

# AMP for Endpoints에서 오탐 파일 분석 트러블슈팅

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[AMP for Endpoints에서 오탐 파일 분석 트러블슈팅](#)

[파일 SHA 256 해시](#)

[파일 샘플 복사본](#)

[AMP 콘솔에서 알림 이벤트 캡처](#)

[AMP 콘솔에서 이벤트 세부 정보 캡처](#)

[파일 정보](#)

[설명](#)

[정보 제공](#)

[결론](#)

## 소개

이 문서에서는 AMP(Advanced Malware Protection) for Endpoints에서 오탐 파일 분석을 수집하는 방법에 대해 설명합니다.

기고자: Jesus Javier Martinez, Cisco TAC 엔지니어

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 주제에 대해 알고 있는 것이 좋습니다.

- AMP 콘솔 대시보드
- 관리자 권한이 있는 계정

### 사용되는 구성 요소

이 문서의 정보는 Cisco AMP for Endpoints 버전 6.X.X 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

# 배경 정보

AMP for Endpoints는 특정 파일/프로세스/SHA(Secure Hash Algorithm) 256에 대해 과도한 알림을 생성할 수 있습니다. 네트워크에 오탐(False Positive) 탐지가 있다고 생각되면 진단 팀이 심층적인 파일 분석을 진행할 수 있습니다. Cisco TAC에 문의할 때 다음 정보를 제공해야 합니다.

- 파일 SHA 256 해시
- 파일 샘플 사본
- AMP 콘솔에서 경고 이벤트 캡처
- AMP 콘솔에서 이벤트 세부 정보 캡처
- 파일에 대한 정보(파일의 출처 및 환경에 있어야 하는 이유)
- 파일/프로세스가 오탐이 될 수 있다고 생각하는 이유 설명

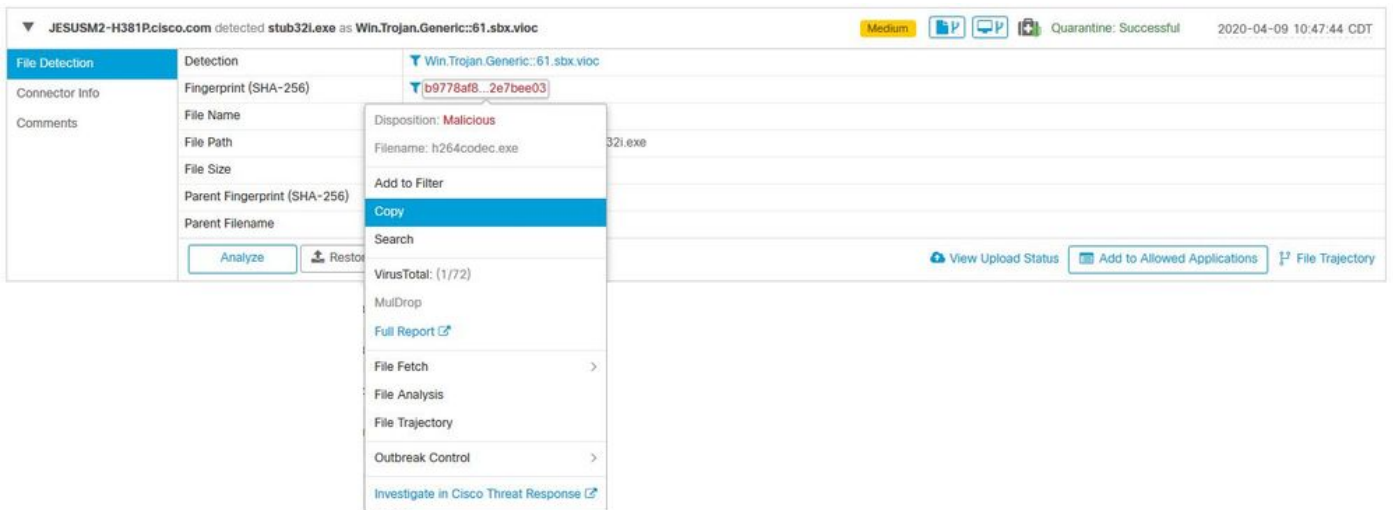
## AMP for Endpoints에서 오탐 파일 분석 트러블슈팅

이 섹션에서는 Cisco TAC에서 오탐(False Positive) 티켓을 여는 데 필요한 모든 세부 정보를 얻는 데 사용할 수 있는 정보를 제공합니다.

