# Watch_dogs
# 用户行为分析系统

小组成员：
李冉、张驰名、宫文

# CONTENTS


01 需求分析

02 系统设计流程

03 项目展示

04 行为分析可视化

05 总结

# 1

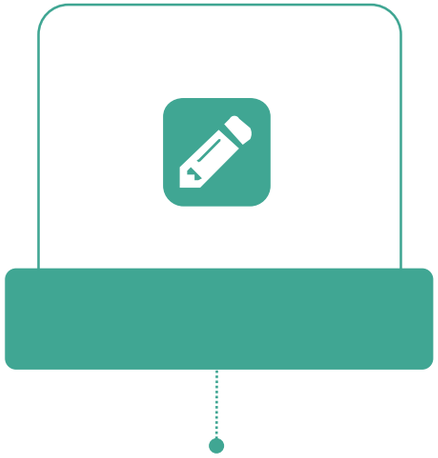
# 需求分析

demand analysis

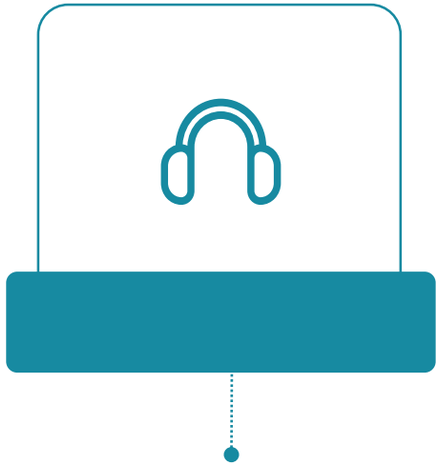
# 需求分析

demand analysis

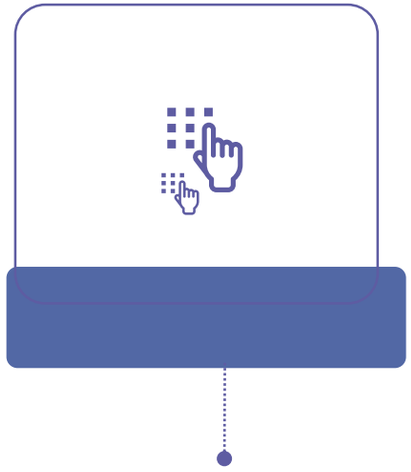




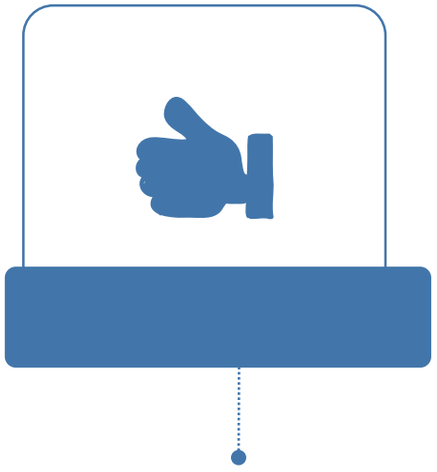
- 用户行为检测
- 流量监控



- QQ登记监测
- 用户影音娱乐监测



- 规则匹配
- 自定义规则添加
- 查询筛选



- 用户行为
  可视化呈现

# 2

# 系统设计流程

SOPC

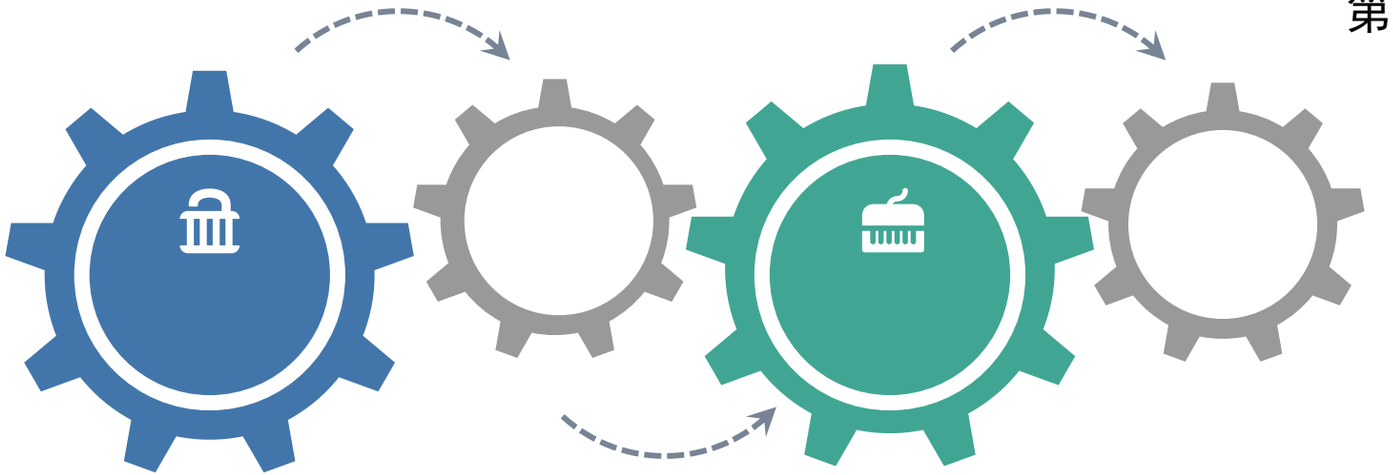
# 计划安排

ANNUAL WORK SUMMARY



1 选择代码同步工具
2 选择代码托管平台

3 确定所要实现的架构
4 选取合适的编程语言
5 寻找能够达到设计目标的第三方库来减少开发周期



6 配置开发环境
7 代码与UI设计分工
8 制定命名规范

9 数据库设计
10 制定周会与讨论计划
11 开始编码

# 系统设计流程

CLICK TO ADD CAPTION TEXT

LOGO

Git是一个开源的分布式版本控制系统，可以有效、高速的处理项目版本管理。


考虑到本系统并不是什么保密项目，并且准备开源，所以选择使用Git.


SVN

Git和svn都是非常好的版本控制工具

一开始选择了B/S架构去实现，但是由于我们之前找到的那个第三方库是google code上的一个小众产品，也没有API，只能看源码，学习成本和时间不划算，所以就中途放弃了。

## B/S

## C/S

考虑到一些技术以及种种原因导致时间问题，就选择了易于实现的C/S架构。

## 开发环配置

1. 安装visual studio2017
2. 安装sharppacp库
3. 安装winpcap驱动
4. 配置git
5. Github配置秘钥
6. 测试同步

## 第三方库选择

- Sharppcap
