软件安全之远程木马

功能测试

题 目： 远程控制木马功能测试

组 员：彭馨勇 2017301510012

徐锦盈 2017301510026

范子颖 2017301510008

邓洋涛 2017301510056

课程名称： 软件安全

任课教师： 彭国军

二零一九年六月二十六日

目录

[**一、** **测试方案** 3](#_Toc12393826)

[**二、** **测试过程和结果记录** 3](#_Toc12393827)

[**2.1 远程控制允许功能** 3](#_Toc12393828)

[**2.1.1 等待连接** 3](#_Toc12393829)

[**2.1.2 连接** 4](#_Toc12393830)

[**2.1.3 成功连接** 5](#_Toc12393831)

[**2.2摄像头监控** 6](#_Toc12393832)

[**2.2.1 server端** 6](#_Toc12393833)

[**2.2.2 client端** 7](#_Toc12393834)

[**2.2屏幕监控** 7](#_Toc12393835)

[**2.2.1 client端** 7](#_Toc12393836)

[**2.2.2 client端** 8](#_Toc12393837)

[**2.3进程管理** 8](#_Toc12393838)

[**2.3.1 client端** 8](#_Toc12393839)

[**2.3.2 server端** 9](#_Toc12393840)

1. **测试方案**

本小组在程序可以运行的情况下，可以把同一主机环境作为server和client，也可以将配有java环境的虚拟机作为client。在以下的测试过程和测试结果中，主控端client为虚拟机，被控端server为主机。我们将针对各个功能单独进行测试和验证。

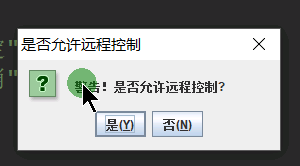
其中测试功能包括：

1. 进程管理；
2. 摄像头监控；
3. 屏幕监控；
4. 在启动服务之前有弹窗提示是否允许进行管理，可以很方便地进行远程主机的管理。
5. **测试过程和结果记录**

