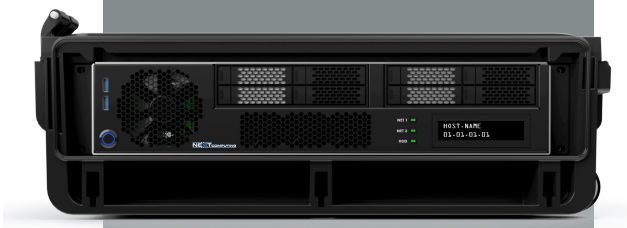


Hunt Forward Malware / Digital Forensics Fly-Away Kit

NextComputing's Hunt Forward Malware / Digital Forensics FAK is a self-contained suite of equipment (hardware and software) for analysis of file-based malware, including data/file extraction from external devices, drives and cell-phones. The kit offers an all-in-one portable solution in two rugged transit cases for reliable travel and deployment anywhere you need to be.

This fly-away kit features NextComputing's innovative NextServer-X hardware with a pre-installed suite of software, including licenses, documentation and support. The result is an expert toolset that is ready to go right out of the box.

Whether you need edge computing server capabilities for analytics in the field, or the flexibility to grow your toolset with your changing needs, the Hunt Forward Malware / Digital Forensics Fly-Away Kit lets you bring your server applications to the network edge.

Compact form factor, incredible performance: High-speed data transfer with the latest hardware

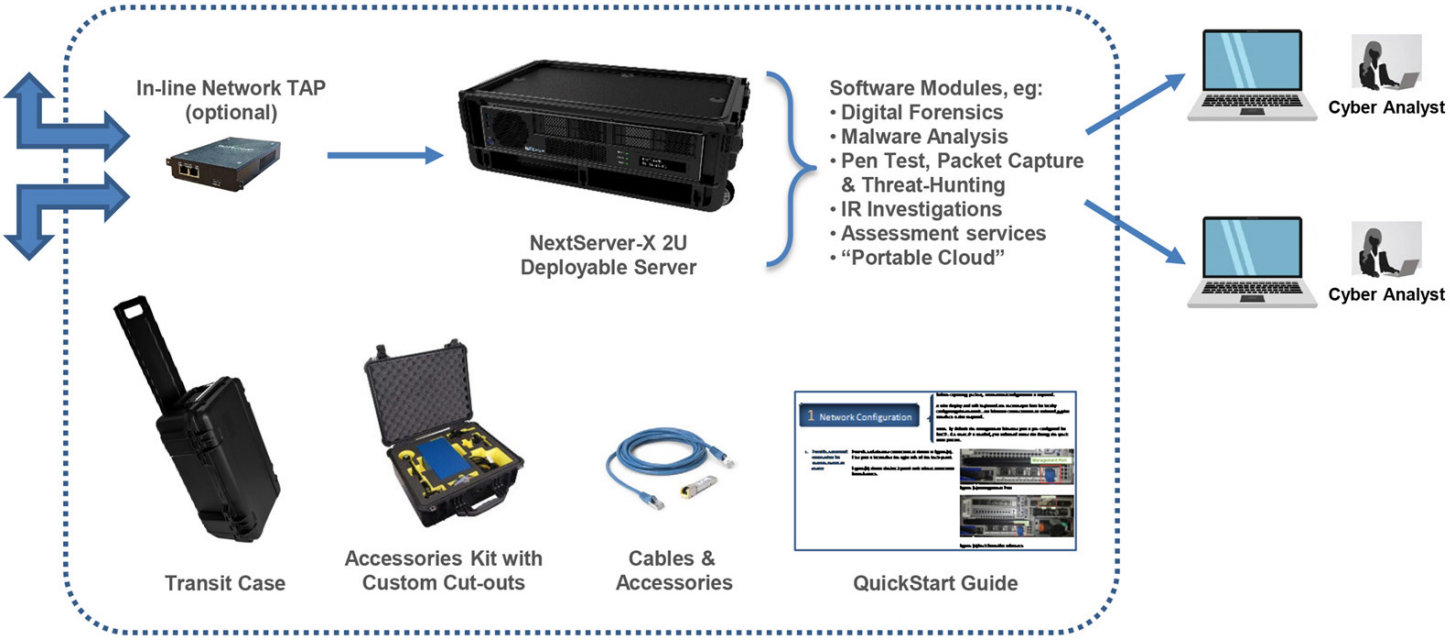
Easy transport: Operate the system from within the rugged travel case for quick setup anywhere