- PacketDotNet

1. 使用sharppcap库抓取数据
2. 通过PacketDotNet来解析数据

# 数据库设计

DBD Database Design



数据库采用Mysql数据库，
用来存储、匹配、分类抓取的信息

## 用户行为表

| 名 | 类型 | 长度 | 小数点 | 不是 null | |
|---|---|---|---|---|---|
| id | int | 11 | 0 | ☑ | 1 |
| sender | varchar | 32 | 0 | ☐ | |
| receiver | varchar | 32 | 0 | ☐ | |
| reason | varchar | 100 | 0 | ☐ | |
| detailreason | varchar | 100 | 0 | ☐ | |
| time | varchar | 30 | 0 | ☐ | |

## 信息总表

| 名 | 类型 | 长度 | 小数点 | 不是 null | |
|---|---|---|---|---|---|
| id | int | 11 | 0 | ☑ | 1 |
| data_id | int | 11 | 0 | ☐ | |
| length | varchar | 1000 | 0 | ☐ | |
| protocol | varchar | 32 | 0 | ☐ | |
| sourceAddress | varchar | 100 | 0 | ☐ | |
| time | datetime | 0 | 0 | ☐ | |
| data | varchar | 1000 | 0 | ☐ | |
| destinationAddress | varchar | 100 | 0 | ☐ | |

## QQ上下线表

| 名 | 类型 | 长度 | 小数点 | 不是 null | |
|---|---|---|---|---|---|
| id | int | 11 | 0 | ☑ | 1 |
| qqnum | varchar | 20 | 0 | ☐ | |
| qqIP | varchar | 30 | 0 | ☐ | |
| qqLogin | varchar | 100 | 0 | ☐ | |
| time | datetime | 0 | 0 | ☐ | |

