Vound

Who | What | Where | When. Simple.

W4 User Manual

Version 1.1.0

Table of Contents

1. Preface

W4 is designed to a be tool that detects user activity.

With W4, you can answer the questions:

- Does the user possess material of type X? (documents, images, emails, chat messages, etc.)
- What USB devices were used and what files might have been copied to those devices?
- What web pages were visited?
- What files were downloaded from the Internet?
- What files were sent or received by email?
- What programs were launched?
- What folders were explored?
- And many more...

2. An introduction to W4

2.1. Key benefits

- Easy to use interface means it has a very low learning curve and suitable for non-specialists.
- Very fast indexing allows to quickly scan and assess the evidence.
- Search during indexing allows to preview first results in a matter of minutes.
- Powerful indexing engine that supports variety of system and registry artifacts.
- Timeline allows to visualize data distribution over time and filter items.
- Innovative Events view allows to see all user actions in a single unified graph. Events can be annotated via tags and notes that allows to create a custom timeline.
- Thumbnails view allows to easily preview all images in the case.
- Simple to use annotation tools allow to tag items and add notes.
- Item Links feature allows to unveil and explore hidden links between artifacts such as documents copied to a USB device, downloaded from the Internet or sent by email.
- Flexible reporting functionality allows to configure each section individually (table, events, image gallery or link graph) to create professionally looking reports.
- Intella integration: W4 case can be directly ingested into Intella with a few clicks to enrich the data.
- Recipes functionality that allows to investigate common cases in one click.
- On-site triage and live acquisition features.

2.2. Supported file formats

Supported disk image formats:

- EnCase images (E01, Ex01, L01, Lx01 and S01 files)
- FTK images (AD1 files), version 3 and 4
- DMG. Supported compression formats: ADC, LZFSE, ZLIB, BZIP2. Supported compressed image formats: UDCO, UDZO, UDBZ, UDCo. Supported uncompressed image formats: RdWr, Rdxx, UDRO.
- DD images
- MacQuisition images (RAW, .00001 files)
- VMware images (VMDK files). Supported types are RAW (flat), COWD version 1 (sparse) and VMDK version 1, 2 and 3 (sparse). Not supported are images that use a physical storage device.
- VHD disk images. Supported type is VHD version 1.
- VHDX and AVHDX disk images.
- AFF4 disk images. AFF4-L format (logical) is not supported. Split images that consist of more than one file are not supported. Images with block deduplication are not supported.
- BitLocker encrypted volumes.
- Volume shadow copies.

Supported cellphone extraction formats:

- Cellebrite UFED XML export or UFDR file.

- Micro Systemation XRY XML and Extended XML exports (Extended XML is strongly recommended).
- Oxygen Forensic Suite XML export.
- iTunes backups. iOS versions 8, 9 and 10 backed up with iTunes 12. Other versions may work but have not been tested.

W4 can detect the following artifacts and data formats:

- System artifacts:
  - Installed operating systems. Windows 7, 8 and 10 were tested.
  - User accounts.
  - User sessions: logon and logoff dates.
  - Windows event log entries. Supported Windows versions: 7, 8.1 and 10.
- Programs:
  - Installed programs.
  - Startup programs.
  - Launched programs extracted from User Assist, BAM (Background Activity Moderator) and RecentApps registry keys and Prefetch files.
  - User and program activity extracted from Windows 10 Timeline database.
- Devices:
  - USB devices.
  - USB device activity.
  - Network interfaces.
  - Network profiles including Wi-Fi network names.
- Files and folders:
  - Recently accessed folders (Shell Bags).
  - Recently accessed files (LNK, Jump Lists, MRU and RecentApps registry key).
  - Deleted files and folders.
- Web browser activity:
  - Visited web pages (Chrome, Firefox, Internet Explorer, Edge, Safari).
  - Cookies (Chrome, Firefox, Internet Explorer, Edge).
  - Form history (Chrome, Firefox).
  - Bookmarks (Chrome, Firefox, Internet Explorer, Edge, Safari).
  - Logins (Chrome).
  - Downloads (Chrome, Firefox).
- Notable items:
  - Encrypted items: documents and emails.
  - Images with geolocation metadata.
  - Files and folders deleted to recycle bin.
  - Files downloaded from the Internet (Zone Identifier).
- Notable program usage:
  - BitTorrent, cryptocurrency, darknet and remote access program usage.
- Communication:
  - Mail formats:
    - Microsoft Outlook PST/OST. Versions: 97, 98, 2000, 2002, 2003, 2007, 2010, 2013, 2016, 2019, 365.

        - Microsoft Outlook Express DBX, MBX. Versions: 4, 5 and 6.
        - Microsoft Outlook for Mac OLM and OLK15* files.
        - Microsoft Exchange EDB files. Versions: 2003, 2007, 2010, 2013, 2016. Locations are not supported yet.
        - IBM Notes NSF (formerly known as Lotus Notes or IBM Lotus Notes). Notes 8.5.x or higher needs to be installed on the computer running W4 to process the NSF files. W4 supports all NSF files that can be processed by the installed IBM Notes version.
        - Mbox (e.g. Thunderbird, Foxmail, Apple Mail)
        - Windows 10 Mail (POP accounts).
        - Saved emails (.eml, .msg)
        - Apple Mail (.emlx). Versions: 2 (Yosemite), 3 (El Capitan), 4 (Sierra), 5 (High Sierra) and 6 (Mojave). Testing concentrated mostly on versions 2, 5 and 6.
        - TNEF-encoded files ("winmail.dat" files).
    - Chat messages extracted from Skype SQLite databases, versions 7.x (stable), 8.x, 11.x, 12.x and 14.x.
    - Contacts, tasks and calendar items extracted from Outlook PST/OST, Exchange EDB and vCard/iCal files.
- Documents:
    - MS Office: Word, Excel, PowerPoint, Visio, Publisher, OneNote, both old (e.g., .doc) and new (.docx) formats, up to MS Office 2019 and MS Office 365. MS OneNote 2007 is not supported.
    - OpenOffice: both OpenDocument and legacy OpenOffice/StarOffice formats
    - Hangul word processor (.hwp files)
    - Corel Office: WordPerfect, Quattro, Presentations
    - MS Works
    - Plain text
    - HTML
    - RTF
    - PDF (incl. entered form data)
    - XPS
- Media:
    - Images (preview and export):
        - Adobe Photoshop (PSD)
        - Apple Icon (ICNS)
        - Apple PICT
        - BMP
        - GIF
        - Icon (ICO)
        - Interleaved Bitmap (IFF)
        - JBIG2
        - JPEG
        - JPEG-2000 (JP2)
        - PCX/DCX (DCX not tested)
        - PNG
        - Radiance HDR
        - SVG

        - TIFF
        - WMF / EMF (partial)
    - Images (metadata extraction):
        - Adobe Photoshop (PSD)
        - BMP
        - GIF
        - HEIF/HEIC
        - Icon (ICO)
        - JPEG
        - PCX/DCX (DCX not tested)
        - PNG
        - TIFF
        - WebP
- Archives:
    - Zip. Supported compression methods: deflate, deflate64, bzip2, lzma and ppmd.
    - 7-Zip. Supported compression methods: lzma, lzma2, bzip2 and ppmd.
    - Gzip
    - Bzip2
    - ZipX
    - Tar
    - Rar
    - RPM Package Manager (RPM)
    - Cpio
    - ARJ
    - Cabinet (CAB)
    - DEB
    - XZ
- Cryptocurrency (detection only):
    - Bitcoin wallets and blockchains
    - Dogecoin wallets and blockchains
    - Litecoin wallets and blockchains
    - Multibit Classic wallets and blockchains
    - Multibit HD wallets and blockchains

When indexing plain text file formats, W4 can essentially handle all character encodings supported by the Java 8 platform. This relates to regular text files and to email bodies encoded in plain text format. See http://docs.oracle.com/javase/8/docs/technotes/guides/intl/encoding.doc.html for a complete listing.

When the encoding is not specified, W4 will try to heuristically determine the encoding. The following encodings are then supported:

- UTF-7
- UTF-8
- UTF-16BE
- UTF-16LE

- UTF-32BE
- UTF-32LE
- Shift_JIS Japanese
- ISO-2022-JP Japanese
- ISO-2022-CN Simplified Chinese
- ISO-2022-KR Korean
- GB18030 Chinese
- Big5 Traditional Chinese
- EUC-JP Japanese
- EUC-KR Korean
- ISO-8859-1 Danish, Dutch, English, French, German, Italian, Norwegian, Portuguese, Swedish
- ISO-8859-2 Czech, Hungarian, Polish, Romanian
- ISO-8859-5 Russian
- ISO-8859-6 Arabic
- ISO-8859-7 Greek
- ISO-8859-8 Hebrew
- ISO-8859-9 Turkish
- windows-1250 Czech, Hungarian, Polish, Romanian
- windows-1251 Russian
- windows-1252 Danish, Dutch, English, French, German, Italian, Norwegian, Portuguese, Swedish
- windows-1253 Greek
- windows-1254 Turkish
- windows-1255 Hebrew
- windows-1256 Arabic
- KOI8-R Russian
- IBM420 Arabic
- IBM424 Hebrew

Several file formats are processed by applying heuristic string extraction algorithms, rather than proper parsing and interpretation of the binary contents of the file. This is due to a lack of proper libraries for interpreting these file formats. Experiments with these heuristic algorithms have shown that their output is still useful for indexing and full-text search. It typically will produce a lot of extra gibberish data, visible in the Previewer, and there is no guarantee that the extracted text is complete and correct. The affected formats are:

- Corel Office: WordPerfect, Quattro, Presentations
- Harvard Graphics Presentation
- Microsoft Project
- Microsoft Publisher
- Microsoft Works
- StarOffice

2.3. Supported sources

Disk image

W4 can open disk image files, including the EnCase, FTK (AD1) and DD formats, and index their contents as if they were mounted and indexed as a regular Folder source. Optionally, files and folders can be recovered from the Master File Table (MFT). System and registry artifacts are extracted when using this source type. Carving of unallocated space and slack space is not supported.

Folder

Folders on local and network file systems can be indexed by W4. Please check the list of supported file formats. The use of external and network drives is not supported, both for stability and performance reasons. Note that system and registry artifacts are not supported when indexing a folder.

Local disk

Physical and logical disks connected to the computer can be indexed by W4. W4 reads the data directly from the volume bypassing the operating system. Therefore, it is possible to index a live running system (e.g. drive C:) without leaving any traces in the system and capture system protected and deleted files. System and registry artifacts are extracted when using this source type. Carving of unallocated space and slack space is not supported. It is recommended to access encrypted volumes by using the logical disk option (e.g. via drive letter) if it's possible.

Local disk source requires W4 to be launched with administrative privileges. When using the portable version, w4.exe will be launched with elevated permissions that allows physical disk access.

Cellphone extraction

Cellphone XML and UFDR reports such as made by Cellebrite XRY, MicroSystemation's XRY and Oxygen Software's Forensic Suite can be indexed by W4. Please check the list of supported file formats. Note that system and registry artifacts are not supported with this source.

2.4. Supported languages

As W4 is entirely based on Unicode, it can index and provide keyword search for texts from any language. There is no specific support for the handling of diacritics. E.g., characters like e and c will be indexed and displayed, but these characters will not match with 'a' and 'c' in full-text queries.

2.5. Supported platforms

We support and test our products on Windows Vista, Windows 7, Windows 8/8.1, and Windows 10. A 64-bit operating system is required. The "Home" or "Starter" editions are not recommended as they limit the maximum amount of memory and CPUs. Please use the "Pro", "Enterprise" or "Ultimate" versions instead.

W4 is tested on the abovementioned operating systems. That said, we have customers who are running W4 on the Windows Server platform, versions 2008, 2012, and 2016. Note that there may be security settings that need to be configured on the server to allow W4 to run on it. This needs to be

addressed by your IT team; we cannot provide advice on these settings.

