

“Finding Digital Evidence, Information”

Digital Forensic [Computer & Network & Server & Database Forensic]
Mobile / Smart Phone Forensic [iPhone & Android Forensic]

Product

Education

Certification

JOESandbox Desktop

JOESandbox X

JOESandbox Complete

JOESandbox Ultimate

JOESecurity



- Mac OS X 샌드박스
- Windows 샌드박스
- Android 샌드박스
- 통합 플랫폼 샌드박스

악성코드 자동화 분석 / 정밀분석 / 모바일 악성코드 분석

Joe Security 국내 총판

Joe Sandbox for Malware

[Mac OS X / Windows / Android **통합 플랫폼**]

(주) 인섹시큐리티 김종광 대표이사

[디지털 포렌식 | 침해사고 분석 | 악성코드 분석 | 취약점 진단 | 모의해킹]

(주)인섹시큐리티 악성코드 전문 통합사이트 | <http://www.securitytotal.co.kr>



INSEC SECURITY

JOeSecurity

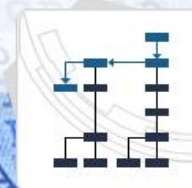
Open and agile malware analysis tools to deeply understand malicious codes



Any Speed



Any File



Any Analysis

www.malwareanalysis.co.kr

악성코드 자동화 정밀 분석 샌드박스



www.malwaresandbox.co.kr

악성코드 자동화 정밀 분석 샌드박스

Joe Security

www.joesecurity.org

전세계 최초! Mac OS X 악성코드 자동화 분석 샌드박스 개발

글로벌 넘버원!
Malware Sandbox!

전세계 최초 [통합 플랫폼 샌드박스] 지원!

▣ Mac OS X 샌드박스

▣ Android 샌드박스

▣ Windows 샌드박스

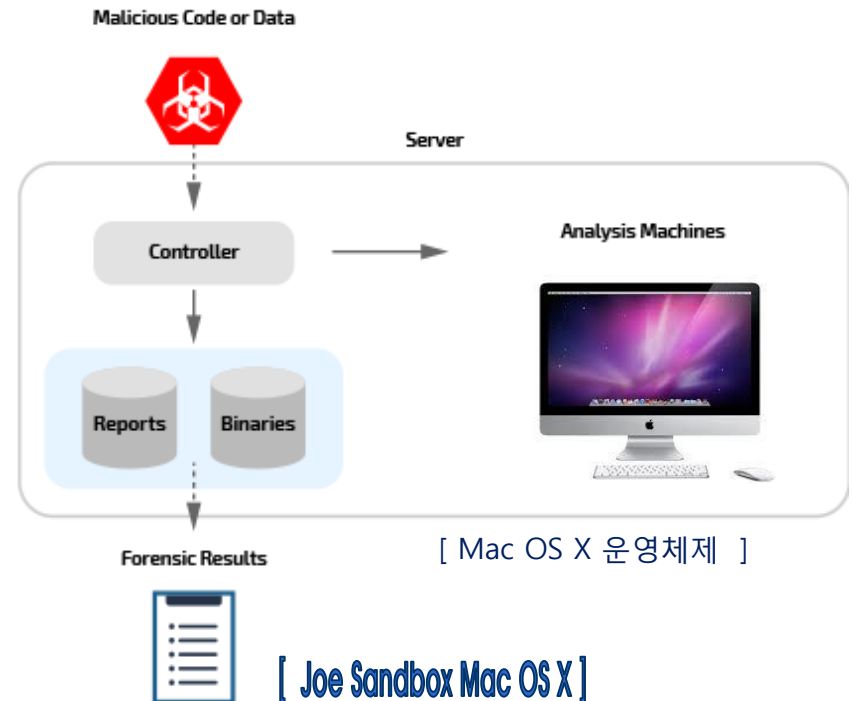
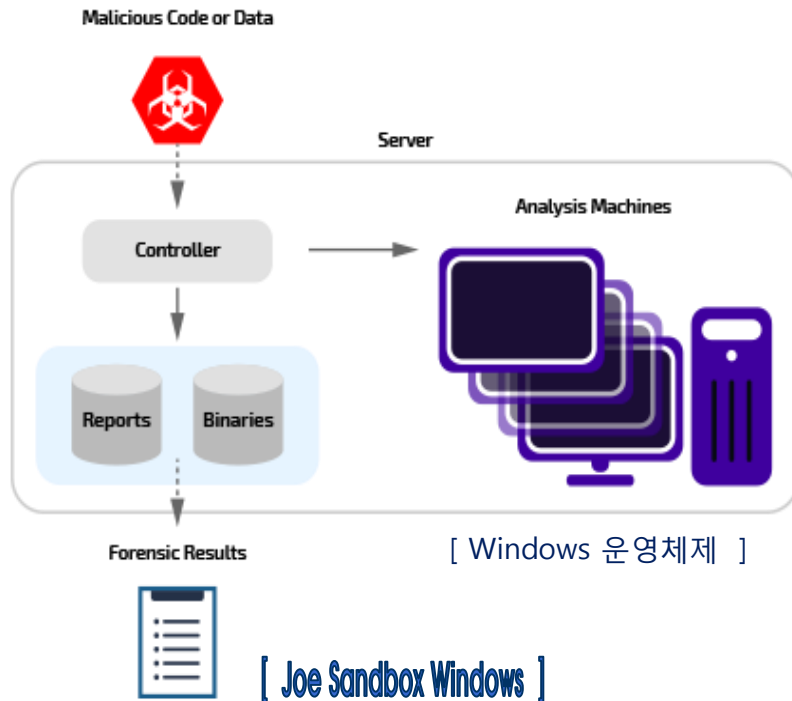
☞ 실행 파일 분석 : <http://www.file-analyzer.net>