3

# 项目展示

project display

# 实现



程序主界面

网卡选择

实时流量图

抓取数据显示

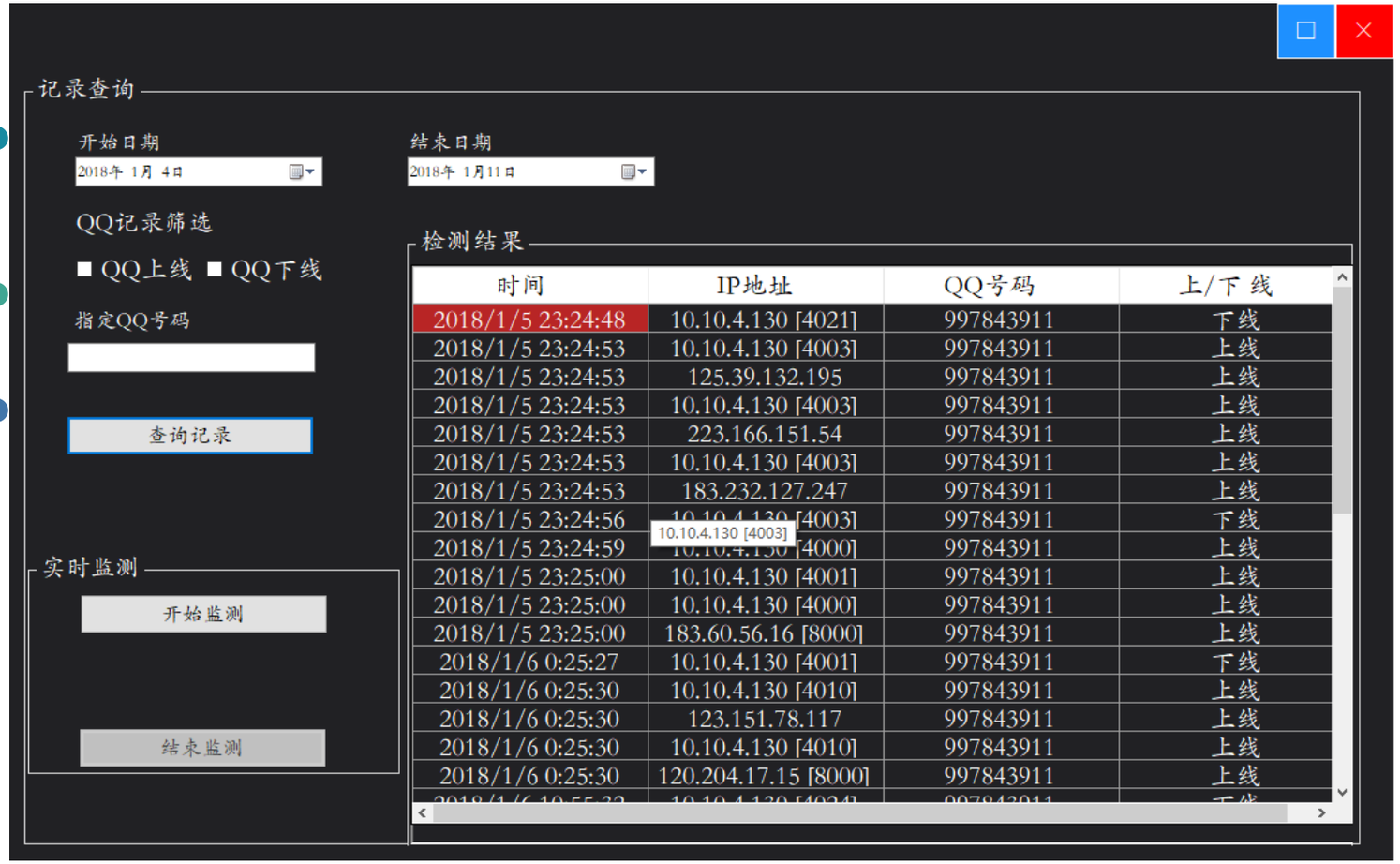
用户行为显示

# 实现



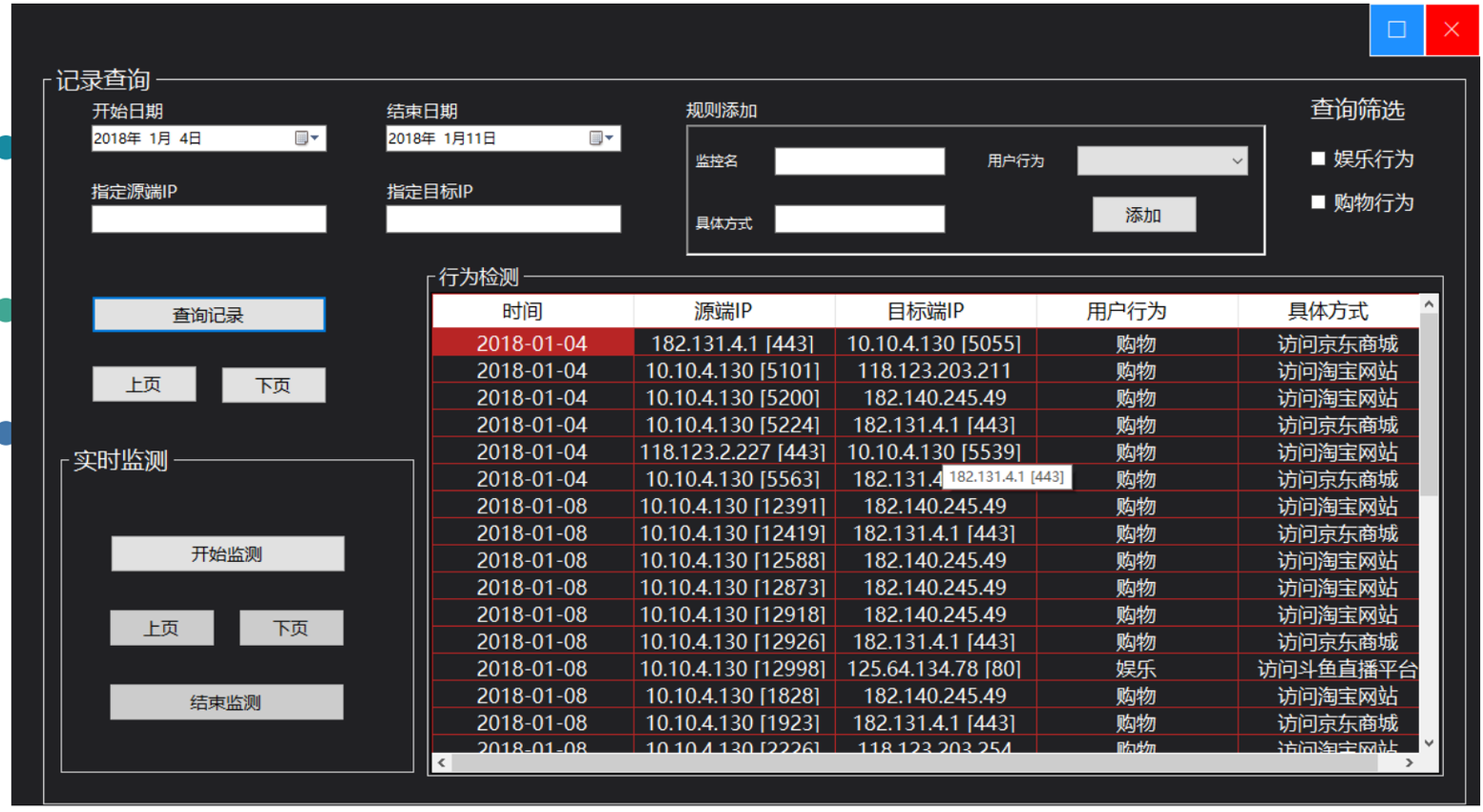
## QQ实时监控界面

- 时间段选取
- 记录筛选
- 指定查询
- 实时监测



## 用户行为实时监控界面

- 时间段选取
- 查询筛选
- 指定查询
- 实时监测
- 规则添加



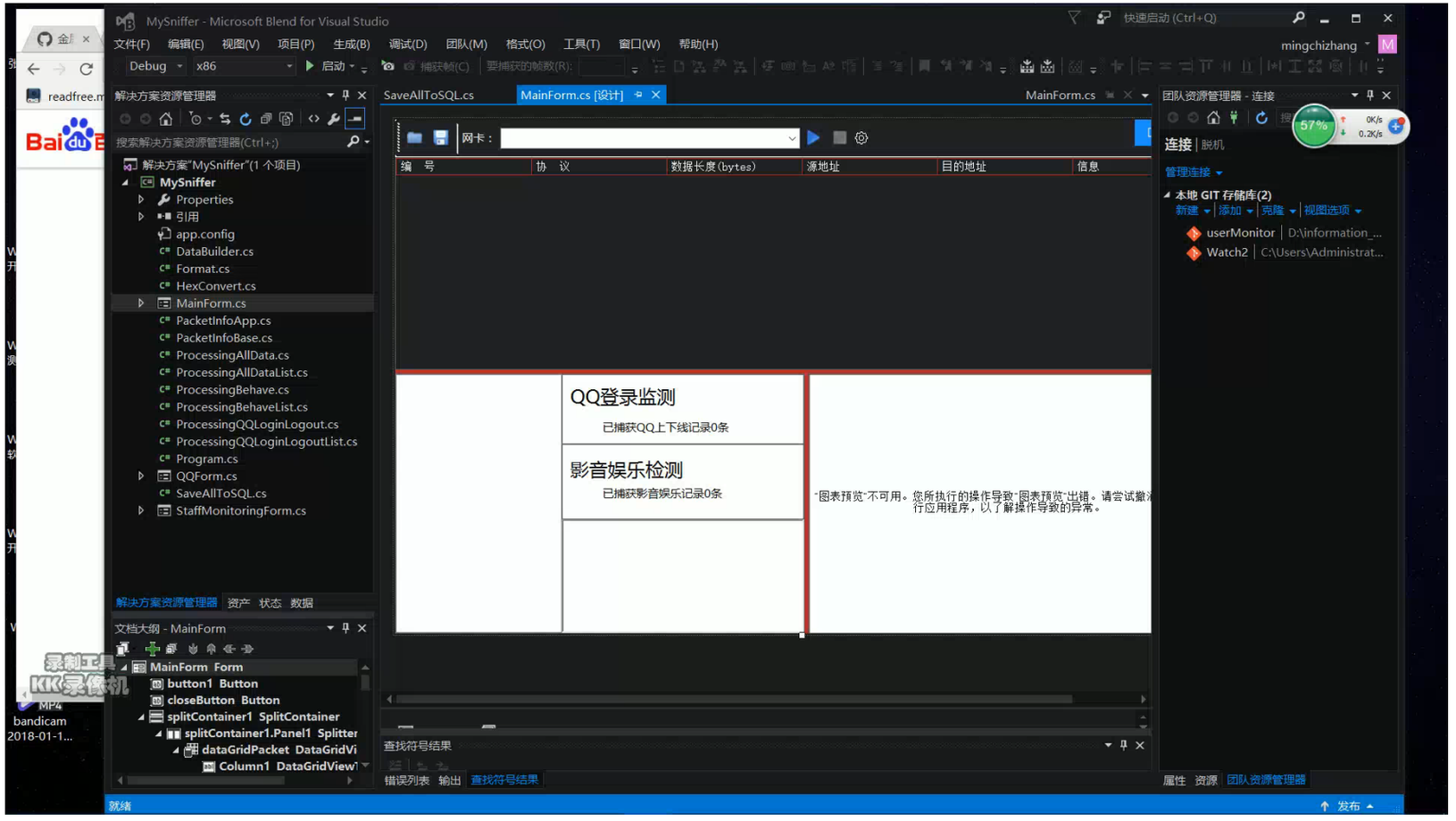
## 规则添加


记录查询
开始日期
2018年 1月11日
结束日期
2018年 1月11日
规则添加
监控名
4399
用户行为
娱乐行为
指定源端IP
