

## 창의코딩 스마트앱 프로젝트 기획서

학과	글로벌학부 정보법과학전공	앱 이름	Mobile Forensic Tool
학번	20166405 20146425	카테고리	<p style="text-align: center;">솔루션</p> <p>(ex : 게임, 학습, 도구, 건강, 스포츠, 기타 등)</p>
이름	박성미 정연석		

### 개발 배경 및 목적

디지털 포렌식, 전자적 감식 과정은 워크스테이션에 연결하여 작업을 시작하는 것이 일반적입니다. 그러나 이런 포렌식 과정은 기초적으로 주기억장치 및 보조기억장치의 본을 뜨는 이미지화를 거치고 별도의 분석 과정을 거쳐야 하는 것을 기본으로 하는데, 특히나 법정과 연관된 경우 이 과정에서 포렌식 소스를 추출해내는 동안 무결성(Integrity)에 대한 보증이 필요하고 이에 높은 주의가 필요함에 따라 포렌식 실무자의 업무 피로도가 상당히 높아지는 단점이 있습니다.

따라서, 기기의 정보를 변화시키지 않는 한에서 기초적인 기기의 정보와 더불어 디스크, 네트워크에 대한 간결한 분석을 통해 단순 작업의 자동화를 야기하고 실무자의 피로도를 줄이는데 일조할 수 있습니다.

### 특징 및 주요 기능

특징	직관적인 UI로 구성되어 사용자로 하여금 손쉬운 사전 포렌식을 할 수 있도록 도와주는 애플리케이션입니다. 루트 기능 체크를 비롯하여 간단한 포렌식 보안 점검 및 포렌식 기능을 제공하고 있으며, 각각 기능 활용시 결과를 추출해낼 수 있는 기능과 최종 보고서 작성 기능을 제공할 예정입니다.
----	--

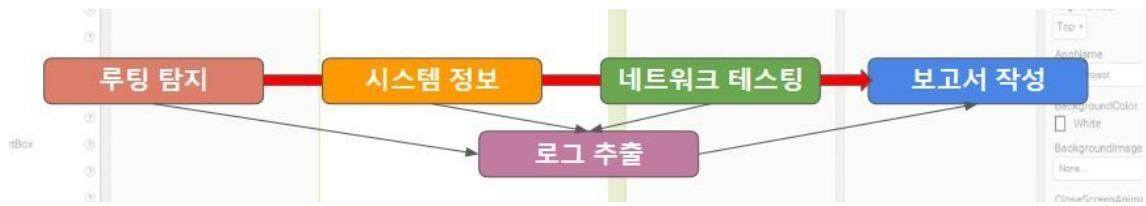
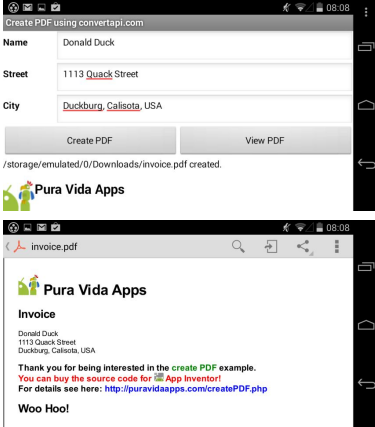
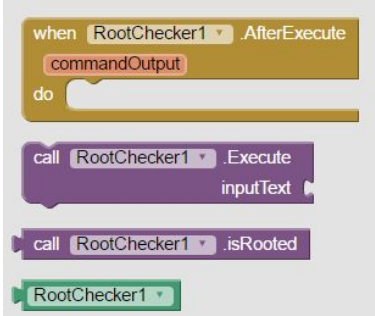
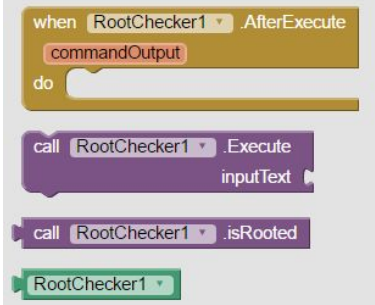
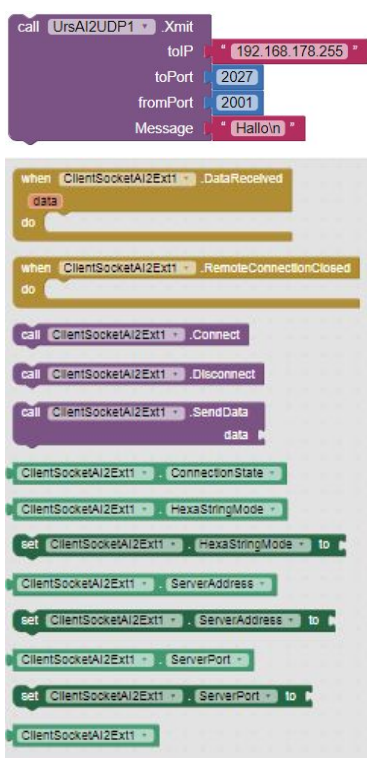
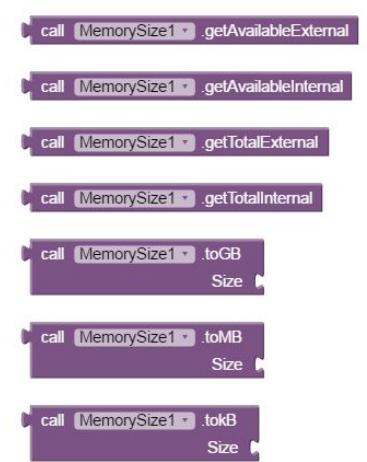



