# Technical Summary (TechSum) Template

## Introduction

A Technical Summary provides other operators with the information about a network or a system that is being surveyed. Just like taking a car to the auto-shop, the auto-shop runs diagnostics on the vehicle to find any potential issues. Incident responders or operators will use the same approach when they examine a box or network.

## Example Technical Summary

|  |
| --- |
| **TECHNICAL SUMMARY**   * **Name of Program:** Example: Kaspersky/1 Love You Virus * **Persistence Vector(s):**  Example: Run Key/Program Flies * **Artifacts:** Example: Associated Files/Pieces * **File Hashes:** N/A * **File Sizes/ Time Stamps:** N/A * **Logs:** Example: Logs created/cleaned/removed/modified by the program * **Network Connection(s):** Example: Netstat output * **Recommendation:** Example: After performing extensive analysis and running through the process list, network statistics, checking persistence vectors and surveying the file system, the Windows XP machine in question did not appear to obtain any malware or security related remnants. As an operator, this box appears safe to continue with operations. As an incident responder, the box appears safe enough to remain on the network because it has no evidence of malicious activity.   **Note:** There was no evidence of malware or a security product in the target box, so no information was needed for the Technical Summary other than providing a recommendation/analysis of the findings at the conclusion of the Technical Summary. In this case, the Technical Summary can contain a brief write-up that informs your client how you arrived at your conclusion. |

## Instructions

Complete this form by filling out all applicable fields every time a piece of malware or a security product on the target is identified. Type N/A if the field is not applicable.

|  |
| --- |
| **TECHNICAL SUMMARY**   * **Name of Program:** * **Persistence Vector(s):** * **Artifacts:** * **File Hashes:** * **File Sizes/ Time Stamps:** * **Logs:** * **Network Connection(s):** * **Recommendation:** |