**102 – File Wiper**

|  |
| --- |
| **Team Information** |

**Team Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Team Member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Email Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |
| --- |
| **Instructions** |

**Description** While analyzing the suspect's PC, I found that several files had been wiped. I need your help on what tool to use to wipe it.

|  |  |
| --- | --- |
| Target | Hash (MD5) |
| 2023-04-26T042142\_DFC2023-102.7z | DD66FDC3156EBE961CEBF85E223D3B96 |

**Questions**

1. When was File Wiping Tool installed? (UTC+0) (50 points)
2. When was File Wiping Tool run? (UTC+0) (50 points)

Teams must:

* Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
* Specify all tools used in deriving the conclusion(s).

|  |
| --- |
| **Tools used:** |

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | Publisher**:** |  |
| Version: |  | | |
| URL: |  | | |

|  |
| --- |
| **Step-by-step methodology:** |

1. When was File Wiping Tool installed? (UTC+0) (50 points)



압축을 풀면 하드디스크 이미지가 나온다.

텍스트, 스크린샷, 번호, 폰트이(가) 표시된 사진

자동 생성된 설명

D:\C\Windows\appcompat\pca\PcaAppLaunchDic.txt를 확인하였다.

텍스트, 스크린샷, 소프트웨어, 웹 페이지이(가) 표시된 사진

자동 생성된 설명

File Wiping Tool처럼 보이는 Moo0 FileShredder v1.23 Installer.exe 파일을 발견하였다.

\*FileShredder은 회사 파일을 파쇄하는 빠르고 안정적인 도구이다.

**2023-04-26 01:00:32.841** 에 다운로드 되었다.

2. When was File Wiping Tool run? (UTC+0) (50 points)

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

파일이 다운로드 된 후 경로가 변경되었다.

FileShredder.exe 파일을 실행한 시간은 **2023-04-26 04:14:27.974** 이다.

**The deadline for this problem is June 30.**

**Please do not post your write-up before the deadline for fair competition!**

**\* Delete this box when submitting your answer.**