### 파일 SHA 256 해시

1단계. SHA 256 해시를 가져오려면 **AMP Console > Dashboard > Events**로 이동합니다.

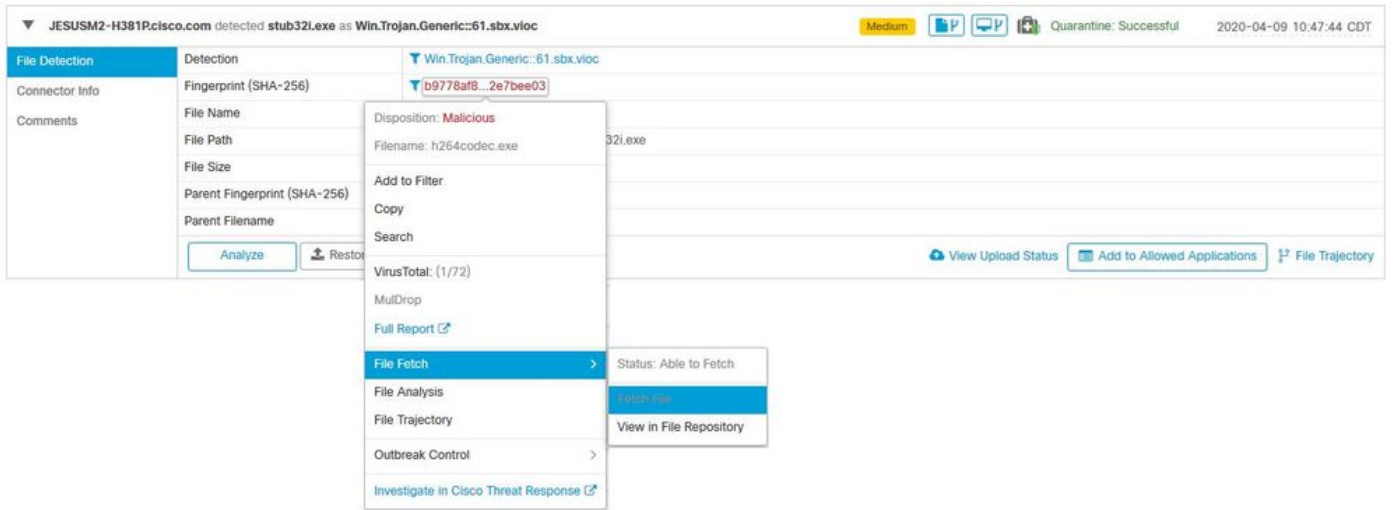
2단계. **Alert Event**(경고 이벤트)를 선택하고 **SHA256**을 클릭한 다음 이미지에 표시된 대로 **Copy**(복사)를 선택합니다.