그림1. 기능 프로세스

표1. 각 기능에 맞는 확장 리소스 및 설명

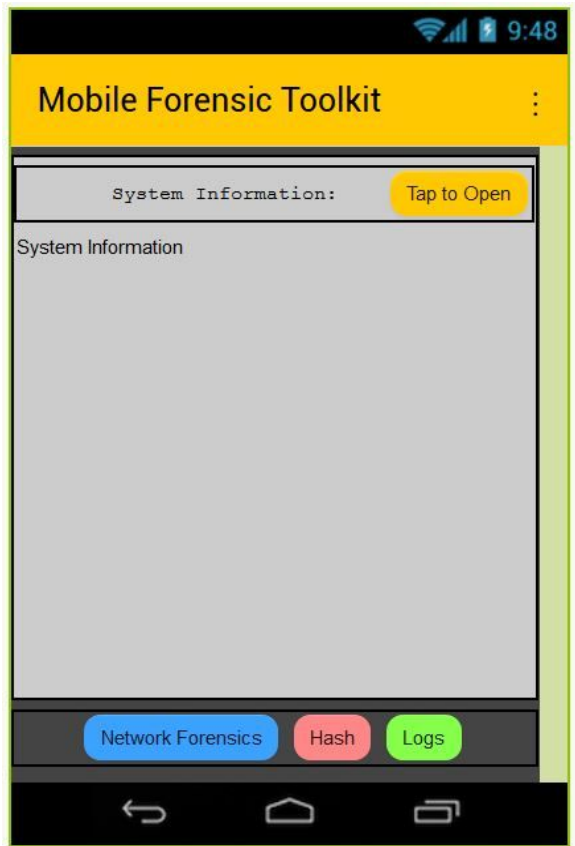
주요  
기능

기능	익스텐션	설명
요약 레포트 작성	<a href="https://puravidaapps.com/createPDF.php">https://puravidaapps.com/createPDF.php</a>	 
루팅 감지	<a href="https://community.thunkable.com/t/free-root-checker-extension/1587">https://community.thunkable.com/t/free-root-checker-extension/1587</a>	

