в основе программ, баз данных, интерфейса;
- **официальные документы**



**Охраняется форма, а не содержание!**

# Авторское право

- автор – физическое лицо (не организация)
- возникает «в силу создания» продукта, не требует формальной регистрации
- обозначение: ***© Иванов, 2014*** (год первого выпуска)
- действует в течение жизни и 50 лет после смерти автора
- передается по наследству

# Права автора

**Личные**:

- *право авторства* (право считаться автором)
- *право на имя* (свое имя, псевдоним, анонимно)
- *право на неприкосновенность* (защита программы и ее названия от искажений)

**Имущественные**: осуществлять или разрешать

- выпуск программы в свет
- копирование в любой форме
- распространение
- изменение (в т.ч. перевод на другой язык)

# Использование программ и БД

**Основания:**

- *договор* в письменной форме
- при массовом распространении – *лицензионное соглашение* на экземпляре

**Можно без разрешения автора:**

- хранить в памяти *1 компьютера* (или по договору)
- вносить *изменения*, необходимые для работы на компьютере пользователя (но не распространять!)
- исправлять явные *ошибки*
- изготовить *копию* для архивных целей
- *перепродать* программу

# Защита от копирования

- **инсталляция программ** (нельзя просто скопировать)
- **регистрационный код** (привязка к оборудованию, серийным номерам) –
- **защита CD, DVD** (теряется при копировании)
- **не работает без диска**
- **аппаратный ключ**


для параллельного порта


для порта USB

- **сканирование сети** (обнаружение копий)
- **сервер в Интернете** проверяет серийные номера
- **техподдержка** – косвенная защита (!)

# Компьютерные преступления

**Экономические**

- обогащение путем взлома информационных систем
- компьютерный шпионаж
- кража программ («пиратство»)

**Против личных прав**

- ложная информация
- незаконный сбор информации
- разглашение банковской и врачебной тайны

**Против общественных и государственных интересов**

- разглашение государственной тайны
- утечка информации
- искажение информации (подсчет голосов)
- вывод из строя информационных систем (диверсии)

# Компьютерные преступления

**Нарушение авторских и смежных прав.**

*присвоение авторства* (плагиат) — до 6 мес. лишения свободы

*незаконное использование*, а также приобретение, хранение, перевозка в целях сбыта – до 2 лет

*группой лиц*, в особо крупном размере или с использованием служебного положения – до 5 лет

**Признаки преступления:**

уничтожение, блокирование, модификация или копирование информации, нарушение работы компьютера или сети

**Неправомерный доступ к компьютерной информации.**

до 2 лет лишения свободы; группой лиц – до 5 лет

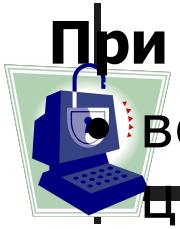
**Создание, использование и распространение вредоносных программ.**

до 3 лет лишения свободы; с тяжкими последствиями – до 7 лет

**Нарушение правил эксплуатации компьютеров и сети.**

до 2 лет лишения свободы; с тяжкими последствиями – до 4 лет

# Авторские права в Интернете

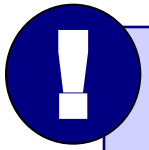


**При нелегальном использовании**:

- всегда есть косвенная выгода (достижение своих целей);
- ущерб авторам, снижение дохода;
- снижение посещаемости и цитируемости сайтов ⇒ снижение дохода.

**Правила**:

- при использовании материалов в учебных работах ссылаться на источник;
- для публикации в Интернете текста или фотографии получить разрешение автора или издателя.



**Официальные документы – не объекты авторского права!**

# Что можно без спроса…

- скопировать себе картинку (текст)
- послать картинку (текст) другу
- отсканировать книгу

**Разместить на сайте**

- ~~картинку с другого сайта~~
- Указ Президента
- цитату из статьи с указанием автора
- ~~статью с другого сайта (или из книги) с указанием автора~~
- описание алгоритма
- ~~отсканированную книгу~~
- повесть А.С. Пушкина

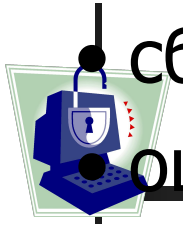
# Защита информации

**Информационная безопасность** – это защищенность информации от случайных и намеренных действий, способных нанести недопустимый ущерб. Включает

- **доступность** информации за приемлемое время (управление производством, продажа билетов, банковские расчеты)
- **целостность** – непротиворечивость, актуальность (рецепт, описание процесса)
- **конфиденциальность** – защита от несанкционированного доступа (сведения о зарплате, пароли)

**Защита информации** – мероприятия, направленные на обеспечение информационной безопасности.

# Угрозы



- сбои оборудования
- ошибки в программном обеспечении
- вредоносные программы (вирусы, «черви»)
- хакерские атаки
- ошибки персонала
- диверсии («обиженные работники»)
- информационный шпионаж
- подделка информации
- «дыры в головах» – неграмотность пользователей

# Меры по защите информации

- **законодательные** (правовые)
- **административные** – политика безопасности предприятия
- **процедурные** – должностные обязанности работников
- **программно-технические** – защита с помощью программных и аппаратных средств

# Доктрина инф. безопасности

принята Советом Безопасности в 2000 г.

**Национальные интересы :**

- соблюдение прав и свобод человека в области получения и использования информации
- информационное обеспечение политики РК
- развитие информационных технологий
- защита информации от несанкционированного доступа

**Принципы политики :**

- соблюдение законов (РК и международных)
- информирование общества о работе госорганов
- равенство всех перед законом
- приоритет – казахстанским разработкам

# Законодательные меры

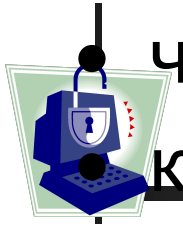
## Уголовный кодекс РК

- *ст. 272* – неправомерный доступ к компьютерной информации (включая копирование)
- *ст. 273* – создание, использование и распространение вредоносных программ
- *ст. 274* – нарушение правил эксплуатации компьютеров и компьютерных сетей

**Закон «Об информации, информационных технологиях и защите информации»** (2006)

- защиту государственной тайны и персональных данных берет на себя государство
- **сертификация** информационных систем, баз и банков данных (проверка надежности)
- **лицензии** на право работы в области защиты информации

# Политика безопасности



- что нужно защищать в первую очередь?
- какие угрозы наиболее опасны?
- как организуется защита информации?
- кто имеет право доступа к информации (чтение, изменение)?
- кто отвечает за информационную безопасность?
- что запрещено и как наказывают за эти нарушения?

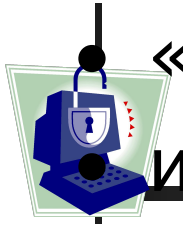
# Процедурные меры

- управление **персоналом** (разделение обязанностей, минимум привилегий)
- ограничение доступа (**охрана**)
- защита системы **электропитания**
- **пожарная** сигнализация
- защита от **перехвата данных**
- защита **ноутбуков и сменных носителей**
- запрет устанавливать постороннее **программное обеспечение**
- **резервное копирование** данных
- **резервирование** (дисковые RAID-массивы)

# Программно-технические меры

- вход в систему по **паролю** (смарт-карте, отпечаткам пальцев и т.п.)
- **ограничение прав**
- **протоколы** работы (вход в систему, обращение к файлам, изменение настроек, выход и т.д.)
- **шифрование** данных (алгоритмы RSA, DES)
- **контроль целостности** данных
- **межсетевые экраны** (брандмауэры)

# Возможности взлома защиты



- «слабые» алгоритмы шифрования
- используются простые пароли
- пароли не меняются длительное время
- пароли записаны на бумажке
- ненадежное программное обеспечение
- **человеческий фактор**
  - невыполнение инструкций
  - не установлены обновления программ
  - сообщники внутри организации

# Защита информации (итог)

- «абсолютной» защиты нет
- защита должна быть комплексной («со всех сторон»)
- надежность защиты = надежности «слабого звена»
- «слабое звено» – человек

- Под **информационной безопасностью** понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
- **Защита информации** – комплекс мероприятий, направленных на обеспечение информационной безопасности.

- **Угроза информационной безопасности** (ИБ) – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
- Попытка реализации угрозы называется **атакой**.
- Классификация угроз ИБ можно выполнить по нескольким критериям:
  - **по аспекту ИБ** (доступность, целостность, конфиденциальность);
  - **по компонентам ИС**, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура);
  - **по способу осуществления** (случайные или преднамеренные действия природного или техногенного характера);
  - **по расположению источника угроз** (внутри или вне рассматриваемой ИС).

# Свойства информации

- Вне зависимости от конкретных видов угроз информационная система должна обеспечивать базовые свойства информации и систем ее обработки:
  - **доступность** – возможность получения информации или информационной услуги за приемлемое время;
  - **целостность** – свойство актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения;
  - **конфиденциальность** – защита от несанкционированного доступа к информации.

# Примеры реализации угрозы нарушения целостности данных

- Одними из наиболее часто реализуемых угроз ИБ являются кражи и подлоги. В информационных системах несанкционированное изменение информации может привести к потерям.
- Целостность информации может быть разделена на **статическую** и **динамическую.**
- Примерами нарушения статической целостности являются:
  - ввод неверных данных;
  - несанкционированное изменение данных;
  - изменение программного модуля вирусом;
- Примеры нарушения динамической целостности:
  - нарушение атомарности транзакций;
  - дублирование данных;
  - внесение дополнительных пакетов в сетевой трафик.

# Классификация атак

**Внутренние угрозы**

- Утечки информации
- Неавторизованный доступ

**Внешние угрозы**

- Вредоносные программы
- Атаки хакеров
- Спам
- Фишинг
- Прочее вредоносное и нежелетельное ПО (spyware, adware)
- root kits, botnets

# Понятие атаки на информационную систему

- **Атака** – любое действие или последовательность действий, использующих уязвимости информационной системы и приводящих к нарушению политики безопасности.
- **Механизм безопасности** – программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.
- **Сервис безопасности** - сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление *атаки*. *Сервис* использует один или более механизмов безопасности.

# Классификация атак

- Классификация атак на информационную систему может быть выполнена по нескольким признакам:
  - По месту возникновения:
    - Локальные атаки (источником данного вида атак являются пользователи и/или программы локальной системы);
    - Удаленные атаки (источником атаки выступают удаленные пользователи, сервисы или приложения);
  - По воздействию на информационную систему
    - Активные атаки (результатом воздействия которых является нарушение деятельности информационной системы);
    - Пассивные атаки (ориентированные на получение информации из системы, не нарушая функционирование информационной системы);

# Классификация сетевых атак

- При описании сетевых атак в общем случае используется следующее представление:
  - существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):

# Сетевые атаки

- **I. Пассивная атака**
- Пассивной называется такая *атака*, при которой *противник* не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью *пассивной атаки* может быть только прослушивание передаваемых сообщений и анализ трафика.

# Сетевые атаки

- Активной называется такая *атака*, при которой *противник* имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы *активных атак*:
- **Отказ в обслуживании** - *DoS-атака (Denial of Service)*
  - Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. *Противник* может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной *атаки* является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов.
  - Классическим примером такой *атаки* в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения.
  - В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.

# Сетевые атаки

- **Модификация потока данных** - *атака "man in the middle"*
- Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

# Сетевые атаки

- **Создание ложного потока (фальсификация)**
- *Фальсификация* (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого

# Сетевые атаки

- **Повторное использование**
- Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая *replay-атака*.
- На самом деле *replay-атаки* являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов *атаки* для получения несанкционированного доступа, его часто рассматривают как отдельный тип *атаки*.

# Принципы обеспечения информационной безопасности

- Системность;
- Комплексность;
- Непрерывность защиты;
- Разумная достаточность;
- Гибкость управления и применения;
- Открытость алгоритмов и механизмом защиты;
- Простота применения защитных мер и средств.