2.6. Feedback

We take great care in providing our customers with a pleasant experience, and therefore greatly value your feedback. You can contact us through the form on http://support.vound-software.com/ or by mailing to one of the email addresses on the Contact page.

3. Getting support

3.1. Different ways to get support

Vound offers three support options designed to assist users that experience problems while working with W4™:

1. Standard technical support
2. User support contract
3. Vound User Support portal

3.2. Standard technical support

Standard technical support is offered free of charge to all Vound customers that have a current support and maintenance contract.

Standard technical support can be requested at the Vound support page, http://support.vound-software.com.

Support is provided on business days, Monday through Friday. We attempt to give you a first answer within 2 business days.

All communication will be remote – e-mail, GoToMeeting, and other means – and not in person unless otherwise arranged.

Standard technical support will only be provided if your computer and operating system meet the minimum recommended specifications listed in the latest version of the W4™ manual.

Who is eligible for technical support?

Our goal at Vound is to provide our customers high quality and timely technical support. To do this we limit technical support to the registered owners of W4. Companies that allow a third party to use their W4 licenses must have that third-party channel all technical support through the original registered owner of the software.

To ensure that we support our customers, Vound regrets it cannot support users who are not the original registered owner of W4.

What technical support is included?

- Installation and set-up support limited to one computer in your environment.
- Configuration technical support and user support on use for standard W4™ options.
- Support for errors in the software (bugs).

Please note that Vound will make reasonable efforts to correct identified software errors. However, this may not be achievable until a later date or version release. If this is the case, the user should make efforts and take responsibility to achieve the required outcomes via other methods. Where the errors relate to or are caused by corrupt data (within source files), Vound reserves the right to charge for the work needed to rectify the issue.

No support can be provided...

- When your computer does not meet the minimum or essential system requirements.
- When you made any kind of modifications to the installed software.
- When you are not using the software for its intended purpose.
- When 3rd party applications, like virus scanners, firewalls, and other forensic applications, interfere with W4™.
- Explaining the method needed to use each feature to achieve a set outcome.

At no time should Vound technical support be seen as legal or forensic advice. Our support is given with no knowledge of the specific case or matter W4 is being used on. Technical support is focused on the correct installation and usage of W4 features. We do not warrant that we are aware of all facts around the case that may be under investigation. As such, our replies should not be seen as advice or the only way to achieve the required outcome.

3.3. User support contract

A paid user support contract is offered to those customers that want additional user support. The user support contract provides assistance that falls outside the standard support package (see 3.1.1 Standard technical support).

What can be included in the user support contract?

- Help with the case or setup configuration of W4™.
- Assistance in using the basic and advanced features of W4™ such as searching, tagging, and exporting.
- Help with the installation of W4™, or help with the configuration and set-up of your computer that runs W4™.
- Detailed explanation of W4™ case management and help with W4™ case setup.
- Help with the export of search results found with W4™ for use with other applications.
- Support for using W4™ in combination with software from other vendors.
- Support for issues that a newer W4™ release has addressed.

How to buy to a user support contract?

User support contracts are based on your specific needs. If you want to know more, please contact your nearest Vound representative or your local W4™ reseller.

3.4. Working with Vound support

It is highly recommended that customers and users take advantage of the Vound support page when seeking assistance. The support portal takes care of collecting all necessary information such as the W4 version, Windows version, source types used, etc. and will suggest relevant articles from the W4 knowledge base.

3.5. Upgrade contract

Vound customers that purchased an W4™ license are entitled to install free upgrades of the software for a period of one-year. In other words: an W4™ license comes with a one-year upgrade contract.

After this period purchasing an upgrade subscription will continue the upgrade contract. Please contact your nearest Vound representative for more information.

Please know that you will only have access to standard technical support if you have an upgrade contract.

4. Installation and configuration

4.1. Installation

4.1.1. Step 1: Check the hardware requirements

W4 is supported on Windows Vista, Windows 7, Windows 8/8.1, and Windows 10.

CPU, memory, and disk space requirements depend on how W4 is intended to be used:

Indexing

- As a rule of thumb, the case folder requires between 150% and 200% of the size of the combined evidence data, depending on data complexity and amount of compression used on the evidence data.
- For better indexing performance, we suggest storing the case data folder on a physically different disk than the one with the evidence data.
- Disk access times for the case indexes are critical for performance. We therefore strongly suggest not using USB or network drives for the case data folder.
- See the section on Storage Recommendations for more storage-related tips.
- When indexing MS Exchange EDB files, the memory sizes in the table below should be doubled and the memory settings will need to be adjusted (see the Memory Settings section).

Main memory and CPU requirements for indexing:

Evidence size	Minimum memory	Recommended memory	Number of CPU cores
Up to 10 GB	4 GB	8 GB	2
10 to 100 GB	8 GB	16 GB	4
100 to 500 GB	16 GB	32 GB or more	4 or more

4.1.2. Step 2: Check the software requirements

The following external applications may also be necessary to use some of W4's functionalities:

- IBM Notes

IBM Notes

To index NSF files, IBM Notes 8.5 or higher is required. Only the application files are necessary, IBM Notes does not have to be fully setup to be used by W4. In principle, all IBM Notes 8.5.x versions or later can be used, but the following versions will produce a warning:

- 8.5.3 FP 3
- 8.5.3 FP 4
- 8.5.3 FP 5
- 9.0

These versions contain a bug described here that cause emails with multiple "Received" headers to

be altered: all Received headers will get the value of the first header. At the time of writing IBM Notes 9.0.1 was available, in which this bug has been fixed.

To index files made with IBM Notes 9.x, we recommend installing IBM Notes 9.x.

W4 needs to know the location of IBM Notes to index NSF files. By default, W4 will try to auto-detect the location. If the location is not standard (`C:\Program Files (x86)\IBM\Notes`), then it needs to be configured via the following configuration file:

```
C:\Users\user\AppData\Roaming\W4\prefs\user.prefs
```

The location of IBM Notes can be set by using the following line:

```
NotesLibraryPath=C:\Program Files (x86)\IBM\Notes
```

4.1.3. Step 3: Learn about licenses and dongles

Notes on the trial license that is bundled with the software that you have downloaded:

14-Day evaluation period

The trial version runs under a HASP Software License, which gives you the ability to use W4 for 14 days. The 14-day evaluation period cannot be extended. The only way to continue using W4 is to purchase a dongle.

Continue working with a USB dongle

If you would like to continue using W4 after this 14-day period, you will need to buy a license. After buying the license you will receive a USB dongle that will allow you to continue using the version you already installed. A dongle provides a perpetual license.

Free one-year license

W4 comes with a free one-year license that doesn't require a dongle. When this period expires, W4 can still be launched in Viewer mode that allows to open existing cases. When W4 is launched in Viwerer mode, it is not possible to create new cases, add new sources and index or re-index data.

System clock

Changing the clock on your system will cause the trial to automatically expire. When this occurs, the only way to continue using W4 will be to purchase a license.

Virtual Machines, VMware

The evaluation version not work in VMware without a dongle.

RDP (Remote Desktop Protocol) connection

When using RDP, the dongle or trial license must be in/on the computer running the W4 software,

not in the computer running the RDP viewer.

Other dongle-protected software must be closed

All other HASP protected software, like EnCase (Guidance), Smart Mount (ASR Data), HBGary and i2 products, must be closed when installing W4.

4.1.4. Step 4: Install the software

- Download W4 through the download page on the Vound support website: http://support.vound-software.com/
- Double-click on the downloaded .exe file to launch the installer. Accept the license.
- Enter the location to store the application files and shortcuts or accept the default settings. All files will be extracted to the location of your choosing and a W4 shortcut is (optionally) placed on your desktop and in your Start menu.

The application folder contains an executable called "w4.exe" that can be used to launch the application. The desktop and menu shortcuts also start this executable. The program will start with the Case Manager window.

W4 will not install in an installation folder of an earlier version. Install a new version of W4 in a folder with a new name, for example: `C:\Program Files\Vound\W4 1.0.0\`

It is possible to install multiple W4 versions side by side.

4.1.5. Step 5: Using portable version

W4 can be used as a portable application. That means it can be used on any machine without installation. To do that you need to:

- Download the portable ZIP archive through the download page on the Vound support website: http://support.vound-software.com/
- Unpack the archive to a folder.
- Run w4.exe to start the application.

Differences between normal and portable versions:

- Portable version will store its configuration files in the app folder (e.g. `F:\w4-portable\config`), while the normal version uses the system AppData folder (e.g. `C:\Users\<USERNAME>\AppData\Roaming\Vound\W4`). That makes the configuration fully portable and allows to run W4 from a USB flash drive.
- Portable version will store cases in the app folder by default instead of the sytem AppData folder.
- Portable version will store all temporary files in the app folder instead of the system temp folder.
- Portable version will run with administrative privileges allowing live system indexing and acquisition.
- Portable version contains an additional executable, `w4_triage.exe`, that can be used to process a new machine in almost one click.

In general, the portable version is aimed to be used for on-site triage and evidence acquisition

minimizing the amount of changes made to the system W4 is running on. W4 is usually launched from a USB flash drive in such case.

It might take a little longer than usual to start W4 for the first time.

W4 will add itself to the Windows Firewall exception list on first start automatically.

This is the list of changes made to the system when W4 is launched in the portable mode:

- Any changes that are normally made to the system when an application is launched (e.g. prefetch files, shellbags, etc).
- The license driver is installed to `C:\ProgramData\SafeNet Sentinel`
- A new rule is created for Windows Firewall using the following command:

```
netsh advfirewall firewall add rule name=W4 dir=in action=allow program=w4.exe
enable=yes
```

- This folder might be modified: `C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA`

4.2. Storage considerations

Besides the memory and CPU requirements above, there are other hardware considerations that impact performance.

Use of USB drives

Our testing shows that USB drives are generally slower than internal hard drives or eSATA drives.

Please note that Windows allows you to use USB drives in two performance modes: the default “Quick Removal” mode and the “Better Performance” mode. Using the latter helps a lot to achieve better performance, but you will have to make sure to properly remove the drive in Windows before unplugging the drive. Not doing so means you risk damaging your case files beyond repair.

Evidence on external drives

Many users like to keep their evidence data on an external drive, for a variety of reasons. A common question is whether they can still use the case when this drive is disconnected after indexing. This is certainly possible. Access to the original evidence files is only necessary when you want to export the original evidence files themselves. For the rest, the case folder is completely self-contained as all extracted items are stored in the case folder and can be exported without access to the original evidence files.

For example, when you index a folder with PST files, any email and other embedded items extracted from those PST files are stored in the case folder and can always be exported. The PST files themselves are not copied into the case folder.

