

What is F-Response®?

F-Response® is an easy to use, vendor neutral, patented software tool that enables “Live” forensics and eDiscovery over IP networks using the examiner’s tools of choice. Physical memory, disks, and volumes of the machines under inspection appear on the examiner’s machine as locally attached, read-only devices.

F-Response provides read-only access to full physical disks, logical disks, Cloud-based data, Databases and physical memory (RAM) over the network.

F-Response significantly increases the efficiency and affordability of digital forensics, incident response, data recovery, and eDiscovery efforts by presenting a means to manage the collection, preservation, and analysis process over any TCP/IP network, including the Internet.

Is F-Response Court Approved?

There is no such thing as court-approved software. Courts approve experts and their methods, and courts admit evidence. Evidence collected with F-Response® has been and continues to be used successfully in courts across the country and around the world. Because F-Response® works. Accurately. Securely. Verifiably.

How F-Response works:


F-Response creates an authenticated, read-only connection between the examiner’s computer and the computer under inspection, over the network.

Why Use F-Response?






F-Response is inexpensive, flexible, vendor neutral, and does not require extensive training. Practitioners can learn to use it in a fraction of a day, and then fully leverage their existing arsenal of tools and training. Other network ready solutions are expensive, require considerable training to use, and force you to use the proprietary integrated vendor analysis tool.

F-Response Options:







F-Response® term licenses are sold on an annual basis (F-Response Now is available weekly/monthly) with no limitation on the number of installations or uses. F-Response® product options are as follows:

 F-Response **Universal (UNIV)** is an appliance-based solution that permits many machines to be examined simultaneously over a network, and facilitates “stealthy” deployments for covert operation. F-Response Universal integrates well with

standard corporate architectures. Software deployment is available to all users.


-  F-Response **Enterprise (EE)** is a dongle-based solution that permits many machines to be examined simultaneously over a network, and facilitates “stealthy” deployments for covert operation. F-Response target code is easily deployed and managed via the F-Response Enterprise Management Console (FEMC).
-  F-Response **Consultant+Covert (CE+C)** has all the features of Consultant edition, plus a covert, Enterprise Edition push style, deployed target for use on any one machine at any given time.
-  F-Response **Consultant (CE)** is a solution that permits many machines to be examined simultaneously. GUI-based target code is executed on each machine to be examined.
-  F-Response **TACTICAL (TAC)** is an intuitive, easy to use, GUI-based point solution that permits an examiner to review one machine at a time. A matched dongle pair facilitates the automatic connection between the Examiner and Subject computers.
-  F-Response **Now** is the “on demand” computer forensics, incident response and e-discovery cloud service providing remote access to systems over the Internet.

F-Response Highlights:

-  **Forensically Sound & Secure:** The examiner cannot alter Metadata, files, or make any change to the machine under inspection because all write operations are silently ignored by F-Response.
-  **Supported Platforms:** Provides network accessible, authenticated, RAW, read-only drive access to most computers.
-  **Versatile:** F-Response was designed to be completely vendor neutral. If your analysis software reads a hard drive, it will work with F-Response.
-  **Highly Efficient:** F-Response maintains a small active memory (RAM) Footprint and will not bog down the user’s workstation or entity’s network.
-  **Scriptable:** A language neutral fully scriptable COM object is available, allowing a technical user of F-Response Enterprise to script actions typically initiated manually in the FEMC.
-  **Affordable:** Fixed yearly license or on demand access (F-Response Now). No seat limits. No add-ons. No surprises.


Capabilities	T A C	C E	C E + C	E E	N O W	U N I V	Comments
Unlimited Installs	✓	✓	✓	✓	✓	✓	F-Response may be installed on an unlimited number of machines.
Unlimited Seats	✓	✓	✓	✓	✓	✓	F-Response may be used on an unlimited number of machines, and shared among an unlimited number of examiners.
Image Collection Support	✓	✓	✓	✓	✓	✓	Collect forensic images of connected Target machine files, drives, volumes and/or RAM using your imaging tool of choice.
F-Response Imager	✓	✓	✓	✓	✓	✓	Forensic imager for all F-Response connected devices including, DiscoveryShares™, F-Response Connector Volumes, and MemoryShares™.
Dongle-Based Hardware License	✓	✓	✓	✓			F-Response products well suited to investigative teams and consultants that perform their duties in multiple locations, accessing data within LAN environments.
Appliance-Based Software License					✓	✓	F-Response products deployed as fixed (Universal) or temporary (NOW) appliance installations for remote data access over the Internet or LAN.
Physical Memory Support	✓	✓	✓	✓	✓	✓	Physical Memory support is currently available for 32 & 64 bit Microsoft Windows products.
Windows Support	✓	✓	✓	✓	✓	✓	Microsoft Windows XP+ (32 and 64 bit)
Linux Support	✓	✓	✓	✓	✓	✓	Linux distributions (2002+) (32 and 64 bit)
Apple OSX Support	✓	✓	✓	✓	✓	✓	Apple OSX 10.3+
3rd party Connector Support (Cloud, Email, DB)	P	✓	✓	✓			Connector provides support for mapping diverse remote data stores as local read only shares.
Scriptable COM Object		✓	✓	✓	P	P	F-Response provides a fully scriptable Microsoft COM object to automate various stages in the F-Response process. COM objects differ by version.
Local Authentication	✓	✓	✓	✓	✓	✓	Leverages locally defined usernames and passwords for authentication.
Local Audit Log		✓	✓	✓		✓	Updates Windows Event log on license manager machine or the F-Response Universal appliance with login, logout, and connection messages.
SIEM Compatible Remote log						✓	F-Response Universal appliances are capable of sending log information to remote syslog servers.
Encryption (AES 256) for data in transit				P	✓	✓	F-Response Enterprise offers encryption in transit optionally, Universal/Now all traffic is encrypted by default.
Active Directory Authentication						✓	F-Response Universal supports integration with Active Directory for Authentication.
Android Support					✓	✓	F-Response Now and Universal support Android subjects.
Mission System						✓	Provides an optional on demand access provisioning model built around 3 rd party approvers.
Compression					✓	✓	F-Response Now and Universal use cutting edge compression technology to improve performance over LAN, WAN, and Internet connections.

Key: ✓ = Included with product, "Blank" = Not available with product, P = Partial support




Tactical

- One to one connections
- Dual dongle solution
- Simple and inexpensive




Consultant

- Unlimited Subjects and Examiners
- Dongle based
- Non Covert




Consultant + Covert

- Portable
- Single Covert Connection
- Unlimited non-covert connections
- Dongle based
- Includes all Consultant Features




Enterprise

- Portable
- Unlimited Subjects and Examiners
- Dongle based
- Covert deployment



Now

- Cloud Service
- Internet Accessible
- Non covert
- Compression



Universal

- Active Directory Authentication
- SIEM Logging
- Unlimited Subjects and Examiners
- Multiple covert deployment options
- Compression