# Методы обеспечения ИБ

- Рассмотрим пример классификации методов, используемых для обеспечения информационной безопасности:
  - **препятствие** – метод физического преграждения пути злоумышленнику к информации;
  - **управление доступом** – метод защиты с помощью регулирования использования информационных ресурсов системы;
  - **маскировка** – метод защиты информации путем ее криптографического преобразования;
  - **регламентация** – метод защиты информации, создающий условия автоматизированной обработки, при которых возможности несанкционированного доступа сводится к минимуму;
  - **принуждение** – метод защиты, при котором персонал вынужден соблюдать правила обработки, передачи и использования информации;
  - **побуждение** – метод защиты, при котором пользователь побуждается не нарушать режимы обработки, передачи и использования информации за счет соблюдения этических и моральных норм.

# Средства защиты информационных систем

- Такие средства могут быть классифицированы по следующим признакам:
  - **технические средства** – различные электрические, электронные и компьютерные устройства;
  - **физические средства** – реализуются в виде автономных устройств и систем;
  - **программные средства** – программное обеспечение, предназначенное для выполнения функций защиты информации;
  - **криптографические средства** – математические алгоритмы, обеспечивающие преобразования данных для решения задач информационной безопасности;
  - **организационные средства** – совокупность организационно-технических и организационно-правовых мероприятий;
  - **морально-этические средства** – реализуются в виде норм, сложившихся по мере распространения ЭВМ и информационных технологий;
  - **законодательные средства** – совокупность законодательных актов, регламентирующих правила пользования ИС, обработку и передачу информации.

В наши дни одной из главных угроз информационной безопасности любой компании стали **инсайдеры** – остальные угрозы (хакеры, вирусы и т.п.) более-менее успешно нейтрализуются специализированным софтом и сотрудниками IT-отделов. Именно на совести инсайдеров большинство громких утечек конфиденциальной информации, зафиксированных по всему миру в последние годы. Чаще всего к инсайдерам относят:

- *сотрудников, сознательно работающих на конкурентов (нанятых или предварительно трудоустроенных ими);*
- *сотрудников, прямо или косвенно связанных с криминальными структурами;*
- *просто недобросовестных сотрудников, ставящих свои интересы заведомо выше интересов фирмы;*
- *сотрудников, обиженных на начальство и по этой причине скрытно вредящих, не получая от этого какой-либо выгоды.*

# Каналы утечки данных:

1. Мобильные накопители – 74%
2. Электронная почта – 58%
3. Интернет-пейджеры (IM) – 17%
4. Интернет (web-почта, форумы, блоги) – 26%
5. Принтеры – 18%
6. Фото-видео-устройства – 2%
7. Другие – 5%

Пусть вас не удивляют цифры, дающие в сумме более 100%: ни один инсайдер не пользуется единственным каналом передачи данных

# Мобильные угрозы

Во втором квартале 2014 года было обнаружено:

- 727 790 установочных пакетов;
- 65 118 новых мобильных вредоносных программ;
- 2 033 мобильных банковских троянцев.

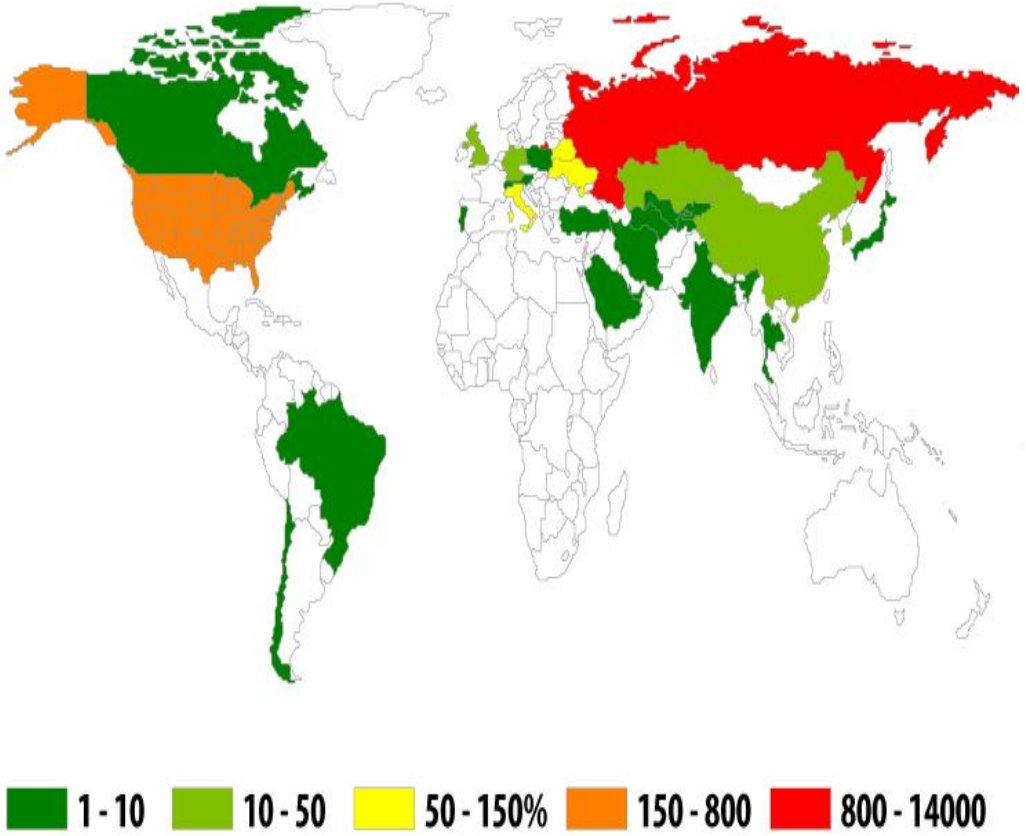
Суммарное количество обнаруженных мобильных вредоносных объектов в 1,7 раз меньше, чем в первом квартале.

Интерес к мобильным банковским троянцам обусловлен 2 факторами:

- интересом киберпреступников к «большим» деньгам;
- активным противодействием со стороны антивирусных компаний.

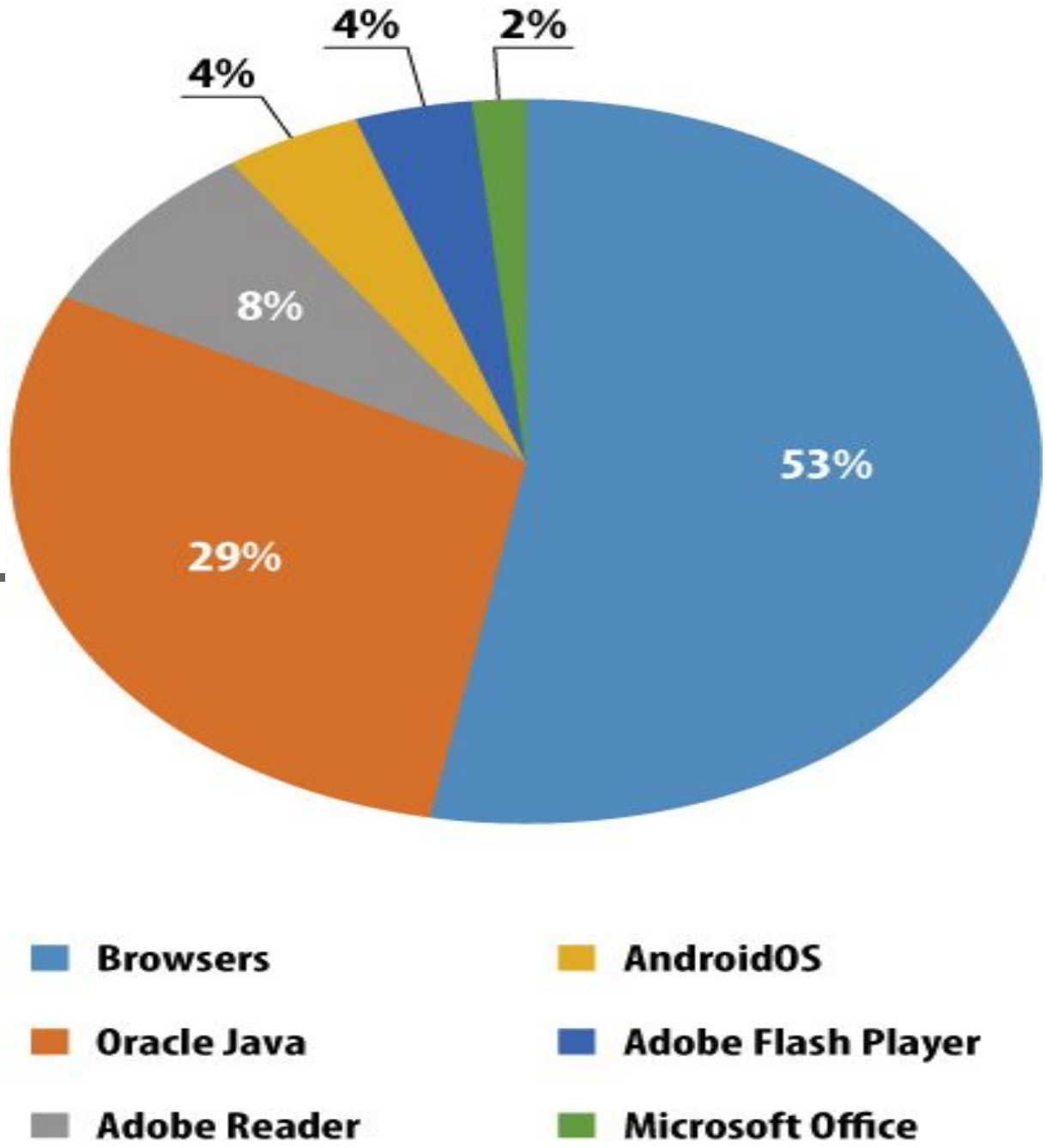
# Топ 10 стран,атакуемых банковскими троянцами 2кв. 2014:

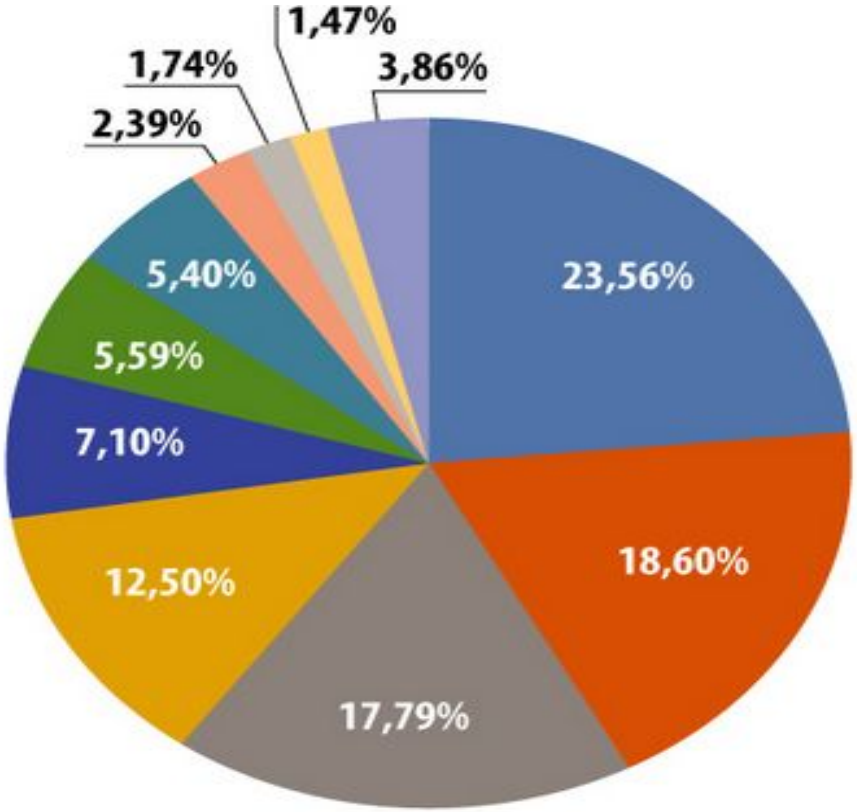
| | Страна | Количество атак | % от всех атак |
|---|---|---|---|
| 1 | Россия | 13800 | 91,7% |
| 2 | США | 792 | 5,3% |
| 3 | Украина | 136 | 0,9% |
| 4 | Италия | 83 | 0,6% |
| 5 | Белоруссия | 68 | 0,5% |
| 6 | Республика Корея | 30 | 0,2% |
| 7 | Казахстан | 25 | 0,2% |
| 8 | Китай | 19 | 0,1% |
| 9 | Великобритания | 17 | 0,1% |
| 10 | Германия | 12 | 0,1% |




На первом месте в этом рейтинге, как и ранее, Россия, а вот на второе место со значительным отрывом от остальных стран вышли США. Казахстан, который в первом квартале занимал в этом рейтинге второе место, во втором квартале оказался на седьмом.