Selection and configuration of hard drives

Because W4 is an intensive user of a system's hard drive, we recommend careful selection and configuration of the hard drives to optimize performance. Generally, newer hard drives will outperform older drives in that they benefit from design improvements and new technology. Consider the following when using W4:

- **Separate disks for evidence and case indexes.** During indexing, W4 accesses the database continually performing read and write functions. To use the hardware resources more efficiently, it is recommended that the evidence data and the case data be allocated to separate hard drives. For example, put the case data on the "C" Drive and the evidence data on the "E" Drive. See the hardware requirements section for appropriate drive sizes given the case at hand.
- **Optimization folder.** You can optionally specify a third folder for optimization purposes. This folder is used for storing temporary indexing data that else would be stored in the case folder. When the optimization folder resides on a different drive than the case folder or evidence folder(s), this can further improve indexing performance. Optimization folder can be specified via "case.json" file by adding "optimizationFolder" parameter. Here is an example of setting the optimization folder to "Z:\W4 Optimization" in case.json:

```
"optimizationFolder": "Z:\\W4 Optimization"
```

- **Disk space.** The amount of disk space needed to store your case depends heavily on the nature of your evidence data. As a rule of thumb, you should reserve twice the size of your evidence data for storing the case folder. The optimization folder has the same storage requirements as the case folder.
- **Proper connection.** To realize maximum benefit from W4's multi-disk optimization architecture, ensure that the hard drives are appropriately connected to the computer's motherboard to benefit from the higher available bandwidth. For example, connect the drives to the SATA-300 or SATA-600 connector rather than the smaller bandwidth carrying SATA-150.
- **Configure the system's BIOS correctly.** Typically, the computer's BIOS defaults to the lowest common denominator to facilitate compatibility for connected hardware components. As a result, performance and speed can suffer. To address this possibility, check the BIOS to:
  - Ensure the hard drive supports Native Command Queuing – it should!
  - Confirm that the SATA control mode is set to either AHCI or RAID. Note: if the setting is at IDE (typically the default), W4's performance will suffer with slower indexing and searching as a result.
- Use of external and/or network drives. **Internal drives are always the preferred option for W4.** W4's indexing and search performance can deteriorate significantly when used with external or network drives.
  - If required, external drives such as a USB can be used to hold the evidence data. However, it is recommended that the fastest available connection option be used. USB 3.0 or eSATA should offer acceptable performance. Avoid USB 2.0 drives as they are significantly slower.
  - Network drives may be acceptable for holding evidence files if on a fast network. When using network drives, it is imperative that no other users access the files at the same time. You should also ensure that no network antivirus or filtering software blocks the indexing processes.
- When processing a large case (> 100 GB of evidence files), it is advisable to format the NTFS disk with a cluster size that is larger than the default (usually 4 KB). This reduces the chance of

defragmentation issues during indexing. Furthermore, it is recommended to turn off disk compression.

4.3. Installation troubleshooting

4.3.1. Error codes

Error code 7 (H0007)

“HASP key not found (H0007)”

This error code might be caused by other HASP dongle protected programs. Please close all HASP related programs (i.e. EnCase, Smart Mount) and reinstall W4.

Error code 31 (H0031)

“Could not find a valid W4 license, please insert a dongle”

This error message is shown when your trial license has expired, or when you unplug your dongle while W4 is running and it cannot fall back to a non-expired trial license. You can only continue using W4 by inserting a dongle.

Error code 33 (H0033)

“Unable to access HASP SRM Run-Time Environment (H0033)”

This error code may be triggered if you run antivirus software. It is probably due to the antivirus software incorrectly blocking access to the HASP install. Please update your antivirus software to the latest virus definition file.

If this problem persists, reboot your computer, open a Command Prompt, and run (as administrator)

```
<w4-dir>\bin\haspdinst.exe -i -kp
```

and restart W4.

Error code 37 (H0037)

Other HASP dongle protected software may cause this error. Please close all HASP related programs (i.e. EnCase, Smart Mount) and reinstall W4.

If this problem persists, open a Command Prompt, and run (as administrator)

```
<w4-dir>\bin\haspdinst.exe -i -kp
```

and restart W4.

If problem persists after running this command, please open a Command Prompt as administrator and run

```
net start hasplms
```

Error code 41 (H0041)

“Your W4 (trial) license has expired (H0041)”

This error will be triggered if W4 is run and your trial license has expired. Once the trial has expired, you can only continue using W4 by inserting a dongle.

Error code 51 (H0051)

“Virtual machine detected, cannot run without a dongle (H0051)”

To protect our intellectual property, the evaluation version of W4 WILL NOT run in a virtual machine (VM) environment. A “stand-alone” machine is required. This is only true for the evaluation version; W4 will run in a VM environment using a dongle.

Solution 1: Reconnect the USB dongle to your computer

Solution 2: Install the W4 evaluation version outside a virtual machine

4.4. Memory and crawler count settings

The W4 process and its child processes (one for each case that you open + additional processes during indexing and exporting) are limited by the amount of RAM that the process can maximally use, despite how much memory is installed in the machine. On some data sets this limitation can cause issues when indexing or reviewing the data. These issues can be recognized by errors in the log files containing the text “OutOfMemoryError” or “java heap space”.

When such errors occur, a workaround may be to increase the automatically managed memory settings, especially when the machine meets the recommended hardware settings (at least 8 GB of RAM).

To increase these limits, edit the “case.json” file in the case folder. Add or change the parameter “heapSize” (number of megabytes, e.g. “heapSize”: 6000). Note that you can never specify more than half of the available system RAM. This is to make sure that W4’s child processes and the OS still have sufficient memory available to them.

When the memory issue relates to the processing of evidence files (you may need to contact tech support for that diagnosis) or to exporting, then locate the file: `<case folder>\prefs\case.prefs` and open it in a text editor. Add the following line or change it if the setting is already there:

```
ServiceMaxHeap=2048M
```

This instructs W4 to use maximally 2048 MB of memory for service processes. Increase this number to the higher value suggested to you by tech support. For processing of EDB files, a minimum of 3 GB will be necessary, e.g.:

```
ServiceMaxHeap=3G
```

By default, W4 will use up to 4 parallel crawlers when processing evidence files. In some cases, the limit can be increased by using the CrawlersCount setting in the same case.prefs file. The number of crawlers should never exceed the number of CPU cores on your PC. Setting a too high number might result in non-optimal performance. As an example, the following setting will tell W4 to use 8 crawlers:

```
CrawlersCount=8
```

4.5. Where are W4's data files located?

There is a W4 data folder in your home folder. Typically, it is in

```
C:\Users\<USERNAME>\AppData\Roaming\Vound\W4
```

Portable version stores its data folder in the app folder, e.g. in:

```
F:\w4-portable\config
```

4.6. Where can I find W4's log files?

W4 has two types of log files:

- Case-specific log files. These will contain any messages (errors, warnings, status messages) relating to your activities in the case, such as indexing, searching, and exporting. They are in

```
...\W4\cases\<CASE FOLDER>\logs
```

- Log files of operations performed in the Case Manager, such as exporting or importing a case. These are in

```
...\W4\logs
```

The log files can be opened in any text editor like TextPad or Notepad++. Be aware that Windows' default text editor Notepad may have issues opening large files.

Click Help > Open Log Folder to open the log folder of the current case.

5. Managing cases

A case is a collection of evidence sources that can be searched by W4 as a single collection. You use cases to organize your investigations.

When you start W4, the Case Manager will first show up. Here you can define new cases, open, and edit existing cases and remove old ones.

5.1. Adding cases

To create a new case, select “New” in the Case Manager window. Use this option to create a new case from scratch to index a new set of evidence files on your machine. When the New Case dialog is displayed, give the case a name, enter an optional description and select a location where you want to store the case data.

To add an existing case, select “Browse” option. Use this when you have a case folder already on your system, but it is not yet in the list of cases shown by the Case Manager.

The default location for data storage is

```
C:\Users\<username>\AppData\Roaming\W4\cases
```

When you use a different parent folder, subsequent cases will default to a subfolder in that parent folder.

When processing a large case (> 100 GB of evidence files), it is advisable to format the NTFS disk with a cluster size that is larger than the default (usually 4 KB). This reduces the chance of defragmentation issues during indexing. Furthermore, it is recommended to turn off disk compression.

5.2. Editing a case

In the Case Manager, use “Edit…” to open the “Edit case” dialog to change the case name or description.

You cannot change the Data folder.

5.3. Deleting a case

In the Case Manager, use “Remove” to remove the selected case from the Case Manager’s cases list. You will be asked to confirm the deletion.

By default, only the reference to the case is removed, the case folder is left intact. By checking “Also remove the case folder from disk”, the case folder will be permanently removed as well.

Removal of the case folder cannot be undone. Also, all files that you may have placed manually in the case folder will also be removed.

5.4. Exporting a case

In the Case Manager, use “Export” to export data from the selected case to a new case. Use this option to:

- Create a subset of the case by filtering out sensitive or unwanted items.
- Create a portable case that could be given to a third-party for review who doesn’t have W4 installed.

It’s not possible to export data to an existing case. This feature might be added in a future version.

In the export dialog use the “Target case” field to set the name of the new case. Choose a location for the new case using the “Target case folder” field. Select the case type:

- Use “Regular” option to create a regular case for the use on this or other machine with W4 installed. The created case will be added to the case list in the Case Manager.
- Use “Portable” option to create a portable case. Portable case is a self-contained folder that includes the case data and a copy of W4 viewer. To open the portable case click “open_case.exe” in the case folder.

Portable case can be opened on any machine and doesn’t require to have a license or W4 installed. Portable case is opened in viewer mode by default. That means no new data can be added to the case, and the case cannot be re-indexed. However, it is possible to add tags and notes and export items.

Portable case is not protected from modifications by itself. If the case is opened with a full version of W4, it will be possible to add new sources and re-index data.

Select the export scope:

- Use “Entire case” option to export all data from the case including tags and notes.
- Use “Selected tag only” option to export the selected tag only. With this option it will also be possible to select whether to export tags, notes, keyword lists and item links.

Selected items are exported to the target case along with their metadata and original content (if it’s present in the source case).

W4 will not export family items automatically. For example, if you need to export emails and their attachments, you would need to select both email and attachment items for export.

If “Export tags” option is selected, it will export *all* tags from the case. If you don’t want certain tags to be present in the target case, you can open the result case and delete the tags manually.

If “Export item links” option were not selected during the export, it is possible to rebuild the links in the target case later.

5.5. Processing a case in Intella

For cases that need to go to the next step of detailed analysis and review, all results identified by W4 can be incorporated into your Intella case via the new W4 import to Intella feature called the WIN import. In this way your case can go from first look all the way to multiuser review and load file. W4 coupled with Intella offer a powerful suite of investigative tools not seen in other platforms.

In the Case Manager, use the “Process in Intella...” button to convert the selected W4 case to Intella case. You must have a compatible Intella version installed (2.3 and higher). If there is no compatible Intella version is found, the button will be greyed out. More details about W4 to Intella case conversion can be found in the Intella User Manual in section 10.2.6 Importing Vound W4 Case.

6. Case tab

Sources are one of the key concepts of W4. They represent the locations where items such as registry artifacts, emails and documents can be found. The user explicitly defines the sources, providing full control over what information is searched.

6.1. Source types

The supported source types are:

- **Folder.** A single folder with source files on a local hard drive or on a shared/network drive. Such source files could be:
  - Regular loose files like MS Word, Excel and PDF files.
  - Email containers such as MS Outlook PST/OST, IBM Notes NSF files, Mbox files.
- **Disk image.** A single disk image in one of the supported formats.
- **Local disk.** A physical or logical disk connected to this computer.
- **Cellphone extraction.** A single cellphone extraction in one of the supported formats.

Notes on mail formats

W4 supports PST and OST files created by the following versions of Microsoft Outlook: 97, 98, 2000, 2002, 2003, 2007, 2010, 2013, 2016, 365. Make sure that W4 has exclusive access to the PST or OST file; it cannot be open in Outlook or other application at the same time.

W4 will try to recover the deleted items from the file. Recovered items will be placed in a special folder named `<RECOVERED>`. Furthermore, W4 may encounter items outside the regular root folder. Any such items are placed in a special folder called `<ORPHAN ITEMS>`. Recovered emails may contain traces of other emails. This should be considered when reviewing such items. There is limited ability to recover deleted emails from OST 2013 files.

Orphan items may contain unreliable data. For example, some orphan items can contain pieces of the message body, and message metadata from different emails. This may be due to the way the email client caches message data in the email container.

You should consider whether this information should be included in exports. Some clients may not want this information exported due to its unreliable nature.

To index NSF files, IBM Notes 8.5 or higher needs to be installed. For NSF files made with IBM Notes 9 it is recommended to install IBM Notes 9. W4 supports all NSF files that can be processed by the installed IBM Notes version. Make sure that W4 has exclusive access to the NSF file; it cannot be open in a Notes client or other application at the same time. Only NSF files containing emails are supported by W4, all other types are not supported. Make sure to use a default Notes installation and user configuration. A “corporate” Notes installation is often problematic for indexing, e.g. because of installed plugins interfering with access to the NSF file, the installation being tied to the corporate identify management system, etc.

The IBM Notes tool “nupdall.exe” can be used to convert older NSF files to NSF files that can be processed by IBM Notes 8.5 and higher.

