Software Requirements Specification
for
Human Trafficking Detection System (HTDS)

February 13, 2014
Version 1.0

Prepared by
Qutaiba Albluwi, Younghun Chae, Tripti Garg, Zach Oliveira

Document Status Sheet

Document Title	Software Requirements Specification Document
Author(s)	Q. Albluwi, Y. Chae, T. Garg, Z. Oliveira
Version	1.0
Document Status	Proposed

Version	Submission Date	Changes
1.0	02-13-2014	N/A

Table of Contents

1. Introduction

Human trafficking is one of the most serious violation of human rights in our modern history. It is considered by most scholars as a modern form of slavery. Millions of children, women and men are trafficked every year for purposes of prostitution, forced labor or other forms of exploitations. The crime is normally managed by organized crime circles operating in a large number of cities around the world imposing real challenge to the detection and investigation of the crime.

The fast paced advancements of technology has severely contributed to the spread of this crime and facilitation of its operations. The complex communication systems has provided traffickers with secure channels of communication, while open access to pornography has facilitated communication with clients.

Combating this crime is a collective process between local law enforcement, interpol and non-governmental organizations (NGOs). Due to this, most systems used in the detection and investigation are classified and can only be accessed by authorized personnel. There is an emerging need to provide workers not affiliated with law enforcement with computer systems and application tools to facilitate their work. The proposed HTDS system is one step towards achieving this goal.

1.1 Purpose

The purpose of this document is to describe the software requirement specifications and the system architecture of the Human Trafficking Detection System (HTDS). This document will be used to draft the contractual terms between the developers (QYTZ) and the expected organization clients. Preparation of the document is mandated as a part of the requirements for CSC 505 - Advanced Topics In Software Engineering in 2014 Spring semester at University of Rhode Island.

1.2 Scope

The Human Trafficking Detection System (HTDS) is designed to provide the community working on human trafficking with an open source tool that would help in the detection and investigation processes. The main audience of the tool is members of NGOs and private investigators, although it could be used by law enforcement officials too.

The main purpose of the tool is to search for potential human trafficking activities by analyzing some known patterns of the operation of traffickers. Specifically, the tool analyzes phone number lists for repetitive patterns which might indicate potential human trafficking activities.

Traffickers normally operate a large number of exploited victims at the same time, while taking

control of all communication with clients. For example, it has been observed that various advertisement for commercial sex provide (fake) names of girls along with phone numbers. Since pimps take control of communication with clients, often times the advertisements of different girls in various geographical locations have the same phone number listed: the phone number of the pimp. The HTDS takes advantage of this observation to analyze phone number lists and report the likelihood of suspicious activity.

The main functionality of HTDS is data analysis. Data collection is assumed to be done offline using other applications, not necessarily interfaced with HTDS. Besides data analysis, HTDS maintains a database of alerts which could be used by investigators to perform time analysis, which is crucial to most investigations. Therefore, the alerts generated by HTDS are meant to be used as an element in the larger investigation process.

1.3 Definitions and Abbreviations

1.3.1 Abbreviations

ADB	Alert Database
CSC 505	Advanced Topics In Software Engineering Course Number at University of Rhode Island
DAT	Data Analyzer Terminal
DCT	Data Collector Terminal
DW	Data Warehouse
GUI	Graphical User Interface
HTDS	Human Trafficking Detection System
NGO	Non-Governmental Organization
SRS	Software Requirements Specification
QYTZ	Development team: Qutaiba, Young, Tripti and Zach
USB	Universal Serial Bus