Уязвимые приложения (статистика 2014)






# Распределение установленных у пользователей OS Windows по версиям

Степень риска заражения через Интернет по версии пользователей продуктов «Лаборатория Касперского». Полученные данные являются показателем агрессивности среды, в которой работают компьютеры в разных странах.

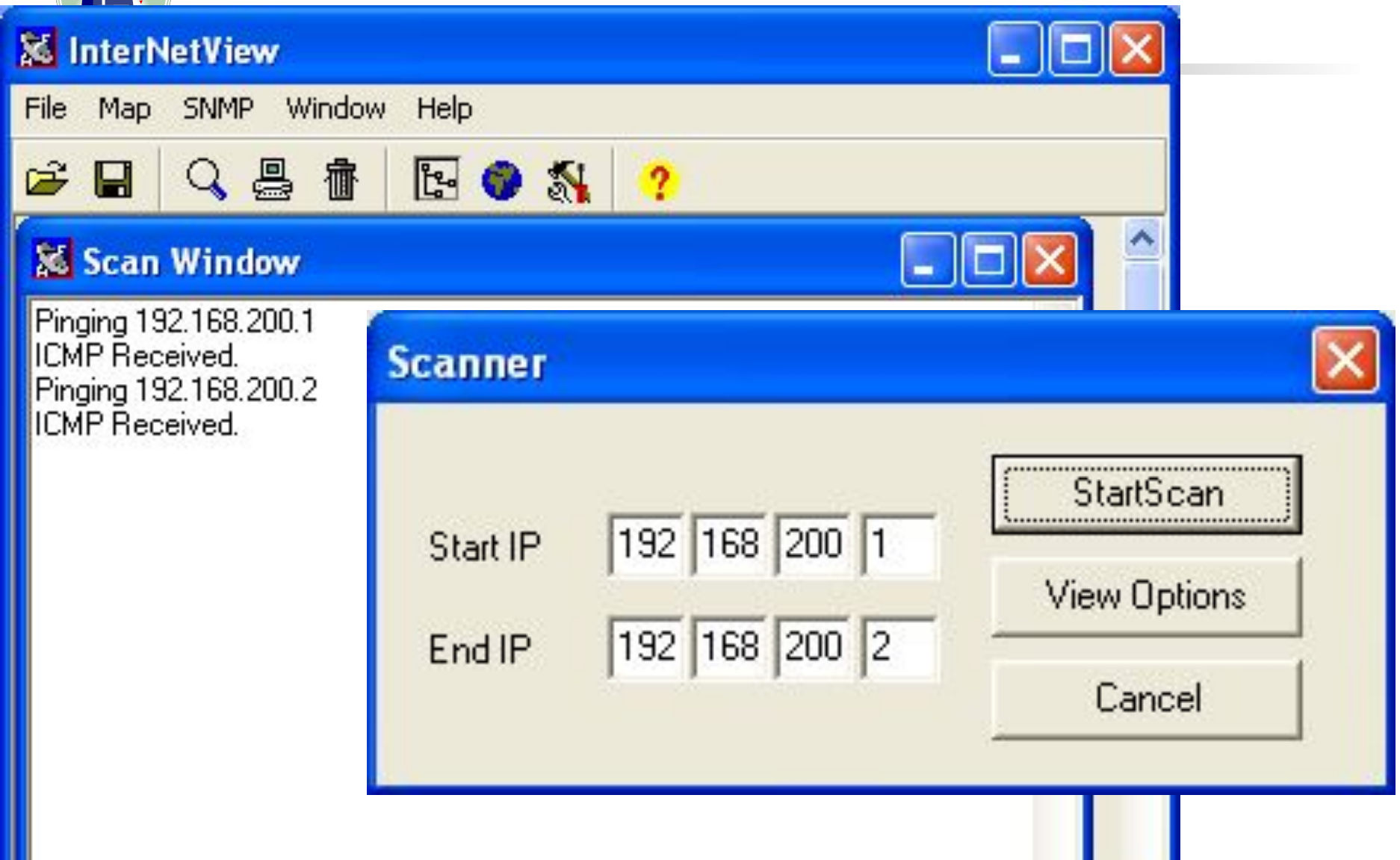
| | Страна | % уникальных пользователей |
|---|---|---|
| 1 | Россия | 46,53% |
| 2 | Казахстан | 45,35% |
| 3 | Армения | 42,26% |
| 4 | Украина | 41,11% |
| 5 | Азербайджан | 40,94% |
| 6 | Вьетнам | 39,59% |
| 7 | Белоруссия | 37,71% |
| 8 | Молдова | 36,65% |
| 9 | Монголия | 33,86% |
| 10 | Киргизия | 33,71% |

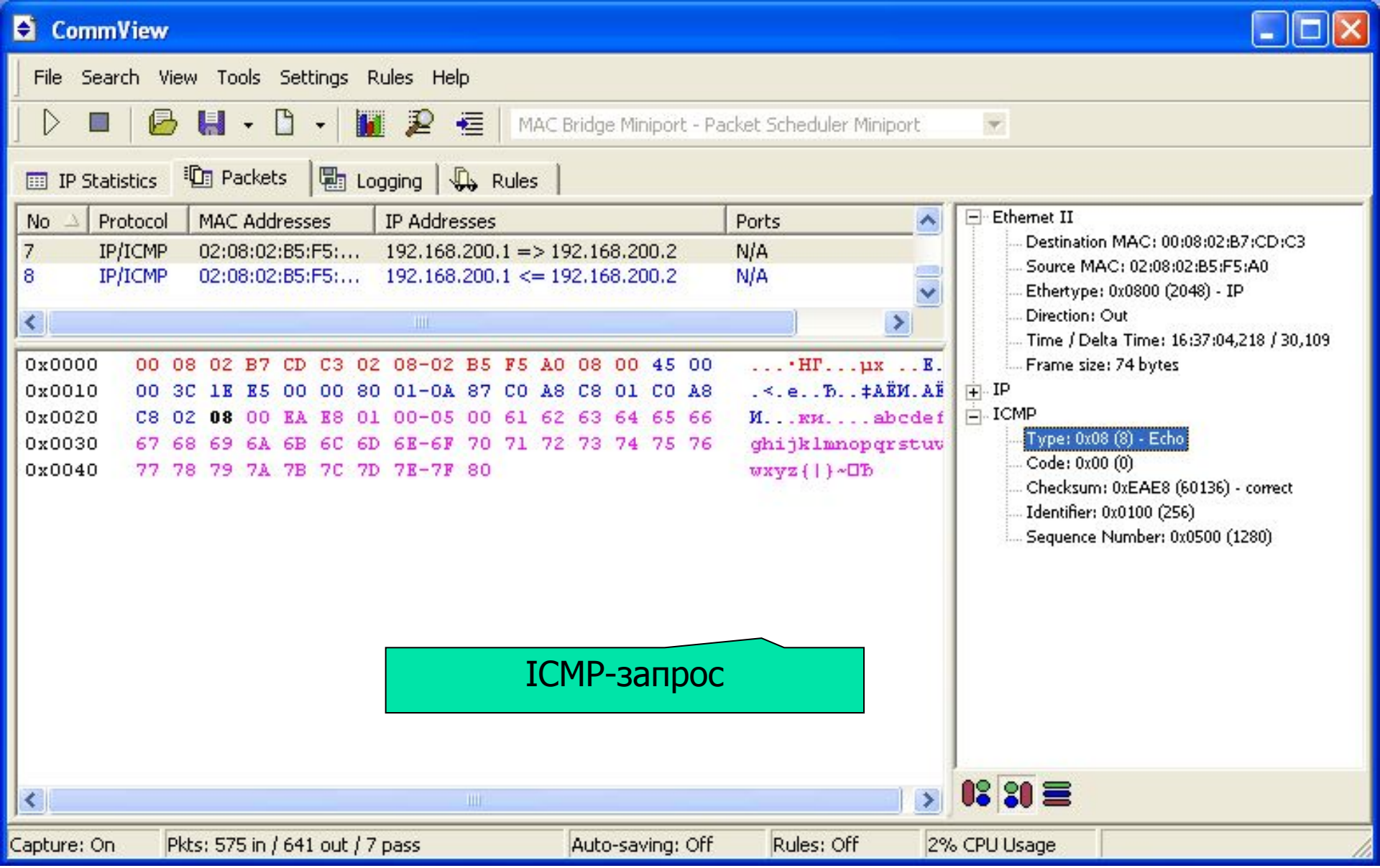
# ICMP-сканирование

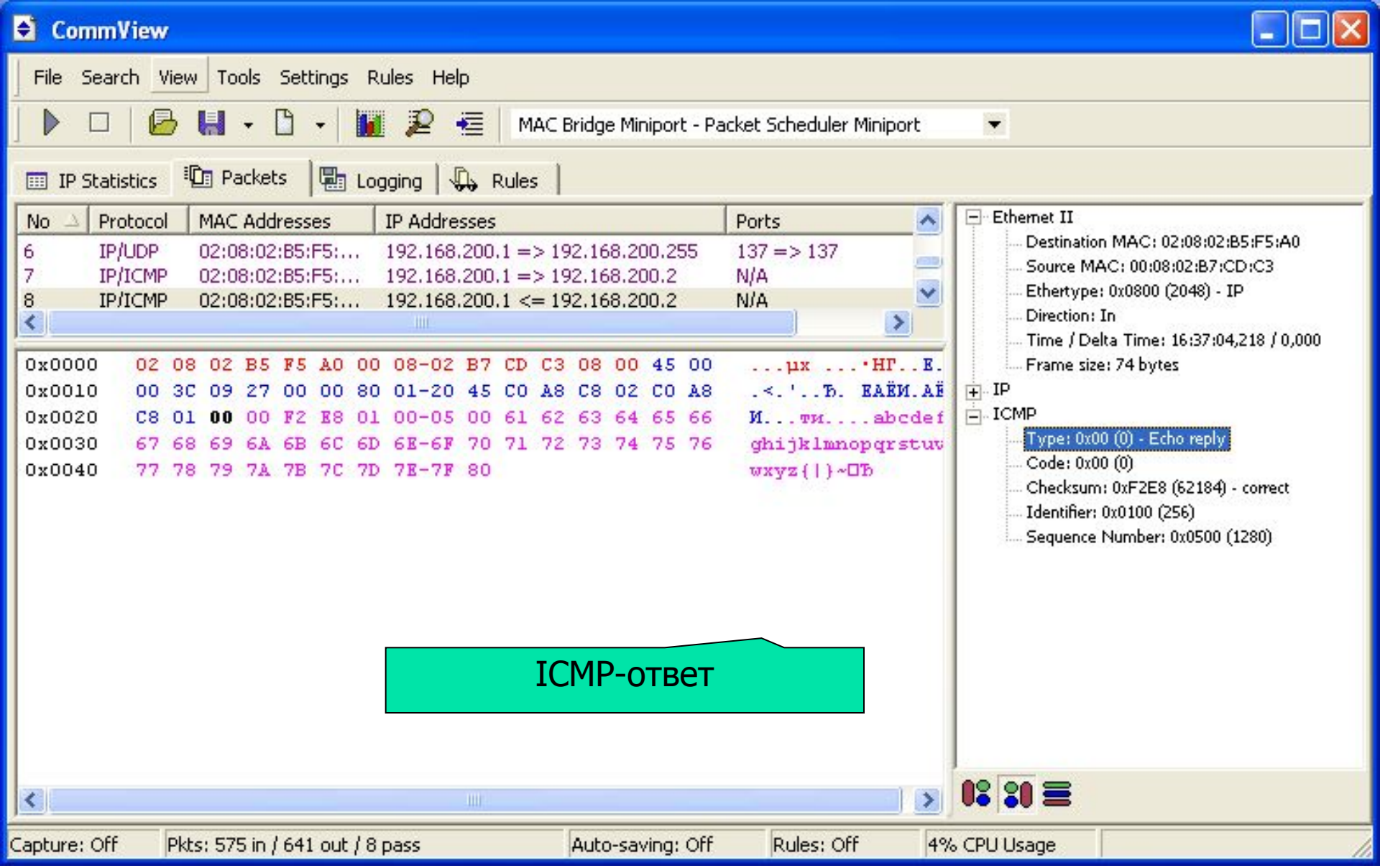
Сканер портов — программное средство, разработанное для поиска хостов сети, в которых открыты нужные порты. Эти программы обычно используются системными администраторами для проверки безопасности их сетей и злоумышленниками для взлома сети. Может производиться поиск как ряда открытых портов на одном хосте, так и одного определённого порта на многих хостах. Последнее характерно для деятельности ряда сетевых червей.

