GUIDE

A GUIDE TO FINDING IMPORTANT BUSINESS APPLICATIONS & OS ARTIFACTS FOR YOUR DIGITAL FORENSICS INVESTIGATIONS

MAGNET FORENSICS®

TABLE OF CONTENTS

A GUIDE TO FINDING IMPORTANT BUSINESS APPLICATION & OS ARTIFACTS FOR YOUR DIGITAL FORENSICS INVESTIGATIONS

When conducting forensic examinations, investigators can sometimes lose sight of the fact that they're investigating the actions of a person, not a computer. Almost every event or action on a system is the result of a user doing something (or not doing something) at a particular time to create that event. It's important for you, as a digital forensic investigator, to understand how events on a system correlate to the actions of a person in the real world – and that can be done by finding digital evidence from important business applications and OS artifacts commonly used today.

When investigated together, artifacts like documents, email, USB device history, LNK Files, prefetch files, shellbags, and other Windows system artifacts can be used to understand a user's activity on a system, and gain insight into what they have done on a computer. You can often piece together information from one artifact with another to get a timeline of events that details how a user traversed a system over a given time, which may help you see the complete picture (and solve your case).

Here are some important business applications & OS artifacts to search for in your digital forensics investigations, when you're looking to understand user activity on a system.

DOCUMENTS

Document analysis is a common task for forensic examiners and includes searching for document files such as Microsoft Excel, PDF, Microsoft PowerPoint, and Microsoft Word. These documents may either contain evidence in their content or in the metadata stored when creating and editing the files. It is essential for investigators to have the ability to collect all the relevant documents found on a system whether they still reside on the system or are recovered and carved from unallocated space.

WHY ARE DOCUMENTS IMPORTANT TO YOUR DIGITAL FORENSICS INVESTIGATION?

Analyzing documents to prove their authenticity has been one of the cornerstones of computer forensics and is still an important part of the investigative process to this day. Whether you're investigating documents in a fraud case, an IP theft, or from a malware/phishing intrusion, proper document analysis is essential to help uncover the truth in many investigations.

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING DOCUMENTS

Most documents have two primary sources of evidentiary value to examiners depending on the investigation: the content of the document itself, and the metadata around the creation and modification of the file. Analyzing the content of a given document is relatively straightforward and very dependent on the case you're investigating. For example, the content of an Excel spreadsheet containing financial records would be far more valuable to investigate for a potential fraud case, versus a malware or phishing investigation, where the focus would be around searching for malicious scripts or links. The biggest challenge is to recover any deleted documents from unallocated space, as sometimes the files are fragmented and/or overwritten, which means the full content of a document may not be recovered.

More often than not, the metadata around a particular document can be just as important, if not more, than the contents of the file itself. Details around when the file was created, last edited – and by whom – can be quite valuable for an investigator trying to determine the authenticity

of a document, or to verify its contents. The metadata included with a document depends on the individual document being analyzed. Typically you'll find the MAC times for the file, as well as the created and last edited time for the document, which is often more accurate than the MAC times; this is especially true if it was shared between computers and drives. The original author and last person to edit the document are also included, along with the document title when available.

EMAIL

Email is everywhere and is used by almost everyone on the planet. From short correspondence to multinational negotiations, email is used in business and in personal life as a fast, lightweight communication tool. It can also be used in the commission or provide evidence of a crime. Some of the more popular email clients in use are Microsoft Outlook and Mozilla Thunderbird. Outlook stores its email data in PST and OST while Thunderbird uses the common MBOX format.

WHY IS EMAIL IMPORTANT TO YOUR DIGITAL FORENSICS INVESTIGATION?

Like documents, email analysis has been one of the primary resources of evidentiary value for investigators in a multitude of different cases. Email contents can provide details of fraud, harassment, and even admission of violent crimes such as assault and murder. Proper email analysis can also help investigators track where a message originated and if it is potentially malicious to its recipient.

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING EMAIL

Email artifacts, including Outlook and Thunderbird, can assist examiners further by providing them with additional evidence to help piece together relevant data.

