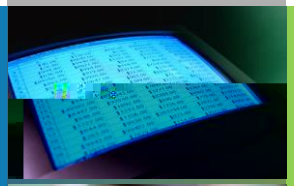
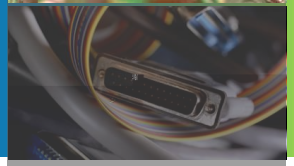
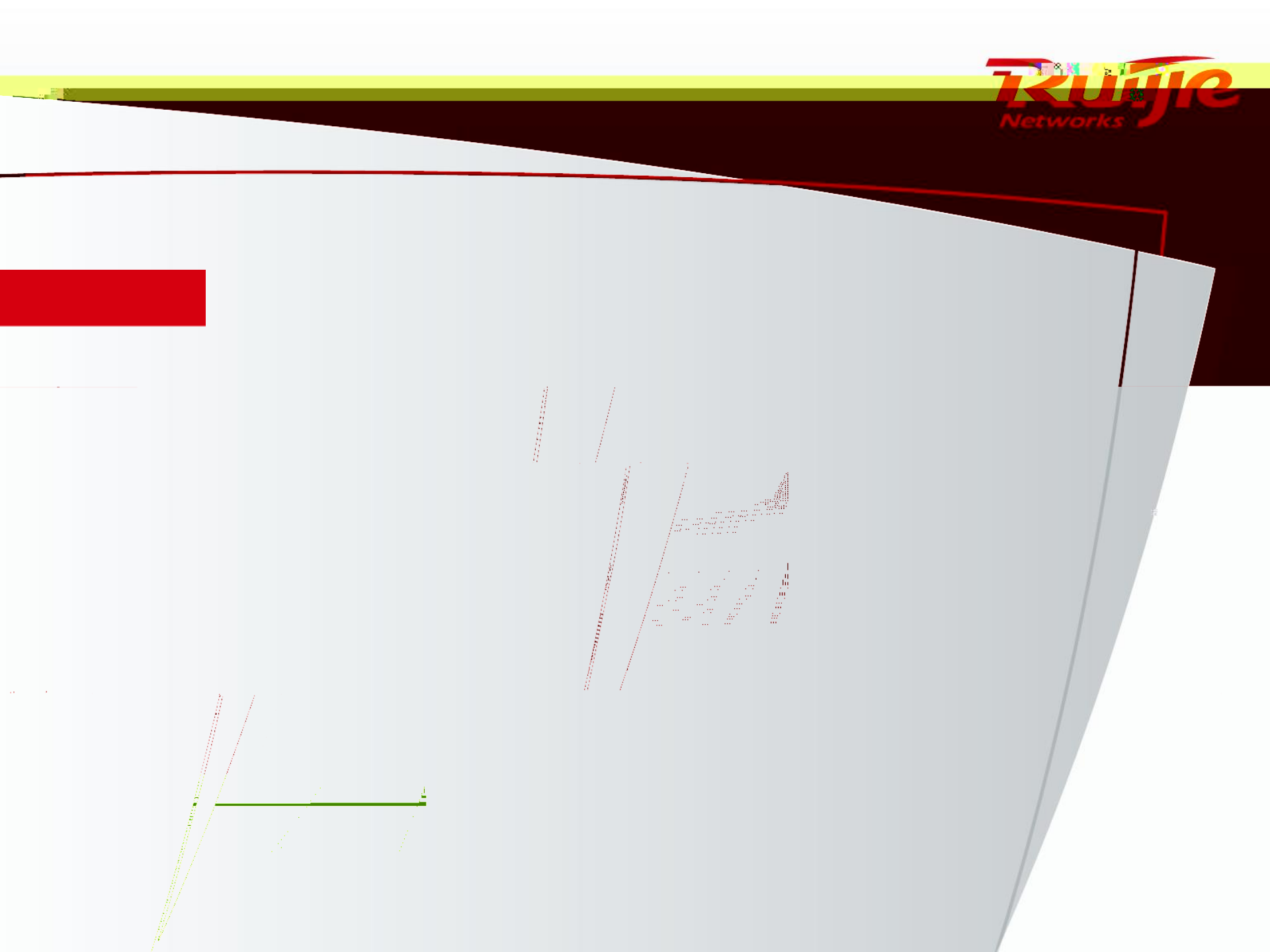
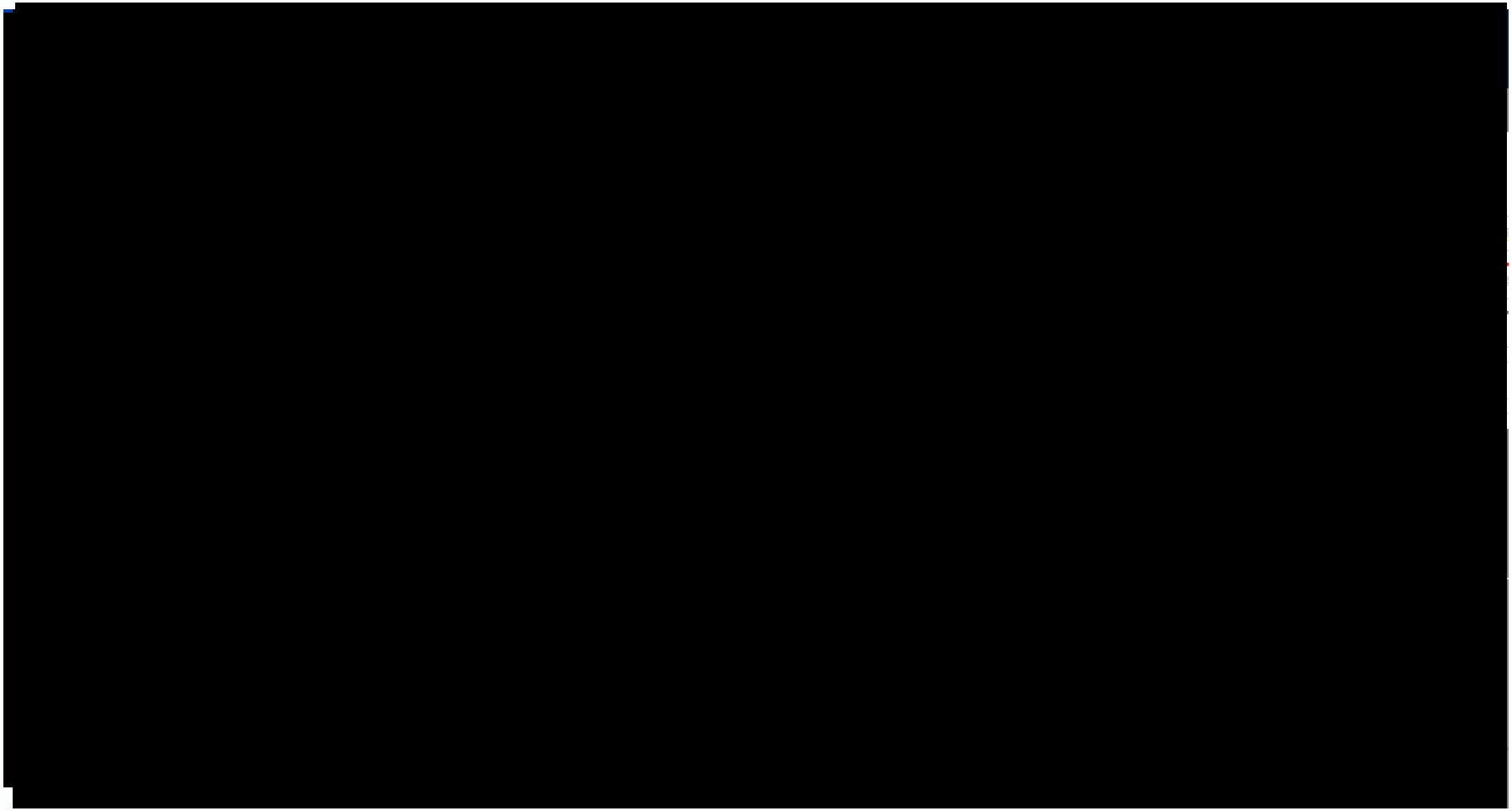
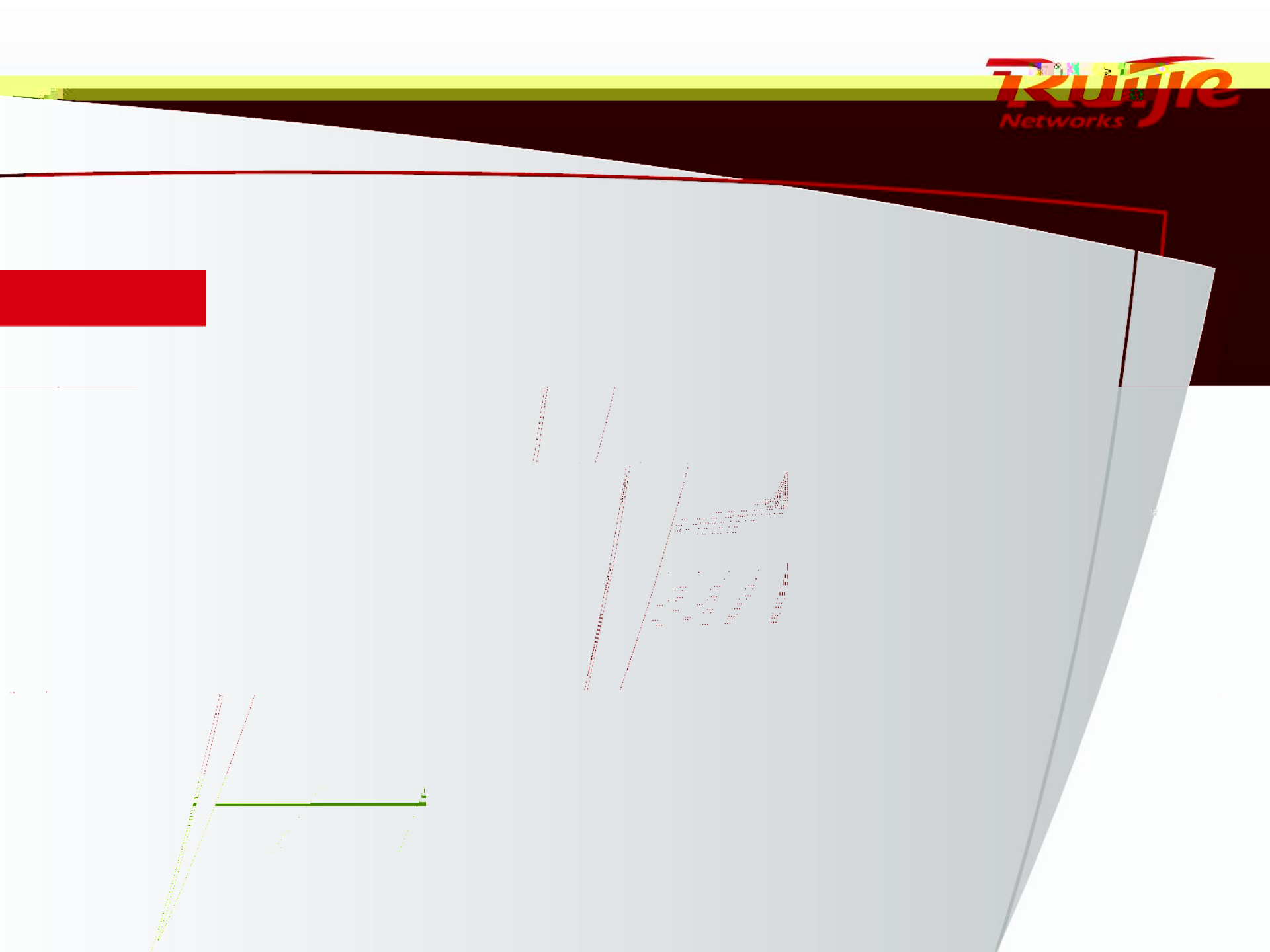
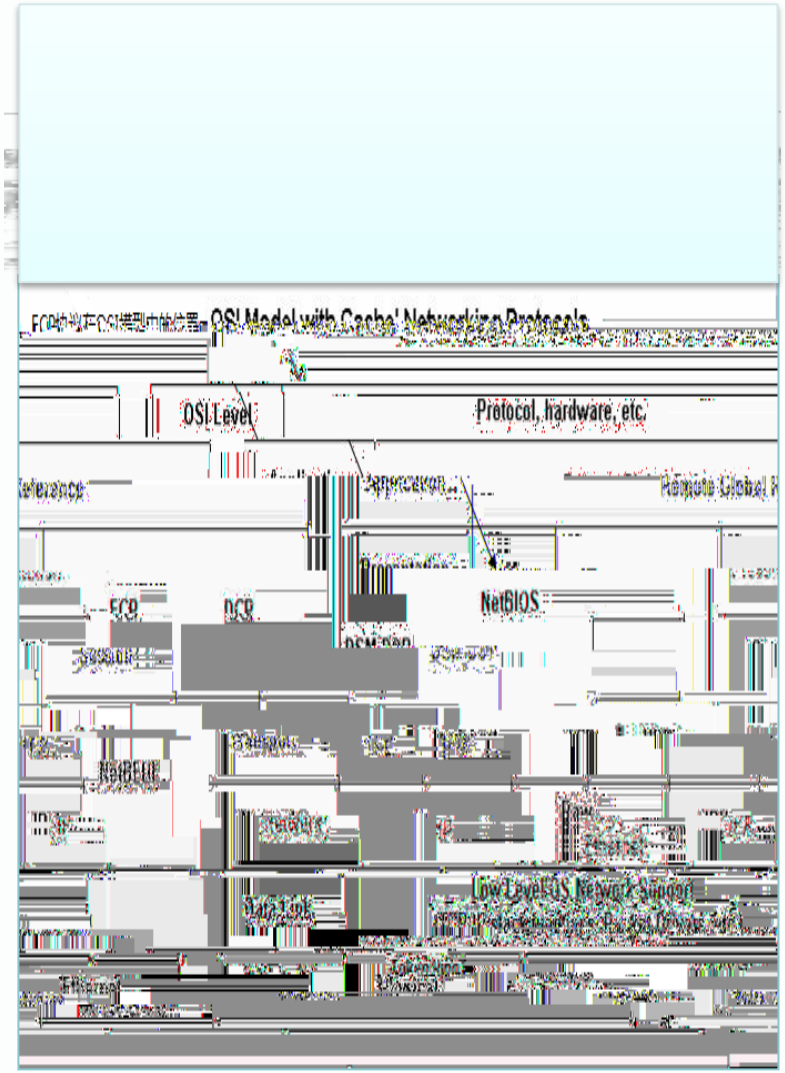