Table 1.1: Abbreviations

1.3.2 System Definitions

Administrator	A user of HTDS responsible for performing configuration and administrative tasks like setting the analysis parameters and adding new users to the system. Administrators shall have full access privileges to HTDS.
Agent	Any user of HTDS with standard access privileges, i.e. non-administrative privileges. An agent shall be able to perform the basic functionalities of HTDS.
Alert	The result of analyzing an input data file for potential human trafficking activity. The alert is presented by a color according to a risk scale corresponding to various levels of probabilities.
Alert Database	All alert messages generated by HTDS stored in a structured format in the Data Warehouse (DW).
Data Analyzer Terminal (DAT)	A computing device where HTDS application is installed. All DATs are connected via the Secure network and have access to the Data Warehouse (DW).
Data Collector Terminal (DCT)	A computing device used to collect data that would be analyzed at DATs. All DCTs are connected through the Public network.
Data Warehouse	A central storage location at the Secure network where the alert database (ADB), the input files and the configuration files are stored.
Human Trafficking Detection System (HTDS)	An application to detect Human Trafficking activities by analyzing files containing suspect phone numbers to generate alerts according to defined risk levels.
Public Network	A network that connects Data Collector Terminals (DCTs) which provides access to the internet.
Secure Network	A network that securely connects all Data Analyzer Terminals along with the Data Warehouse (DW). The network does not provide access to the internet and is physically separated from the public network.

Table 1.2: System Definitions

1.3.3 Human Trafficking Definitions

Buyer	Anyone who pays for or trades something of value for sex. This can

	be a family member, teacher, baseball coach, and member of the clergy; anyone, male or female. (sharedhope.org)
Child Pornography	The visual representation of minors under the age of 18 engaged in sexual activity or the visual representation of minors engaging in lewd or erotic behavior designed to arouse the viewer's sexual interest (the free legal dictionary)
Facilitator	Any business or person allowing a trafficker/pimp to carry out exploitation. These facilitators include taxi drivers, hotel owners newspapers where girls are advertised work in direct and indirect partnership with pimps. (sharedhope.org)
Human trafficking	The recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs (United Nations Office of Drugs and Crime)
Pimp/Trafficker	Anyone who receives money or something of value of the sexual exploitation of another person (sharedhope.org)
Prostitution	The practice or occupation of engaging sexual activity for someone with payment

Table 1.3: Human Trafficking Definitions

1.4 Document Overview

The rest of this document is divided into three sections. Section 2 provides an overview of the proposed system and the assumptions made about the system. Section 3 provides the functional and non-functional requirements. Section 4 describes how changes to SRS will be handled.

2. General Description

2.1 Product Perspective

This product is part of a larger vision of designing an open source investigation tool for NGOs, where various detection applications are used to detect and produce various alerts according to the probability of human trafficking activities. Besides HTDS, other systems could be proposed to analyze advertisements of common human trafficking terminologies or perform cross analysis of advertisements in multiple languages.

The system is designed for professionals working in non-governmental organizations which include members of NGOs and private investigators.

The HTDS is provided as an open source with no charges associated with downloading or using it.

2.2 Product Functions

Performing phone number analysis, producing the corresponding alerts, and maintaining a history of theses alerts are the main functions of HTDS. The HTDS provides functionalities for storing and retrieving data from the DW.

In the analysis phase, HTDS retrieves specified input files from the DW for analysis. The HTDS then finds phone numbers that are repeated in the input file. The HTDS transforms this synthesized data into alerts depending on the probability of human trafficking.

The standard US Homeland Security Advisory System comprising of five-color alert system will be used. Based on the analysis configuration parameters, the HTDS should produce one of the following five alerts.

Level	Color	Note
1	Red	Severe Risk
2	Orange	High Risk
3	Yellow	Significant Risk
4	Blue	General Risk
5	Green	Low Risk

In cases no potential signs of human trafficking are detected, HTDS shall produce a White alert, indicating no risk.