- Outlook stores email, contacts, appointments, notes, tasks, and additional data that it receives from POP, IMAP, or Exchange servers in PST and OST archives for its users.
- MBOX is a commonly used format to store mail data and

is popular with many UNIX or LINUX based mail clients, most notably, Mozilla Thunderbird. MBOX data includes the Details, Body, Headers, and Attachments views.

MICROSOFT LYNC

Microsoft Lync is a commonly used instant messaging client in the enterprise. Formerly known as Microsoft Office Communicator (OCS), Lync integrates well with Outlook Exchange. Beyond just chat and IM, Lync is also able to do voice and video calling, screen sharing, and file transfers. Unlike Skype and MSN Messenger, it was designed to work in an enterprise setting and not for consumers.

- These artifacts can provide chat messages, call logs, and file transfers from allocated and unallocated space from a number of different sources, including Windows, Mac, and Windows Phone.

USB DEVICE HISTORY

Whether you're a corporate examiner working an intellectual property theft, or a law enforcement investigator searching for illicit images, most forensic examiners have investigated the USB device history of a computer. When examining USBs, it's just as important to identify the user who connected the device as it is to analyze the data that may have been transferred to or from the system.

WHY IS USB DEVICE HISTORY IMPORTANT TO YOUR DIGITAL FORENSICS INVESTIGATION?

With the data from the USB device history, you can better understand how USB devices have been used on a given system, and possibly how a suspect might have used a USB device in the commission of a crime or incident.

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING USB DEVICE HISTORY

The Windows registry stores quite a few artifacts that need to be examined when investigating USB device history.

- The USBSTOR located in the SYSTEM hive (SYSTEM\CurrentControlSet\Enum\USBSTOR), which contains details on the vendor and brand of USB device connected, along with the serial number of the device that can be used to match the mounted drive letter, user, and the first and last connected times of the device.
- The MountedDevices key (SYSTEM\MountedDevices), which allows you to match the serial number to a given drive letter or volume that was mounted when the USB device was inserted. It's possible that you won't be able to identify the drive letter if several USB devices have been added, since the mapped drive letter only shows the serial number for the most recently mounted device for each letter assigned.
- The MountPoints2 key found in a user's NTUSER.dat hive (NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2). This information will reveal which user was logged in and active when the USB device was connected. MountPoints2 lists all of the device GUIDs that a particular user connected, so you might need to search through each NTUSER.dat hive on the system to identify which user connected a particular device.
- The USB key in the SYSTEM hive (SYSTEM\CurrentControlSet\Enum\USB, which provides investigators with vendor and product ID for a given device, but also provides the last time the USB device was connected to the system. Using the last write time for the key of the device serial number, you can identify the last time it was connected.
- The setupapi log (ROOT\Windows\inf\setupapi.dev.log for Windows Vista/7/8)(ROOT\Windows\setupapi.log for Windows XP). Searching for the serial number in this file will provide you with information on when the device was first connected to the system in local time. Examiners must exercise caution as unlike the other timestamps mentioned in this article, which are stored in UTC, the setupapi.log stores its data in the system's local time and must be converted to UTC to correctly match any timeline analysis being performed.

LNK FILES

LNK files are a relatively simple but valuable artifact for forensics investigators. They are shortcut files that link to an application or

file commonly found on a user's desktop, or throughout a system and end with an .LNK extension. LNK files can be created by the user, or automatically by the Windows operating system, and each has its own value and meaning. Windows-created LNK files are generated when a user opens a local or remote file or document, giving you valuable information on a suspect's activity.

WHY ARE LNK FILES IMPORTANT TO YOUR DIGITAL FORENSICS INVESTIGATION?

LNK files are excellent artifacts when you are conducting a forensic investigation to try to find files that may no longer exist on the system you're examining. The files might have been wiped or deleted, or stored on a USB or network share, so although the file might no longer be there, the LNK files associated with the original file will still exist (and reveal valuable information as to what was executed on the system).