**2.1 远程控制允许功能**

**2.1.1 等待连接**

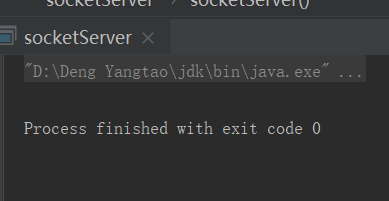
* 首先将被控端上线：



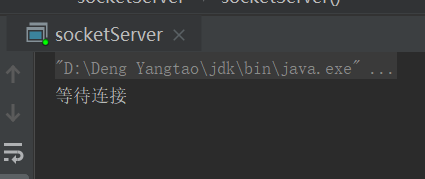
* 若点击否，会直接结束进程：



* 可以看到，以0退出了。



* 若点击是，会显示正在等待控制端的连接：



**2.1.2 连接**

* 接下来运行控制端程序，准备连接。会有弹框弹出，提示输入被控端的ip地址和端口：

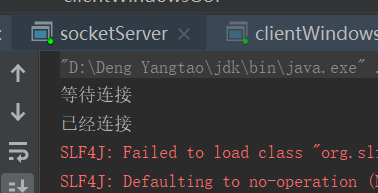


* 接下来输入被控端的ip和端口（代码中默认端口为3333），然后点击连接。可以看到在控制端会有弹框提示连接成功：



**2.1.3 成功连接**

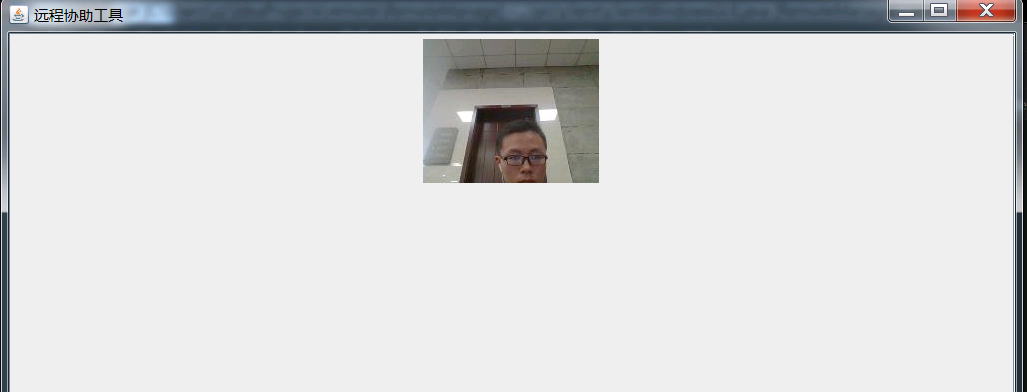
* 与此同时，在被控端会显示已经连接成功：