2.3 Assumptions

1. There exist two types of networks: Secure Network and Public Network. The Secure Network is physically separated from the Public Network with no access to the internet. On the other hand, the Public Network supports internet access. Having two separate networks is a conventional architecture for organizations that perform digital forensics to ensure the security of data and the credibility of the investigation process.
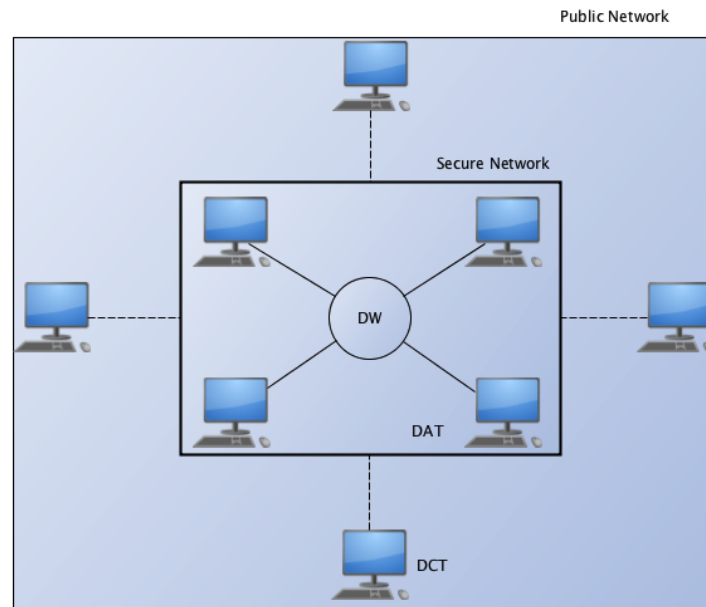

Figure 2.1

2. The Secure Network is assumed to be secure with no extra security measures required from applications running on that network.
3. There is a Data Warehouse (DW) which all terminals in the secure network (DCTs) have access to.
4. The Data Warehouse has enough space to store both the input files and the Alert Database (ADB).
5. The input files stored at DW are formatted according to a predefined format. It is assumed that the agent only uploads files with valid formatting to DW.

3. Specific Requirements

3.1 Environment and System Architecture
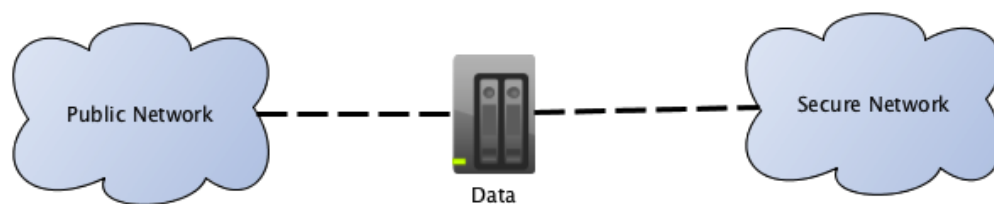
3.1.1 Environment

Figure 3.1

1. Each user in the organization has a computing device, referred to as: "Data Analyzer", connected to the internet. These are used for general activities including data collection. These devices are connected with each other through an intranet, referred to as: "Public Network"
2. The organization hosts multiple computing devices connected through an intranet, referred to as: "Secure Network". This intranet is neither connected to the internet nor to the other (general) computing devices in the organization. The intranet is used for storing sensitive information, investigation reports and digital forensics results.
3. The Secure Network has a central storage, where input and output files could be accessed by any device connected to that intranet.
4. Data is transmitted between the Public and Secure networks through physical storage mediums like USBs, CDs and DVDs.
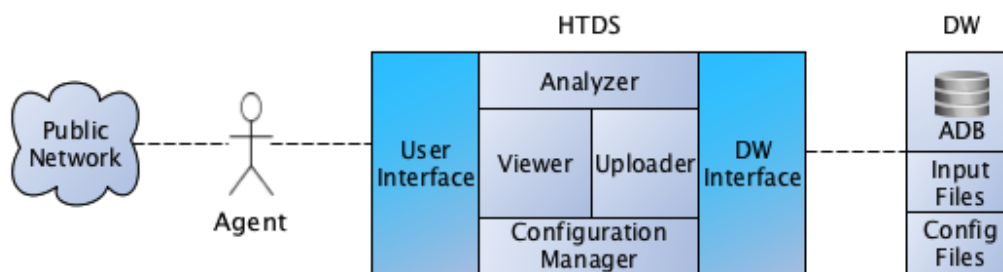
3.1.2 System Architecture

Figure 3.2

The HTDS is composed of four core modules and two interfaces. The first interface is a Graphical User Interface (GUI) to enable communication between the agents and HTDS. The second interface provides communication channels between the DCT's running HTDS and the DW. This interface is invisible to the agents.