Modular and purpose-built: Hardware and software configured for your needs and expandability for future tasks

Application support: We work directly with our customers every day to ensure that our computers continue to meet their unique requirements

HUNT FORWARD MALWARE / DIGITAL FORENSICS FAK

CAPABILITIES

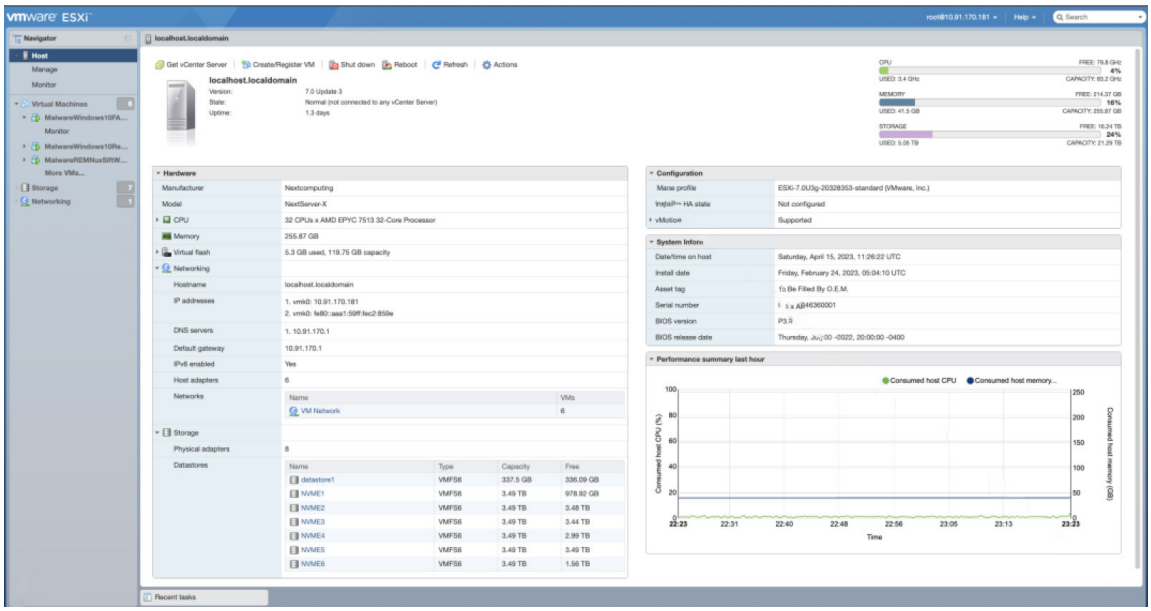


- Recover and analyze data from computers, smartphones, and other electronic devices including data extraction adaptors
- Digital forensic tools to conduct remote forensics by connecting to remote computers or servers over a network to analyze data on live systems without the need for physical access to the target machine
- Access information stored in a variety of mobile devices. It can perform logical and over-the-air acquisition of iOS, Windows Phone, BlackBerry, and Android devices. It helps in extracting data such as call logs, messages, multimedia files, and more.
- Access information stored on encrypted disks and containers. It supports a variety of encryption methods and file systems.
- Auditing the security of wireless networks by attempting to recover Wi-Fi passwords. It can perform dictionary attacks and brute-force attacks on WPA/WPA2-PSK passwords.
- Distributed password recovery across multiple computers, enabling faster recovery times for encrypted files and documents.
- Reset or recover lost or forgotten Windows passwords, allowing access to locked user accounts.
- Recovering passwords saved in various web browsers, email clients, and instant messaging applications.
- In-depth analysis of digital evidence, recover deleted files, examine file systems
- Editing binary and hex data including integers, floats, doubles, and strings, allowing users to interpret and edit binary files easily.
- Powerful Scripting Engine: It includes a powerful scripting engine that allows users to automate tasks, create custom file formats, and perform complex data analysis. The scripting language used in 010 Editor is called "010 Script," which offers a wide range of functions and capabilities.

