Desktop Triage

USE CASE STUDY

Summary

Desktop Triage is the most-advanced computer forensics field kit. It captures both volatile and non-volatile data on operating Windows, keeping critical information such as USB devices connection log and opened files. It helps law enforcement take a step further towards evidence competency.

To name one of the Desktop Triage use cases in Taiwan:

- Telecommunications Investigation Corps, Criminal Investigation Bureau, National Police Agency

BlockChain Security
Make Digital Evidence Dependable

CASE STUDY:
Collecting Volatile Evidence On-Site

The Client: Telecommunications Investigation Corps (hereinafter TIC) is one of the most important subordinate agencies of the Criminal Investigation Bureau, Taiwan. It is in charge of investigation of major criminal cases, collection of special information, cyber-crime fighting, etc.

Challenge

In the case of digital forensic, information stored on the digital assets has served as strong evidence, including critical data such as emails, messages, network connections, etc. This kind of information comes from the activities on the computers, since to execute any program on the computer, it must be first loaded on the memory, making it critical for forensic to identify attacks or other suspicious activities.

Among this information, volatile data is the trickiest one, having the risk to be lost if the running device shuts down for any reason. TIC officers have thus been struggling to cope with volatile data; while the existing tools are far from being a great help to them.

Solution

To collect volatile data right on site, TIC has opted Desktop Triage as the secret weapon to solve the issue. Desktop Triage possesses features like Screenshot Collection, Screen Recorder, Windows PSR and most importantly Artifacts Collection, granting TIC officers the ability to collect data on the spot when the desktop is already powered on and logged in. It can also be used to preserve chat history and messages presented on the screen, making it easier for the investigator to later map out suspects' social network. With the automation of these features, Desktop Triage can collect all this critical information timely and safely, solving the crux of the collection issue.

Results

With Desktop Triage, volatile information is no longer a stumbling block for TIC officers. Instead, volatile data has greatly assisted the investigation, leading to:

- Reduction in the risks of losing any information or evidence showing on the device's screen.
- Reduction of the investigation cost by having critical evidence preserved during initial response.
- Reduction of artifacts collection time from 4-6 hours to within 1 hour.

"We used to spend days and weeks to find critical data. But with Desktop Triage, we're able to collect volatile evidence right on site within hours, timely and without compromising the quality."

my-triage.com / service@chainsecurity.asia

BlockChain Security