The four core components of HTDS are the Analyzer, Viewer, Uploader and Configuration Manager. The analyzer is the module that performs the analysis on input files to generate alerts. The Viewer is the module that provides agents with the capability of reading alerts generated by previous analysis or by other agents. The Uploader module enable agents to upload input files containing raw data for future analysis. The Configuration Manager provides administrators with services to control access to the system and customize the analysis algorithm.

The Data Warehouse (DW) hosts three types of data files: input files, configuration files and the alert database (ADB). The input files are files containing raw data uploaded by the Agents to DW through the Uploader module. The configuration files are stored upon the installation of the system and could be updated by administrators. These files are also accessed by the Analyzer module to retrieve the analysis parameters. The alert database is a single file storing all alerts generated by all agents along with timestamps and event parameters.

3.2 Functional Requirements

3.2.1 Software Features

Each HTDS agent should be able to:
1. Perform detection analysis on input files containing phone number lists
2. Upload input files containing raw data to the DW
3. Generate alerts based on the severity of the analysis results for each input file
4. Keep track of who performed the analysis, at what time, which method and using which input file
5. Share the alerts with other agents within a network
6. Perform All of the above through an accessible graphical user interface (GUI)

Each HTDS system administrator should be able to:
1. add, delete and assign privileges to users.
2. configure the parameters of the Analyzer module
3. configure the settings of the Data Warehouse.
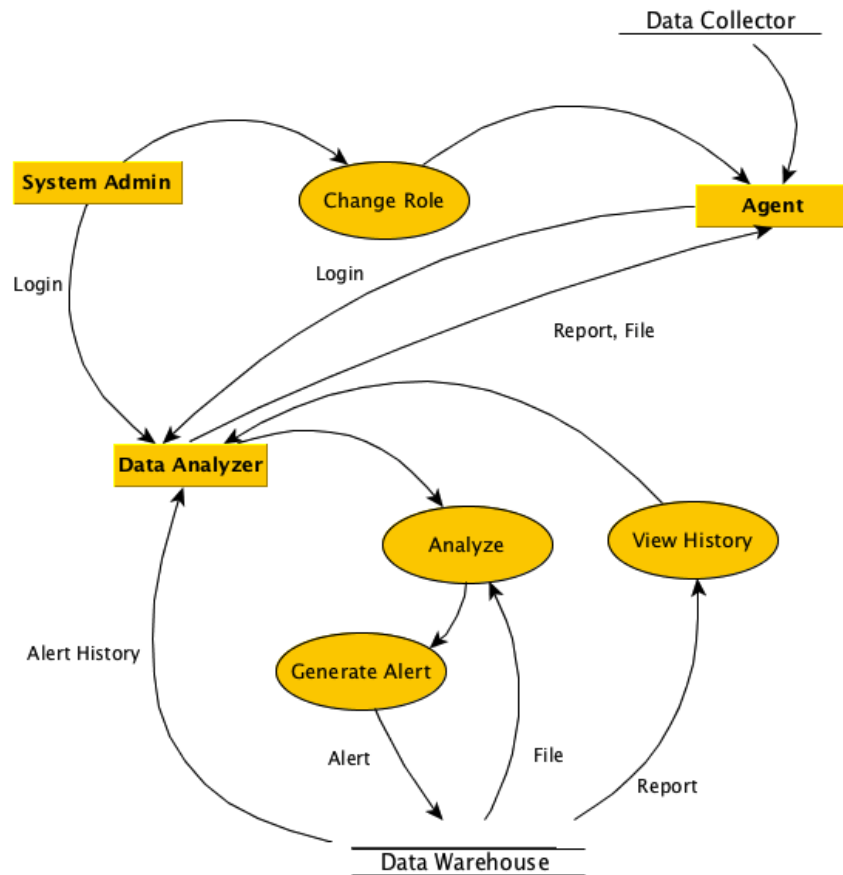
3.2.2 Data Flow Diagrams