Сам процесс называется сканированием портов или (в случае, когда осуществляется проверка многих хостов) сканированием сети. Сканирование портов может являться первым шагом в процессе взлома или предупреждения взлома, помогая определить потенциальные цели атаки. С помощью соответствующего инструментария путем отправления пакетов данных и анализа ответов могут быть исследованы работающие на машине службы (Web-сервер, FTP-сервер, mail-сервер, и т. д.), установлены номера их версий и используемая операционная система.

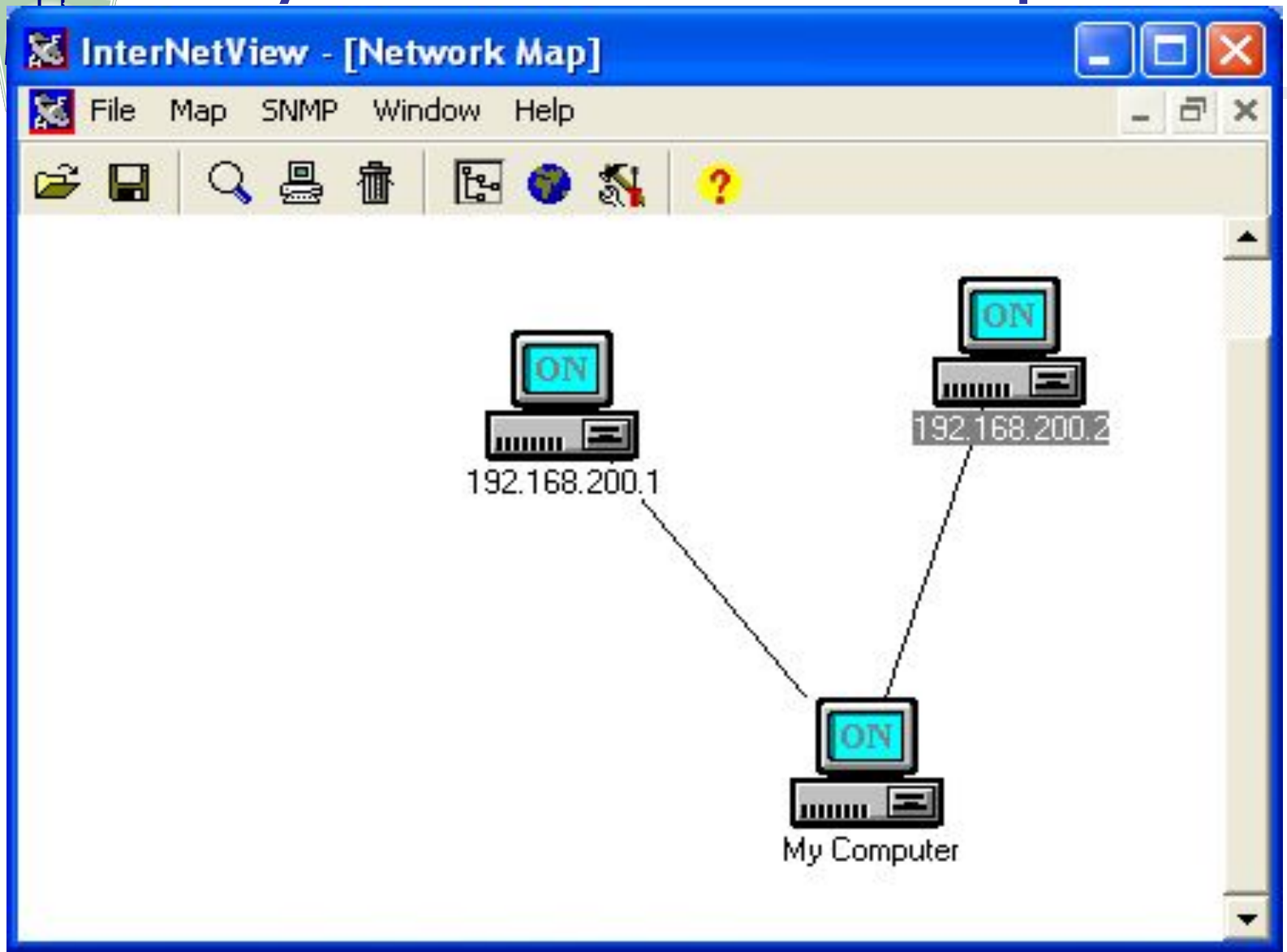
# ICMP-сканирование



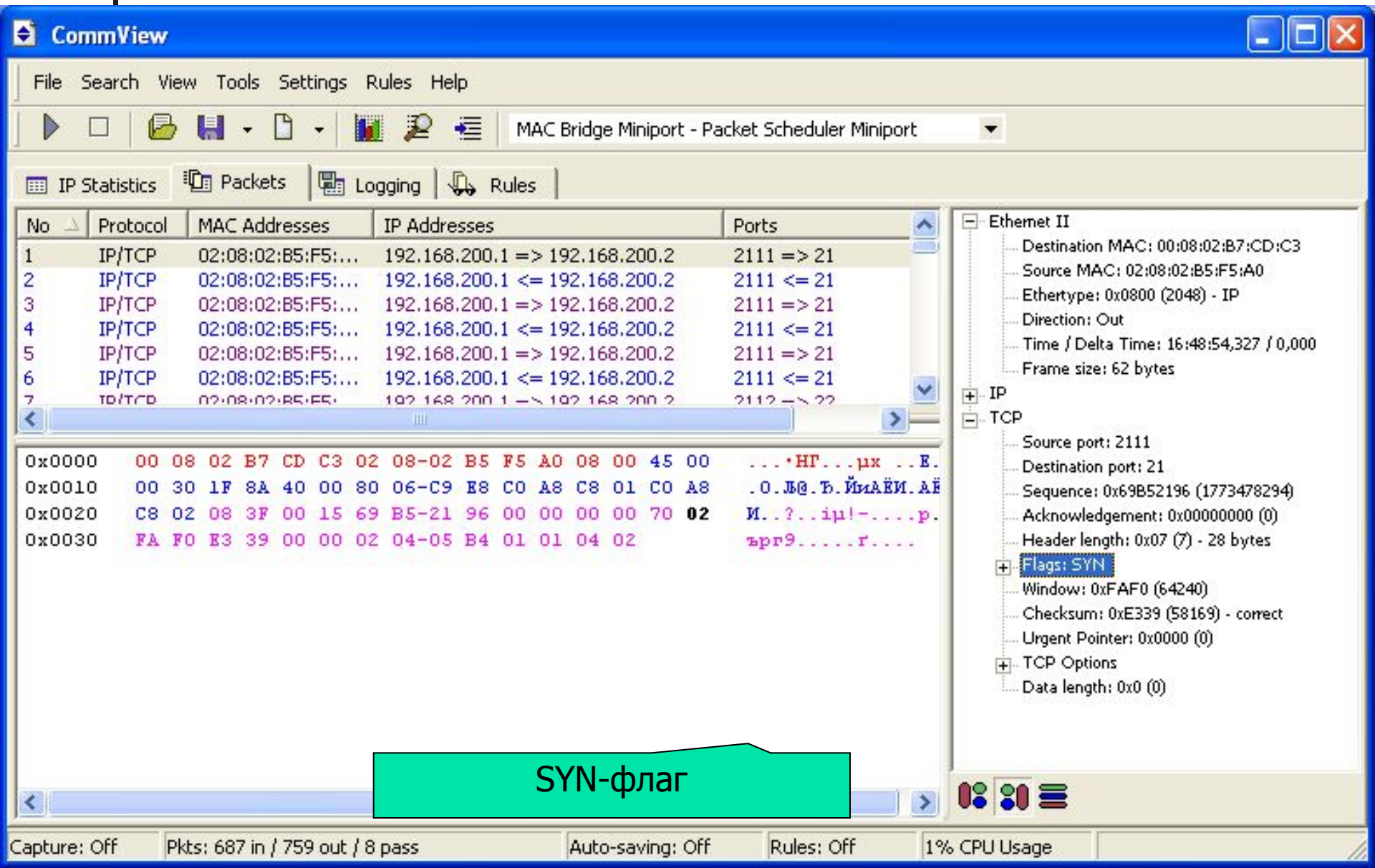

CommView
File Search View Tools Settings Rules Help
MAC Bridge Miniport - Packet Scheduler Miniport
IP Statistics
Packets
Logging
Rules
No Protocol MAC Addresses IP Addresses Ports
7 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.2 N/A
8 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 <= 192.168.200.2 N/A
0x0000 00 08 02 B7 CD C3 02 08-02 B5 F5 A0 08 00 45 00
0x0010 00 3C 1E E5 00 00 80 01-0A 87 C0 A8 C8 01 C0 A8
0x0020 C8 02 08 00 EA E8 01 00-05 00 61 62 63 64 65 66
0x0030 67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76
0x0040 77 78 79 7A 7B 7C 7D 7E-7F 80
Ethernet II
Destination MAC: 00:08:02:B7:CD:C3
Source MAC: 02:08:02:B5:F5:A0
Ethertype: 0x0800 (2048) - IP
Direction: Out
Time / Delta Time: 16:37:04,218 / 30,109
Frame size: 74 bytes
IP
ICMP
Type: 0x08 (8) - Echo
Code: 0x00 (0)
Checksum: 0xEAE8 (60136) - correct
Identifier: 0x0100 (256)
Sequence Number: 0x0500 (1280)
ICMP-запрос
Capture: On
Pkts: 575 in / 641 out / 7 pass
Auto-saving: Off
Rules: Off
2% CPU Usage


CommView
File Search View Tools Settings Rules Help
MAC Bridge Miniport - Packet Scheduler Miniport
IP Statistics Packets Logging Rules
No Protocol MAC Addresses IP Addresses Ports
6 IP/UDP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.255 137 => 137
7 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.2 N/A
8 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 <= 192.168.200.2 N/A
0x0000 02 08 02 B5 F5 A0 00 08-02 B7 CD C3 08 00 45 00
0x0010 00 3C 09 27 00 00 80 01-20 45 C0 A8 C8 02 C0 A8
0x0020 C8 01 00 00 F2 E8 01 00-05 00 61 62 63 64 65 66
0x0030 67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76
0x0040 77 78 79 7A 7B 7C 7D 7E-7F 80
Ethernet II
Destination MAC: 02:08:02:B5:F5:A0
Source MAC: 00:08:02:B7:CD:C3
Ethertype: 0x0800 (2048) - IP
Direction: In
Time / Delta Time: 16:37:04,218 / 0,000
Frame size: 74 bytes
IP
ICMP
Type: 0x00 (0) - Echo reply
Code: 0x00 (0)
Checksum: 0xF2E8 (62184) - correct
Identifier: 0x0100 (256)
Sequence Number: 0x0500 (1280)
ICMP-ответ
Capture: Off
Pkts: 575 in / 641 out / 8 pass
Auto-saving: Off
Rules: Off
4% CPU Usage