W4 supports Windows 10 Mail mailboxes, provided that the account uses the POP protocol. Accounts that use the IMAP protocol are not supported, as only POP accounts store mails locally. Furthermore, Windows 10 mails do not keep track of BCC-ed email addresses and of the email headers.

W4 supports DBX files created by the following versions of Microsoft Outlook Express: 4.0, 5.0, 6.0.

W4 has been tested on Thunderbird Mbox files.

W4 supports MS Exchange EDB files of Exchange versions 2003, 2007, 2010, 2013 and 2016.

Some items may turn out to only contain email headers and are lacking an email body. Examples of such items are messages typically sent back by mail servers to indicate undeliverable mails, e.g. due to an unknown recipient or a mailbox quota that has been reached. Such items are typed as “Email Headers” rather than “Email Message”.

Notes on folder sources

W4 doesn’t support extraction of system and registry artifacts for folder sources. This feature might be added in a future version though.

Notes on local disk sources

W4 reads data from local disks at the file system level bypassing the operating system. That makes it possible to capture system protected and deleted files while not leaving traces in the system. W4 needs to be run with administrative privileges to access data on local disks. The physical disk option can be used if the disk is not encrypted. It allows to access hidden partitions (such as the OS recovery). The logical disk option can be used to access BitLocker protected or RAID volumes.

6.2. Adding sources

Adding sources to W4 is done in the Sources tab. Select “Click or Drop Sources here”, then select the source type. For disk images it’s enough to select the first disk image part only (such as image.e01). W4 will find the remaining parts automatically (image.e02, image.e03 and so on).

Supported file systems and partition types

The following file systems have been tested: FAT16, FAT32, ExFAT, NTFS, Ext2, Ext3, Ext4, HFS, HFS+, APFS and ISO 9660. Other file systems such as YAFFS2, ISO 13346 (UDF), UFS 1 and UFS 2 may work but have not been tested yet.

MBR and GUID partition tables (GPT) partitions are supported. Apple Partition Maps (APM) have been tested but results were mixed. When W4 fails to index such an image, we recommend mounting it manually and indexing the mounted drive using a “File or Folder” source.

APFS and BitLocker encrypted volumes are supported. When W4 detects such an encrypted volume, a dialog will be shown where it’s possible to enter a password or recovery key.

File recovery

When the “Recover deleted emails and files” option is turned on in the source definition, W4 will attempt to recover deleted files and folders using information found in the Master File Table (MFT). The content of the deleted files will only be extracted from NTFS partitions when possible (see below). For all other supported file systems, only the metadata will be extracted, no file content. W4 will NOT recover deleted files and folders from unallocated or slack space. The recovered content may contain data blocks that didn’t belong to the original file. Additional verification is required.

When indexing a disk image or local disk, W4 will scan all the MFT entries. Those entries marked as unallocated will be reported as deleted items. Additionally, for NTFS file systems, W4 will analyze the allocation status of all the data blocks referred to by the MFT entry. The entire content of the deleted file is extracted if any of the following conditions is true:

- There is at least one unallocated data block referred to by the MFT entry, or
- The MFT entry has only resident data. That means that the entire file content is located inside the MFT and therefore can be extracted.

In all other cases, only the metadata will be reported.

6.3. Source configuration

After the source has been added to the list, it can be configured. There are three sections on the source configuration panel: General, Artifacts, Volume Shadow Copies and Advanced.

General

In the General section you can define source name, description, examiner and evidence number. Source name and description will be shown in the source list in the left panel.

When the Processing Scope option is set to "Registry artifacts and user folders", W4 will index the following items only:

- Registry artifacts such as operating systems, user accounts, devices, programs
- System artifacts found at common locations such as Windows Event Log, recently accessed files and folders, recycle bin, prefetch files
- Any other artifacts, emails, documents and media files found in user folders (e.g. C:\Users).

When the option is set to "Entire Disk", W4 will index the entire disk image. Note that the option applied to disk image and local disk sources only.

A suspected system base time zone can be entered. This setting indicates the time zone of the system from which the evidence file(s) were obtained. By entering this time zone, all dates associated with items from this source will be processed using that time zone, rather than the time zone of the investigator’s system. This often makes it easier to correctly interpret those dates, e.g. determine whether a given timestamp falls inside regular business hours. By default, the local time zone is used for new sources. Time zones supporting Daylight Savings Time (DST) are marked with an asterisk (*).

Note that a separate setting called Display Timezone (see Preferences) is used to determine in which timezone all dates are displayed in W4. That can be used if the case contains several sources (disk

images) that came from different timezones.

Artifacts

The Artifacts section allows to select which categories need to be processed.

Volume Shadow Copies

Volume shadow copies (VCS) is a mechanism in Windows OS that preserves previous versions of files in a special hidden area on the disk. A new VSC snapshot is often created by Windows automatically when installing major system updates or drivers.

This option allows to extract and index files from VCS potentially revealing previous versions of documents and deleted files.

For disk image and local disk sources you can select specific snapshots that need to be processed. For folder sources, if the option is turned on, W4 will try to detect and extract all volume shadow copies from all disk images found in the folder.

By default W4 will only extract the files that were changed between snapshots. That allows to save a lot of processing time and disk space by not indexing the same files many times:

- Select "Prefer oldest files" option to extract all files from the oldest snapshot and only the changed files from the newer snapshots.
- Select "Prefer newest files" option to extract all files from the current file system and only the changed files from the older snapshots.

W4 uses the last modified date of the file to determine whether it changed. It is also possible to take the last access date into account.

Enabling volume shadow copies processing might considerably slow down the indexing process.

Advanced

This section contains advanced option that can be used to fine-tune the indexing engine:

- Select *Process images embedded in emails and documents* if you want to extract images embedded in emails, MS Office, OpenOffice, PDF, and XPS documents. This will make these images separately searchable and viewable.
- Select *Process archives* if you want to index files inside archives such as ZIP and RAR files.
- Select *Recover deleted emails and files* to enable the processing of deleted emails from MS Outlook (PST, OST) and MS Exchange (EDB) files, deleted files and folders from disk images.
- Select *Index full email headers* to enable full-text indexing of email headers. If this option is turned off W4 will not be able to search email headers via the instant keyword search.
- Select *Determine geographic location of emails* to let W4 estimate the geographic location of an email senders IP address, using a lookup table. To be able to use this feature, a GeoIP2 or GeoLite2 database needs to be present. See the Preferences section for how to properly set up a GeoIP2/GeoLite2 database.
- Select *Extract and index raw data* to extract and index raw data for items (low-level metadata).

6.4. Keyword lists

The keyword list feature can be used to automate searching with sets of previously determined queries. Keyword lists need to be added before you index the data. Then, during the indexing, if W4 finds any hits, the results will be immediately reported under the Keyword Lists category in the Search tab.

The most basic keyword list is a text file in UTF-8 encoding that contains one search term per line. It is also possible to use regular expressions. In this case the text patterns are defined using IEEE POSIX regular expressions syntax. See http://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1_chap09.html for documentation on this syntax. Use Regex Enabled checkbox to specify keyword lists that should be treated as regular expressions. Note that using a lot of regular expressions may slowdown the indexing.

The following options can be applied to keyword lists:

- **Search scope.** The option controls which parts of the item W4 will search in:
  - *Name only* to search in item names only.
  - *Metadata* to search in all item metadata fields (including item name and message headers).
  - *Full text* to search in all item text including extracted text, metadata and item name.
- **Artifacts.** The option controls the list of artifacts which W4 will search in. For instance, sometimes it is required to search in emails and documents only, but not in system logs.
- **Case sensitive.** The option controls whether lower- vs. uppercase should be considered by the search operation.
- **Regex enabled.** If turned on, each line of the keyword list is treated as a regular expression.
- **Highlight hits.** Turn this option on to highlight the hits found in this keyword list. This applies to the table view and previewer only.

To add a keyword list click Add keyword list button in Sources tab in the Keyword lists section. Click Delete button to remove a list.

6.5. Hash filters

MD5 hash filters can be used to exclude or tag items that have a specific known MD5 hash from a case. The so-called "De-NISTing" of evidence data is the most well known application of such hash lists: it excludes many files that belong to the operating system or common software applications from your case. But you can also add other types of MD5 hash lists, or create your own.

When selecting one or more of the hash filters for the source, W4 will ignore or tag any items that have an MD5 hash that is in at least one of the filters. After the source has been indexed, the filtered items will not be visible in your case.

W4 can create an MD5 hash filter from a CSV file, where the MD5 hash is encoded as a hexadecimal value. To do so, click "Create" to open the "Create hash filter" dialog. After specifying the path to the CSV file W4 will analyze the CSV file and show you the values for the first few lines. If there's a single column that contains MD5 hash values then that column will be automatically selected. After specifying an appropriate name for the hash filter you can start the filter creation by clicking "Create hash filter".

W4 can process plain CSV files, but also CSV files that are compressed using ZIP or GZIP. Processing the files in compressed form is often preferable as the uncompressed files can be very large (multiple gigabytes).

The Reference Data Set (RDS) that is made available by the National Institute of Standards and Technology (NIST) comes in the form of an ISO file. You will need to extract the `NSRLFile.txt.zip` file that is stored in this ISO. This `NSRLFile.txt.zip` file is a ZIP-compressed CSV file that can be processed by W4. You can find the most recent versions of the RDS at https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download/current-rds. For the "Modern RDS" set the "minimal" version is the smallest download that still contains the complete set of hashes.

Any MD5 hash filters that you create will also be available for use in other W4 cases. They are stored in the folder `C:\Users\<USERNAME>\AppData\Roaming\Vound\W4\hash-filters` (click *Open folder* to open this folder in Windows Explorer). The files in this folder can be copied to/from other computers to make them available there as well. Clicking *Rescan folder* will update the list of available filters.

In portable version the hash filters are stored locally in the app folder (e.g. `F:\w4-portable\config\hash-filters`). To transfer hash filters from normal to portable version you can either copy the file manually or use the search profile feature.

Deleting MD5 hash filter files will affect the ability to re-index other cases that use the same hash filter.

6.6. Indexing

After defining a source, you can index it by pressing “Index all sources” button. Indexing is a background procedure. That means you can continue using W4 interface to search, preview and report items. The indexing status is displayed in the top right corner (Case Status label). The number of processed items and the indexing time can also be seen in Summary tab.

You can stop the index process at any time by clicking the small "Stop" button just next to the “Indexing...” label in the top right corner of the main window. When the indexing is interrupted by user, all the items that have been processed so far will be saved in the case.

Once indexing is complete, W4 will start building item links. When it’s done the Case Status will change to “Complete”. That means the case is ready and contains all the items.

Having anti-virus software active during indexing can lead to certain items not being indexed. This will usually be restricted to the files that are blocked by the anti-virus software, but this cannot be guaranteed. Running anti-virus software may also affect indexing performance.

When indexing was interrupted by clicking the Cancel button, it would not be possible to continue indexing at a later point in time. A full re-index is required if a complete index is desired.

We recommend that you back up the case after indexing it.

Re-indexing a case

There may be circumstances when you want to re-index the entire case, e.g. to use extraction features offered by a newer W4 version or fix a broken index.

To rebuild the case index from scratch, use the Re-index all sources button in the Sources tab. W4 will remove all indices it has previously created and create new ones.

For this to work, all evidence files must be present at the location they had during the initial indexing.

Any tags and notes will be retained during re-indexing. The item IDs will remain the same after re-indexing.

6.7. Editing sources

To see the configuration of a source, go to the Sources tab and select it in the source list. You can change source name, description and any other options.

If you want to change the options that affect indexing (e.g. Process archives), a full re-index will be required.

7. Summary tab

The Summary tab contains several sections that together give a concise overview of the information inside the case, revealing suspect behavior, and giving rise to follow-up investigative questions.

7.1. Case status

The Case status section contains the following information:

- **Case status** that tells whether the case is empty, being indexed or complete.
- **Indexing time** shows the time of the last indexing attempt or the current indexing time if the case is still being indexed.
- The number of **processed items** for the last indexing attempt.