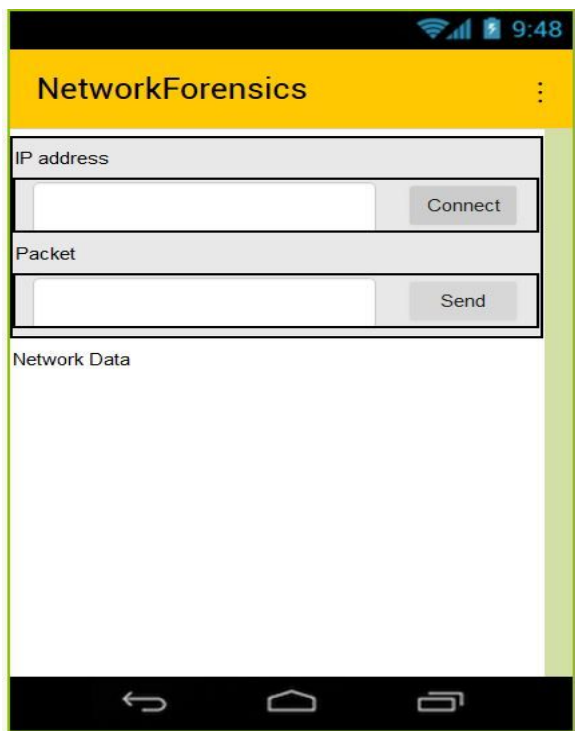
<p>네트워크 패킷 인터페이스 캡처</p>	<p>및 <a href="https://groups.google.com/forum/#!category-topic/mitappinventortest/app-inventor-extensions/OCzEzC4FpEU">https://groups.google.com/forum/#!category-topic/mitappinventortest/app-inventor-extensions/OCzEzC4FpEU</a></p> <p><a href="http://bienonline.magix.net/public/android-AI2-UDP.html">http://bienonline.magix.net/public/android-AI2-UDP.html</a></p>	 <p>The code block shows a sequence of actions for a Scratch project. It starts with a 'call' block for 'UrsAI2UDP1' with parameters: 'Xmit', 'toIP' (192.168.178.255), 'toPort' (2027), 'fromPort' (2001), and 'Message' ('Holloin'). This is followed by a 'when' block for 'ClientSocketAI2Ext1' with the condition '.DataReceived' and a 'do' block. Then, another 'when' block for 'ClientSocketAI2Ext1' with the condition '.RemoteConnectionClosed' and a 'do' block. The sequence continues with several 'call' blocks for 'ClientSocketAI2Ext1': '.Connect', '.Disconnect', and '.SendData' (with a 'data' input). This is followed by a series of 'set' blocks for 'ClientSocketAI2Ext1' properties: '.ConnectionState', '.HexStringMode', '.ServerAddress', and '.ServerPort', each followed by a 'to' block. The final block is a 'call' block for 'ClientSocketAI2Ext1'.</p>
<p>시스템 정보 요약 (HW, Network, Kernel Version, API Version, Host Name,. etc)</p>	<p><a href="https://community.appybuilder.com/t/memoryinfo-extension/1897?u=taifun">https://community.appybuilder.com/t/memoryinfo-extension/1897?u=taifun</a></p> <p><a href="https://community.thunkable.com/t/memory-size-extension-21-05-2017/3764?u=taifun">https://community.thunkable.com/t/memory-size-extension-21-05-2017/3764?u=taifun</a></p>	 <p>The code block shows a series of 'call' blocks for 'MemorySize1'. The first four blocks are: '.getAvailableExternal', '.getAvailableInternal', '.getTotalExternal', and '.getTotalInternal'. These are followed by three blocks for converting sizes: '.toGB Size', '.toMB Size', and '.toKB Size'.</p>

	로그 추출	<a href="https://community.thunkable.com/t/logs-extension/6037?u=sander0542">https://community.thunkable.com/t/logs-extension/6037?u=sander0542</a>	
	파일 검색 및 선택	<a href="https://puravidaapps.com/pick.php">https://puravidaapps.com/pick.php</a>	
	해쉬 (MD5, SHA256)	직접 제작 예정	직접 제작 예정
유사 앱	tPacketCapture (패킷 캡처 애플리케이션)		