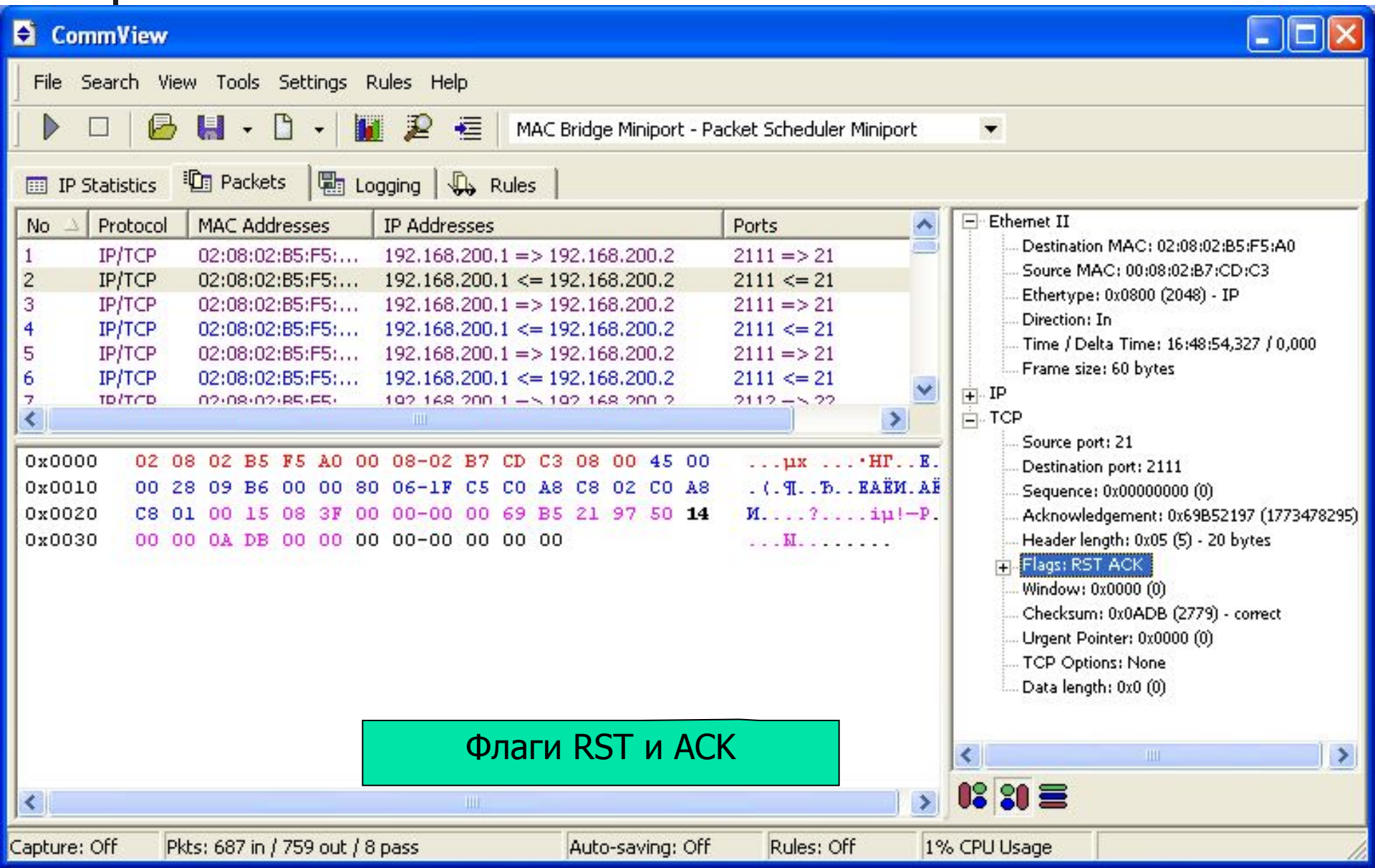
# Результат ICMP-сканирования



# TCP-сканирование

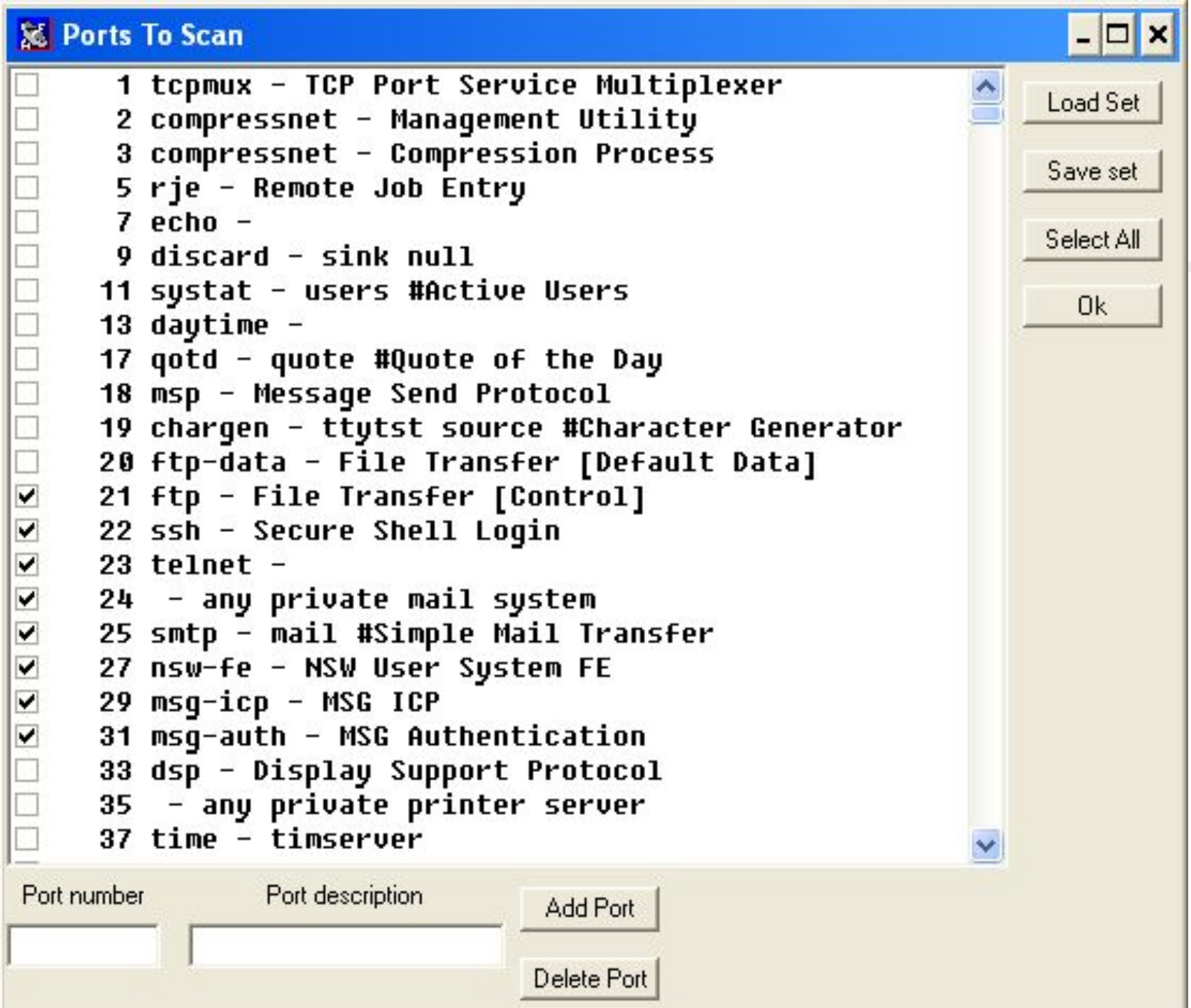


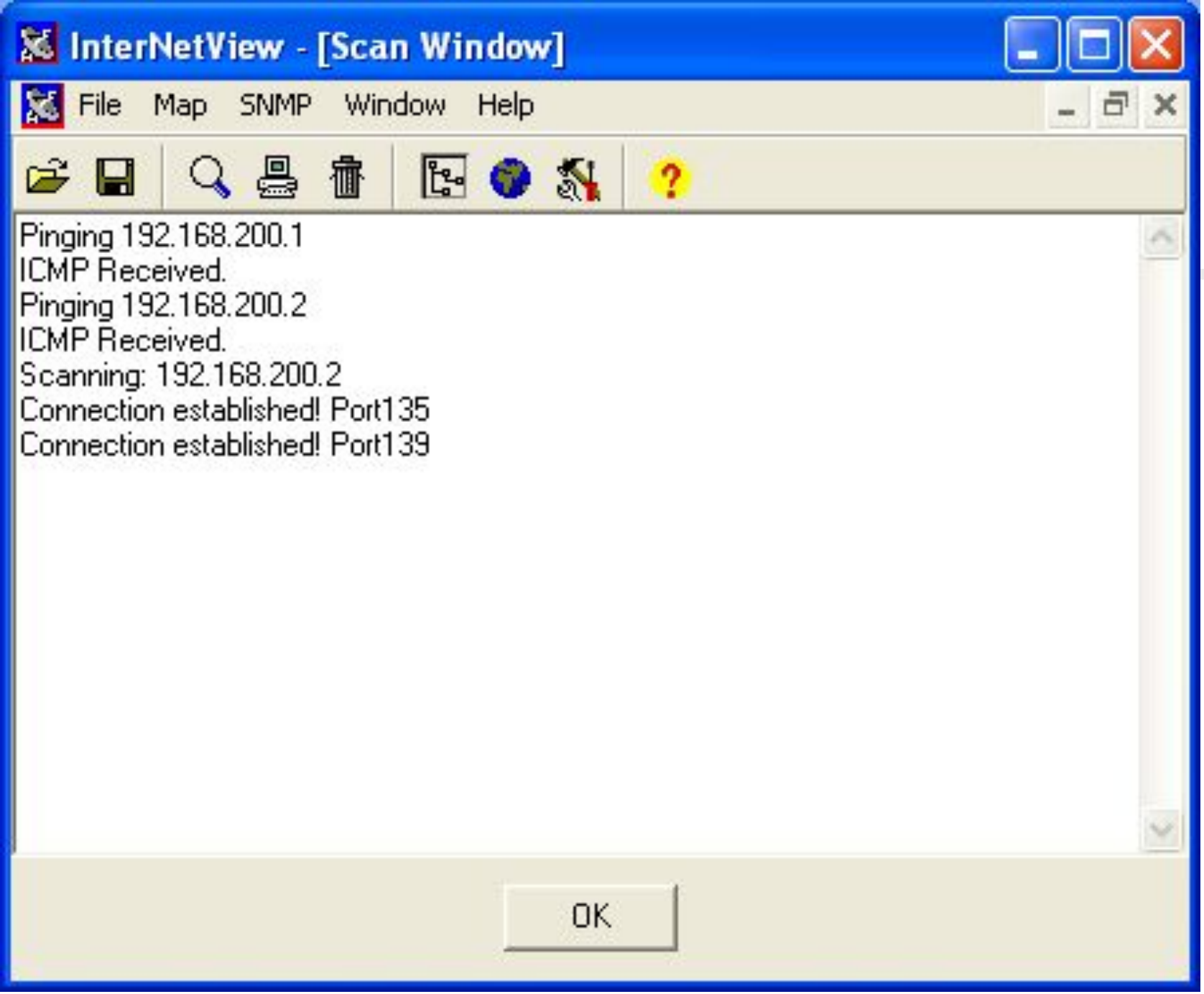
# Искомый узел присутствует



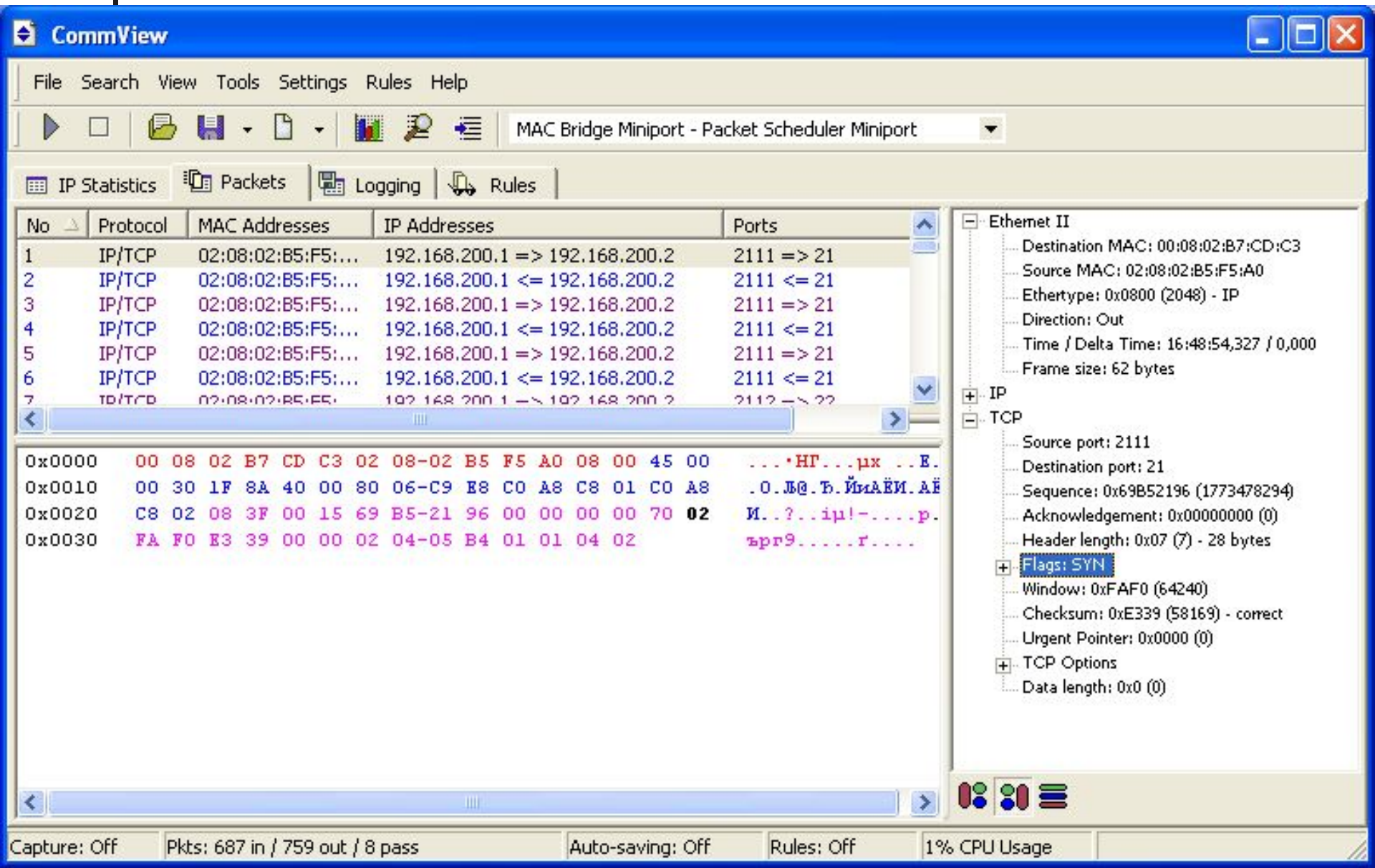
# Сканирование портов

- Определение функционирующих сетевых служб
  - TCP-21- ftp
  - TCP- 23- telnet
  - TCP- 25- smtp
  - TCP- 80- http
  - TCP- 110- pop3
  - TCP- 135- RPC
  - TCP- 139- NetBIOS
  - TCP- 445- RPC, DFS

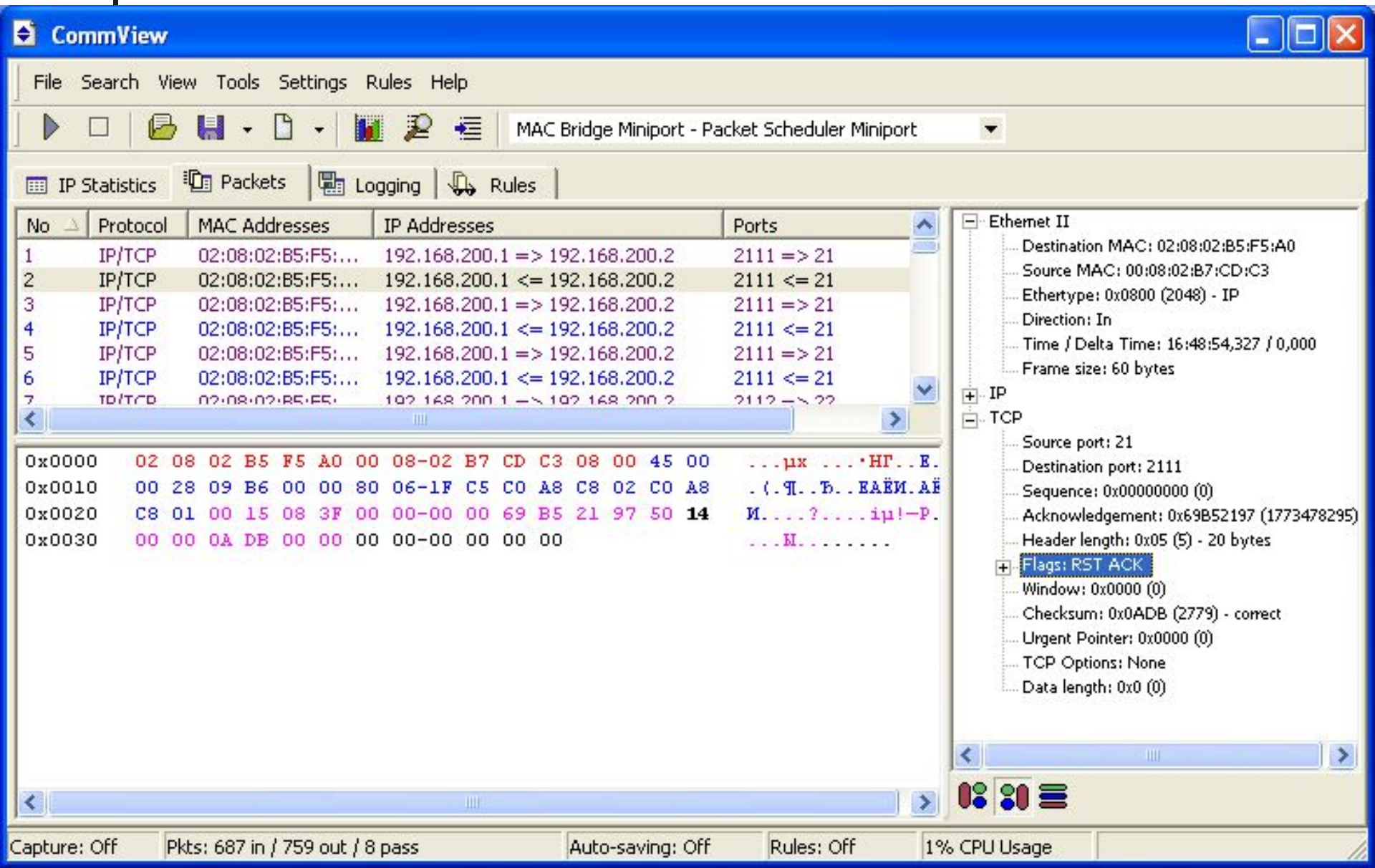

Ports To Scan
1 tcpmux - TCP Port Service Multiplexer
2 compressnet - Management Utility
3 compressnet - Compression Process
5 rje - Remote Job Entry
7 echo -
9 discard - sink null
11 systat - users #Active Users
13 daytime -
17 qotd - quote #Quote of the Day
18 msp - Message Send Protocol
19 chargen - ttytst source #Character Generator
20 ftp-data - File Transfer [Default Data]
21 ftp - File Transfer [Control]
22 ssh - Secure Shell Login
23 telnet -
24 - any private mail system
25 smtp - mail #Simple Mail Transfer
27 nsw-fe - NSW User System FE
29 msg-icp - MSG ICP
31 msg-auth - MSG Authentication
33 dsp - Display Support Protocol
35 - any private printer server
37 time - timserver
Load Set
Save set
Select All
Ok
Port number
Port description
Add Port
Delete Port


InterNetView - [Scan Window]
File
Map
SNMP
Window
Help
Pinging 192.168.200.1
ICMP Received.
Pinging 192.168.200.2
ICMP Received.
Scanning: 192.168.200.2
Connection established! Port135
Connection established! Port139
OK