NEXT COMPUTING

4 Townsend West, Building 17, Nashua, NH 03063
Phone: 1 (603) 886-3874 • Fax: 1 (603) 886-1736
www.NextComputing.com • sales@Nextcomputing.com

- Calculation of various checksums and hash values (such as CRC32, MD5, SHA-1, and SHA-256) for selected data, providing users with methods to verify data integrity.
- Search text for regular expressions, allowing users to search for specific patterns within binary or text data.
- File Recovery and Carving: includes advanced file recovery and carving capabilities, allowing users to retrieve deleted files and extract files from unallocated space on storage devices.
- Keyword and File Signature Searching: Investigators can search for specific keywords, file signatures, or regular expressions within acquired data. This feature helps in identifying relevant files and information related to the investigation.
- Timeline Analysis, allowing investigators to visualize activities and events over time. This timeline analysis helps in reconstructing events and understanding the sequence of actions taken on the system.
- Mobile Device Forensics including the analysis of data from mobile devices, including smartphones and tablets. It can extract data from various mobile operating systems, such as iOS and Android.
- Hexadecimal and Text Editing: tools for editing binary data in hexadecimal, ASCII, and Unicode formats. It allows users to edit, cut, copy, paste, insert, and overwrite data at the binary level.
- Disk and RAM Editing: tools to edit disks, drives, and RAM in raw mode, enabling users to inspect and modify data directly on storage devices or in the computer's memory.
- Disk Cloning and Imaging: tools for disk cloning and imaging, allowing users to create exact copies (clones) of disks or specific partitions. It can also create forensic disk images for analysis and preservation purposes.
- Data Recovery and File Carving tools for data recovery and file carving, allowing users to salvage lost or deleted files. It can recognize and extract files based on file signatures, even if file system information is missing or corrupted.



NEXT COMPUTING
4 Townsend West, Building 17, Nashua, NH 03063
Phone: 1 (603) 886-3874 • Fax: 1 (603) 886-1736
www.NextComputing.com • sales@Nextcomputing.com