**2.2摄像头监控**

**2.2.1 server端**

* Client端点击“打开摄像头”按钮，从而可以立即通过server的摄像头查看：



* 可以在任务管理器看到正在运行进程：

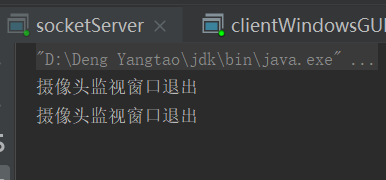


* 点击右上角的关闭按钮，回到刚才的界面：



**2.2.2 client端**

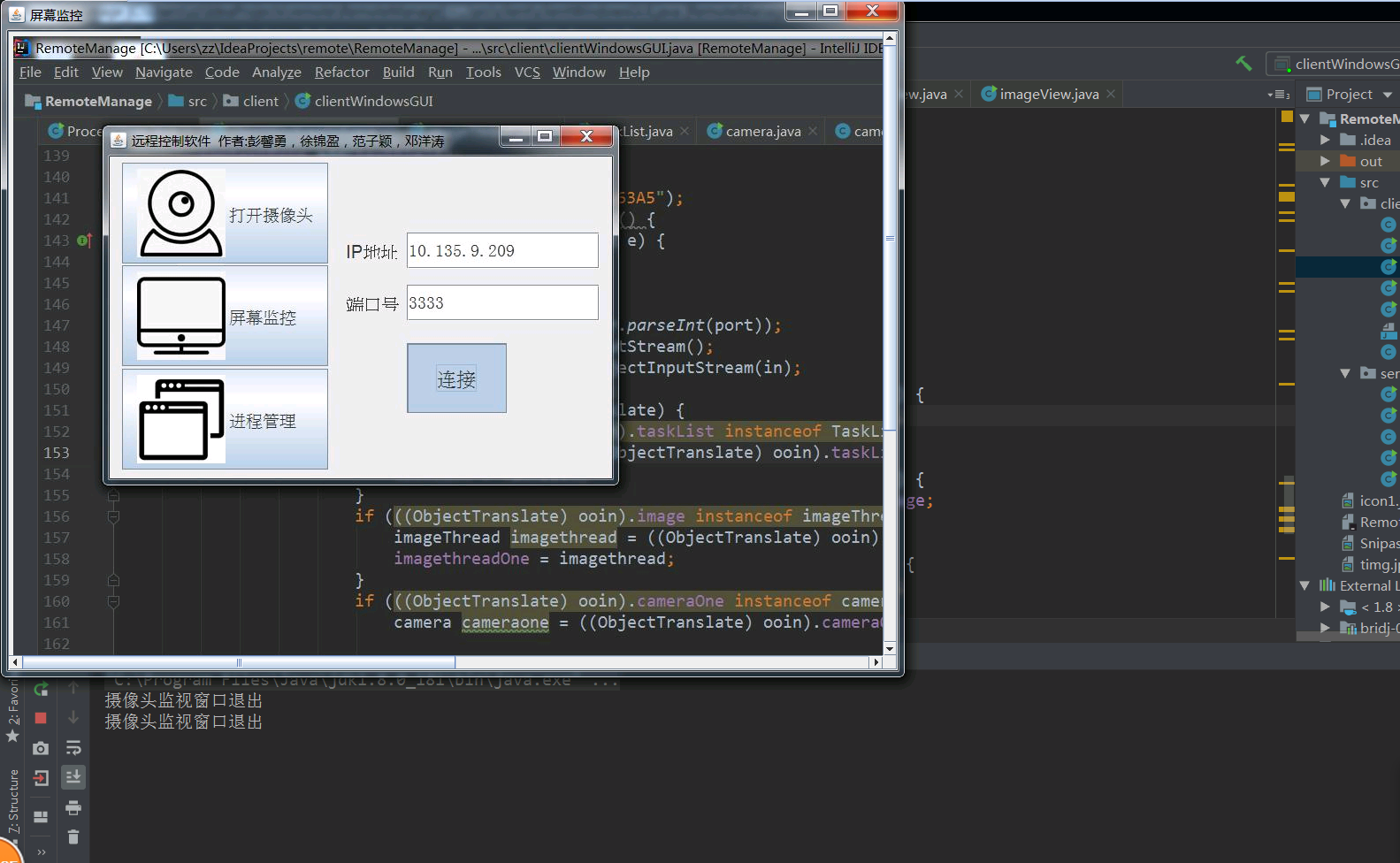
* 此时，在client端可以看到有提示摄像头窗口退出：



**2.2屏幕监控**

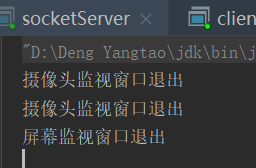
**2.2.1 client端**

* Client端点击“屏幕监控”按钮，从而client可以立即查看到server端的屏幕界面：



**2.2.2 client端**

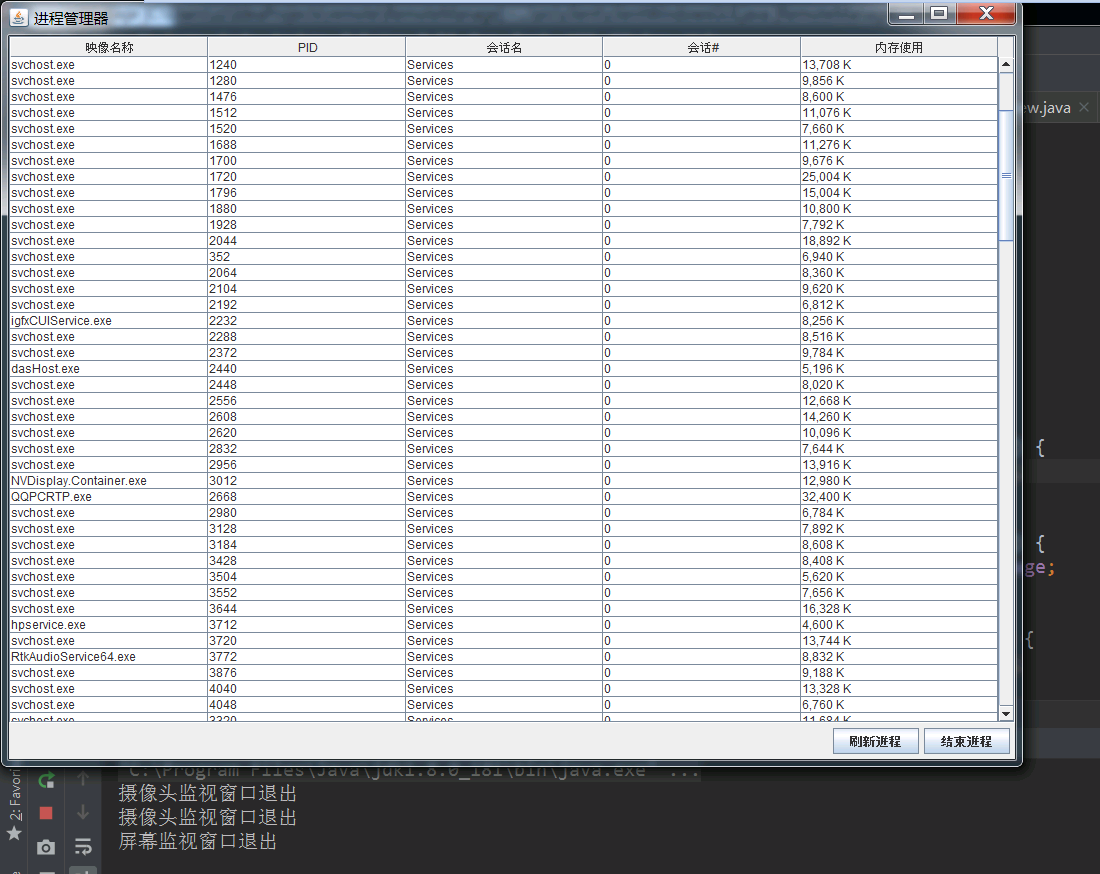
