# Problem this is one of the problem

Literature, Russian Literature

Problem Context Forensic investigator faces many problems of gettinglive windows analysis information.

The main reason is the use of traditionalway of getting information by unplugging the power to a computer and thenacquiring a bit-stream image of the system hard drive through a write blocker. Forexample, investigator face servers that are used for business operation such ase-commerce continues to grow and cannot be shut down because shutting down theirservers is measured in hundreds or thousands of dollars per minute. Therefore, shutting down a system and acquiring information was not an option and this isone of the problem where investigator cannot investigate. Other example is whenmalicious software program gets into a system and steal information such aspassword or sensitive information these type of program usually exist on thememory and when the computer is shut down all the evidence of the maliciousprogram will be disappeared. Nowadays the number of size of the hard drive isgetting bigger and bigger and usually it will take four to eight hours for acomplete hard drive image of a 80GB.

Imagine how long it will take to image ahard drive of 1TB or 2TB or even 10TB? That’s a lot of time. What if theinvestigator only wants the activities of the process and not the whole imageof the hard drive? Investigator use the traditional waybecause there is no open source software which can analysis windows live. Itmakes them to spend more time getting information manually by using commandprompt (CMD), task manager, services and etc. After getting that informationthey need to save and preserve it and this may take hours or even days for themto get a complete information.

Sometimes the information they want might bealter or disappear within a second. So, getting a complete and full informationis not 100% accurate and might miss some important evidence. Rationale Live Windows Analysis System is anindividual software which allow user (Forensic Investigator or First Responder)to analysis windows live without shutting down the system and getting all theimportant information.

This software will collect information about the systemwhile it is still running. Information about process, network connection, listof dlls, and etc will be collected by the software. By using this software, itis the only way of getting information before it disappears when the system isshut down. This software will definitely reduce the time consuming, more userfriendly which allow user to understand and use it well, and faster datagathering.

There a two type of benefits tangible and intangible: Tangible· Save moretime. As this software can gather information faster and user don’t need to waitlonger and spend more time searching for the evidence. · Reduceworkload of user. Investigator don’t need to use the traditional way of gatheringinformation by unplugging the plug of a system. Intangible· Decreasethe rate of missing important evidence as this software is used while thesystem still running.· Much moreconvenience for user to use because the software is user-friendly and easy togenerate report. Nature of Challenge Java Object-Oriented Programming will be the challengethroughout my project. I need to make sure that the software runs commandprompt (CMD) in an administrator to allow the system to gather informationwithout any error this is because

without running as an administrator thesoftware is not allowed to run few commands which will affect the informationgathering.

Besides that, gathering information of the browser is one of thechallenge in this project because CMD doesn’t not allow to get informationabout the browser such as Google Chrome, Mozilla or etc. Saving the output to usercreated folder using the software is one of the challenge too because theoutput is manually saved to the NetBeans folder and when try to change thedirectory it will access denied. Books 1. Name: Microsoft Access 2013: Programming byExample with Vba, XML, and ASPAuthor: Julitta Korol Publisher: Mercury Learning & Information 2. Name: Intro to JavaProgramming, Comprehensive Version, Global Edition Author: Y. Daniel Liang Publisher: Pearson Education Limited 3.

Name: Learn Java in OneDay and Learn It Well Author: Jamie Chan Publisher: Createspace Independent Publishing Platform 4. Name: Learning Java Author: Patrick Niemeyer Publisher: O’Reilly Media, Inc, USA 5. Name: Learn Java The EasyWay: A Hands-On Introduction to Programming Author: Bryson Payne Publisher: No Starch Press, US 6. Name: Microsoft OfficeAccess 2007 All-in-one Desk Reference For Dummies Author: Alan Simpson, Margaret LevineYoung, Alison Barrows, April Wells, Jim McCarter Publisher: John Wiley and Sons Ltd 7. Name: How to Do Everything with Microsoft OfficeAccess 2003 Author: Virginia Andersen Publisher: McGraw-Hill Education-

Europe 8. Name: Microsoft Access2003 Database by Examples

Author: Sheila Ababio Publisher: Authorhouse