Figure 3.3

- System Admin can directly access Data Analyzer by logging in.
- System Admin can act as Agent by changing his/her role.
- Agent login into Data Analyzer system.
- Analyze input files collected from Data Collector.
- Alert messages are generated.
- Alerts generated are saved in Data Warehouse.
- Data Analyzer can retrieve report history from the Data Warehouse.
- Data Analyzer can retrieve history of alerts from the Data Warehouse also.
- Agent can access all reports and files from Data Analyzer.

3.3 Use Cases

Use Case # 1	Login to HTDS
Primary Actor	Agent

Precondition	HTDS is installed and successfully launched
Main Success Scenario	1. HTDS displays login screen 2. Agent enters username 3. Agent enters password 4. HTDS authenticates agent credentials 5. Agent is permitted access to Data Analyzer

Exception Scenarios:	Exception 4a)
	    Agent authentication fails due to invalid username, invalid password, or mismatch between username and password
	Resolution:
	   · HTDS displays an authentication error message
	   · HTDS displays login screen

Use Case # 2	Select a Task
Primary Actor	Agent
Precondition	Agent has logged in

Main Success Scenario	1. HTDS displays main screen with three choices:
	    a. View Alerts
	    b. Upload Files
	    c. Analyze Files
	2. Agent selects a task
	3. HTDS displays the proper task screen

Exception Scenarios	None

Use Case # 3	View Alerts
Primary Actor	Agent
Precondition	Agent has logged in
Main Success Scenario	1. HTDS displays View Alerts screen 2. Agent specifies date range 3. HTDS queries Alert DB at Data Warehouse 4. HTDS retrieves alerts 5. HTDS displays alerts to agent

Exception Scenarios	Exception 2a)
	    Agent specifies invalid dates or invalid date range
	Resolution:
	    HTDS displays "invalid date" error message
	    Agent is requested to enter another date
	
	Exception 3a)
	    HTDS is unable to communicate with Data Warehouse
	Resolution:
	    Display "Communication Failure" error message
	    Return agent to main screen

Use Case # 4	Upload Input Files
Primary Actor	Agent
Precondition	Agent has logged in
Main Success Scenario	1. HTDS displays Upload Files screen 2. Agent specifies location of input file 3. HTDS transfers file from local machine to Data Warehouse 4. HTDS informs user of successful transfer

Exception Scenarios	Exception 2a)
	    agent selects a file incompatible with HTDS
	Resolution:
	    HTDS displays "invalid input file" error message
	
	Exception 3a)
	    HTDS is unable to communicate with Data Warehouse or unable to transfer file
	Resolution:
	    Display "Communication Failure" error message
	    Return agent to main screen

Use Case # 5	Analyze Input File
Primary Actor	Agent

Precondition	Agent has logged in
Main Success Scenario	1. HTDS displays "Analyze Files" screen 2. Agent selects a file from Data Warehouse 3. HTDS analyzes file 4. HTDS displays alert result 5. HTDS stores alert at alert DB at Data Warehouse

Exception Scenarios	Exception 2a)
	    HTDS unable to load files from Data Warehouse
	Resolution:
	    HTDS displays "communication failure" error message
	    Return Agent to main screen
	
	Exception 5a)
	    HTDS is unable to store alert at Data Warehouse
	Resolution:
	    Display "Communication Failure" error message
	    Return agent to main screen

Use Case # 6	Add Agent
Primary Actor	Administrator
Precondition	Agent has logged in with administrative privileges
Main Success Scenario	1. HTDS displays "Configuration" screen 2. Administrator selects "Add User" task 3. Administrator enters agent username 4. Administrator enters agent password 5. Administrator specifies agent privileges 6. HTDS updates user profiles at Datawarehouse 7. New agent successfully added to HTDS