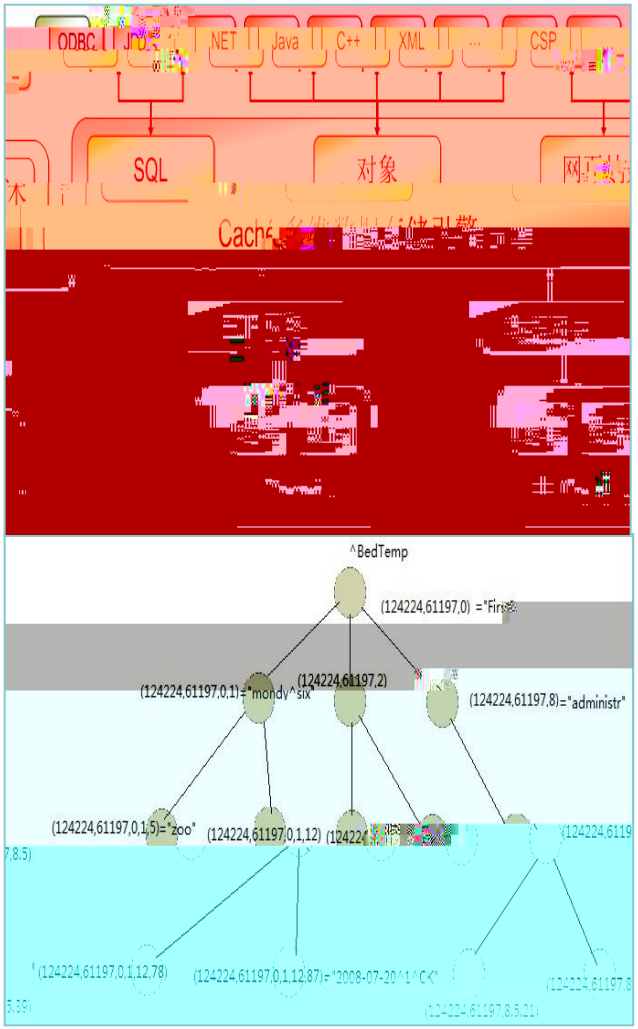


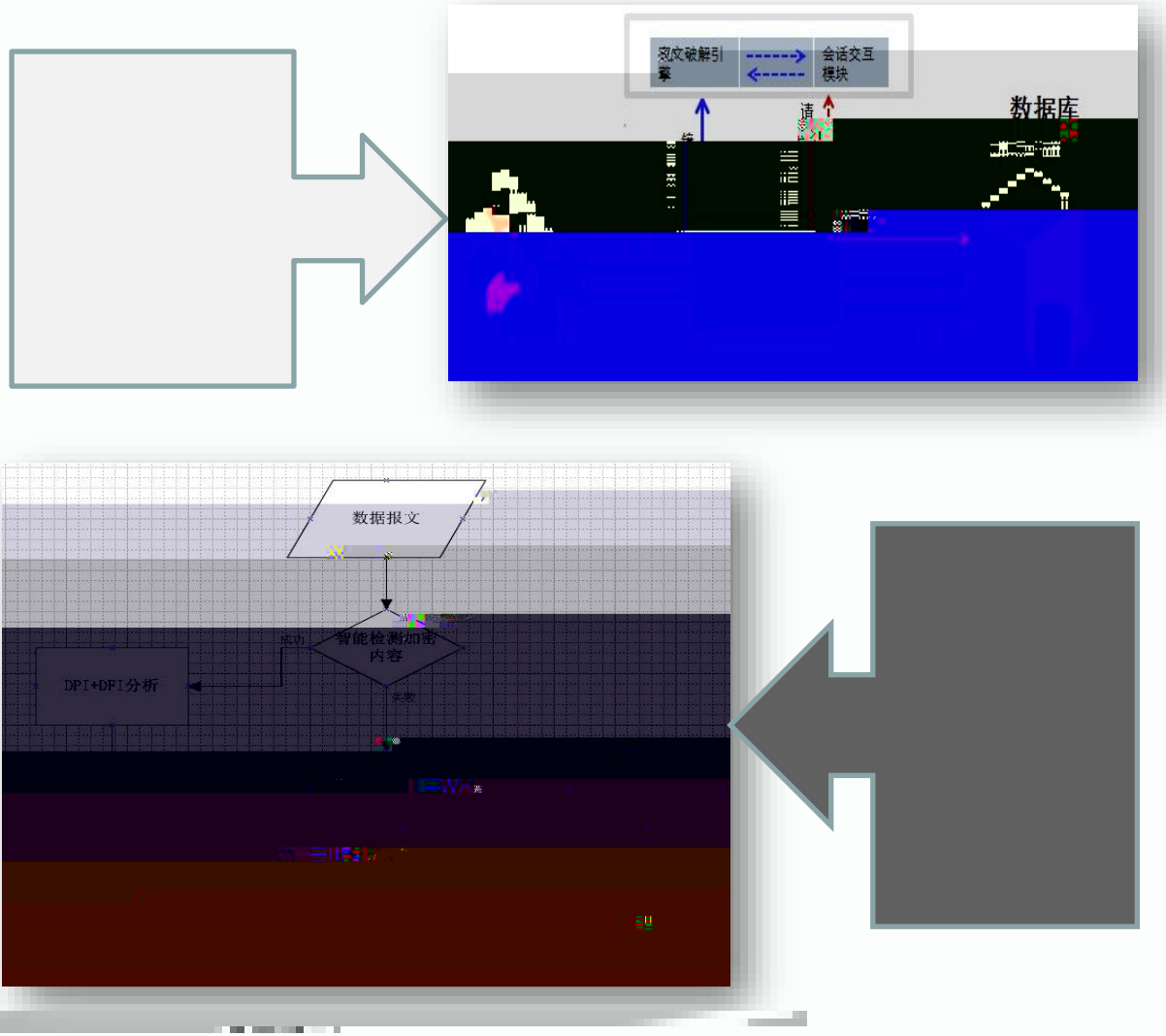




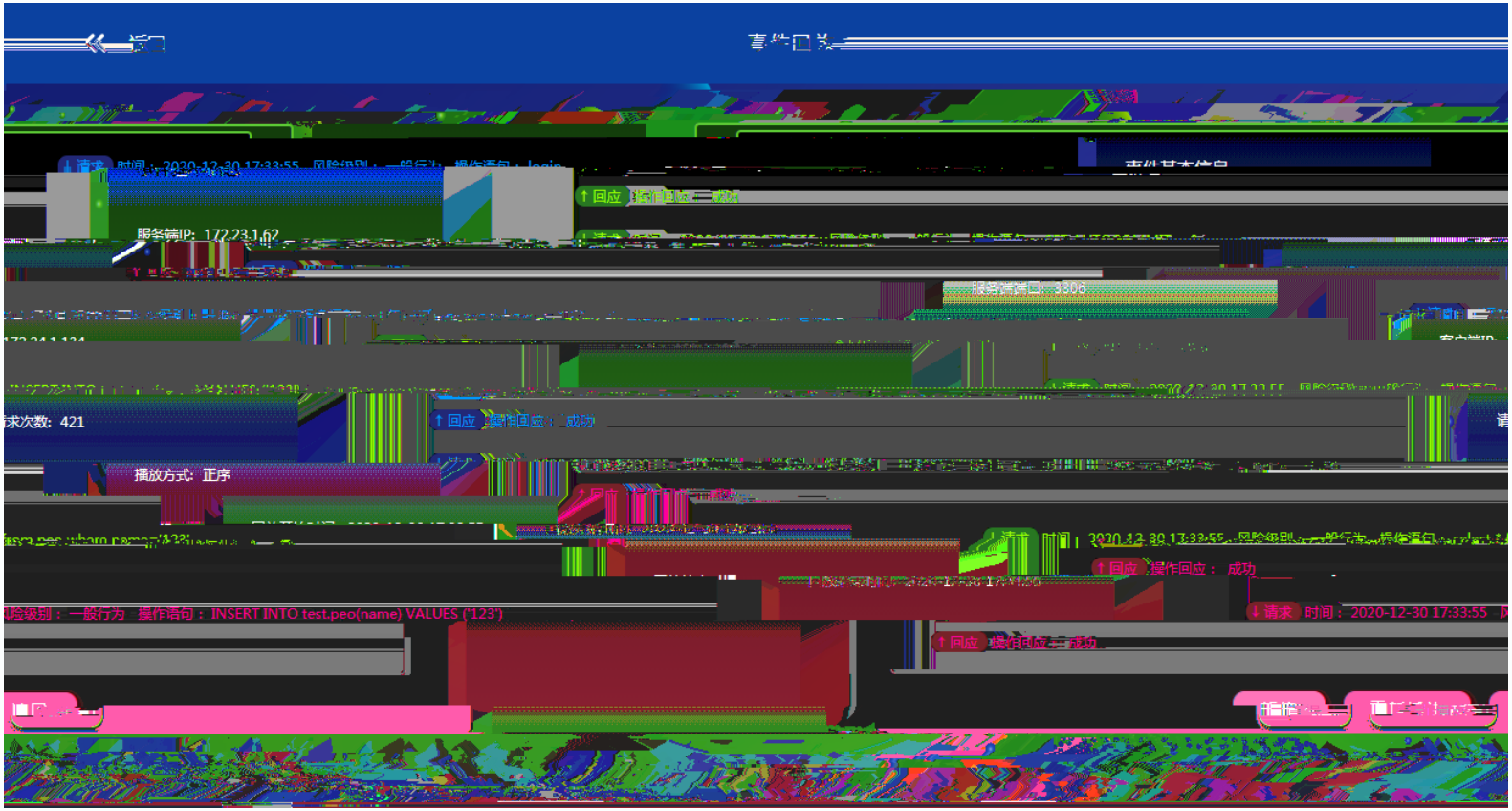


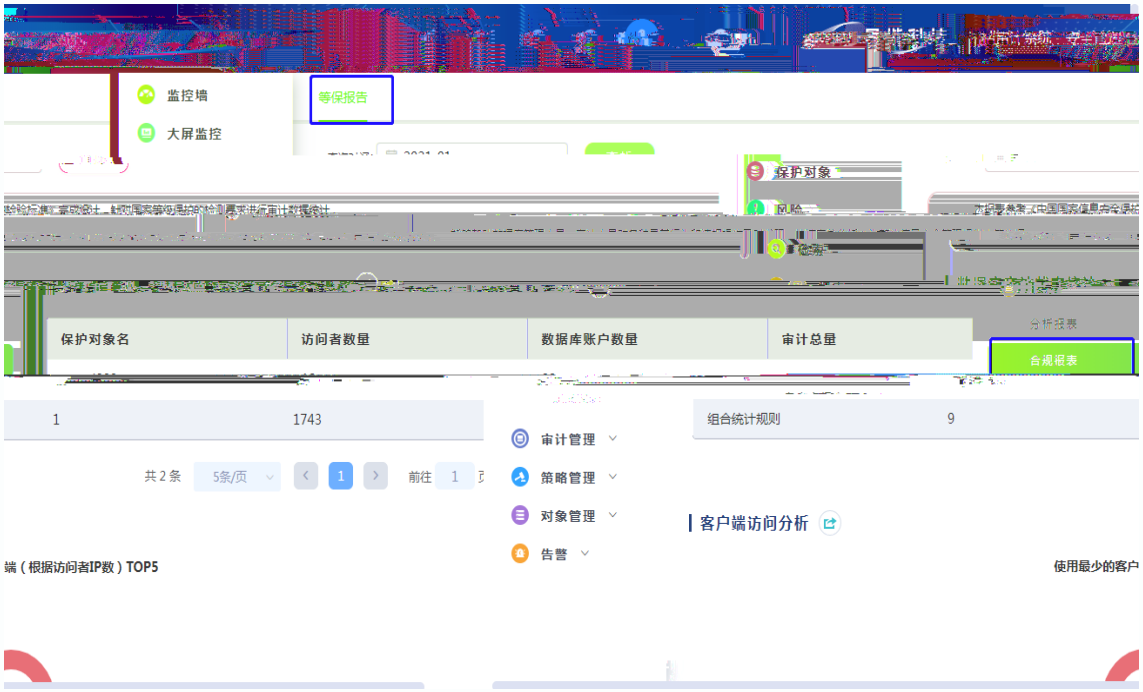

OSI Model with Cache' Networking Protocols