☞ 문서 파일 분석 : <http://www.document-analyzer.net>

☞ APK 파일 분석 : <http://www.apk-analyzer.net>

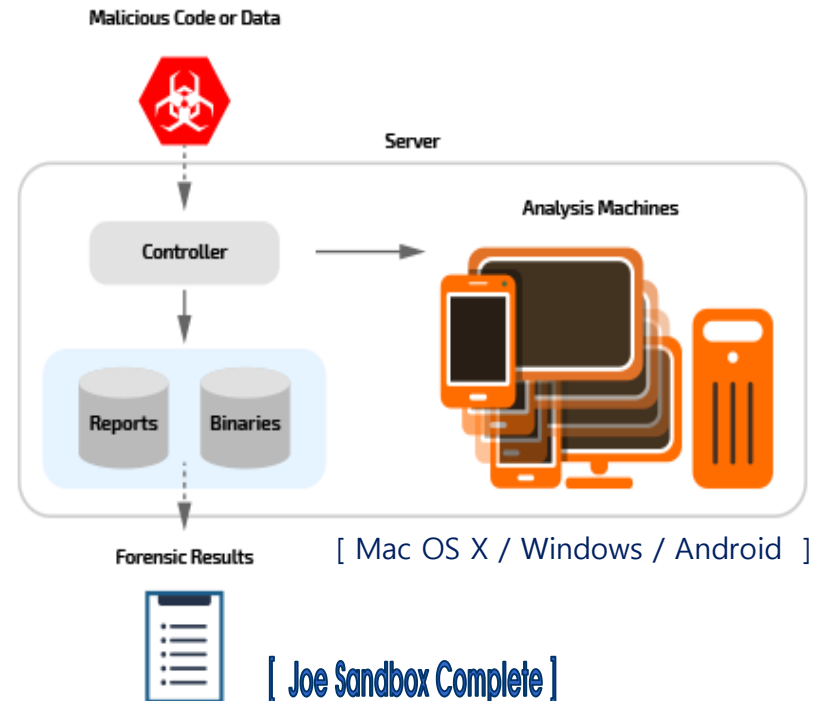
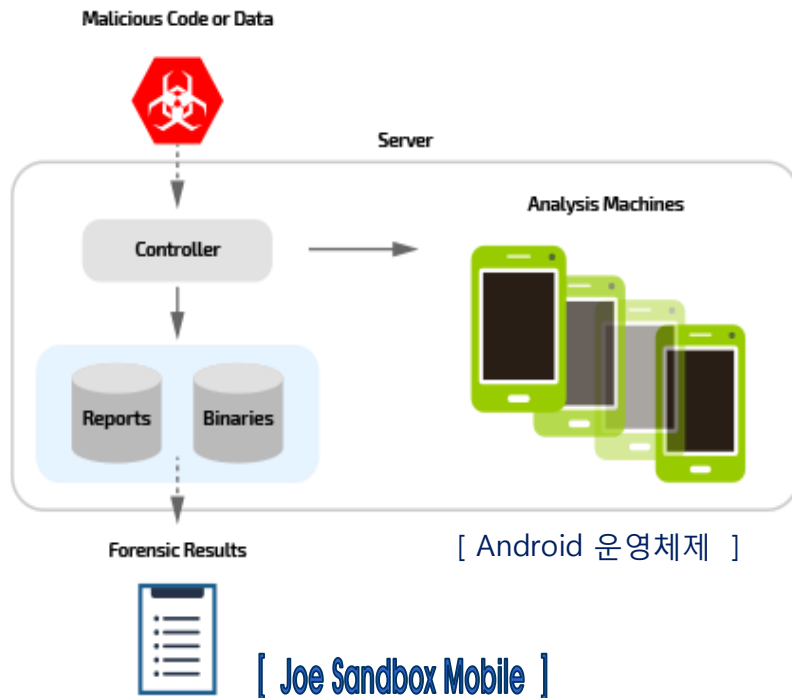
◆ 악성코드 전문 분석 [정밀분석] 샌드박스