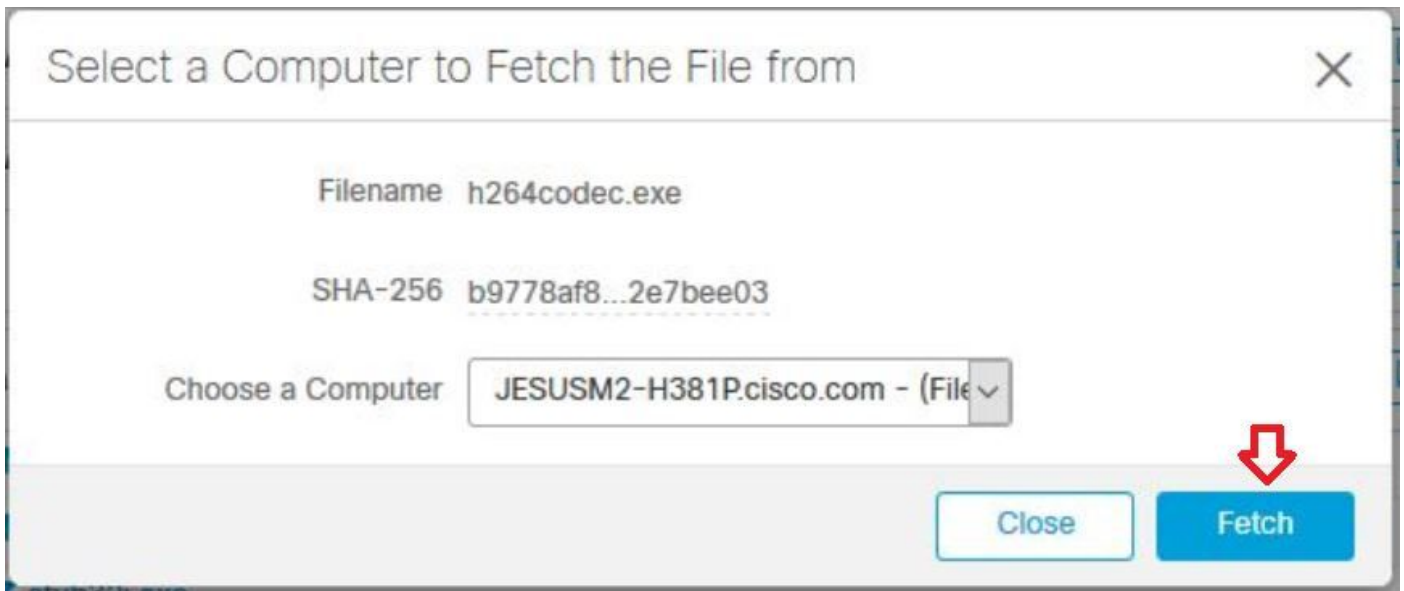
### 파일 샘플 복사본

1단계. AMP Console에서 파일 샘플을 가져오고, **AMP Console > Dashboard > Events**(대시보드)로 이동합니다.