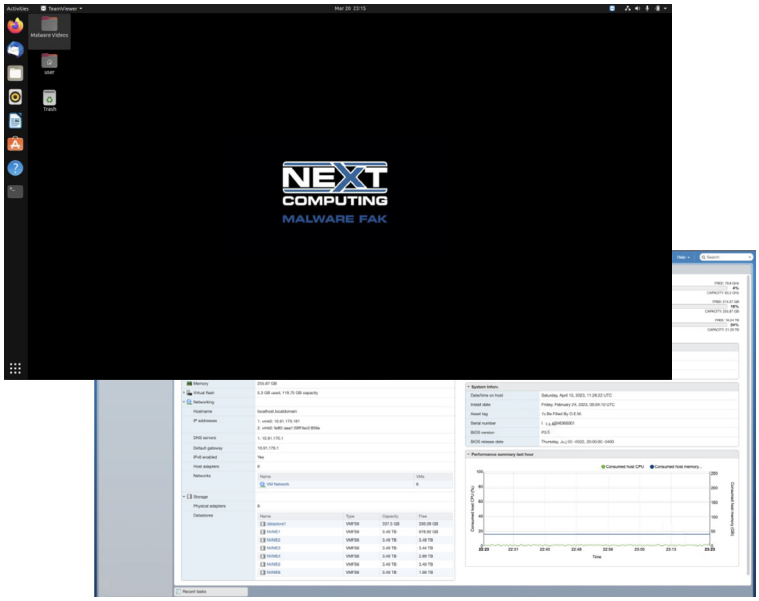
Rev 1.0c—10/23

- File Comparison and Analysis tools to compare binary files and highlight differences, making it useful for identifying changes between different versions of files or identifying tampered data.
- Support for Various File Systems: WinHex supports a wide range of file systems, including FAT, NTFS, exFAT, HFS+, Ext2/3/4, and UFS, allowing users to analyze and edit data on different operating
- Decompilers to translates low-level assembly code into a more readable and understandable high-level programming language representation, making it easier for analysts to comprehend the functionality of the code.
- Code Reconstruction tools so that decompiled code can be analyzed and reconstructed to aid in understanding the logic and structure of the original source code.
- Binary analysis tools that allows security researchers, malware analysts, and reverse engineers to analyze and understand binary code. It provides a user-friendly interface and powerful features for reverse engineering tasks. For a wide range of architectures, including x86, x86-64, ARM, MIPS, PowerPC, and more. It allows users to analyze binaries for various platforms and architectures.
- Wireshark: A popular network protocol analyzer that allows examiners to capture and analyze network traffic. Wireshark helps in understanding network communications and identifying suspicious activities.
- Extracting and analyzing information from Windows registry hives. It helps examiners identify user activities, installed software, and system configurations.
- Extracting various types of information (such as email addresses, credit card numbers, and URLs) from digital evidence files. Bulk Extractor scans binary files and identifies patterns indicative of specific data types.
- File carving tool that allows examiners to recover files based on file headers and footers. It is useful for recovering files from fragmented or corrupted disk images.
- Generating timeline of system and application events based on various log files and artifacts found on the system.
- Memory image comparison, allowing examiners to identify changes between different memory captures.
- Network forensics analysis tool that extracts data from network traffic, including emails, web sessions, and files transferred over the network.
- Malware analysis and reverse engineering

NEXT COMPUTING
4 Townsend West, Building 17, Nashua, NH 03063
Phone: 1 (603) 886-3874 • Fax: 1 (603) 886-1736
www.NextComputing.com • sales@Nextcomputing.com

FAK THIN-CLIENT

- Thin-client laptop (1080p) - 15.6” with integrated keyboard/glide pad
- ESXi user analyst browser UI interface, and IPMI system management control UI
- MicroSD card slot, USB 2.0 port, USB 3.2 Gen 1, USB 3.2 Type C, HDMI output
- Includes USB to RJ45 network adapter
- Includes power cord. Runs on battery up to 8 hours on a full charge.



EASE OF USE

- Software tools are installed and ready to go, accessible from NextComputing’s pre-configured interface
- We provide step-by-step documentation to get you up and running

NEXT COMPUTING

4 Townsend West, Building 17, Nashua, NH 03063
Phone: 1 (603) 886-3874 • Fax: 1 (603) 886-1736
www.NextComputing.com • sales@Nextcomputing.com