OSI Level
Protocol, hardware, etc.
NetBIOS
Low Level OS Network Support


ODBC
NET
Java
C++
XML
CSP
SQL
对象
^BedTemp
(124224,61197,0) ="Firs
(124224,61197,0,1)="mondy^six"
(124224,61197,2)
(124224,61197,8)="administr"
(124224,61197,0,1,5)="zoo"
(124224,61197,0,1,12)
(124224,61197,0,1,12,78)
(124224,61197,0,1,12,87)="2008-07-20^1^CK"
(124224,61197,8,5,21)


数据库
数据报文
智能检测加密内容
DPI+DFI分析

三层关联
添加为系统语句
事件回放
PC→App Server
访问者：
操作系统主机名： localhost
用户
数据库账户： SCOTT
客户端
MAC： 00:0C:29:D8:A5:62
操作系统用户名：
客户端进程：
数据库
数据库类型： Oracle
表名： posts
地址： 172.23.1.62 : 1521
字段名： 所有字段
数据库名： orcl
操作回应： 成功
操作类型： select
操作耗时： 0.076毫秒
地址（MAC地址）为：00:0C:29:D8:A5:62，电脑名称为：localhost
操作语句： select count(*) from posts where isPostsDel = :1 order by postPublishTime desc(1 = 1)


事件回放
请求 时间：2020-12-30 17:33:55 风险级别：一般行为 操作语句：login
事件基本信息
回应 操作回应：成功
服务端IP：172.23.1.62
服务端端口：3306
客户端IP：
求次数：421
回应 操作回应：成功
播放方式：正序
2020-12-30 17:33:55 风险级别：一般行为 操作语句：login
回应 操作回应： 成功
险级别： 一般行为 操作语句： INSERT INTO test.peo(name) VALUES ('123')
请求 时间： 2020-12-30 17:33:55
回应 操作回应： 成功


监控墙
大屏监控
等保报告
保护对象
保护对象名
访问者数量
数据库账户数量
审计总量
分析报表
合规报表
1
1743
组合统计规则
9
共 2 条
5条/页
1
前往
1
审计管理
策略管理
对象管理
告警
客户端访问分析
端（根据访问者IP数）TOP5
使用最少的客户