Exception Scenarios	Exception 3a)
	    Username already exist in HTDS
	Resolution:
	    HTDS requests choosing another username
	
	Exception 6a)
	    HTDS is unable to load/update user profile file at Data warehouse

	Resolution:
	    Display "Communication Failure" error message
	    Return agent to main screen

Use Case # 7	Configure Data Warehouse
Primary Actor	Administrator
Precondition	Agent has logged in with administrative privileges

Main Success Scenario	1. HTDS displays "Configuration Screen"
	2. Administrator selects "Data Warehouse Configuration"
	3. Administrator performs one of the following:
	    a. Update default location for storing input files
	    b. Update location for storing alert DB
	    c. Update location of HTDS configuration files
	4. HTDS successfully updates the proper configuration file

Exception Scenarios	Exception 4a)
	    HTDS fails to update configuration files
	Resolution:
	    Display "Communication Failure" error message
	    Return agent to main screen

Use Case # 8	Configure Analysis Algorithm
Primary Actor	Administrator
Precondition	Agent has logged in with administrative privileges
Main Success Scenario	1. HTDS displays "Configuration" screen 2. Administrator sets/updates parameters for analysis algorithm 3. HTDS successfully updates configuration files
Exception Scenarios	Exception 3a) HTDS fails to update configuration files

	Resolution:
	    Display "Communication Failure" error message
	    Return agent to main screen

3.4 Non-functional Requirements

3.4.1 Performance

To find how many times a phone number occurs in a phone list provided by the agent, HTDS needs to invoke two algorithms: one to sort the list and one to perform the counting. Poor selection and/or implementation of these algorithms is known to cause critical underperformance of the system. It is expected that HTDS should perform at least as well as the average case scenario of these algorithms.

3.4.2 Security

Both the System Administrator and Agent will be able to log into the HTDS. The System Administrator will have access the Data Analyzer and the Data Warehouse, and will be able to configure the Data Warehouse as well. The Agent will have access to the Data Analyzer and will be able to retrieve files from Data Warehouse, but not configure it. Access to the HTDS will be protected by a user login screen that requires a username and password. The system should provide mechanisms for resetting and recovering passwords.

3.4.3 Availability

The availability of HTDS depends on the reliability of the secured network and the availability of the Data Warehouse (DW).

3.5 Design Constraints

3.5.1 Time Constraints

The development cycle of HTDS is confined by the following deadlines:

Jan 30	Project Proposal
Feb 13	Requirements analysis Document
Feb 27	Architecture diagram and object models
March 13	Revised object models and activity models
March 27	Class models
April 10	Integration and test plans

April 24	User and software manuals, implementations, sample I/O from test cases, and discussion.
May 8	Final project presentations and demo Demonstration.

Table 3.1: Deadlines

3.5.2 Prototype constraints

The prototype will not be simulated on actual Public/Secure Network architecture. Without affecting the functionality of the system, testing and product demonstration will be performed on a local machine. Furthermore, with the absence of actual data sets, the system will be tested on phone lists designed to demonstrate the system functionalities.

3.5.3 Hardware and software Constraints

The HTDS should run on any computing device with basic hardware requirements. Computing devices hosting HTDS should have the following software installed: Java, MySQL and a text editor.
The Data Warehouse (DW) should have enough storage space to host all files associated with HTDS.

3.5.4 Development Constraints

The HTDS shall be implemented in Java to support portability. The poor stability in Java Development Kit (JDK) is one potential development constraint. The database will be implemented using SQL.

3.6 System Evolution

Regardless of the communication identification method, HTDS functionalities should not be affected by the introduction of new technologies. Instead of phone numbers, IPs or alternative device identification could be used.

4. Change Management Process

As changes are made to the SRS, the table on the first page of the document will be updated. This table will keep track of the version number, the date of the modification, the sections modified and a short description. Anyone is able to submit changes to the SRS, but all changes must be approved by the Team Manager before they are accepted. The Team Manager will then notify the Dropbox Manager of the acceptance, and the Dropbox Manager will upload the new version of the SRS.