Atola TaskForce

Atola TaskForce is a high-performance evidence acquisition tool capable of working with both good and damaged media, developed specifically for forensic use.

The system consists of TaskForce hardware unit and software accessible in Google Chrome browser.

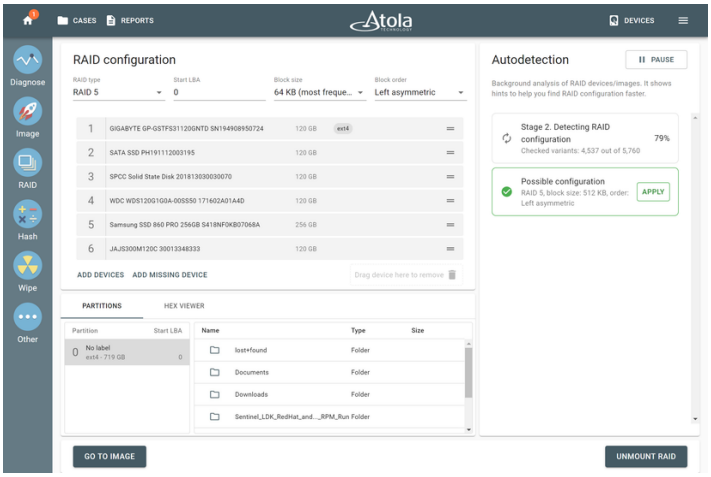
TaskForce can operate in standalone mode or be used by multiple users from devices within the same local network.

It has 18 ports and supports SAS, SATA, USB, IDE and other interfaces via Thunderbolt, Apple PCIe, and M.2 SSD extension modules.

12+ simultaneous imaging sessions. 15 TB/hour

Atola TaskForce combines vast multi-tasking capabilities with the fastest imaging engine. Its hardware including server-grade motherboard, 8-thread Xeon CPU 3.7 GHz and ECC RAM, sustains 12+ parallel imaging tasks.

- **15 TB/hour** cumulative speed of imaging
- Imaging to up to 5 targets
- Source/target switch on all ports
- Write protection in Source mode on all ports
- 2 x 10Gb Ethernet ports
- Forensic imaging to E01, RAW, AFF4 files
- Logical imaging to L01 files
- Express mode (self-launched imaging)
- Integration with other forensic software via API
- Imaging to a file on an encrypted target

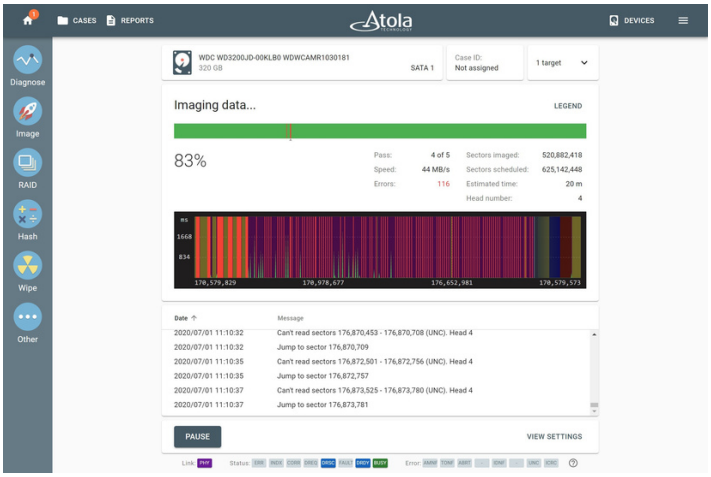


RAID autodetection, reassembly and imaging

Autodetection for RAID arrays with an unknown configuration:

- identifies RAID type by reading data on connected drives
- runs through thousands of potential configuration variants
- one-click application of a suggested configuration
- partition preview for easy confirmation of successful assembly
- rebuild of RAID even with a missing or damaged device (for certain types of redundancy-enabled RAID)

Imaging of a complete RAID or its individual partitions.



Damaged drive support

Atola TaskForce's imaging engine is fully automated and is designed to achieve the best results getting as much data as possible.