* 点击右上角关闭按钮之后，client端有提示：屏幕监视窗口退出：



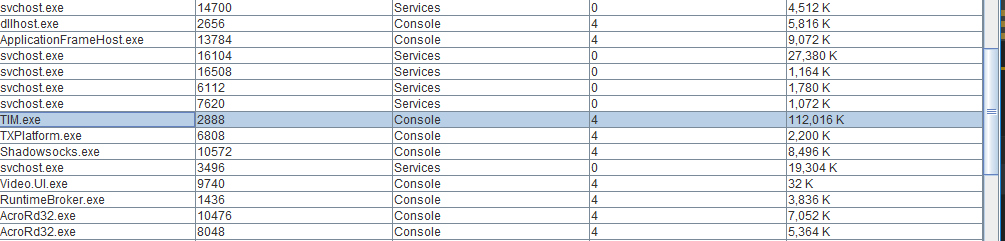
**2.3进程管理**

**2.3.1 client端**

* Client端点击“进程管理”按钮，从而client可以立即查看到server端当前的所有进程：

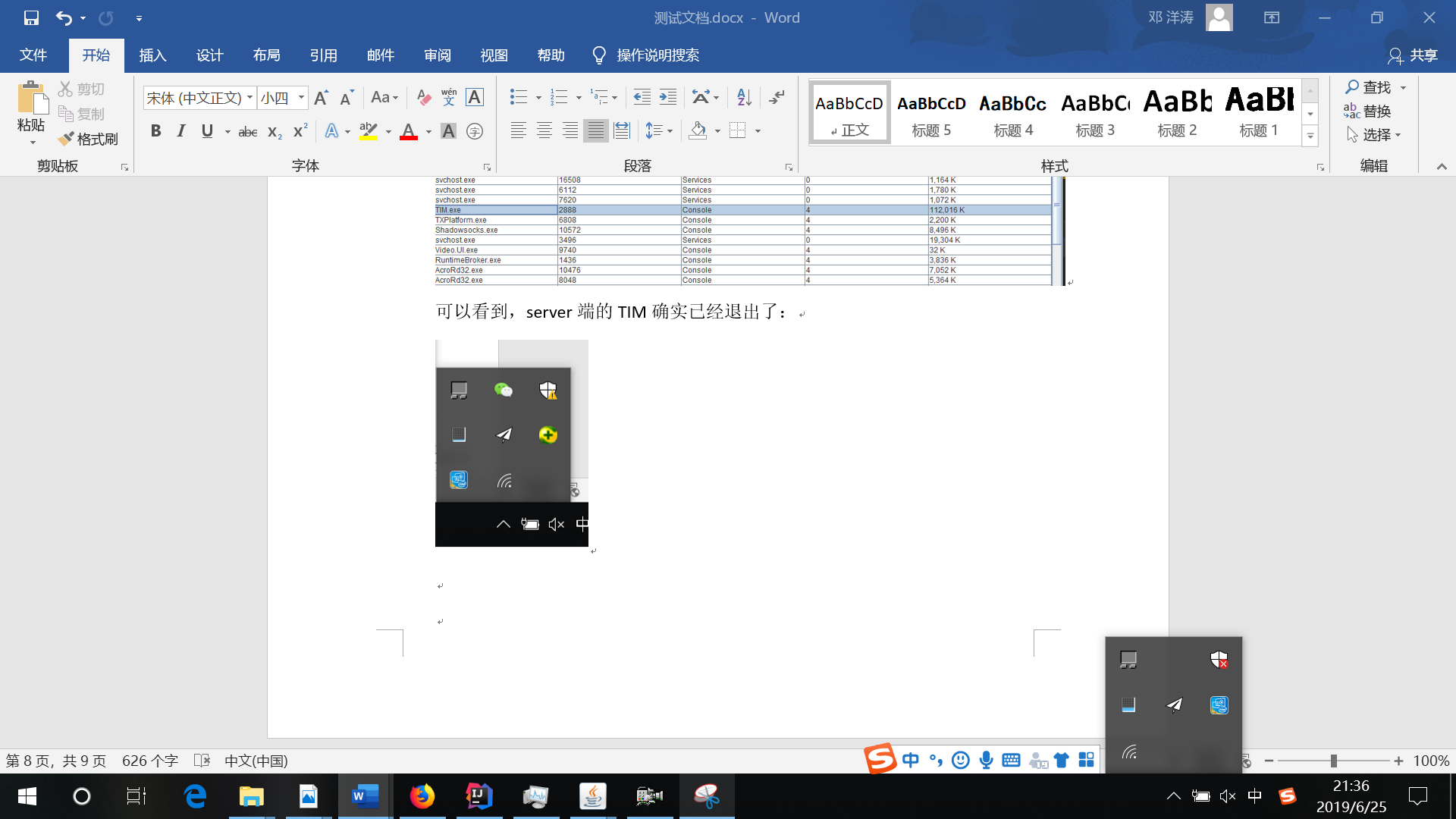


* 选择一个进程，比如“TIM.exe”，然后点击结束进程：

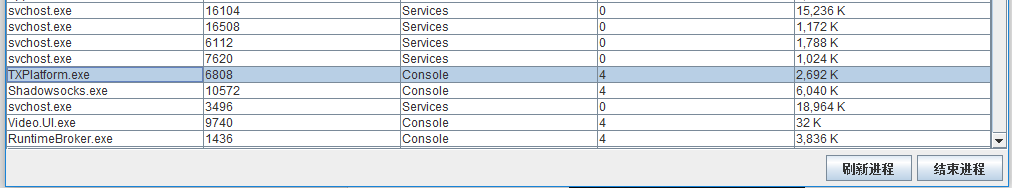


**2.3.2 server端**

* 可以看到，server端的TIM确实已经退出了：



* Client端继续点击“刷新进程”，然后检测，发现“TIM.exe”确实不在了：



* 点击右上角关闭按钮之后，client端显示“进程监视窗口退出”：