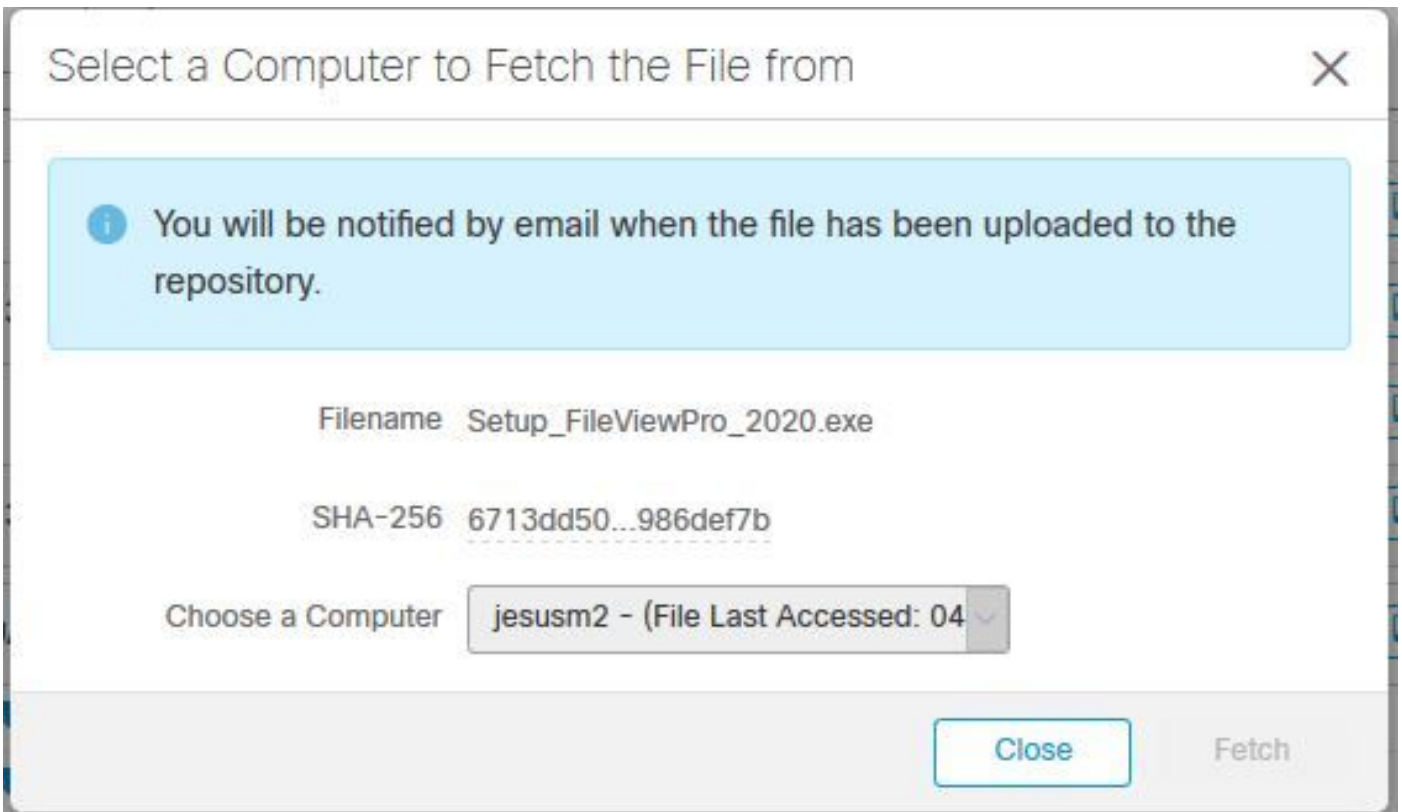
2단계. **Alert Event**를 선택하고 **SHA256**을 클릭한 다음 이미지에 표시된 대로 **File Fetch**(파일 가져오기) > **File Fetch**(파일 가져오기)로 이동합니다.



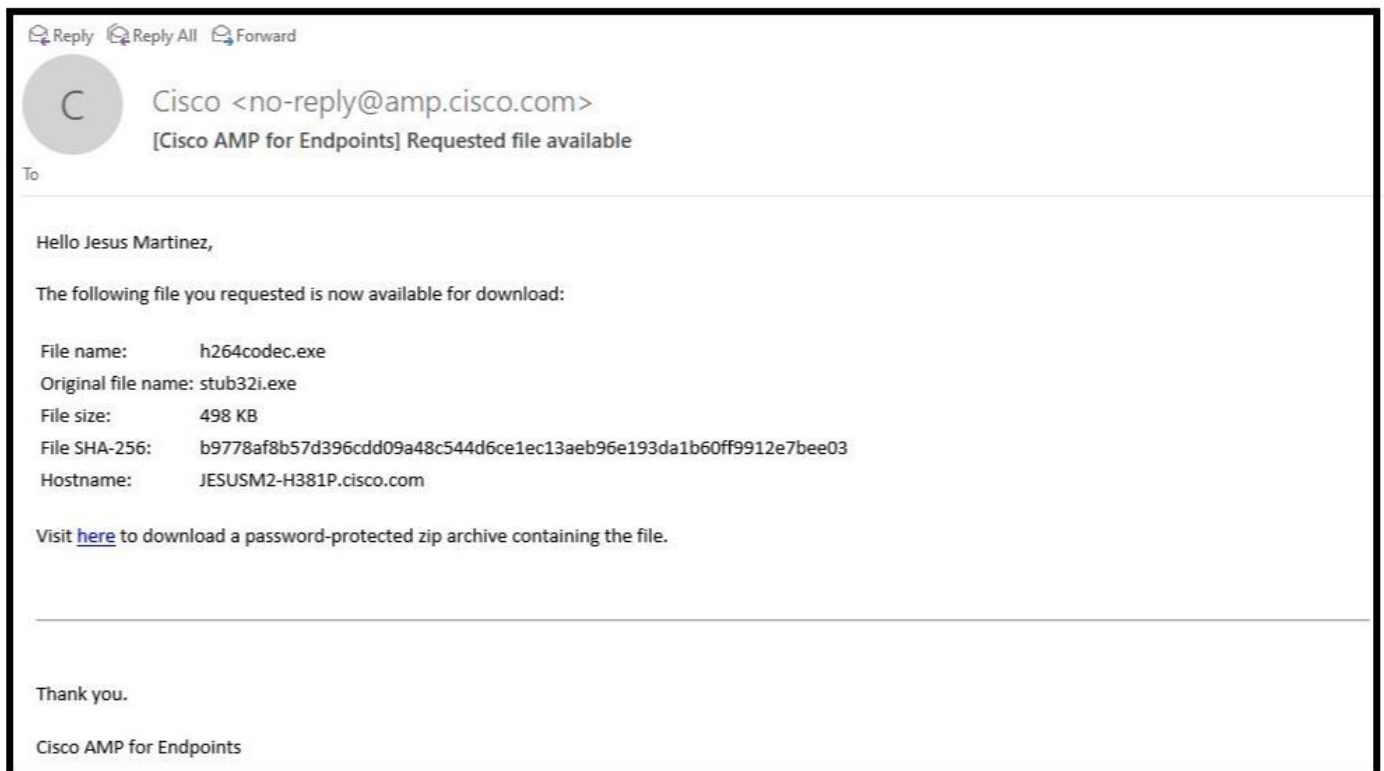
3단계. 파일이 탐지된 디바이스를 선택하고 이미지에 표시된 대로 **Fetch(가져오기)**를 클릭합니다 (디바이스가 **ON**으로 설정되어야 함).