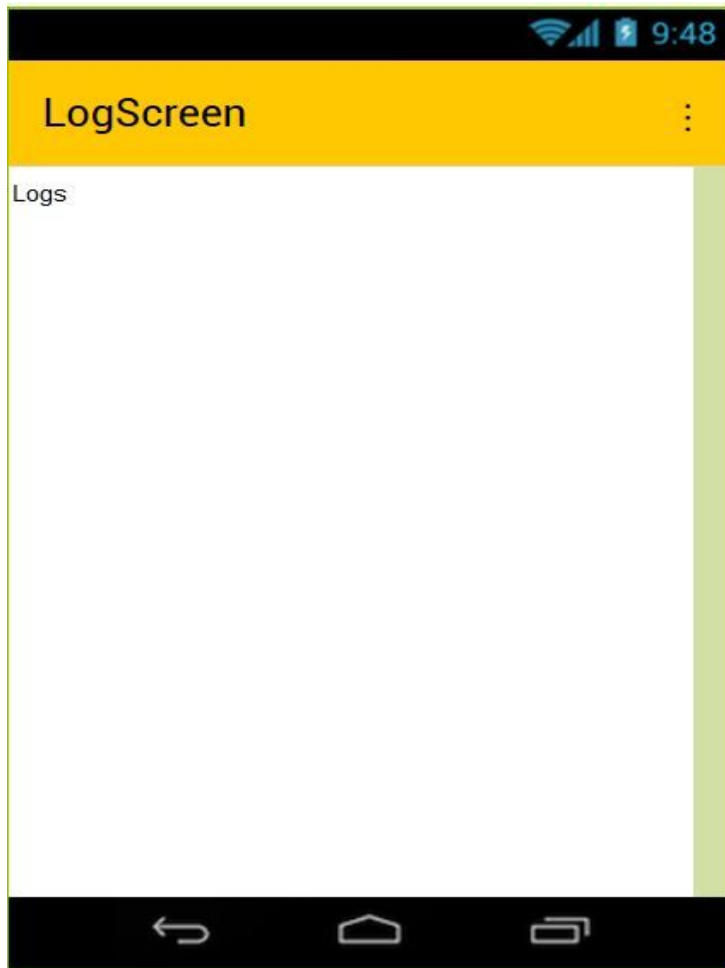
화면  
설계



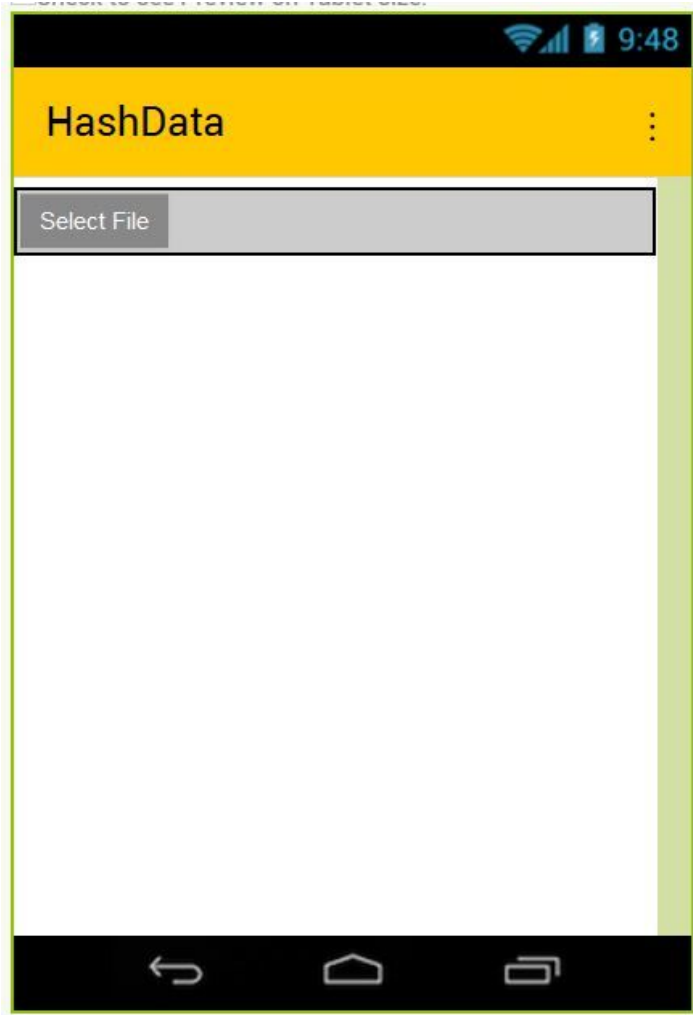
메인스크린 : 기능에 대한 선택 및 기본적인 시스템 정보를 나열합니다.



네트워크 분석 : 특정 아이피에 대한 접속 시도, 아이피 대역에 대한 호스트 및 포트 스캐닝, 패킷 센터를 비롯하여 접속되어있는 AP나 인터페이스와 같은 네트워크 정보를 보여줍니다.



로그 : 시스템 로그를 보여주며, 확장 기능을 이용하여 ADB 로그 수준으로 정확한 로그를 출력 및 추출해낼 수 있는 기능입니다.



해시 계산 기능 : 파일의 무결성을 체크하는 기능으로, 파일 하나를 불러들여 해쉬값을 계산하는 기능입니다.

--	--