Rev 1.0c—10/23

HUNT FORWARD MALWARE / DIGITAL FORENSICS FAK

HARDWARE SPECS

CPU	Single AMD EPYC 7513 32 core processor
Memory	256GB RAM DDR4 3200MHz RAM (32GB x 8 RDIMMs)
PCI Expansion	• Slot 1 - PCI Express 3.0 x16 / x16 Perforated Slot Blocker • Slot 2 - PCI Express 3.0 x8 / x8 Perforated Slot Blocker • Slot 3 - PCI Express 3.0 x16 / x16 HBA NVMe Quad Port Slot 4 - PCI Express 3.0 x8 / x8 PEXUSB3S4V Quad-Port USB 3.0 Card - 5Gbps per port - 4x USB-A – PCIe for malware analysis USB devices • Slot 5 - PCI Express 3.0 x16 / x16 Intel Network Card I350T4V2BLK Ethernet Server Adapter • Slot 6 - PCI Express 3.0 x8 / x8 Perforated Slot Blocker • Slot 7 - PCI Express 3.0 x16 / x16 Network adapter, PCIe x8, 10 Gigabit SFP+ SR modules
Storage	• (2) 1TB NVMe M.2 boot drives • (4) removable 3.84TB NVMe data drives • Bays for up to (8) additional NVMe drives
Network	(2) 10G RJ45 LANs PXE Bootable, (1) RJ45 dedicated IPMI LAN HTML5 and Redfish compatible Out of Band (OOB) management connection
Extraction Devices / Adaptors	Accessory Kit hardcase includes external extraction adaptors, write blockers, and off-loaders devices, anti tamper evidence bags and array of accessories for digital evidence collection
Monitoring	Thin-client laptop (1080p) - 15.6" with integrated keyboard/glide pad, external USB mouse, USB-c to Ethernet cable and NextComputing's thin client Raytheon FAK automation, ESXi user analyst browser UI interface, and IPMI system management control UI
Operating Systems	vSphere (ESXi 7.0) Hypervisor (Licensed)
Power	• 1+1 hot swap redundant 600W 80 Plus Platinum PSU (Option for 850W single 80 Plus Platinum PSU)
Display	Configurable front embedded LCD to display hostname and IP address
Environmental	• 0°C–40°C / 32°F–104°F. Non-Operating: -20°C–70°C, -4°F–158°F. • Relative humidity (5-95%) non-condensing • FCC Class A, CE, TUV, ROHS, Conflict Minerals Free
Physical	• 3.46" H x 17.25" W x 12.60" D standard rack mount (2 and 4 point) • 9" H x 21.75" W x 13.875" D (complete system including operational hard case)
Transport Case	• System includes operational TSA carry-on operational compliant case with telescoping handle and wheels • Accessories included in identical case with foam cutouts for secure, organized storage.
Additional Accessories	• World travel power adapter kit • Dual-band Wireless-N USB antenna and accessories • 6-outlet commercial power strip surge protector with 6ft. power cord and rotating plug

TSA carry-on compliant dimensions

NEXT COMPUTING

4 Townsend West, Building 17, Nashua, NH 03063
Phone: 1 (603) 886-3874 • Fax: 1 (603) 886-1736
www.NextComputing.com • sales@Nextcomputing.com

Rev 1.0c—10/23

- NextComputing MALWARE/Digital Forensics FAK software tools and framework include:
- NextComputing Thin Client Ubuntu/automation/setup/scripts/software
- NextComputing ESXi operational software framework for thin client
- Oxygen Forensic Detective v.13.6 with USB Dongle (includes 12 months of updates)
- F-Response-Consultant + Covert Edition w/1 year subscription
- Elcomsoft password recovery Bundle Forensic Edition w/1 Yrs MNT Total
- Elcomsoft Mobile Forensics Bundle (Elcomsoft Phone Breaker) w/1 Yrs MNT Total
- Elcomsoft Explorer
- Elcomsoft Explorer WhatsApp
- Elcomsoft Phone Breaker
- Elcomsoft Phone Viewer
- Elcomsoft Blackberry Backup Explorer
- X-Ways Forensic Software w/Dongle License
- Microsoft Windows 10 Pro x64 (Guest Operating System)
- Microsoft Office 2019 Professional
- NextComputing Greylog Open
- Event Log Explorer SW
- 010 editor (Commercial version)
- Winhex (Professional)
- IDA Pro Base Floating License (MS Windows)
- IDA Pro x86 Decompiler Base License (MS Windows)
- IDA Pro x64 Decompiler Base License (MS Windows)
- IDA Pro ARM32 Decompiler Base License (MS Windows)
- IDA Pro ARM64 Decompiler Base License (MS Windows)
- Binary Ninja commercial
- FTK International PostgreSQL-FOSS - Comes with FTK International
- Adobe Reader-FOSS -Comes with FTK International
- Clonezilla-FOSS
- Registry Viewer - Part of FTK International
- License Manager - Part of FTK International
- FTK Imager-FOSS
- Tableau Imager-FOSS
- Volatility-FOSS
- Redline-FOSS
- LiME - Memory collection-FOSS
- Winpmem - memory collection tool-FOSS
- Windows Defender - part of Windows OS-FOSS
- Python-FOSS
- mozilla firefox-FOSS
- Windows SysInternals suite-FOSS
- Wireshark-FOSS
- Regshot-FOSS
- PEiD-FOSS
- Process Hacker-FOSS
- OllyDbg-FOSSImmunity Debugger-FOSS
- Putty FOSS
- Magnet RAM Capture FOSS
- Autopsy v.4.10 - 64 Bit FOSS
- SANS SIFT Workstation
- SANS REMNUX Workstation

