

# Cpr/SE 491 Weekly Report    **MAY15-06**    **Week 5 (9/27/14-10/3/14)**

---

**Advisors:** Joseph Zambreno

**Client:** Curtis Schwaderer (IP Fabrics, Inc)

## **Members (roles):**

Altay Ozen (Team Leader and Team Key Concept Holder)

Andrew Heintz (Team Communication Leader)

Abraham Devine (Team Webmaster)

**Project Title:** Network Forensics User Interface

---

## **Weekly Summary**

Finished project plan and submitted it  
Compiled and ran DeepSweep  
Uploaded pcap files to Xplico via command line  
Created basic outline of web site

See individual contributions for more details

## **Meeting Notes:**

### **10/03 Advisor Meeting**

**Duration:** 30 min

**Members Present:** All

Discussed details of system diagram

- Split DeepSweep in two – Both device and API
- Unclear how the data from DeepSweep is formatted
- Need include how client starts DeepSweep

Discussed what risks would be more project-specific

- Risks are too general, i.e. apply to any project
- Test environment e.g. access to data or device

Discussed project schedule and next step

- Project schedule looks good
- May flesh out parts of it as we continue
- Next step is create working demo of DeepSweep

Discussed what type of test environment is needed

- Need raw traffic from them
- Might need to “spoof” traffic (i.e. fake traffic)

## 10/03 Group Meeting

**Duration:** 90 min

**Members Present:** All

Discussed last week's tasks and what pending issues arose

Discussed and assigned tasks for next week

Discussed issues with compiling Go Collector

### **Pending Issues**

Problem: Need test environment or raw traffic for DeepSweep

Solution: Need contact client and request traffic or environment

Problem: Go Collector compile produces errors

Solution: Go Collector needs to be connected with DeepSweep

Problem: Uncertain what role the Go Collector plays

Solution: Setup Collector and run it to figure out what it does

Problem: Xplico has no report generation functionality

Solution: Look into how difficult it is to extend Xplico

### **Plans for next week**

Fix compile of Go Collector (Altay, 3 hours)

Create instructions for DeepSweep (Altay, 2 hours) \*

Determine setup for testing (Altay, 1 hour)

Try to verify DeepSweep works (Altay, 2 hours)

Finish web site and upload (Abraham, 4 hours)

Import DeepSweep and Go Collector (Abraham, 2 hours)

Look into extending Xplico (Abraham, 2 hours)

Import DeepSweep and Go Collector (Andy, 2 hours)

Install and experiment with pcap libraries (Andy, 4 hours)

Look into extending Xplico (Andy, 2 hours)

\* Alternatively/Preferably, put in source control

Note: Discuss design document at next meeting (i.e. 10/10)

## Individual Contributions (this week)

Names	Time Spent (hrs)	Date Finished	Details of Task	How it got Completed	Why is it Important
Andrew Heintz	6.5	10/2	Completed 1 <sup>st</sup> draft of project plan	Revised/Proofread the project plan, particularly requirements, risks, and market survey	Project Plan is a key artifact of the course
Andrew Heintz	2	10/2	Looked into Java pcap libraries	Googled pcap libraries for Java and read documentation	The Pcap Creator will need to use some sort of pcap library
Altay Ozen	4	10/1	Compiled and ran DeepSweep	Requested missing libraries from client and downloaded other missing libraries	DeepSweep is a key project component
Altay Ozen	2	10/2	Uploaded pcap files via command line	Read man pages and trial/error to figure out how to upload	Pusher will need to upload files via command line
Altay Ozen	2.5	10/2	Try to compile Go Collector	Downloaded Go compiler and imported project	Go Collector is a key project component
Abraham Devine	1.5	10/2	Worked on website	Use weebly to create template for web site	Web site is required part of course
Abraham Devine	0.5	9/30	Worked on DeepSweep	Reviewed some of the code for DeepSweep	DeepSweep is a key project component

## Total contributions for the project

Andrew Heintz (36 hrs)

Altay Ozen (36.5 hrs)

Abraham Devine (14 hrs)