指定目标IP
具体方式
打游戏
添加
查询筛选
娱乐行为
购物行为
查询记录
行为检测
时间
源端IP
目标端IP
用户行为
具体方式
2018-01-11
10.10.4.130 [6070]
118.123.203.211
购物
访问淘宝网站
2018-01-11
10.10.4.130 [6088]
171.217.255.49 [80]
娱乐行为
打游戏
上页
下页
实时监测
开始监测
上页
下页
结束监测

# 视频



## 视频演示


MySniffer - Microsoft Blend for Visual Studio
解决方案"MySniffer"(1 个项目)
MySniffer
Properties
引用
app.config
DataBuilder.cs
Format.cs
HexConvert.cs
MainForm.cs
PacketInfoApp.cs
PacketInfoBase.cs
ProcessingAllData.cs
ProcessingAllDataList.cs
ProcessingBehave.cs
ProcessingBehaveList.cs
ProcessingQQLoginLogout.cs
ProcessingQQLoginLogoutList.cs
Program.cs
QQForm.cs
SaveAllToSQL.cs
StaffMonitoringForm.cs
网卡：
编 号
协 议
数据长度(bytes)
源地址
目的地址
信息
QQ登录监测
已捕获QQ上下线记录0条
影音娱乐检测
已捕获影音娱乐记录0条
userMonitor
Watch2
57%
录制工具
KK录像机
bandicam
2018-01-1...