7.2. Windows user accounts

The User Accounts panel shows the list of all found Windows user accounts in the case.

7.3. Artifacts

The pie chart in this section shows the distribution of all found artifacts in the case. Each section of the chart represents a top-level category.

The artifacts panel below shows the number of items for each category. You can click on a category to see the number of items for its sub categories. Clicking on a sub category will open the selected category in the Search tab.

7.4. Keyword lists and hash filters

Keyword lists and hash filters panels show any matches that have been found in the case. Note that the hash filters chart only shows the tagged items.

7.5. Last activity

The Last Activity section consists of three panels:

- Last 10 events when a user logged on or off.
- Last 10 events from web browser category such as visited pages or downloaded files.
- Last 10 events related to USB device usage such as device removal or accessing files on a USB device.

8. Recipes

Recipe is a mechanism to configure and run searches based on common case types. Each recipe consists of a set of filters that define the result items.

8.1. Using recipes

Each case consists of its own set of recipes. The Recipes tab shows all the recipes in the case. The number of matched items for each recipe is shown in the recipe title.

To run a recipe click the *Run* button in the recipe panel. That will open up a new search tab with the name of the recipe. The Recipe Search tab works almost the same as the normal Search tab. The only difference is that the displayed items are limited to the recipe items.

The recipe search tab contains the additional menu shown in the top left corner (the gear icon):

- *Refresh* entry will refresh the content of the recipe, if the indexing is in progress.
- *Show empty categories* option controls whether to show categories without items.
- *Show Recipe categories only* option controls whether to show only the categories defined in the *Artifacts* section of the recipe. Otherwise, all categories are shown. This option is useful when you only need to see specific categories. But for categories like "Last Activity" or "Odd Hours" it is useful to see all the categories in the case.

You can have multiple recipe search tabs opened at the same time. Recipe search tabs can be closed at any time using the small cross icon in the tab title. W4 will restore all opened recipe search tabs when the application is restarted.

The items shown in the Recipe Search tab are not updated automatically when the indexing is in progress. To update the items manually click the *Refresh* button in the recipe menu.

8.2. Managing recipes

It is possible to edit any existing recipe. To do that move the mouse cursor over the recipe panel and the Edit, Export and Remove buttons will appear. Click the *Edit* button to edit the recipe:

1. The *Source* section allows to include items from a specific source only. By default it is set to "All Sources".
2. The *Date Range* section allows to filter items by date. Click the *Edit* button to set a date range.
3. The *Artifacts* section controls which artifact categories will be included in the recipe. Click the *Add* button to add a new category. To remove a category right click on its icon and select *Remove* in the context menu.

To remove a recipe from the case click *Remove* button. Note that this operation cannot be undone.

It is possible to create a custom recipe by clicking the *Add New* button on the recipe list panel. That will open up a dialog when you enter recipe title, description, icon and define whether to show recipe categories only when it's evaluated. See the description of *Show Recipe categories only* option above.

8.3. Transferring recipes between cases

Recipes can be transferred to a different case by first exporting the recipe to a JSON file, and then importing it into the second case. Click the *Export* button on the recipe edit panel to export it to a file. Click the *Import* button on the recipe list panel to add it to another case.

Another method of re-using recipes in another case is search profiles.

9. Search tab

The Search tab allows to search and explore items in the case.

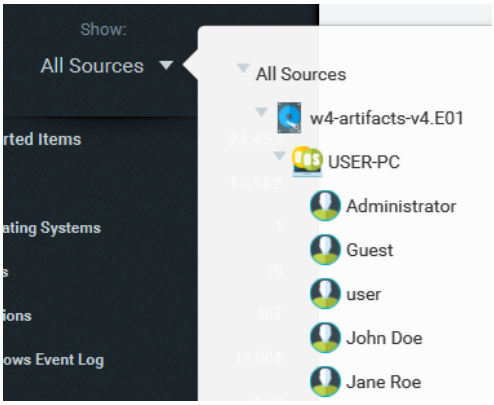
9.1. Categories

Click one of the categories on the left to see items from this category. It is possible to select multiple categories at once. Click several categories while holding the CTRL button. There is a special category “All Supported Items” that is just a convenient way to show all items in the case.

9.2. Filtering

Location

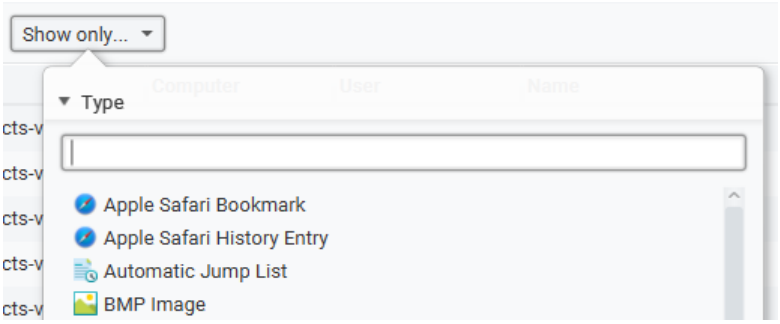
By default, the Search tab displays information about the entire case. It is possible to show information from a specific source, computer or user only. To do that, click “All Sources” in the top left corner and select a location node:



Type

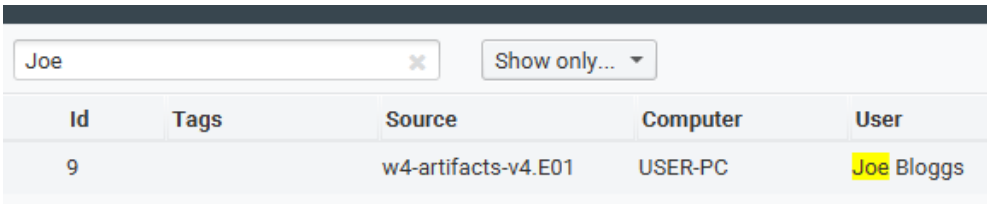
When a category is selected the result items will be shown in the panel on the right. There is an option to filter the results shown in the panel by type. To do that, click “Show only” and a type. After that only the items of the selected type will be shown in the panel below. It is possible to have more than one type filter.

Additionally it is possible to filter items by file and image size.



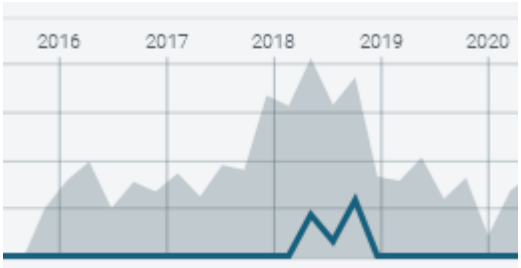
Keyword search

Another way to filter items shown in the panel is to use keyword search. See “Keyword search” section for more details.

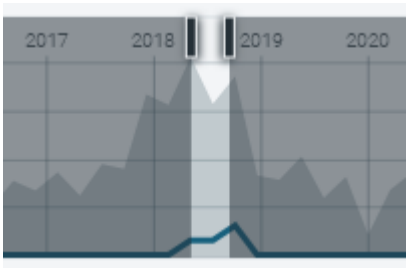


Timeline filter

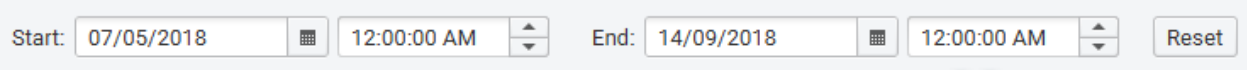
The timeline at the bottom shows the item distribution over time for the entire case no matter which category is selected. The gray area shows all the items in the case, while the blue bold line shows the current selection.



It is possible to use the timeline as a filter. Click and drag the mouse to select the desired time interval. The result panel will show items from the selected interval only in this case.



An alternative way to do the same is to use Start and End fields. You can also use these fields to adjust the selection. Click Reset button to reset the timeline filter.



When the Events view is selected, the bottom timeline will highlight (with orange color) the date range that is currently visible in the Events view. When you scroll the results up and down, you will see how the highlighted area is shifted left and right.

9.3. Result view types

When a category is selected, the results can be shown as:

- Table
- Events
- Thumbnails
- Geolocation

Use the switch at the top right corner to select the view type.

9.4. Table view

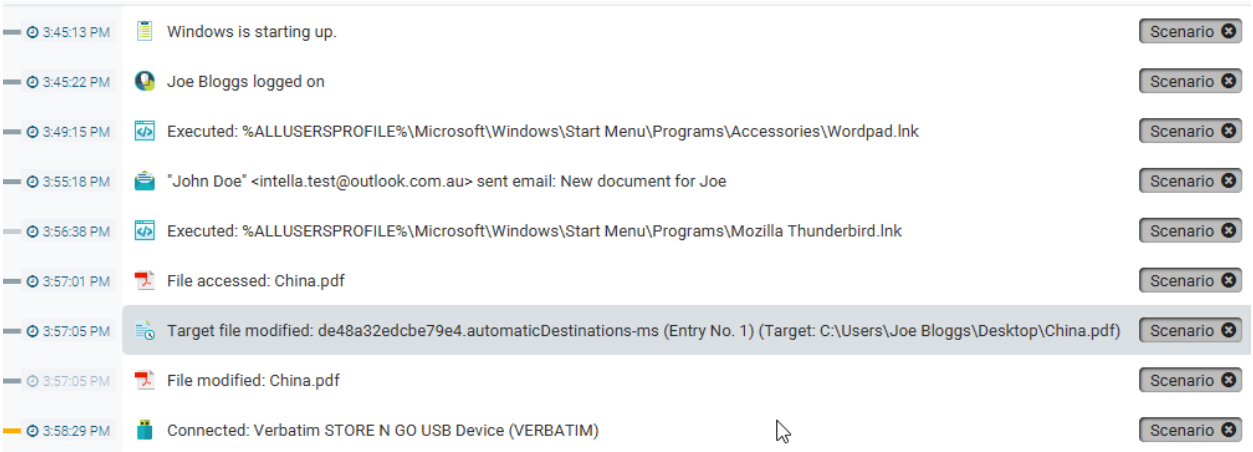
Table view is the default view. It works well for tabular data like registry artifacts.

The columns can be reorganized by dragging a column header to a different location in the table.

By clicking on a column header, the search results will be sorted alphabetically, numerically, or chronologically, depending on the type of information shown in that column. By clicking the header once more, the sort order will be reversed. Clicking one more time will remove the sorting, letting the results be displayed in their original order.

9.5. Events view

Events view allows to see the results as a list of events sorted chronologically. Selecting an event will show the details of the item that the event belongs to in the preview panel.



9.6. Thumbnails view

Thumbnails view displays the thumbnails of the images. If there are no images in the result set it will show nothing.

9.7. Geolocation view

The Geolocation view shows the (estimated) locations of all search results that have geolocation information on the world map.

Currently, geolocation data is extracted from the following sources:

- Images – GPS coordinates in the EXIF metadata.
- Cellphone reports – available information depending on the device model, extraction utility and extraction method.
- Emails – through geolocation lookup of the sender IP.
- Google Maps URLs – e.g. from browser histories and bookmarks.

Using this information, a set of search results can be mapped to a set of geographic coordinates, roughly representing the “where” of the found items. Any items that do not have any geolocation information associated with them are omitted in this view.

Showing each item’s estimated location on the map would make the view very cluttered. Items laying in the same area are therefore grouped into clusters, shown as a blue circle in the screenshot above. The number in a cluster represents the number of items whose geolocation falls in that area.

When zooming in, the geographic size of what constitutes the “same area” will be reduced, resulting in clusters getting split up into smaller clusters. Zooming out of the map consolidates clusters into fewer and larger clusters again. This cluster management allows the user to inspect specific locations in detail.

Zooming can be done using the control buttons in the top-left toolbar or by using the mouse wheel. To pan (move sideways) in a zoomed map, move the mouse while holding down the left mouse button.