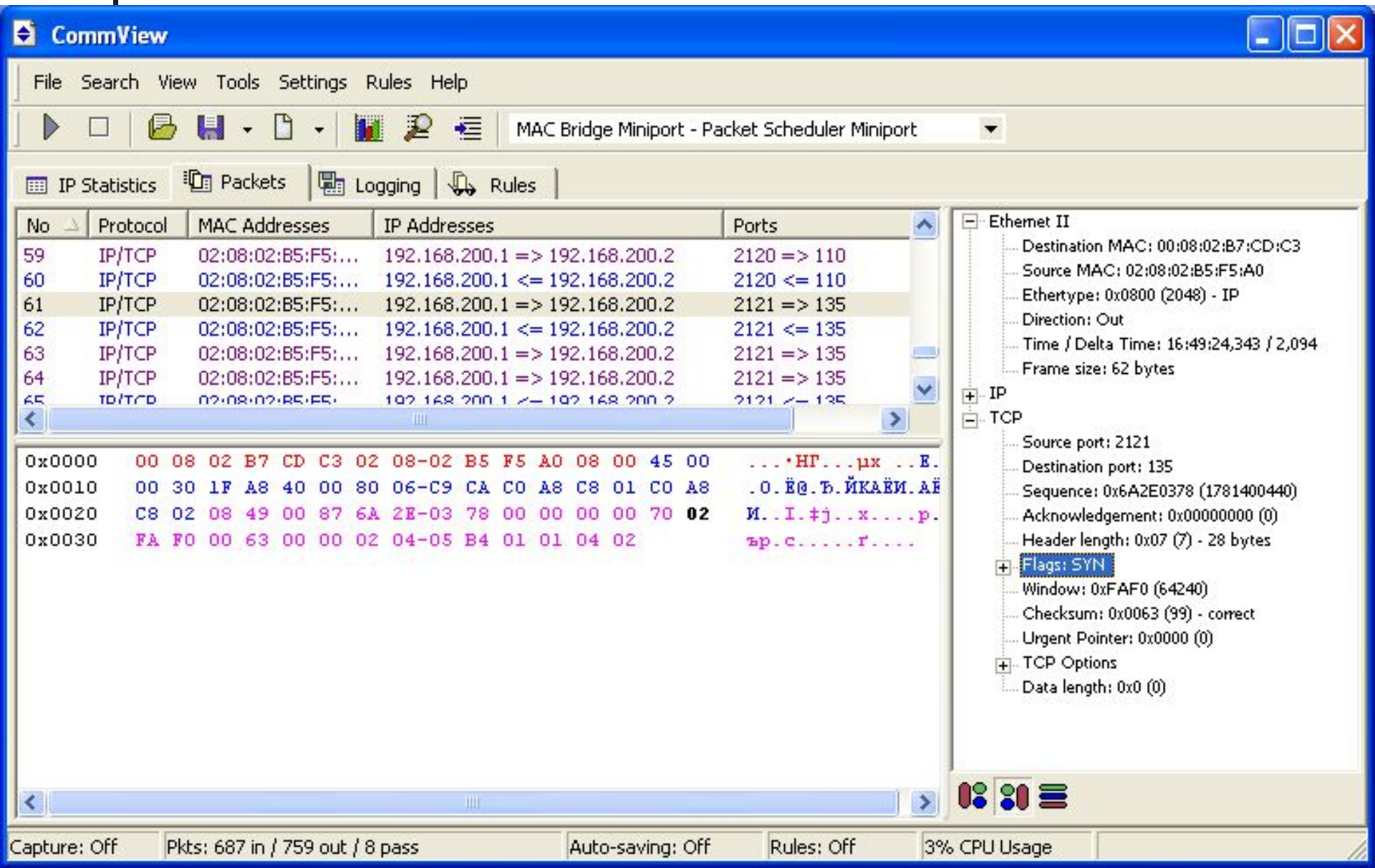
# Connect()-сканирование, порт 21



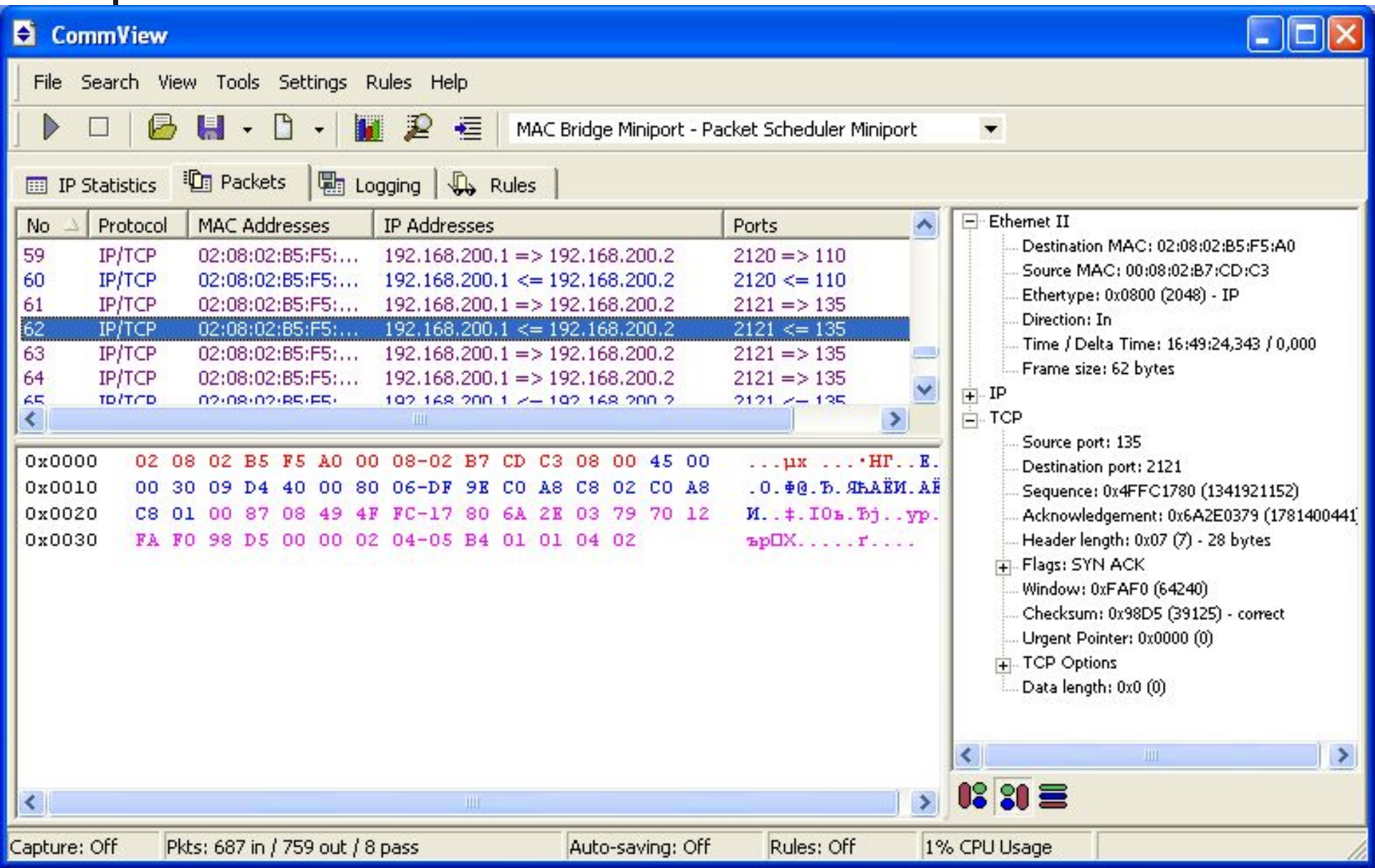
# Ответ - «закрытый порт»



# Connect()-сканирование, порт 135

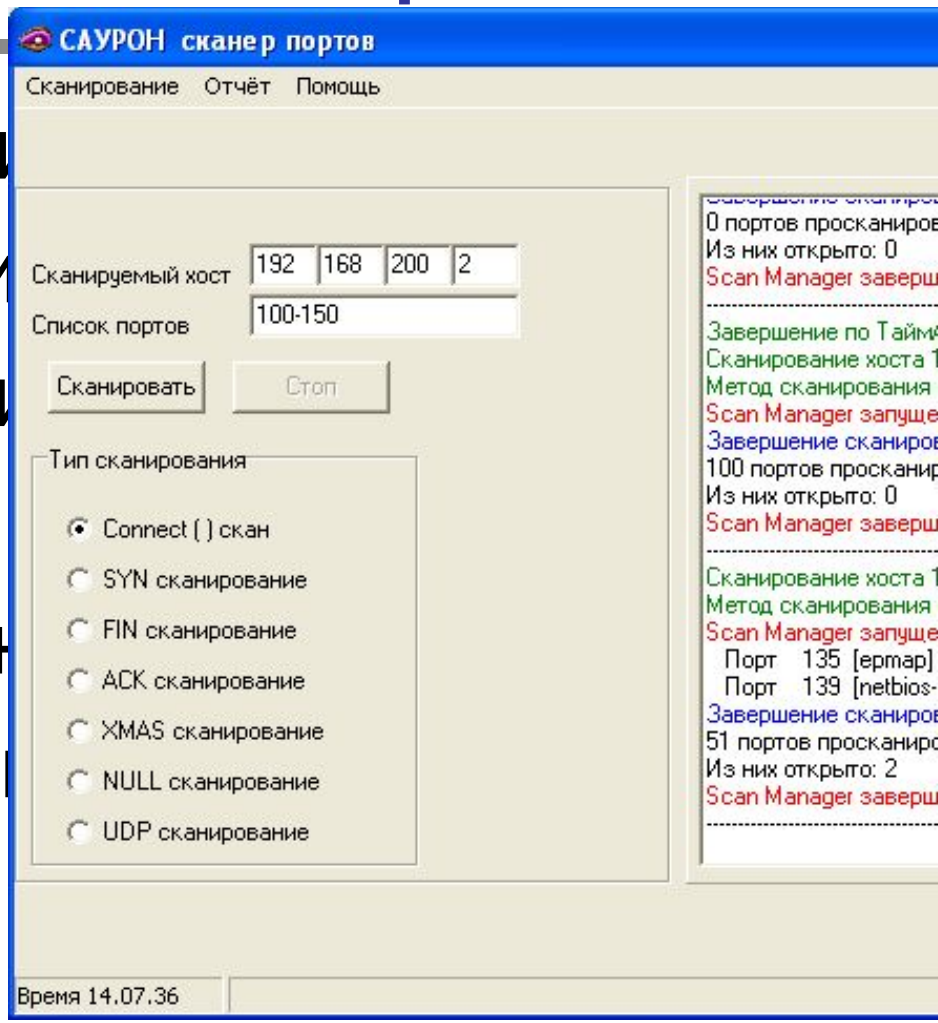


# Ответ - «открытый порт»

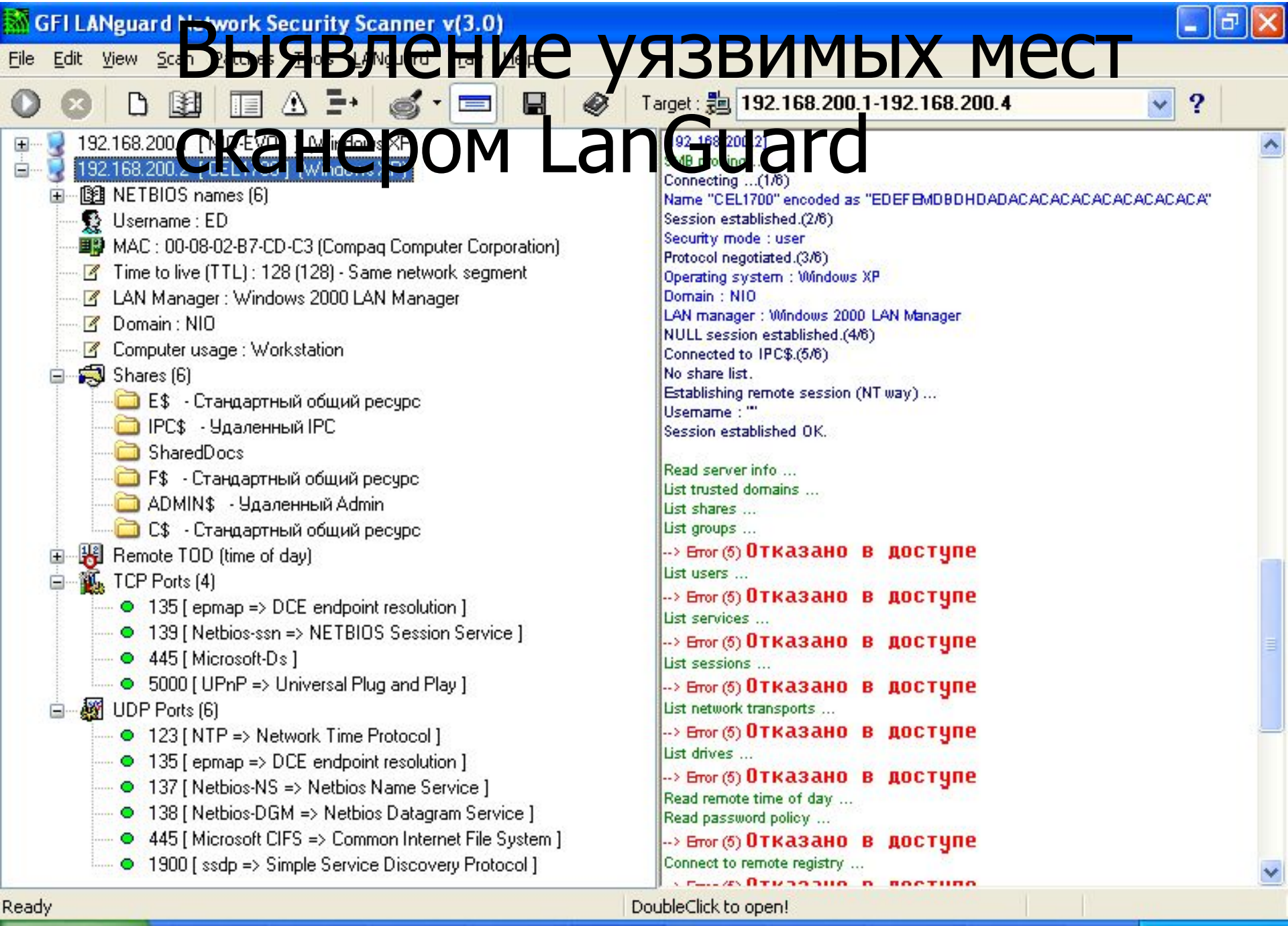


# Иные способы сканирования

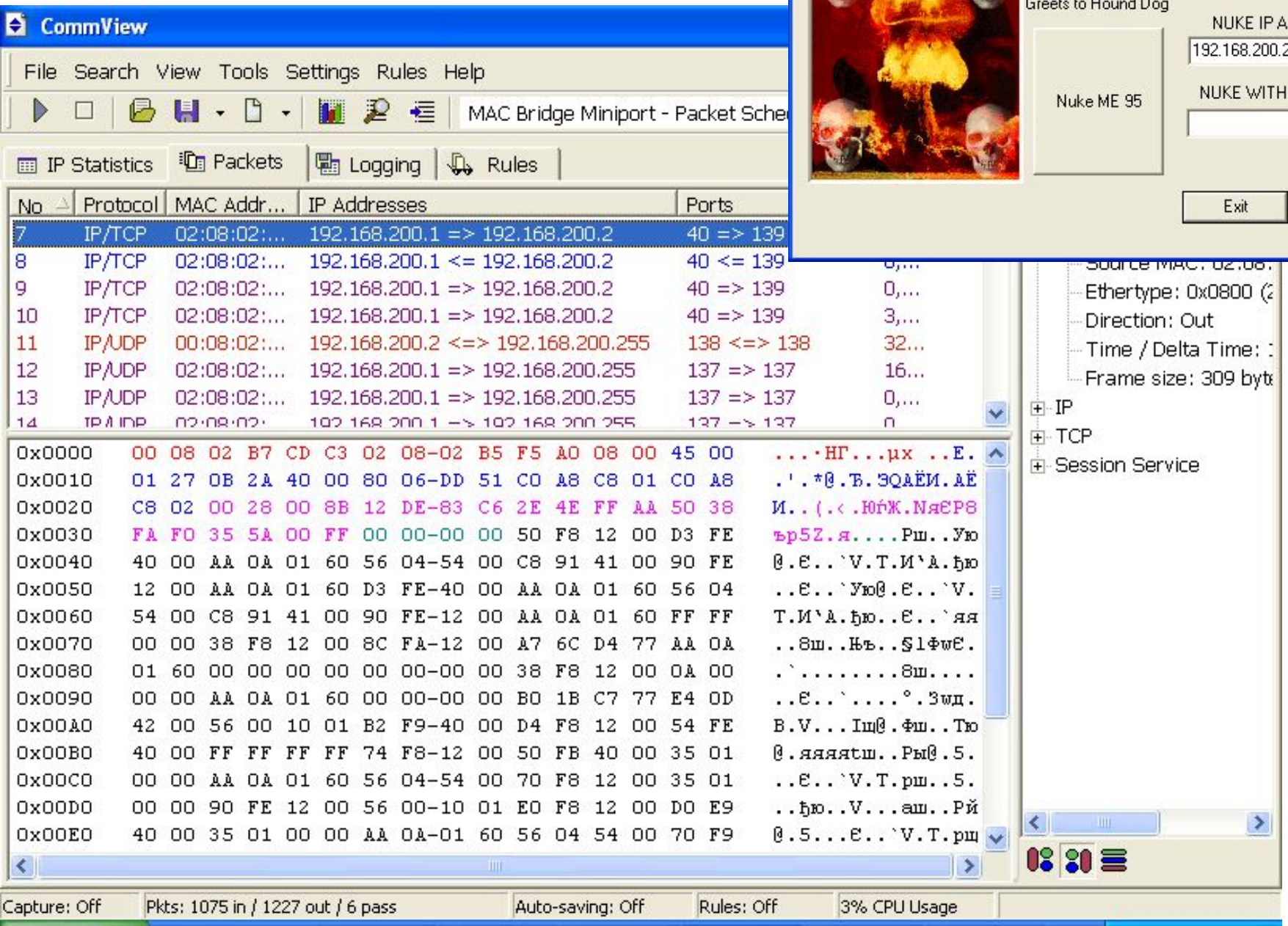
- SYN-сканирование
- FIN-сканирование
- ACK-сканирование
- XMAS-сканирование
- NULL-сканирование
- UDP-сканирование



