C4i
communication

EXPERIENCE THE DIFFERENCE
YOUR SECURITY & SAFETY PRODUCTS

FORENSIC WORKSTATION

C4I-FCW-1

Forensic Workstation
Model: C4I-FCW-1

Description

Forensic Workstation is a high power, great value forensic platform **for all professional forensic investigators**. This Digital Forensic System was designed with today's forensic investigator in mind; it combines a **high-speed multi-core processor** and **ultra-fast memory** with a **high performance SSD** to give you the most performance at a great value. Our all Forensic Systems are user friendly, and support all Windows based forensic platforms.

The Forensic Workstation supports SATA, SAS and Notebook drives. If your department is considering doing digital forensics and you need a lot of power in a tight budget, our forensic workstation is the product for you. Only high end, powerful, energy efficient components have been used in the production of the series.

Our forensic workstation come with forensic bridges, providing full write protect for SAS/SATA, USB and Flash Card. Thunder Forensic Workstation is ideal to do forensic analysis of any type of evidence.

NOTE: Due to the rapid replacement of electronic products, this configuration is only for reference to prevail in kind.

Specification :

- CPU: Intel® Silver 4110 CPU*2
- RAM: 32GB DDR4 2400 ECC Registered
- Hard Disk : 256GB SSD + 4TB*3
- Display: 3* 21"LED
- CD/DVD/BD *1
- Write Protect Bridges：
  - SATA/SAS/USB3.0 Read Only Bridge *1
  - CF/MD/MS/MS Pro/SM/xD/SD/MMC Read Only Adapter *1
  - 3.5" SAS / SATA Read Only hot swap Dock ＊4
  - 3.5" SAS / SATA Read / Write hot swap Dock ＊4
  - 2.5" SAS / SATA Read Only hot swap Dock ＊4
  - 2.5" SAS / SATA Read / Write hot swap Dock ＊4

- OS: Windows7 64Bit
- Preinstall Software: Forensic Guru,   VMF

VMF :

- Boot a forensic image of a suspect's computer.
- Forensically launch a suspect machine in its native environment.
- Experience the 'desktop' as seen by the original user.
- Work from E01 or DD Image.
- Work directly from a physical, write blocked hard drive.

With VMF:

- There is no need to have access to a full Computer Forensics application (such as EnCase) or any additional disk emulation modules.

- There is no need to restore Computer Forensics image files to another PC to try and boot them.

- Either connect the HDD directly through a write blocker or mount the image file and boot it with VMF in seconds!

The latest version of VMF has the following features and functions:

- Bypass any Windows user account password
- Rewind a machine utilising restore point forensics
- Added detection of VMware work station 11 and Player 7
- Added support for parsing partitions on GPT formatted disks
- Added support for PWB routines when using a GPT formatted target disk

VMF has been successfully applied to every Windows version from Windows 95 through to Windows 8.1 along with additional support for MAC OSX, Linux and Sun Solaris.
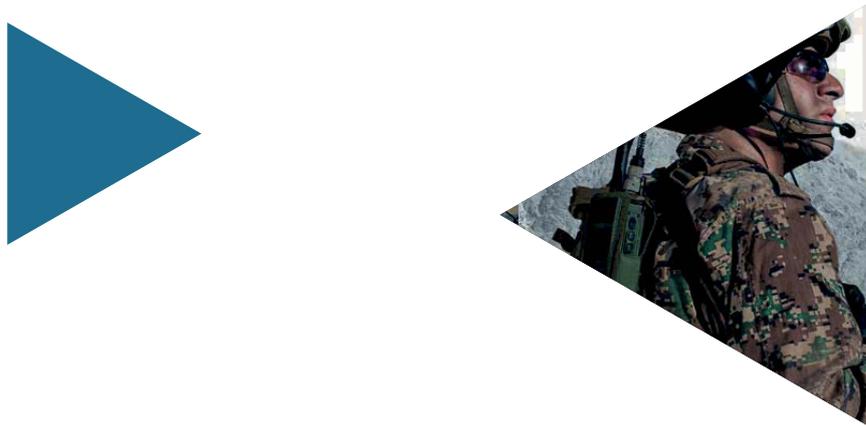
Forensic Guru

A fully functional electronic data evidence acquisition and comprehensive analysis tool. With the combination of many leading enterprise technologies in this industry, it contains many functions including one-step extraction, image loading, smart analysis, data recovery, memory, behavior analysis, correlation analysis, mail, registry, database analysis, custom reports on evidence. Whole functions in one, it is tailor-made for professional users to detect and analyze terabytes huge amounts of electronic data.

► Live extract the chat log of QQ 2016, and acquire the chat history and QQ friends of the user has ever saved his QQ password.

► Internet history analysis. Only in one step can extract the history of network access, cache, download, Cookies etc. and can automatically sort them out by website, time and other conditions. Based on the smart compare with thousands website records in built-in management module, it can generate a report on Internet history .

► Online behavior analysis. The internet, download, chat, E-mail, and file access records can be classified with descriptions and displayed in column, line, form and other diagrams for dynamic online behavior.

► Automatic analysis of Email. It also includes attachments view filtering, Word/Excel embedded image extracting, bookmarking, advanced search, correlation analysis, attachment gallery viewing, E-mail delivery time and email record statistics etc.

► Link analysis of Network communication technology. Display the correlated characters adaptively in the chat record, mail communications in diagram. With many professional association analysis function such as adaptive display, extension of the screen, character tags, the times of specified correlations, hide and jump, it is so convenient to use and user friendly that users can quickly determine the relationships.

► Auto identification of iOS and Android backups generated by iTunes, 91, 360, Baidu, and SnapPea etc.

► Advanced hex view and editor in support of Hex bookmarks

► NTFS file system disk change Log analysis

► Analysis of the whole process of file modification - create, rename, modify and delete etc.

Built-in modules

▶ Live extract. It can directly run on the target computer and extract classified files, make images, recover deleted files and acquire sensitive information (over 80 types) with the support of network share and copy of classified files.

▶ Offline extract. Help boot target computer or external hard drive, mounted Image and after that, extract images, specific files, delete files and sensitive information.

▶ Memory extract. Dump Physical, Virtual and process Memory and have direct access to online account password information.

▶ Flexible extract. Data extraction between Source disk and target disk can be flexible.

  ▶ One-to-many or many-to-one, as you choose.

  ▶ Custom automatic extract and save patterns in classification

  ▶ Multiple case mode. Support multiple case data synchronization loading and extraction, custom multiple case and data distribution as well.

  ▶ Breakpoint resume with no trace left.