To inspect the content of cluster, the user can select it by clicking on it. The contents of the selected cluster will be displayed in the list below.

Resources

W4 may need two resources to make the most out of the Geolocation visualization:

- Tile server.
- IP geolocation database.

Tile server

By default, W4 uses tiles (images containing parts of the map) that are embedded in W4 to construct the world map. This makes it possible to use the Geolocation view without any configuration and without requiring an Internet connection to download these tiles.

Due to the enormous size of a complete tile set covering all zoom levels of the entire world map, the embedded tile set is limited to the first 6 zoom levels. As a rule of thumb, this usually shows the major cities in most countries, but it will not let you zoom in to see where in the city an item is located.

To zoom in beyond that zoom level, a connection to a tile server is needed. This can be a public tile server or one located in your network. See the Preferences section on how to configure a tile server.

A tile server may not only let you zoom in and create more fine-grained maps, it can also let you apply a different map rendering, e.g. a map containing elevation data, infrastructural information, etc.

IP geolocation database

To determine the geolocation of emails, W4 uses the chronologically first IP address in the Received email headers (i.e. the one nearest to the bottom of the SMTP headers). Next, a geolocation lookup of that IP address is done using MaxMind's GeoIP2 or GeoLite2 database. These databases are not distributed with W4 and therefore one needs to be installed manually.

See the Preferences section on how to acquire and install an IP Geolocation database.

Caveats

While the Geolocation view can quickly give a unique and insightful overview of a data set, there are some aspects of geolocation visualization to be aware of. Geolocation data is approximative by nature and manual verification of the findings will always be required. This is not a W4 limitation; it is inherent to the complexity and unreliability of the systems producing the geolocation information. Make sure that you are fully aware of these aspects and their consequences before relying on the findings.

GPS coordinates

GPS coordinates, such as obtained from the EXIF metadata of images or location-bound items extracted from cellphones, are usually quite accurate. However, they are subject to the limitations of GPS:

- In the best-case scenario, the accuracy is typically in the range of several meters. The accuracy can be lower or coordinates can even be completely wrong when the GPS hardware cannot receive a good signal (e.g. in the direct vicinity of buildings), due to hardware limitations of the GPS device (the theoretical maximum precision possible varies between devices) or simply due to bugs and hardware faults in the device.
- The same applies to comparable satellite-based navigation systems such as GLONASS.
- Geolocation coordinates may also have been determined using other techniques, e.g. based on geolocation information about nearby Wi-Fi networks and cell towers.
- Some devices combine several of these techniques to improve accuracy and coverage. Therefore, what is commonly referred to as "GPS coordinates" may not have been established through GPS at all.
- Coordinates may have been edited after the fact by a custodian using an image metadata editor. A set of different images with the precise same coordinates may point in that direction. This may

be harmless, e.g. to fill in the coordinates of images taken with a camera that does not have GPS functionality.

IP geolocation

The determination of an email's geolocation by using its sender's IP address is imprecise by nature, typically even more so than GPS coordinates. First, the determined Source IP address may be incorrect due to several reasons:

- Some email servers mask such IP addresses. Instead, it may in fact be the second IP address of the transport path that is being used.
- A web email client (e.g. Gmail used through a web browser) may have been used to send the email.
- The IP address may have been spoofed.
- The IP address may not reflect the sender's location due to the use of a VPN, Tor, etc.

Second, IP geolocation databases are typically never 100% accurate and the accuracy varies by region. See MaxMind's website for statistical information on their accuracy. Reasons for this imprecision are:

- The geolocation of an IP address may change over time.

Remember to take this into account when indexing an older data set!

- Some IP addresses may only be linked to a larger area like a city or even a complete country, yet the precise coordinates may give a false sense of GPS-style precision.
- The techniques behind the collection process for creating this database introduces a certain amount of imprecision.

Tile servers

Using a public tile server may reveal the locations that are being investigated to the tile server provider and anyone monitoring the traffic to that server, based on the tile requests embedded in the retrieved URLs. **Note** that to use a public tile server, you need to ensure that you comply with the tile server's usage policy. This is your responsibility, not Vound's.

Attribution

We are grateful for obtaining the data we have used for the embedded tiles generation from the OpenStreetMap project, ©OpenStreetMap contributors. See http://www.openstreetmap.org/copyright for more information on this project. The tile set is made available under the Open Database License: http://opendatacommons.org/licenses/odbl/1.0/. Any rights in individual contents of the database are licensed under the Database Contents License: http://opendatacommons.org/licenses/dbcl/1.0/.

9.8. Previewer

When you click an item in either table, events or thumbnails view, the Previewer panel will show the details of the selected item.

Toolbar

At the top of the Previewer there is several buttons that allow to perform certain actions with the item:

- **Tags.** This button will open a dialog that allows to add or remove item tags.
- **Add note.** This button will open a dialog that allows to add a note to the item.
- **Show item links.** This button will show item links in the Links tab. See Item Links section for more details.
- **Show parent.** This button will show the item's parent item (e.g. a parent email for an attachment).
- **Open in application.** This button opens the item using the computer's default application (e.g. a PDF file would be opened with Adobe Acrobat Reader if that is the default PDF viewer on your computer).
- **Save.** This button opens the "Save as" dialog. Enter a name and location if you want to store the item. This exports the item in its original format.

The tabs show the various aspects of the current item. The set of tabs shown for an item can differ from item to item, depending on the item type and which information that item holds.

Tabs

The following tabs are supported:

- **Preview.** This tab allows to preview item content as it was opened in its native application (e.g. Word document in MS Word). The Preview tab is only shown when the format of the current item is supported, and the Contents tab is not already showing it in its native form. The following file formats are supported:
  - Emails (when the email contains an HTML body)
  - Legacy MS Office formats (doc, xls, ppt)
  - New MS Office formats (docx, xlsx, pptx)
  - RTF
  - HTML
  - PDF
  - XPS
  - CSV and TSV files
  - WordPerfect
  - Open Office (Writer, Calc, Impress)
  - Images
- **Headers.** This tab shows the complete header of the email item. This tab is only shown when you open an email item.
- **Properties.** This tab shows a list of properties connected to the item. The list of properties shown depends on the type of the item and what data is available in that item.
- **Attachments.** This tab lists the attachments of an email. Double-click an attachment to open it.
- **Geolocation.** This tab shows item location on the world map.

10. Keyword search

To search for text, go to the Search tab and enter a query in the Search panel. The search will be executed automatically after a few seconds when you stopped typing. The search will only affect the currently selected category.

For query syntax rules, refer to the “Search query syntax” section below.

Instant keyword search in W4 is limited to metadata only. However full text search is available via keyword list functionality.

10.1. Search query syntax

In the text field of the Search panel you can use special query syntax to perform complex multi-term queries and use other advanced capabilities.

Lowercase vs. uppercase

Keyword searches work in a case-insensitive manner: during indexing all characters are lowercased, as are the characters in a keyword query.

This means that the query “john” will match with “john”, “John” and “JOHN”.

Use of multiple terms (AND/OR operators)

By default, a query containing multiple terms matches with items that contain all terms anywhere in the item. For example, searching for:

```
john johnson
```

returns all items that contain both “john” and “johnson.” There is no need to add an AND (or “&&”) as searches are performed as such already, however doing so will not negatively affect your search.

If you want to find items containing at least one term but not necessarily both, use one of the following queries:

```
john OR johnson
john || johnson
```

Minus sign (NOT operator)

The NOT operator excludes items that contain the term after NOT:

```
john NOT johnson
john -johnson
```

Both queries return items that contain the word “john” and not the word “johnson.”

```
john -"john goes home"
```

This returns all items with “john” in it, excluding items that contain the phrase “john goes home.”

The NOT operator cannot be used with a single term. For example, the following queries will return no results:

```
NOT john
NOT "john johnson"
```

Phrase search

To search for a certain phrase (a list of words appearing right after each other and in that order), enter the phrase within full quotes in the search field:

```
"john goes home"
```

will match with the text “John goes home after work” but will not match the text “John goes back home after work.”

Phrase searches also support the use of nested wildcards, e.g.

```
"john* goes home"
```

will match both “John goes home” and “Johnny goes home”.

Grouping

You can use parentheses to control how your Boolean queries are evaluated:

```
(desktop OR server) AND application
```

retrieves all items that contain “desktop” and/or “server,” as well as the term “application.”

Single and multiple character wildcard searches

To perform a single character wildcard search you can use the “?” symbol. To perform a multiple character wildcard search you can use the “*” symbol.

To search for “next” or “nest,” use:

```
ne?t
```

To search for “text”, “texts” or “texting” use:

```
text*
```

The “?” wildcard matches with exactly one character. The “*” wildcard matches zero or more characters.

Fuzzy search

W4 supports fuzzy queries, i.e., queries that roughly match the entered terms. For a fuzzy search, you use the tilde (“~”) symbol at the end of a single term:

```
roam~
```

returns items containing terms like “foam,” “roams,” “room,” etc.

The required similarity can be controlled with an optional numeric parameter. The value is between 0 and 1, with a value closer to 1 resulting in only terms with a higher similarity matching the specified term. The parameter is specified like this:

```
roam~0.8
```

The default value of this parameter is 0.5.

Proximity search

W4 supports finding items based on words that are within a specified maximum distance from each other in the items text. This is a generalization of a phrase search.

To do a proximity search you place a tilde (“~”) symbol at the end of a phrase, followed by the maximum word distance:

```
"desktop application"~10
```

returns items with these two words in it at a maximum of 10 words distance.

Like phrase searches, proximity searches also support nested wildcards.

Special characters

There is no specific support for the handling of diacritics. E.g., characters like é and ç will be indexed and displayed, but these characters will not match with 'a' and 'c' in full-text queries. A workaround can be to replace such characters with the '?' wildcard.

The following characters need to be escaped before they can be used in a query:

```
+ - && || ! ( ) \{ } [ ] ^ " ~ * ? : \ /
```

They can be escaped by prefixing them with a \ character.

During indexing, most of the characters in this list are typically filtered out and will never make it into the index. The rules for handling specific characters depend on the context in which they occur. For instance, punctuation characters like dots ('.') or dashes ('-') are significant within numbers, email addresses or host names, while being ignored (i.e. interpreted as whitespaces) between regular words. In the latter case, escaping them in the query will not make them searchable.

11. Tagging

W4 supports two types of annotations: tags and notes.

Tagging is the process where you connect a descriptive word to an item or event. For example, one of your items is a PDF document containing valuable information. You decide to tag the item with the word “Important”. Tagging helps you to organize results, for example by separating important and unimportant information.

Note is a single comment that can be assigned to an item or event.

Tagging and adding notes can be done in several ways:

- Context menu in table, events or thumbnails view
- Buttons in previewer

Item and event annotations

Item and event tags and notes work independently of each other. The following rules apply:

- When you tag an item, it would also tag all its events automatically.
- When you tag an event, it would also tag the parent item automatically.
- When you remove a tag from an item, it would also remove this tag from all events associated with this item automatically.
- When you remove a tag from an event, it would NOT remove the tag from the parent item if there are other item events associated with this tag.
- When you remove a tag from the last event, it would also remove the tag from the parent item.
- When you add or remove a note from an item, it would NOT affect its events and vice versa.

The above mechanism allows certain flexibility when constructing so-called custom timelines. For example, you may want to tag only certain connection events associated with a USB device, but not all of them.

11.1. Tagging via context menu

To add tags:

1. Select one or more items from the table, events or thumbnails view.
2. Open the context menu (right mouse click) and select “Add or edit tags”.
3. In the “Add or edit item tags” dialog you can select already defined tags or define a new tag with optional description.
4. You can optionally select a color that will be assigned to the new tag.
5. When you click OK, the marked tags will be linked to the selected items or events.

A color can be assigned to any tag. This color will be used in the Tags column in the table. To change the tag color click the box next to the tag name in the tag list.

When creating a new tag, a parent tag can be specified. Parent tags can be used to logically group tags, e.g. grouping custodian names, reviewers, locations, or priorities.

