Jonathan Kelly

ITP 470

February 7th, 2013

IT Practicum Proposal v1.0

**Description:**

The project will involve the creation, testing and documentation of a liveCD linux distribution built for forensic acquisition of systems and servers. The distribution will include a basic front-end UI which will allow the user to handle device mounting and acquisition without knowledge of terminal commands. The distribution will include records of testing on various systems to confirm proper forensic practices. The distribution will be supported by an online repositiory designed to store documentation about creation and use.

**Purpose:**

The purpose of this project is to create a functional, easy-to-use linux liveCD distribution designed for forensic acquisition of connected devices. Documentation for this project should allow future students/academics/professionals to identify the methodology used in creation, testing and application of this tool.

**Projected project goals:**

The project will result in an organized repositiory with documentation about all phases of the project

The project will result in a functional, usable, useful forensic acquisition tool

The project will establish an initial benchmark for future projects of similar nature

The project will encourage other students to participate in directed forensic research

The project will encourage members of industry to take interest in student directed research at USC.

**Student goals:**

The student hopes to improve knowledge of linux operating systems

The student hopes to learn about forensic best-practices first-hand

The student hopes to learn about proper testing of forensics devices

The student hopes to learn to write documentation and proposals for self-directed work

**Project approach and methodology:**

The student will proceed according to the list of deliverables listed below.

1. Organization of previous documentation
2. Testing of distribution and modifications should testing fail
3. Front-end application development
4. Re-upload and organization of the repository
5. Final delivery

**Project technologies:**

The student will require access to at least one accepted standard forensic acquisition tool to be used as a comparative benchmark for testing against the project.

The student will require access to various types of systems, possibly as virtual machines, with differing operating systems for testing of project compatibility.

The student will require access to some form of online repository where project documentation can be posted, organized and maintained.

**Deliverables:**

1. The student will create the repository, and upload and organize documentation already created by the student during the fall 2012 semester.
2. The student will test and submit documentation of testing, the nature of which will be determined at a later date, to confirm that the distribution does not auto-mount devices, and that all devices mounted are read-only. The testing must further confirm that devices acquired by this distribution are of comparable forensic quality to devices acquired by other accepted forensic tools.
3. The student will write a basic GUI front-end application that will handle detection, mounting, dismounting, and acquisition of devices.
4. The student will upload and organize all testing results and project documentation to the online repository
5. The student will deliver the finished project, with a full report detailing spring 2013 project documentation with, at minimum, reference to online documentation created for the fall 2012 practicum.

**Deliverable Timeline:**

Physical deliverables shall be submitted weekly on Thursdays to the ITP front office before 2:00pm.

Online deliverables or email submissions shall be submitted weekly on Thursdays to Professor Greenfield before 11:59:59pm.

These deliverable days and times are subject to change by agreement of both the student and the professor.

Thursday, February 14th – online and physical submission

Deliverables:

1. Email containing repository information
2. Proposal for testing methodology for February 28th deliverable
3. Revision of IT Practicum Proposal

Requirements:

1. The repository shall be up-to-date and organized with the documentation from the fall 2012 semester’s directed research project.
2. A brief proposal containing the student’s proposed testing methodology to show that the tool properly handles (read-only, no mount on start) devices
3. The revised version of this IT practicum proposal shall be submitted

Thursday, February 21st – physical submission

Deliverables

1. Proposal of testing methodology for March 7th deliverable
2. Proposal of design, functionality and build methodology for front-end application development

Requirements:

1. A brief proposal containing the student’s proposed testing methodology to show that the tool properly acquires devices
2. A brief proposal containing what the application will do, how it will do it, what it will look like, and how the student will go about creating it.

Thursday, February 28th –physical submission

Deliverables:

1. Documentation of confirmation that the tool successfully handles devices (read-only, no mount on start)

Requirements:

1. The tool must actually handle devices successfully. Modifications required to achieve this must be made to the tool before the delivery on February 28th

Thursday, March 7th – physical submission

Deliverables

1. Documentation of successful testing of forensically sound acquisition

Requirements:

1. The tool must be compared against a known forensic acquisition tool on a variety of devices and acquire files and devices with equal accuracy.

Thursday March 14th – online submission

Deliverables:

1. Back-end application to mount, dismount, detect and acquire devices and files from a system

Requirements:

1. The application must function in a linux environment and accomplish all of the tasks listed by this deliverable.

Thursday, March 21st – online and physical submission (barring spring break)

Deliverables:

1. Revised application proposal – physical
2. Version 0 of application front-end – emailed

Requirements:

1. A physical submission of the revised proposal detailed in the February 21st, submission. This should be updated with changes suggested by the professor and the student between February 21st and March 21st.
2. A functional front-end, performing the tasks listed by the March 14th deliverable.

Thursday, March 28th – no submissions

Thursday, April 4th – online submission

Deliverables:

1. Version 1 of application front-end

Requirements:

1. Version 1 should include all of the functionality listed by the modified proposal submitted March 21st. Version one should be able to seamlessly integrate with the forensic distribution.

Thursday, April 11th – online submission

Description:

1. Email with repository link and details of changes made

Requirements:

1. All documentation and work up to this point shall be uploaded to the repository and organized.

Thursday, April 18th – online submission

Description:

1. The completed front-end application shall be due at this time

Requirements:

1. The application shall incorporate all changes agreed upon by both the student and the professor and shall, at minimum, include all functionality listed in the final proposal deliverable submitted on March 21st.

Thursday, April 25th – online and physical – final submission

Description:

1. Email will repository link and details of changes made
2. Report submission (emailed and physical) containing documentation made this semester, proposals, testing, etc
3. Flash Drive with project installed and completed front-end application

Requirements:

1. All documentation and work up to this point shall be uploaded to the repository and organized.
2. The report shall contain final copies of all submitted paperwork. The report shall additionally contain documentation for usage of the tool.
3. The flash drive shall be submitted and kept by the professor for future use at his discretion.