4단계. 이미지에 표시된 메시지를 수신합니다.



몇 분 후에 이미지에 표시된 대로 파일을 다운로드할 수 있는 경우 이메일 알림을 받게 됩니다.



5단계. **AMP Console > Analysis > File Repository**로 이동하여 파일을 선택하고 이미지에 표시된 대로 **Download**를 클릭합니다.

[Connector Diagnostics Feature Overview](#)

Search by SHA-256 or file name...

Status

Group

Type

---

**h264codec.exe is Available** Requested by **Jesus Martinez**   2020-04-16 03:37:42 CDT

Original File Name	stub32i.exe
Fingerprint (SHA-256)	<b>b9778af8...2e7bee03</b>
File Size	498 KB
Computer	JESUSM2-H381P.cisco.com

6단계. 알림 상자가 나타나면 이미지에 표시된 대로 다운로드를 클릭하고 파일이 ZIP 파일에 다운로드됩니다.

**Warning** X

You are about to download **h264codec.exe**

This file may be malicious and cause harm to your computer. You should only download this file to a virtual machine that is not connected to any sensitive resources.

The file has been compressed in zip format with the password: **infected**

## AMP 콘솔에서 알림 이벤트 캡처

1단계. AMP Console > Dashboard > Events로 이동합니다.

2단계. Alert **Event**를 선택하고 이미지에 표시된 대로 캡처를 수행합니다.

JESUSM2-H381P.cisco.com detected stub32i.exe as Win.Trojan.Generic::61.sbx.vloc Medium   Quarantine: Successful 2020-04-09 10:47:44 CDT

<b>File Detection</b>	Detection	Win.Trojan.Generic::61.sbx.vloc
Connector Info	Fingerprint (SHA-256)	b9778af8...2e7bee03
Comments	File Name	stub32i.exe
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe
	File Size	498.49 KB
	Parent Fingerprint (SHA-256)	2fb898ba...7bf74fef
	Parent Filename	7zG.exe

## AMP 콘솔에서 이벤트 세부 정보 캡처

1단계. AMP Console > Dashboard > Events로 이동합니다.

2단계. Alert Event(경고 이벤트를) 선택하고 이미지에 표시된 대로 Device Trajectory(디바이스 전파 흔적 분석) 옵션을 클릭합니다.