NEXT COMPUTING

4 Townsend West, Building 17, Nashua, NH 03063
Phone: 1 (603) 886-3874 • Fax: 1 (603) 886-1736
www.NextComputing.com • sales@Nextcomputing.com

- NextComputing OEM services included: Build, Integrate, maintain, document, and update VMs, license as applicable, and provide/maintain documentation, Kit and document accessories with QuickStart Documentation, integrate with NextServer-X
- MALWARE/Digital Forensics Accessory Kit hardcase with telescoping handle and wheels
- Thin-client laptop (1080p) - 15.6” with integrated keyboard/glide pad, external USB mouse, USB-c to Ethernet cable and NextComputing’s thin client Raytheon FAK automation, ESXi user analyst browser UI interface, and IPMI system management control UI
- mSATA adapterA4710
- M.2 adapter
- Blade Adapter
- Card Reader
- UltraBlock USB3.0 Kit includes USB3 to USB3 Write Blocker, Power Supply, USB 3.0 A to USB 3.0 B cable, Zippered Bag, Quick Start Guide
- Anti-Tamper Tape
- Evidence Bags (100 bags)
- PALADIN PRO 7 USB - PALADIN PRO Current version USB
- GigaTrue CAT6 Channel 550-MHz Patch Cable (UTP), Snagless Boots, Green, 15-ft. (4.5-m)
- 64GB USB 3.0 Flash Drive
- X0014KSMID (IF145-307-4) - Pro Tech Toolkit
- NetGear ProSAFE GS108 Gigabit Switch
- Multipack Drive Adapter Kit (Tableau TKA5-AD)
- SanDisk Cruser 64 GB USB
- Kingston 8 GB SD card
- SanDisk SSD PLUS 120GB Solid State Drive (SDSSDA-120G-G26)
- UltraBlock PCIe Kit
- PCIe Bundle (Includes: TDA 7-1, 7-2, 7-3 w/Cable)
- Tableau Forensic Duplicator TD2U
- Tableau SAS Protocol Module
- Multipack Drive Adapter Kit (Tableau TKA6-AD)USB 3.1 WriteBlocker - USB 3.1 Write Blocker
- World Travel Adapter Kit by Ceptics - Dual USB + 2 US Outlets, Surge Protection, Plugs for Europe, UK, China, Australia, Japan - Perfect for Laptop, Cell Phones, Cameras - Safe ETL Tested (WPS-2B+)
- Belkin 6-Outlet Commercial Power Strip Surge Protector with 6-Foot Power Cord and Rotating Plug, 1080 Joules (BE106000-06R)
- WD 4TB Elements Portable External Hard Drive - USB 3.0
- TSA Compatible Travel Luggage Locks, Inspection Indicator, Easy Read Dials (2 Pack)
- Rosewill Anti Static Wrist Strap Band, ESD Strap Anti Shock Wristband Bracelet with Grounding Wire Alligator Clip, Detachable Extra Long Cord
- Technical 10 Pair Anti Static Antiskid Glove for PC Computer ESD Electronic Working
- Repair Gloves (White / Gray)
- Extra Large 21.25 x 14.5 Faraday Bag

NEXT COMPUTING

4 Townsend West, Building 17, Nashua, NH 03063
Phone: 1 (603) 886-3874 • Fax: 1 (603) 886-1736
www.NextComputing.com • sales@Nextcomputing.com

Rev 1.0c—10/23