- In-depth drive diagnostics
- Selective head imaging
- Imaging of freezing drives
- Imaging of drives with surface scratches and firmware issues
- Current sensors on all SATA, SAS/SATA, IDE ports
- Overcurrent and short-circuit protection
- Segmented hashing for damaged drive image verification

Atola TaskForce

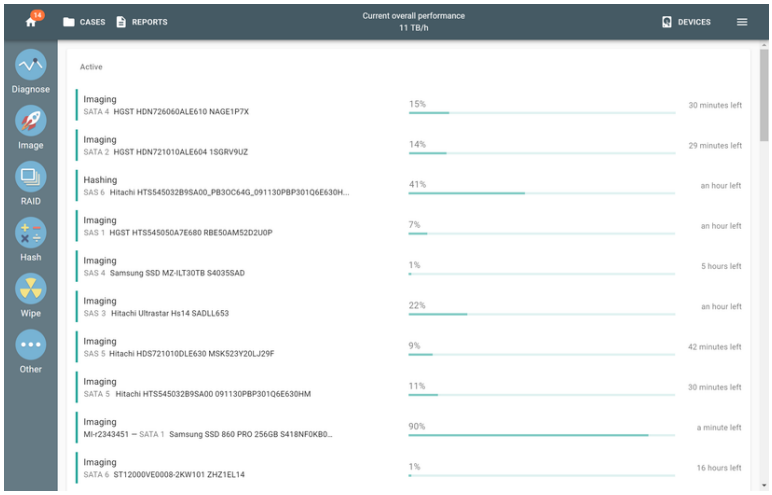
Multi-user access from any device & UI features

The interface is designed to facilitate work with evidence for examiners with different levels of technical proficiency.

- Operate via Chrome browser
- Simultaneous use by multiple operators
- Launch of any operation within 2 - 5 clicks
- Highly intuitive task-oriented user interface
- Managing TaskForce from different operational systems

Connectivity options

1. 10Gb Ethernet network
TaskForce allows access from any device within the same local network by entering the IP address in Google Chrome. To simplify connectivity, hardware unit displays the IP address on the small screen on the front panel.

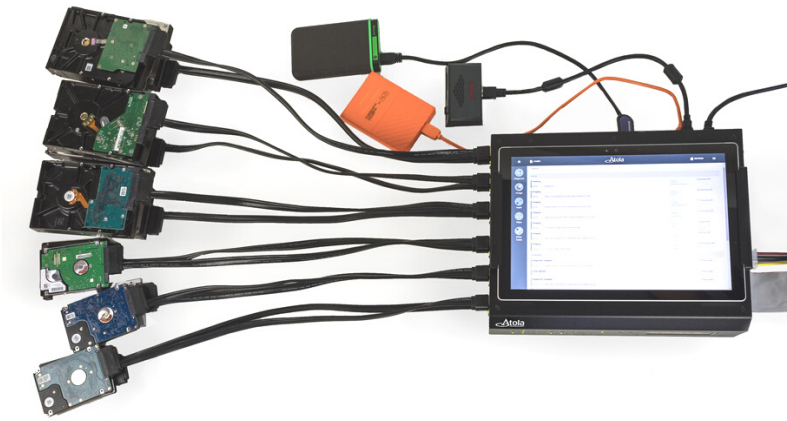


2. Standalone mode
The system has a compact size combined with standalone mode. Beautiful built-in TaskForce touchscreen always works with no need to have other computers involved. Which makes TaskForce perfect for working in the field.

3. Remote Wi-Fi connection
TaskForce includes built-in Wi-Fi access point for easy connection. It is disabled by default. If one enables WiFi, it sets up a secure network available for remote control via laptop, tablet or smartphone.

Other features

- HPA & DCO control and recovery
- Hash calculation: MD5, SHA1, SHA256, SHA512
- Wiping (NIST800-88, DoD 5220.22-M, etc.)
- ATA password recovery
- Automatic report generation
- Case management system
- S.M.A.R.T. view
- Artifact finder (URL, email, GPS, phone, credit card, regular expression, keyword, etc.)



Lifetime warranty

Atola stands behind its product and strives to offer the best warranty terms in the industry. No matter how old your system is, it is covered by the Lifetime warranty, for as long as your software update subscription is active.