File Detection	Detection	Win.Trojan.Generic::61.sbx.vioc
Connector Info	Fingerprint (SHA-256)	b9778af8...2e7bee03
Comments	File Name	stub32i.exe
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe
	File Size	498.49 KB
	Parent Fingerprint (SHA-256)	2fb898ba...7bf74fef
	Parent Filename	7zG.exe

이미지에 표시된 대로 Device Trajectory 세부사항으로 리디렉션됩니다.

Device Trajectory

2 compromise events (spanning less than a ...)

Filters Search Device Trajectory

System

- svchost.exe [PE]
- lsass.exe [PE]
- DigAgent.exe [PE]
- smarterepl.exe [PE]
- ciscoobnhostcf.exe [PE]
- ciscoobnhost.exe [PE]
- wedbar32.zip.part [ZIP]
- hrefax.exe [PE]
- winword.exe [PE]
- 80d9542ab35cc3b5b4... .ink [Link]
- downloads (31) link [Link]
- 5f7bf1f401b3767... automa... [OLE2]
- stub32i.exe [PE]
- 7zG.exe [PE]
- explorer.exe [PE]
- plupdate.exe [PE]
- ptcheck.exe [PE]
- webexapplauncherlatest.exe [PE]
- atmgr.exe [PE]
- webexremote.exe [PE]
- CiscoWebExStart.exe [PE]
- gag-agent.exe [PE]
- gagp.exe [PE]
- scdemon.exe [PE]
- dirmgmt.exe [PE]
- gagp.exe [PE]
- gagp.exe [PE]
- gagp.exe [PE]
- explorer.exe [PE]
- msiexec.exe [PE]
- lenovo.modem.incontrol... .exe [PE]
- Lenovo.Modem.InControl.exe [PE]
- clip\_themedata.thmx [ZPP]
- wuclhst.exe [PE]
- services.exe [PE]
- msbackground.exe [PE]
- sdhshelper.exe [PE]

Event Details

2020-04-09 10:47:43 CDT

Detected **stub32i.exe**, n264codic 4.1.0.0 (b9778af8...2e7bee03) [PE\_Executable] as Win.Trojan.Generic::61.sbx.vioc.

Created by 7zG.exe, 7-Zip 19.00.0 (2fb898ba...7bf74fef) [Unknown] executing as.

The file was quarantined.

Process disposition benign.

File full path: C:\Users\jesusm2\Downloads\stub32i.exe

File SHA-1: 6e05e279e4136e44871b39e3e3e15e2137225.

File MD5: ff4325a7400b4e68e37887e0d11102.

File size: 510450 bytes.

Parent file SHA-1: af22812647e404e015e48eae4903e985250a.

Parent file MD5: 6ab3e795e6bc333125972e907298.

Parent file size: 581632 bytes.

Parent file age: 0 seconds.

Parent process id: 24064.

Detected by the SHA engines.

3단계. 이미지에 표시된 대로 이벤트 세부 정보 상자를 캡처합니다.

**Event Details** ✕

**Medium**

2020-04-09 10:47:43 CDT

Detected **stub32i.exe**, h264codec 4.1.0.0 (b9778af8...2e7bee03)  
[PE\_Executable] as **Win.Trojan.Generic::61.sbx.vioc**.

Created by **7zG.exe**, 7-Zip 19.0.0.0 (2fb898ba...7bf74fef)  
[Unknown] executing as .

The file was **quarantined**.

Process disposition Benign.

---

File full path: C:\Users\jesusm2\Downloads\stub32i.exe

File SHA-1: 6e055a270bdc13dcaa4871b39fac3d15a2137225.

File MD5: f74325a740d0a9cf68e37887ce017102.

File size: 510450 bytes.

Parent file SHA-1: df22612647e9404a515d48ebad490349685250de.


Parent file MD5: 04fb3ae7f05c8bc333125972ba907398.

Parent file size: 581632 bytes.