Parent tags can also be used to tag items. For example, when you have tags called Europe and Asia with subtags representing specific countries, you can choose whether to tag an item with a continent or a country.

The “Add or edit item tags” dialog can also be used to remove tags. It can be done by unchecking the tag boxes.

11.2. Tagging items via previewer

If you want to tag or remove a tag in the previewer, please take the following steps:

1. Select an item in table, events or thumbnails view
2. In the previewer panel click the Add Tag button to open the “Add or edit tag” dialog
3. Enter a new tag or select an existing tag. To remove a tag (to remove the connection between an item and a tag) just deselect the tag from the list.

11.3. Adding notes to items via previewer

If you want to add a note to an item in the previewer, please click the Add Note button. Enter the note and press ENTER. To remove the note, just delete all the text from it.

11.4. Adding, changing or deleting event notes in Events view

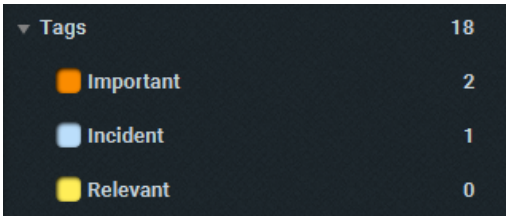
To add or change am event note, switch to the Events view and right-click an event. In the context menu select “Add or edit note”. Enter the note text.

To delete an event note, click the “X” button next to the note text.

11.5. See all tagged items or specific tags

To see all tagged items, click the Tags category.

To see items associated with a specific tag, click a tag under the Tags category.



11.6. Editing or deleting a tag

To edit a tag, please take the following steps:

1. Select a tag under the Tags category and right click on it.
2. Use the dialog that opens to either:

- Edit tag to change its name, color or parent tag.
- Delete tag to delete the tag.

When you delete a tag, it’s no longer in your case.

Please be careful when adding, editing or deleting tags. Tag operations cannot be undone.

12. Item links

W4 can analyze items in the case to build item links. Item link is a connection between items or their attributes. Item links feature allows to unveil hidden connections between items that don't seem connected at first sight. Examples of item links:

- Windows shortcut file (LNK) and its target file on the file system.
- File downloaded from the Internet and download entry in browser history telling when and where the file was downloaded from.
- Document and email address telling that the document was sent to this person.
- File on a local file disk and Jump List entry telling that the file might have been copied to a USB drive.

12.1. Building item links

Item links are built automatically when the indexing is finished. You will see a message at the top right corner "Building links". That means W4 is currently building item links. When it's done the message will change to "Case status: Complete".

There is a way to rebuild item links manually. That can happen if you updated to a new version that has an improved algorithm for detecting links. To do that, click "File → Rebuild links". That would rebuild the item links without re-indexing the entire case which is usually much faster and doesn't require access to the original evidence.

12.2. Exploring item links

There are two ways to explore item links:

- Select an item in table, events or thumbnails view and select "Add to Link graph" in the context menu (right click)
- Click the second button on the Previewer toolbar.

In either case the selected item will be added to the Links graph. W4 will switch to the Links tab automatically.

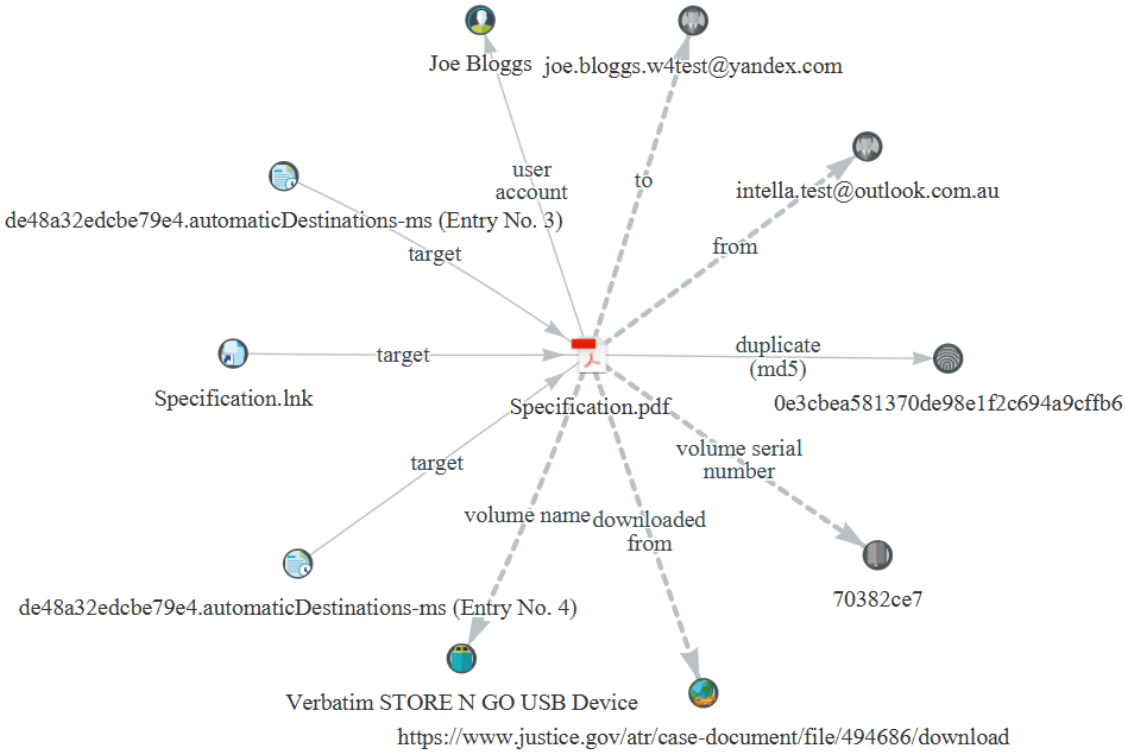
W4 will show all possible links from the selected item to all other items and attributes in the case. The selected item will be placed in the center.

12.3. Interaction with Link graph

You can click any item on the graph to preview its properties and content. You can click and drag any graph node to move it to a different position.

It is possible to explore item links shown on the graph further. Double clicking any node would make

this node a central node instead of the previously selected item. Now you will be able to see all item links for the new node. All previously explored nodes will be kept on the screen.



You can use the button toolbar that is located just above the graph to:

- Restore previous graph states using the Undo (Back) and Redo (Forward) buttons.
- Clear the graph.
- Remove a specific node from the graph. The node must be selected with a mouse click to do that.
- Fit to view button will zoom the graph so that you can see all nodes.
- Hide edge labels will temporarily remove all edge labels from the graph. This may improve readability of the graph if you have too many links. Press this button again to show the labels.
- Save for report button will create a snapshot (image) of the current graph so it can be inserted into a report. See Reporting section for more details.
- Manage saved graphs button allows to see all the saved graphs, edit their descriptions and remove them.
- Export button open the “Export link graph” dialog that allows to save the current graph to PDF or PNG format.

The panel on the left shows the list of items that are currently present on the graph. Clicking the item in the list would also select it on the graph.

Solid lines on the graph represent **direct** links, while dotted lines represent **indirect** ones. When two nodes are connected via a **direct** link that means either:

- an item node is linked to its attribute node such as Word document and its creator.
- two item nodes are linked to each other naturally such as attachment and its parent email.

When two nodes are connected via an indirect link that means it was derived from other links. W4 uses a special algorithm that only finds indirect links that represent means of transportations. In

other words, those links will tell you how a document might have been transferred to or from the computer. Therefore, we also call such links **Transport** links.

An example could be a Word document attached to email and then sent to a person. The link between the document and the person would be indirect (transport).

12.4. Transport links category

There is an easy way to find all items or events that have transport links. Transport Links category in the Search tab contains three subcategories:

- **USB Device Links.** This category contains all items associated with USB device usage. The category might be especially useful when working IP theft investigations.
- **Email Links.** This category contains all items that might have been sent by email.
- **Download Links.** This category contains all items that might have been downloaded from the Internet.

13. Search profiles

Search profile is a mechanism that allows to save and re-use certain case settings in a different case. It includes:

- Preferences. This is everything you can find in the *Preferences* dialog in the file menu. Plus the list of well-known system files used in Common System Files acquisition.
- Processing settings that will be used automatically for any new source.
- Tags.
- Keyword lists and their settings.
- Hash filters and their settings.
- Recipes.
- Reports.

13.1. Creating and managing search profiles

To create a search profile, go to the File menu and select *Search profiles*. The *Search profiles* dialog will show all search profiles available in the system. Search profiles are stored globally (i.e. they are visible in all cases).

Click *Create* to create a new search profile based on the current case. Enter the profile name and optionally case name, description and examiner. You can include or exclude the search profile components by selecting the corresponding check boxes. Click *Configure* button next to the *Processing settings* to configure processing settings that will be used in new sources. Click *Create* button to create a new profile based on the current case.

Click *View* button to view the currently selected profile.

Click *Delete* button to deleted the currently selected profile and all its files. Note that this operation cannot be undone.

Click *Import* button to import a search profile from a ZIP file previously exported from another system or portable version.

Click *Export* button to export the currently selected search profile to a ZIP file so it can be tranferred to another machine or portable version.

Search profiles created in the normal version of W4 will not be automatically visible in the portable version. You would need to use Export/Import functions to transfer the profile.

13.2. Using search profiles

Search profile can be selected when creating a new case either in the Case Manager or in Triage Launcher. Select the required search profile in the *Search profile* combobox to create a case based on this profile.

14. Reporting

Every report in W4 works like a template. That means you can re-use previously created reports with a new item set.

14.1. Creating, editing and removing a report

To create a report, go to the Reports tab and click Create report button. To edit an existing report, just select it from the report list. To remove a report, select it and click Remove report button.

14.2. Report configuration

General

The General section contains two fields: name and description. Those fields are only used to show the report in the list in W4. They are not included in the produced document.

Title

The Title section defines the information shown on the title page of the report. That includes report title and whether to include Vound and W4 logos.

The Custom fields sub section allows to enter one or more custom fields that will be shown just below the report title. By default, W4 adds the following fields: case name, case creation date and report creation date.

Headers and footers

This section allows to configure whether to show report title and page number in footer.

Table of contents

This section allows to configure whether to include the table of contents.

Summary

The Summary section defines whether to include the Summary page of the report. You can also configure which sub sections need to be included:

- **Sources summary.** If selected, the Summary page will include the list of sources with details for all items included in the report.
- **Types summary.** If selected, the Summary page will include the type statistics for all items included in the report.

Sections

This section defines what items will be included in the report.

By default, the section list is empty. Click Add section button to add section based on category. Each category can be configured individually. That allows great flexibility when reporting different types of

items. For example, you may want to show web browser history as a table, USB activity as a list of events and images as an image gallery. Each section has the following options:

- **Title.** This option defines the section title.
- **Description** is shown just below the section title and can include more detailed information about the section.
- **Display** as option allows to configure how the items are displayed. The following types are supported: List, Table, Events, Image Gallery.
- **Sort** by option defines the sort order of items.
- **Page orientation** allows to set the page orientation for this section. It's especially useful for tables and image galleries.
- **Columns.** This option defines the number of columns for image gallery display type.
- If **Export original format files** is selected, W4 will also export original format files along with the report. Report will contain hyperlinks to the export files. Note that not all items can be exported to original format.
- **Column chooser** section allows to configure which columns should be included. This option is only available for lists and tables.

To remove a section, click Remove section button.

The total number of items included in the report is shown just below the table.

The Import and Export section buttons allow to import and export the selected section to a JSON file. It can be used to move a section from one report to another.

Section options

Here you can find the options that are applied to all sections in the report. There are two options that control whether to include tags and notes in Events sections.

Link graphs

You can optionally include one or more link graphs saved using the Save for report button. The report will include both graph name and description.