# 4

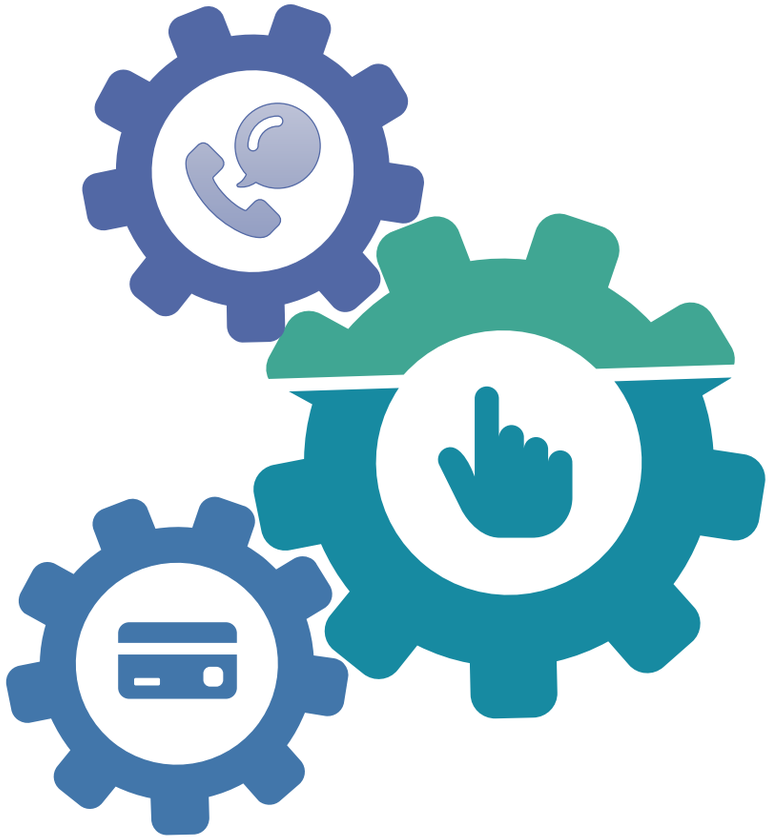
# 行为分析可视化

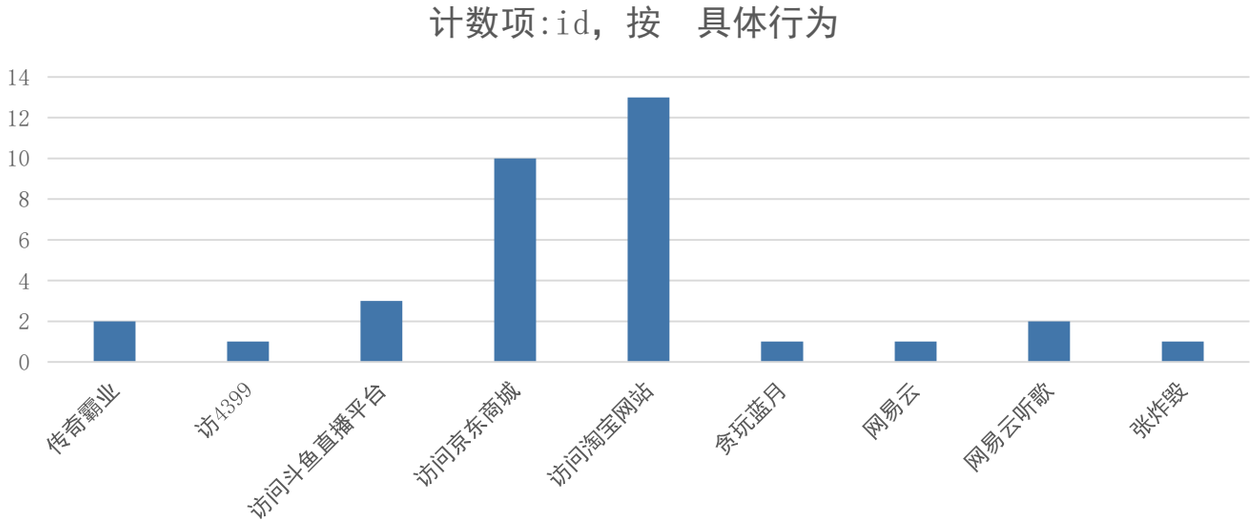
User behavior visualization

# 行为分析可视化

User behavior visualization

Watch_dogs

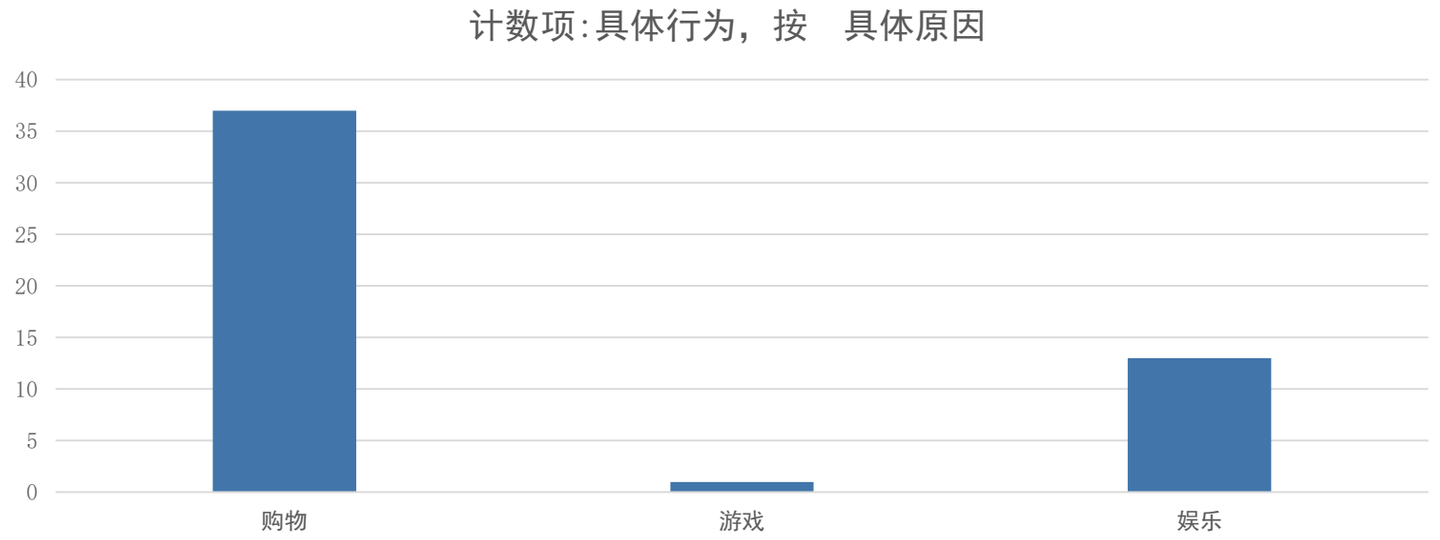


