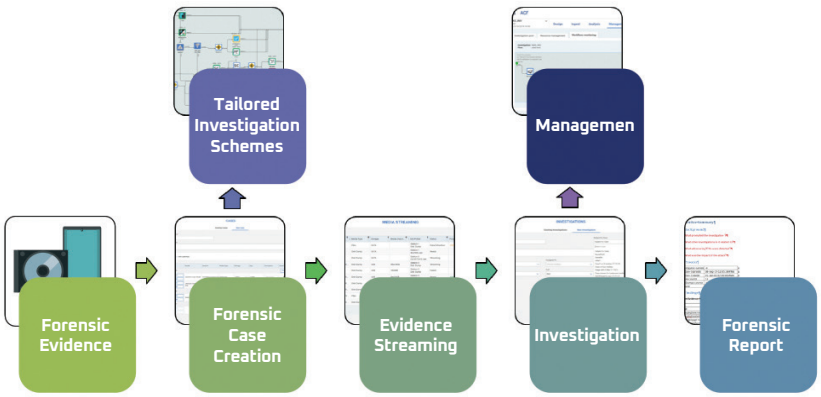

IAI
CyFo
Malware Forensics Platform

CyFo

MALWARE FORENSICS PLATFORM

CyFo is an all-inclusive Malware Forensics Platform that enables investigators to perform the complete malware forensic analysis cycle. The platform is easy to operate and requires very little training and operating knowledge. What once required experienced expertise can now be performed simply and automatically with no need for user interaction. CyFo activates its resources and performs investigations in parallel, optimizing the analysis process. Malware analysis processes are defined with easy to use graphical tools and can be modified internally based on specific requirements. Investigated evidence includes hard drives, file systems, partitions, mount points, volatile memory and firmware dumps based on various operating systems.

SCHEMATIC WORK FLOW:



Media/Mobile Gateway – the complete system image of the suspected device is uploaded to the cyber-secured Media Gateway for regular media devices and Mobile Gateway for mobile devices. Guaranteeing absolute security, the Media Gateway enables streaming data into the system without mounting the source data. The Media Gateway interface supports triage procedures to determine priorities which accelerates the response time to deal with the threat.

System DS - stores safely all the raw data, files, images, workflows, tools, action logs (Chain of Custody), reports, etc.

Case Management System (CMS) – investigations are initiated and set up in the CMS. The investigator defines which investigation workflow will be used on a specific media or on a group of media and files. The stored workflows can be edited and shared between the investigators.

Orchestrator – manages the investigation process. Using simple drag and drop command blocks on a user-friendly GUI, an analyst can simply create complex workflows without writing code. The workflows define the entire forensic process from retrieving the files to generating reports. CyFo includes predefifined workflflows as part of the platform.

Data Analysis Service – based on the workflow, the data – hard disks, memory dump and mobile content - are ingested and automatically analyzed to determine the level of malware threat. Investigators may allow the process to work automatically or intervene during the analysis process. All malware forensic tools operate within a VMware environment, thereby preventing potential contamination and infection from the media's files.

Report Generator – upon completion of an investigation, the platform generates reports to be used internally or as evidence in a court of law.

IAI – ELTA GROUP
WWW.IAI.CO.IL
MARKET@ELTA.CO.IL