# Выявление уязвимых мест сканером LanGuard



# Реализации атак



# Реализации атак

- Анонимное подключение в ОС Windows

**net use *.*.*.*\IPC$ "" /user:""**

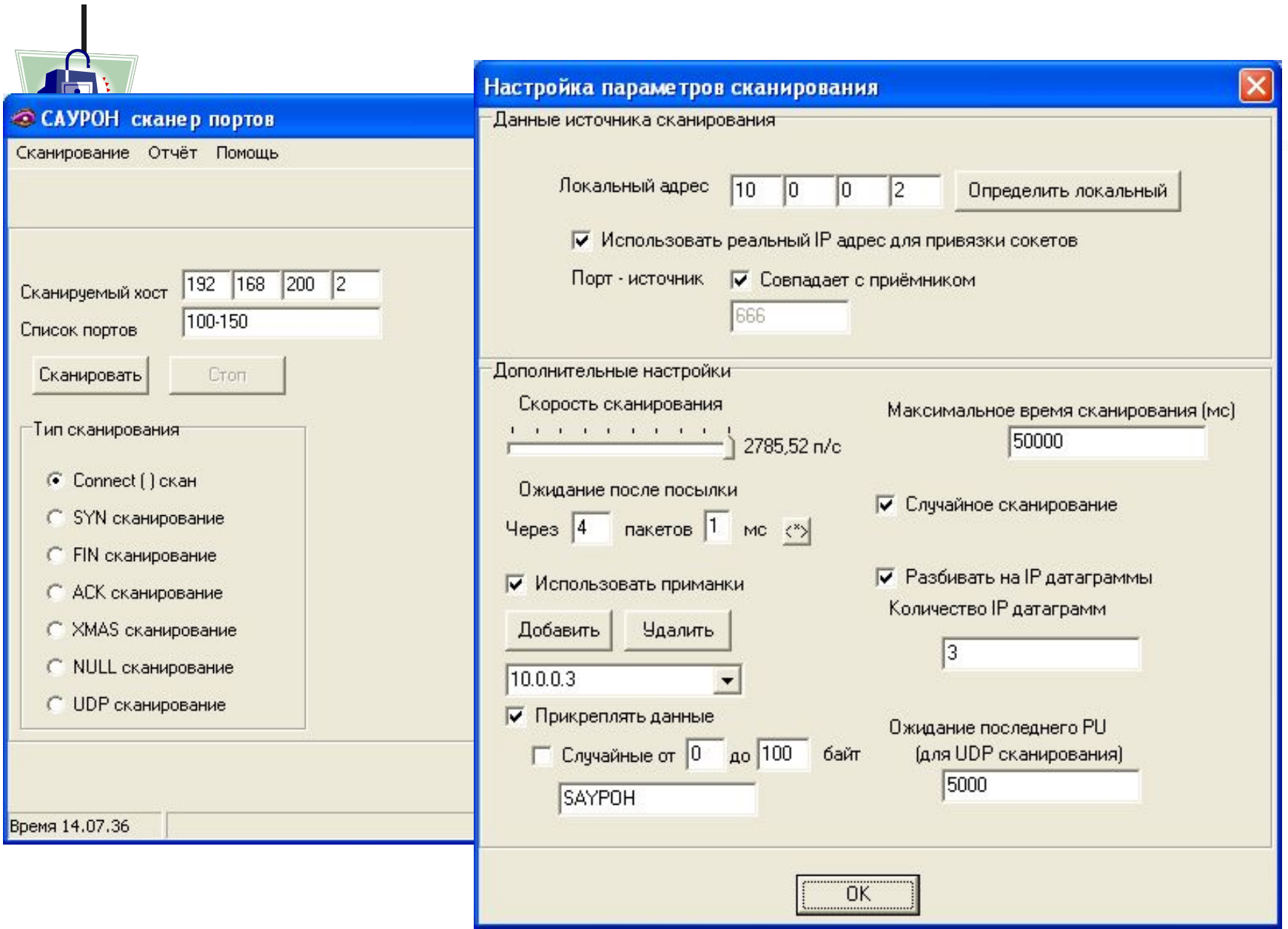
# Общие принципы защиты

- Обнаружение и запрет:
  - входящих ICMP-запросов
  - исходящих ICMP-ответов
  - установки TCP-соединений извне
  - опасных TCP- и UDP-портов

# Усложненные атаки

- последовательность опроса узлов
- 07:11:38.123565 200.0.0.200 > 200.0.0.**34**: icmp: echo request
  07:11:51.456342 200.0.0.200 > 200.0.0.**47**: icmp: echo request
  07:11:04.678432 200.0.0.200 > 200.0.0.**3**: icmp: echo request
  07:12:18.985667 200.0.0.200 > 200.0.0.**12**: icmp: echo request
  07:12:31.024657 200.0.0.200 > 200.0.0.**11**: icmp: echo request
  07:12:44.044567 200.0.0.200 > 200.0.0.**9**: icmp: echo request
  07:12:57.071234 200.0.0.200 > 200.0.0.**104**: icmp: echo request
  ....
- увеличение интервала времени
- 12:01:38.234455 200.0.0.200 > 200.0.0.**67**: icmp: echo request
  12:03:51.543524 200.0.0.200 > 200.0.0.**87**: icmp: echo request
  12:05:04.655342 200.0.0.200 > 200.0.0.**134**: icmp: echo request
  12:07:18.573256 200.0.0.200 > 200.0.0.**23**: icmp: echo request
  12:09:31.676899 200.0.0.200 > 200.0.0.**11**: icmp: echo request
  12:11:44.896754 200.0.0.200 > 200.0.0.**104**: icmp: echo request
  12:13:57.075356 200.0.0.200 > 200.0.0.**2**: icmp: echo request

# Усложненные атаки



# Основные механизмы защиты компьютерных систем

1. идентификация (именование и опознавание), аутентификация (подтверждение подлинности) пользователей системы;
2. разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
3. регистрация и оперативное оповещение о событиях, происходящих в системе (аудит);
4. криптографическое закрытие хранимых и передаваемых по каналам связи данных;
5. контроль целостности и аутентичности (подлинности и авторства) данных;
6. выявление и нейтрализация действий компьютерных вирусов;
7. затирание остаточной информации на носителях;

# Основные механизмы защиты компьютерных систем

8. выявление уязвимостей (слабых мест) системы;
9. изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы и т.д.);
1. обнаружение атак и оперативное реагирование;
2. резервное копирование;
3. маскировка.

Механизмы защиты могут применяться в различных комбинациях и вариациях. Наибольший эффект достигается при их системном использовании в комплексе с другими видами мер защиты.

# Идентификация и аутентификация пользователей

**Идентификация** - это, с одной стороны, присвоение индивидуальных имен, номеров или специальных устройств (идентификаторов) субъектам и объектам системы, а, с другой стороны, - это их распознавание (опознавание) по присвоенным им уникальным идентификаторам.

Наличие идентификатора позволяет упростить процедуру выделения конкретного субъекта (определенный объект) из множества однотипных субъектов (объектов). Чаще всего в качестве идентификаторов применяются номера или условные обозначения в виде набора символов.

# Идентификация и аутентификация пользователей

**Аутентификация** - это проверка (подтверждение) подлинности идентификации субъекта или объекта системы. Цель аутентификации субъекта - убедиться в том, что субъект является именно тем, кем представился (идентифицировался). Цель аутентификации объекта - убедиться, что это именно тот объект, который нужен.

Аутентификация пользователей осуществляется обычно:

- путем проверки знания ими паролей (специальных секретных последовательностей символов),
- путем проверки владения ими какими-либо специальными устройствами (карточками, ключевыми вставками и т.п.) с уникальными признаками или
- путем проверки уникальных физических характеристик и параметров (отпечатков пальцев, особенностей радужной оболочки глаз, формы кисти рук и т.п.) самих пользователей при помощи специальных биометрических устройств.

# Идентификация и аутентификация пользователей

Ввод значений пользователем идентификатора и пароля осуществляется с клавиатуры. Однако многие СЗИ используют и другие типы идентификаторов - магнитные карточки, радиочастотные бесконтактные (proximity) карточки, интеллектуальные (smart) карточки, электронные таблетки Touch Memory. Биометрические методы характеризуется, с одной стороны, высоким уровнем достоверности опознавания пользователей, а с другой - возможностью ошибок распознавания первого и второго рода (пропуск или ложная тревога) и более высокой стоимостью реализующих их систем. Идентификация и аутентификация пользователей должна производиться при каждом их входе в систему и при возобновлении работы после кратковременного перерыва (после периода неактивности без выхода из системы или выключения компьютера).

# Электронно-цифровая подпись (ЭЦП)

ЭЦП - реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий установить отсутствие искажения информации в электронном документе с момента формирования подписи и проверить принадлежность подписи владельцу сертификата ключа подписи. Предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

# Электронно-цифровая подпись (ЭЦП)

Использование позволяет осуществить:

- Контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.
- Защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.
- Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он известен только владельцу, он не может отказаться от своей подписи под документом.
- Доказательное подтверждение авторства документа.

# Электронно-цифровая подпись (ЭЦП)

Существует несколько схем построения цифровой подписи:

- На основе алгоритмов симметричного шифрования. Предусматривает наличие в системе третьего лица - арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.
- На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем, что обусловлено разнообразием задач, решаемых с помощью ЭП.

# www.e-gov.kz

Электронное правительство - система электронного документооборота государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны и служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества. Создание электронного правительства предполагает построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки.

# www.e-gov.kz

Задачи электронного правительства:

- оптимизация предоставления правительственных услуг населению и бизнесу;
- поддержка и расширение возможностей самообслуживания граждан;
- рост технологической осведомленности и квалификации граждан;
- повышение степени участия всех избирателей в процессах руководства и управления страной;

снижение воздействия фактора географического местоположения.

# www.e-gov.kz

Электронное правительство обеспечивает:

- эффективное и менее затратное администрирование;
- кардинальное изменение взаимоотношений между обществом и правительством;
- совершенствование демократии и повышение ответственности власти перед народом.

# КАК пользоваться порталом www.e-gov.kz

РОЛИК

/home/skazka/Desktop/пРедмеТы мои/Информатика 2014/Лекции по Информатике/Лекция №13.egov.kz.mp4