■ Joe Security – Joe Sandbox [Mac OS X / Windows / Android 플랫폼]



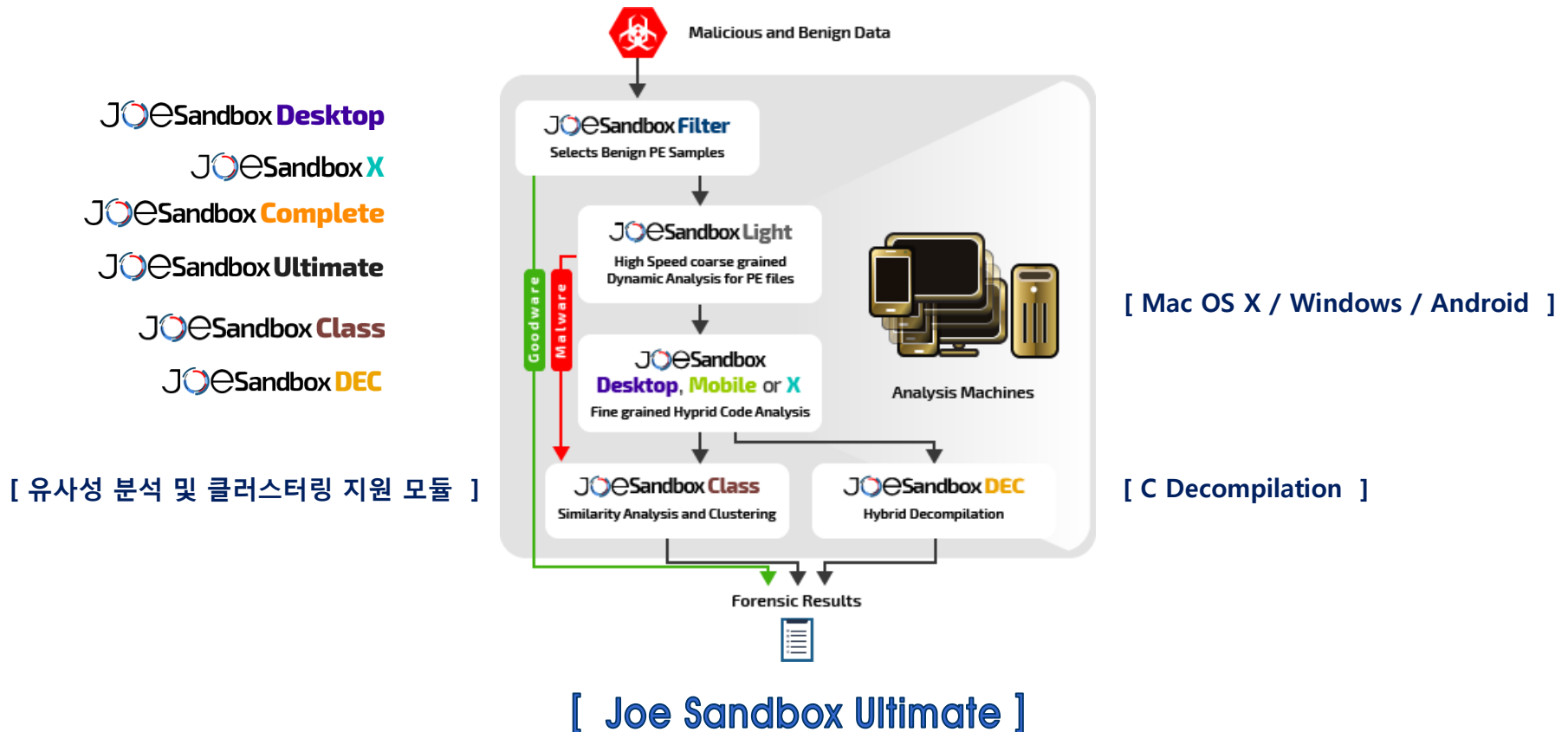
◆ 악성코드 전문 분석 [정밀분석] 샌드박스

■ Joe Security – Joe Sandbox [Mac OS X / Windows / Android 플랫폼]



◆ 악성코드 전문 분석 [정밀분석] 샌드박스

▣ Joe Security – Joe Sandbox [Mac OS X / Windows / Android 플랫폼]



◆ 악성코드 전문 분석 [정밀분석] 샌드박스



품 명	Joe Sandbox Desktop
용 도	Windows 데스크탑용 악성코드 샌드박스
설 명	Windows 운영체제 악성코드 [전문 상세 정밀] 분석

세부기능

- 악성코드 자동화 정밀 분석
- Windows용 실행파일 분석
- Windows x32 on XP, Vista, W7, W8, W10
- Windows x64 on Windows 7
- 모든 PE 파일 분석, 오피스 문서 파일 등 지원
- 950개 이상의 악성코드 행위 패턴 지원
- Browser Plugins, Shellcode 등 분석 지원
- 파일 및 URL 업로드를 통한 악성코드 분석
- 약 5,000개 이상의 파일 타입 지원

- 보고서 제공
[PDF, HTML, JSON, XML, MISP, OpenIOC]
- PCAP 파일 제공, 스크린샷 지원,
- Yara Rules (Editor) 지원, 메모리 덤프 등
- 가상화 우회 기법 포함 악성코드 분석 지원
- 다양한 난독화에 대한 언패킹 수행
- IDA Bridge Plugin 지원
- API, OPEN SDK 지원 및 타 시스템 연동 가능

◆ 악성코드 전문 분석 [정밀분석] 샌드박스

JOESandboxX

품 명	Joe Sandbox X
용 도	Mac OS X 용 악성코드 샌드박스
설 명	Mac 운영체제 악성코드 [전문 상세 정밀] 분석

세부기능

- 악성코드 자동화 정밀 분석
- Mac OS X용 실행파일 분석
- 최신 Mac OS X 버전 지원
- Mach-O, App, DMG, Jar 파일 분석
- 165 개 이상의 악성코드 행위 패턴 지원
- Browser Plugins, Jar, Shellcode 지원
- 파일 및 URL 업로드를 통한 악성코드 분석
- 약 5,000개 이상의 파일 타입 지원