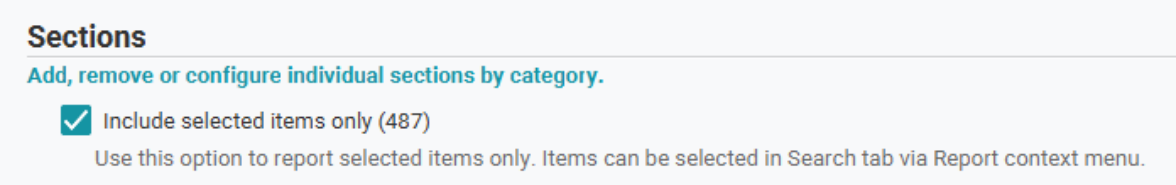
Output format

W4 supports creating a report in PDF or MS Word (DOC) format.

14.3. Limiting report to selected items

The option "*Limit reporting to*" allows to choose between reporting all items in the entire case and a specific subset of the case. To select specific items for reporting:

- Select a range of items in the table and click "*Limit reporting to selected items...*" button in the context menu.
- Select an existing report you wish to use or create a new one.
- W4 will switch to the Reports tab and the option "*Selected items*" will become available.



14.4. Producing a report

When report configuration is complete, you can click the Produce button to produce a report document in the selected format. Report creation is a background task. That means you can continue working with the case while the report is being produced. You can see the status of the task at the top right corner.

15. Acquisition

The Acquisition tab can be is used to acquire evidence when doing on-site triage.

Evidence acquisition features require W4 to be launched with administrative privileges. This is done automatically in the portable version.

15.1. Creating, editing and removing an acquisition

To create a new acquisition click *New acquisition* button, then select the type of evidence. W4 suports four types of acquisition:

- Physical memory (RAM)
- Physical and logical disk
- Folders
- Common system files

The following properties are common for all acquisition types:

- Image name. This will be the name of the produced file. W4 will add the file extension automatically based on the selected format.
- Destination folder. This will be the folder where the result files will be saved to, includeing the report file.
- Hash types. W4 can create hashes for the selected types (MD5, SHA-1). The produced hashes will be recorded in the image metadata (if supported) and report file. If the *Verify* checkbox is also selected, W4 will verify the hashes by reading the result file after the acquisition is complete and comparing the hashes. The result of verification will be recorded in the report file.
- Case number, Evidence number, Description, Examiner and Notes. These metadata fields will be added to the result image and report. If the acquisition format doesn't support metadata fields (such as ZIP), the metadata fields will be saved to the report file only.

Click *Acquire* button to start the acquisition process. Once the acquisition is started, it's no longer possible to change its settings. But you can click the *Duplicate* button to create a new acquisition with the same parameters. Click the *Remove* button the remove the acquisition. Note that it will not remove the associated image and report files.

Acquisition process is a background task, that means you can continue working with W4 while it's acquiring the evidence. You can only have one running acquisition at a time. If you started more than one acquisition task W4 will handle them one by one.

It is not possible to pause or resume an acquisition task. If it's stopped, you would need to restart it again from the beginning.

15.2. Memory acquisition

Physical memory acquisition is done with the help of *winpmem* tool. The result image file is saved in AFF4 format. If your memory analysis tool doesn't support AFF4 directly, it is possible to extract the

raw memory image from the AFF4 file. To do that, open the AFF4 file with any archive tool that supports ZIP format (such as 7zip), then extract the file *PhysicalMemory*. The file *PhysicalMemory\information.yaml* contains additional information about the memory dump that can be required by the memory analysis tool.

The recommended way to acquire memory is by using the Triage launcher (*w4_triage.exe*). See Triage launcher section for more details.

15.3. Physical and logical disk acquisition

To acquire a physical or logical drive select the required drive using the *Drive* box. You can choose between acquiring a physical or logical drive. The *Physical* option will acquire the entire physical device including all unallocated clusters and hidden partitions. The *Logical* option will acquire a logical volume (e.g. drive letter). It is useful when dealing with encrypted drives or RAID volumes.

When acquiring a physical drive that contains encrypted volumes, the result image file will contain the data "as-is", i.e. in an encrypted form. When acquiring an encrypted logical volume that is unlocked by the OS, the result image file will contain the decrypted data.

W4 supports three disk image formats: EnCase (E01), Raw (DD) and AFF4. For E01 and DD it is possible to specify the fragment (segment) size, so W4 will split the image file into segments of the selected size. For E01 and AFF4 formats it is also possible to select compression method and level.

15.4. Folders acquisition

This acquisition type lets you acquire specific files and folders. Use the *Local drives* panel to select the required drive or folder, its content will be shown in the panel on the right. Select a file or folder in the right panel that you wish to acquire and click *Add selected* button. The selected entry will be added to the panel below which contains the full list of paths that will be acquired. Deleted entries are shown as icons with a small red crosses.

Folder acquisition is done on the file system level. That makes it possible to acquire evidence without leaving traces in the operating system and capture system protected and deleted files.

The result is saved to a ZIP file preserving the full folder hierarchy (including drive and partition names) and original timestamps (created, modified and access dates).

15.5. Common system files

This acquisition type is almost the same as the Folders one. The only difference is that it will acquire the well-known system and registry files for the selected drive. If a physical drive is selected, W4 will scan all partitions in the drive and acquire all well-known files in all found partitions.

The following locations are captured:

```
$Recycle.Bin
Logs
ProgramData\Microsoft\Wlansvc\Profiles\Interfaces
users\*\AppData\Local\ConnectedDevicesPlatform
users\*\AppData\Local\Microsoft\Windows\UsrClass.dat*
users\*\AppData\Roaming\Microsoft\Office\Recent
users\*\AppData\Roaming\Microsoft\Windows\Recent
users\*\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat*
users\*\NTUSER.DAT*
windows.old\inf\setupapi*
windows.old\prefetch
windows.old\repair
windows.old\system32\config
windows.old\system32\winevt\logs
windows\inf\setupapi*
windows\prefetch
windows\repair
windows\system32\config
windows\system32\winevt\logs
```

It is possible to edit the list of well-known locations. To do that close W4, edit the following text file located in the case folder and restart the application:

```
<case>\prefs\common_system_files.txt
```

This file can be included in a search profile by selecting the *Preferences* option.

The default list of well-known system files is designed for Windows operating systems only.

15.6. Acquisition report

W4 will create a report in plain text format for each finished acquisition. It will contain all the details including the status, checksums, verification result and the error details if the acquisition finished with an error.

16. Triage launcher

Triage launcher is an alternative way to quickly create and process a new case. It is only available in the portable version and designed for on-site triage in the field.

Double click on `w4_triage.exe` to run the triage launcher.

16.1. RAM capture

By default, the Triage launcher will ask whether you want to capture the physical memory (RAM). If you click OK, it will acquire the RAM using `winpmem.exe` tool. The captured image will be saved in the `ram_captures\<date>` folder along with the acquisition log. The result format is AFF4. Please see the Acquisition section for more details.

It is recommended to capture RAM using the Triage launcher rather than via the Acquisition tab to minimize the potential memory overwrite done by the W4 application itself.

It is possible to turn RAM capture off via the *Triage* menu in the Case Manager or in the *Preferences* dialog.

16.2. Creating a case with Triage launcher

The process of creating of a new case in Triage launcher is the same as in the Case Manager, but also lets you specify case metadata fields and select local drives to process.

Select one or more local drives and then click on:

- *Acquire common system and registry files* to run the *Common system files* acquisition for all selected drives. Please see the *Acquisition* section for more details. The acquired files will be saved in the
- *Index selected drives* to automatically create a source for each selected drive and start indexing them right away.
- *Build item links* to build item links after the indexing is finished. It is recommended to turn this option off if the case is stored on a slow USB drive. Item links can be rebuilt later.

When both acquisition and indexing options are selected, W4 will first acquire the drives and then index them.

W4 will use the processing settings from the selected search profile.

17. Preferences

To open the Preferences dialog, select the File > Preferences menu option.

The specific settings per tab are explained below.

17.1. General

The Check for updates option lets W4 look online for new versions of the software during startup. This lookup will be done once in every 24 hours. New versions will be shown in the upper right corner of the application. A message will also be shown here when this option is turned off or when fetching the last version information has failed.

The Page format lets you select which paper size to use when reporting items. Available options are ISO A4 and US Letter.

The Shutdown section allows to configure whether to show the confirmation dialog on close. This is a global preference.

17.2. Indexing

The Item links section controls whether to build item links right after the indexing is finished.

It is recommended to turn off building item links if the case is stored on a slow USB drive. Item links can be built later via File menu when the case is moved to a faster storage.

17.3. Previewer

The Follow HTML links section controls how to display emails that contain links to external resources or images.

17.4. Results

The Results filtering section controls whether to show recently accessed file events with zero time (12:00:00). This option was introduced because such dates are often incorrect (tested on Windows 10).

The table row height section controls the height of a table row. Compact option allows for more information to be displayed in the table.

The Tags removal section controls whether to show the confirmation dialog when removing a tag.

The Events view tags rendering section controls whether to show the full names of displayed tags or just the indicator with color-coded representation markers of the tags.

The Table columns section controls whether to show *Source*, *Device* and *User* columns in the details table view. By default W4 doesn't show these columns. But if the case consists of several sources you might want to turn this option on.

17.5. Dates

The Locale option allows to choose what Locale to use when displaying dates. Another option is to use a custom date format. Please see this document for the date/time format syntax details: http://docs.oracle.com/javase/8/docs/api/java/text/SimpleDateFormat.html.

The Display Timezone option determines in which timezone W4 displays all the dates. This option is useful when the case contains several sources that came from different timezones.

17.6. Geolocation

The Tile preferences section defines how the world map gets rendered in the Geolocation results view and the Previewer's Geolocation tab.

W4 embeds a set of tiles for rendering this map. By default, this tile set is used. This embedded tile set enables use of the Geolocation views without requiring any configuration and/or network connection. The drawback of using this tile set is that the user can only zoom in six levels.

Another option is to integrate with a custom tile server. To enable use of such a server, select the Integrate with the tile server option. The Geolocation tab will then expand to offer additional settings.

You can use any tile server you wish by typing its address into the Tile server integration URL field. The format for the URL is dependent on the chosen tile server.

To use a public tile servers, you need to ensure that you comply with the tile server's usage policy. This is your responsibility, not Vound's.

The Min. zoom option defines the desired minimum zoom level in the user interface. This should be in the range of supported zoom levels of the chosen tile server.

The Max. zoom option defines the desired maximum zoom level in the user interface. This should be in the range of supported zoom levels of the chosen tile server.

The Tile Size (pixels) option defines the size of a single square tile. This value should match the size of the tiles which are returned by the tile server.

Important: Using a public tile server may reveal the locations that are being investigated to the tile server provider and anyone monitoring the traffic to that server, based on the tile requests embedded in the retrieved URLs.

Tip: If the investigation system has no internet connection, a custom tile server can be set up on the local network. One way of how this can be achieved can be found at http://osm2vectortiles.org/docs/serve-raster-tiles-docker/. This is out of the scope of this manual and Vound's technical support.

Email geolocation allows one to estimate the geographic location of an email's sender using the sender IP address. This process takes place during indexing. See the Geolocation chapter for a description of the process and its caveats.

Determination of the geographic location of an IP address requires the presence of MaxMind's GeoIP2 or GeoLite2 database. These databases associate IP addresses with geographic locations. The databases can be found here:

- GeoIP2 database (commercial) – https://www.maxmind.com/en/geoip2-city
- GeoLite2 database (free) – http://dev.maxmind.com/geoip/geoip2/geolite2/

See the MaxMind website for a description of their differences, beyond price.

The chosen database can be installed here by placing it in the following folder:

```
C:\Users\[USER]\AppData\Roaming\Intella\ip-2-geo-db
```

Alternatively, when you are on an Internet-connected machine, you can let W4 download and install

the GeoLite2 database automatically by clicking the Download GeoLite2 database button.

A license key is required for W4 to download the GeoLite2 database automatically. Click "Information about license keys" link to find out more.

To use the Email geolocation feature, check the Determine the geographic location of an email sender's IP address option when adding a new source.