# 行为分析可视化

User behavior visualization



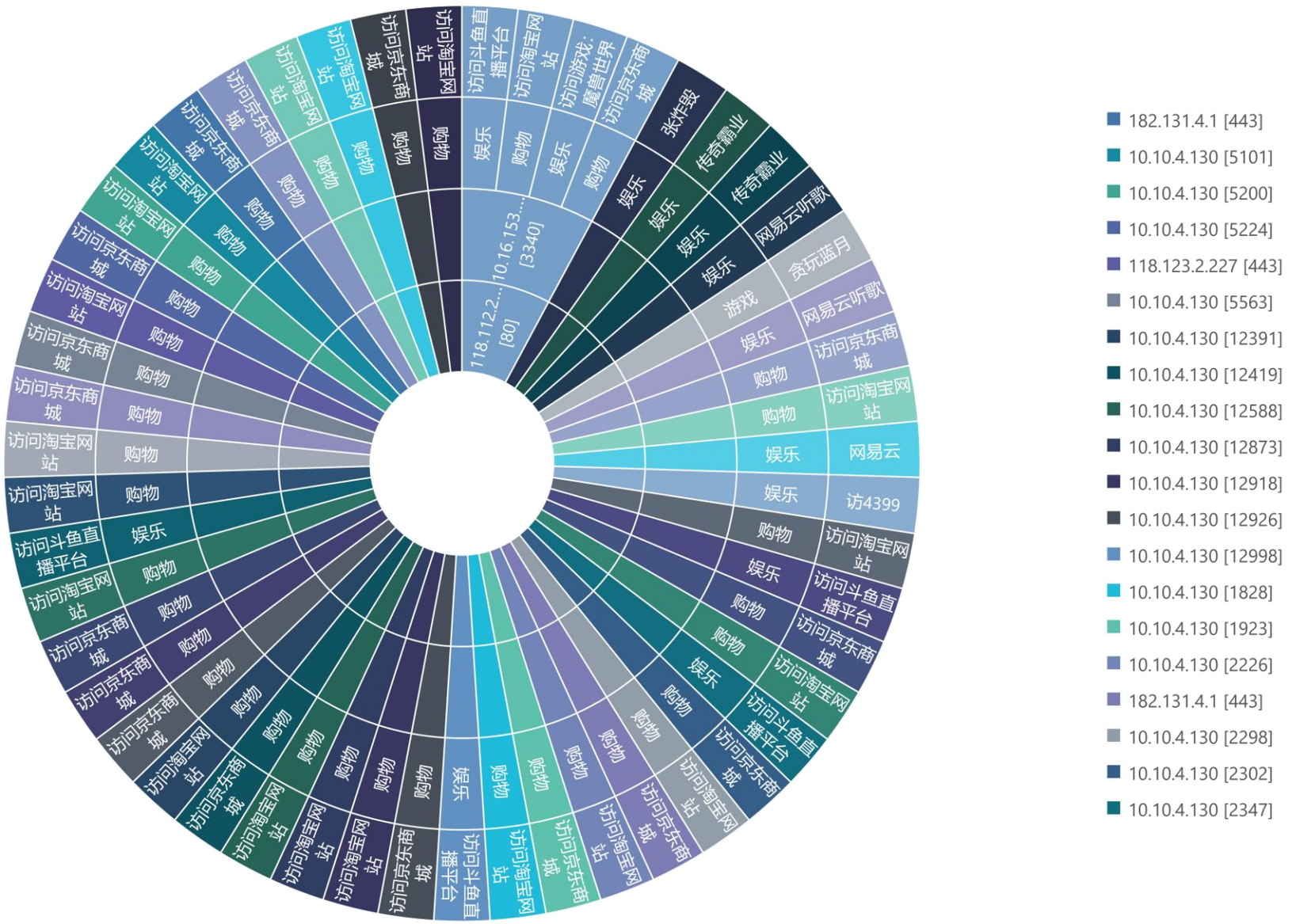


# 行为分析可视化

User behavior visualization



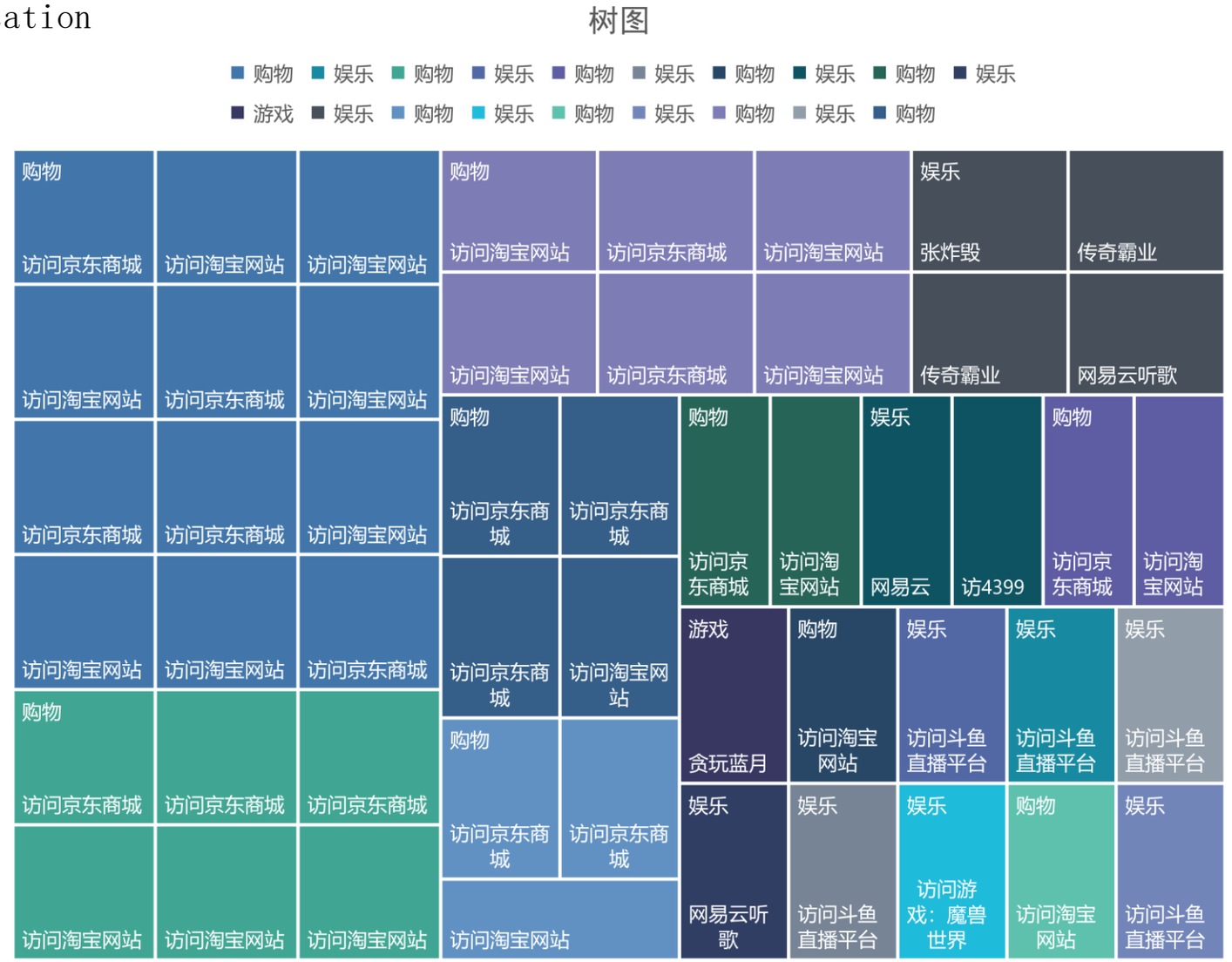
旭日图



# 行为分析可视化

User behavior visualization

Watch_dogs



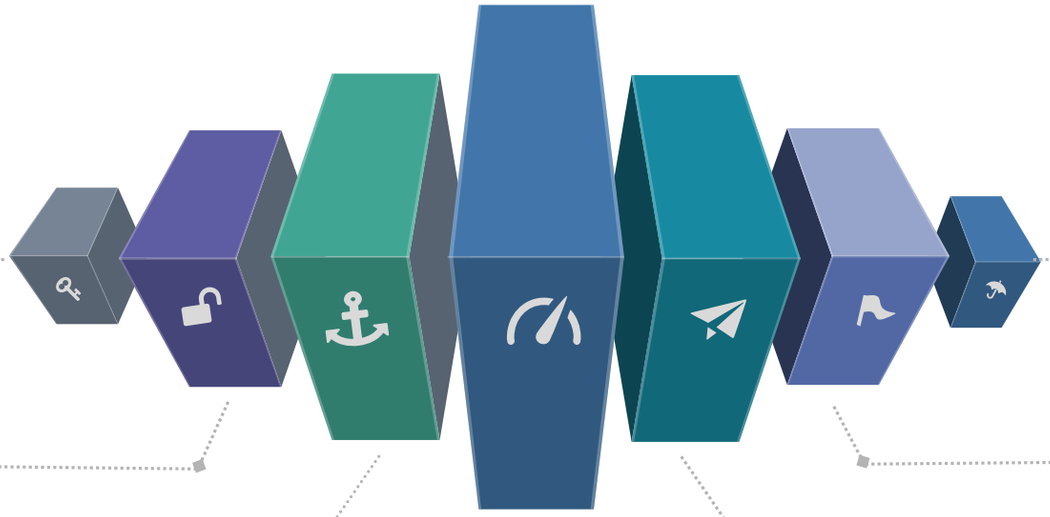
5

# 总结

summary

# 总结





**收获**
本次实验的收获还是很大的

**经历**
没想到研一上学期做了这么多事情，感觉没有荒废

**学习**
通过这次实验学习到了很多的**之前没有接触过的知识**

**成就**
成就感很足

**bug**
这个系统由于各种各样的问题**出了不少的难缠的**bug

**修仙**
总之我们三个人熬了多次，总是在深夜的会后待在实验室改代码

**崩溃**
有一个bug改了一天多，心情极其崩溃


谢谢观看