- 보고서 제공
[PDF, HTML, JSON, XML, MISP, OpenIOC]
- PCAP 파일 제공, 스크린샷 지원,
- Yara Rules 지원, 메모리 덤프 등
- 가상화 우회 기법 포함 악성코드 분석 지원
- 다양한 난독화에 대한 PE 파일 언패킹 수행
- IDA Bridge Plugin 지원
- API 지원 및 타 시스템 연동 가능

◆ 악성코드 전문 분석 [정밀분석] 샌드박스



품 명	Joe Sandbox Mobile
용 도	안드로이드 악성코드 샌드박스
설 명	안드로이드 운영체제 악성코드 [전문 상세 정밀] 분석

세부기능

- 악성코드 자동화 정밀 분석
- 모바일 안드로이드 용 APK 실행파일 분석
- Java / Android API Call 분석
- 203개 이상의 행위 시그니처 분석 지원
- APK 파일 분석
- URL를 통한 악성코드 분석
- Virtual Machine 또는 실제 물리적 폰 혼합 사용
 - ➔ 가상화 머신 탐지 악성코드 분석

- 보고서 제공
[PDF, HTML, JSON, XML, MISP, OpenIOC]
- PCAP 파일 제공, 스크린샷 지원,
- Yara Rules 지원, 메모리 덤프 등
- 가상화 우회 기법 포함 악성코드 분석 지원
- 다양한 난독화에 대한 PE 파일 언패킹 수행
- IDA Bridge Plugin 지원
- API 지원 및 타 시스템 연동 가능

◆ 악성코드 전문 분석 [정밀분석] 샌드박스



품 명	Joe Sandbox Complete
용 도	Windows / Mac OS X / Android 악성코드 샌드박스
설 명	멀티 운영체제 악성코드 [전문 상세 정밀] 분석

세부기능

- 악성코드 자동화 정밀 분석
- Windows, Mac OS X, Android 실행파일 분석
- Windows x32 on XP, Vista, W7, W8, W10
- Windows x64 on Windows 7
- 모든 PE 파일 분석, 오피스 문서 파일 등 지원
- 950개 이상의 악성코드 행위 패턴 지원
- Browser Plugins, Jar, Shellcode 지원
- URL를 통한 악성코드 분석
- 약 5,000개 이상의 파일 타입 지원

- 보고서 제공
[PDF, HTML, JSON, XML, MISP, OpenIOC]
- PCAP 파일 제공, 스크린샷 지원,
- Yara Rules 지원, 메모리 덤프 등
- 가상화 우회 기법 포함 악성코드 분석 지원
- 다양한 난독화에 대한 PE 파일 언패킹 수행
- IDA Bridge Plugin 지원
- API 지원 및 타 시스템 연동 가능

◆ 악성코드 전문 분석 [정밀분석] 샌드박스

JOeSandbox Ultimate

품 명	Joe Sandbox Ultimate
용 도	Windows / Mac OS X / Android / Class / Filter 악성코드 샌드박스
설 명	멀티 운영체제 악성코드 [전문 상세 정밀] 분석

세부기능

- 악성코드 자동화 정밀 분석
- Windows, Mac OS X, Android 실행파일 분석
- Windows x32 on XP, Vista, W7, W8, W10
- Windows x64 on Windows 7
- 모든 PE 파일 분석, 오피스 문서 파일 등 지원
- 950개 이상의 악성코드 행위 패턴 지원
- Browser Plugins, Jar, Shellcode 지원
- URL를 통한 악성코드 분석
- 약 5,000개 이상의 파일 타입 지원

- 보고서 제공
[PDF, HTML, JSON, XML, MISP, OpenIOC]
- PCAP 파일 제공, 스크린샷 지원,
- Yara Rules 지원, 메모리 덤프 등
- 가상화 우회 기법 포함 악성코드 분석 지원
- 다양한 난독화에 대한 PE 파일 언패킹 수행
- IDA Bridge Plugin 지원
- API 지원 및 타 시스템 연동 가능
- C code Decompilation 기능 지원