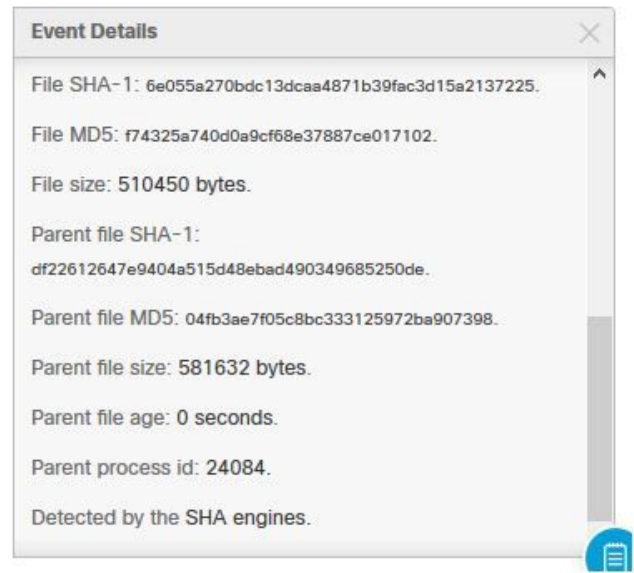
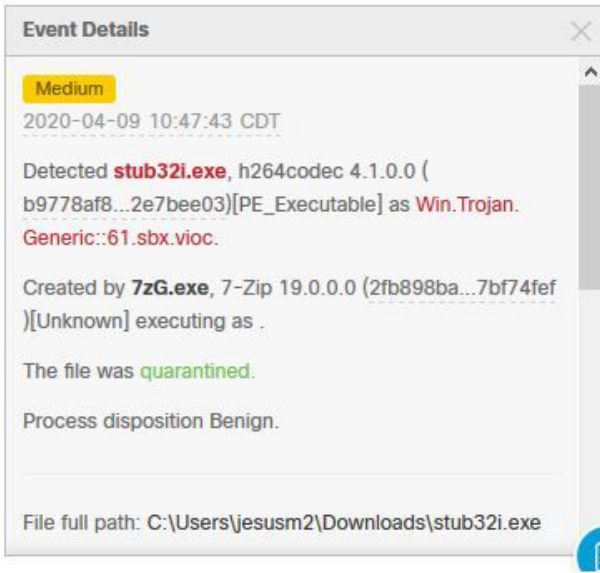
Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.



4단계. 필요한 경우 아래로 스크롤하여 일부 캡처를 수행하여 이미지에 표시된 모든 이벤트 세부 정보를 가져옵니다.



## 파일 정보

- 파일의 출처 정보.
- 파일이 웹 사이트에서 오는 경우 웹 URL을 공유합니다.
- 파일 설명을 공유하고 파일 기능을 설명합니다.

## 설명

- 파일 프로세스가 오탐일 수 있다고 생각하는 이유는 무엇입니까?
- 파일에서 신뢰하는 이유를 공유합니다.

## 정보 제공

- 모든 세부 정보를 수집하면 <https://cway.cisco.com/csc/>에 요청된 모든 정보를 [업로드합니다](#).
- 서비스 요청 번호를 참조하는지 확인합니다.

## 결론

Cisco는 항상 AMP for Endpoints 기술을 위한 위협 인텔리전스를 개선하고 확장하기 위해 노력하지만, AMP for Endpoints 솔루션에서 잘못된 알림을 트리거할 경우, 환경에 더 이상 영향을 미치지 않도록 몇 가지 조치를 취할 수 있습니다. 이 문서에서는 False Positive(오탐) 문제와 관련하여 Cisco TAC에서 케이스를 여는 데 필요한 모든 세부 정보를 얻을 수 있는 지침을 제공합니다. 진단 팀 파일 분석을 기반으로, 파일 속성을 변경하여 AMP Console에서 트리거된 경고 이벤트를 중지하거나 Cisco TAC에서 해당 환경에서 문제 없이 파일/프로세스를 실행할 수 있는 적절한 수정 사항을 제공할 수 있습니다.