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING LNK FILES

LNK files typically contain the following items of evidentiary value:

- The original path of the file.
- The MAC times of the original file; not only will a LNK file contain timestamps for the LNK file itself, it will also contain MAC times for the linked file within its metadata as well.
- Information about the volume and system where the LNK file is stored. This will include volume name, serial number, NetBIOS name, and MAC address of the host where the linked file is stored.
- The network details if the file was stored on a network share or remote computer.
- The file size of the linked file.

The above screenshot shows the contents of a LNK file linking to a virtual machine on a volume mounted as D:.

PREFETCH FILES

Prefetch files are great artifacts for forensic investigators trying to analyze applications that have been run on a system. Windows creates a prefetch file when an application is run from a particular location for the very first time. This is used to help speed up the loading of applications. For investigators, these files contain some valuable data on a user's application history on a computer.

WHY ARE PREFETCH FILES IMPORTANT TO YOUR DIGITAL FORENSICS INVESTIGATION?

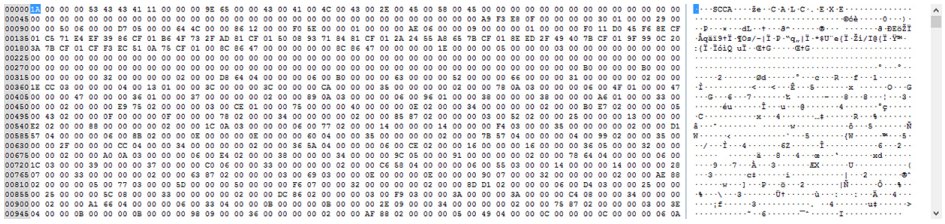
Evidence of program execution can be a valuable resource for you as a forensic investigator. They can prove that a suspect ran a program like CCleaner to cover up any potential wrongdoing. If the program has since been deleted, a prefetch file may still exist on the system to provide evidence of execution. Another valuable use for prefetch files is in malware investigations, which can assist examiners in determining when a malicious program was run. Combining this with some basic timeline analysis, investigators can identify any additional malicious files that were downloaded or created on the system, and help determine the root cause of an incident.

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING PREFETCH FILES

Prefetch files are all named in a common format: the name of the application is listed, then an eight-character hash of the location where the application was run, followed by the .PF extension. For example, the prefetch file for calc.exe would appear as CALC.EXE-0FE8F3A9.pf, with 0FE8F3A9 being a hash of the path from where the file was executed. These files are all stored in the ROOT/Windows/Prefetch folder.

Calculating the original path of the application from the hash provided in the prefetch file is relatively easy, but can be time consuming. Depending on the version of Windows the file was taken from, a different hashing function is used. One function is used for XP/2003, a different one for Vista, and another is used for 2008/7/8/2012. Both the Forensics Wiki and Hexacorn blog go into excellent detail on prefetch files, and provide scripts for investigators to calculate the original path. The location of the executable can be just as important as any timestamp

data. Most seasoned malware investigators can recognize the added concern of a known file executing from a temp folder, versus a more legitimate location such as the Windows\system32 folder. While the information found in the filename can be quite valuable, the contents of a prefetch file contain a wealth of information as well.



Analyzing prefetch files is relatively straightforward. Beyond the name and path mentioned previously, prefetch files contain details on the number of times the application has been run, volume details, as well as timestamp information detailing when the application was first and last run. For Windows 8+, prefetch files now contain up to eight timestamps indicating when an application was last run, giving you several additional timestamps to help build a timeline of events on a system.

SHELLBAGS

While shellbags have been available since Windows XP, they have only recently become a popular artifact as examiners are beginning to realize their potential value to an investigation. In a nutshell, shellbags help track views, sizes, and positions of a folder window when viewed through Windows Explorer; this includes network folders and removable devices.

WHY ARE SHELLBAGS IMPORTANT TO YOUR DIGITAL FORENSICS INVESTIGATION?

One might ask why the position, view, or size of a given folder window is important to forensic investigators. While these properties might not be overly valuable to an investigation, Windows actually creates a number of additional artifacts when storing these properties in the registry that provide valuable information, giving the investigator great insight into the folder browsing history of a suspect, as well

as details for any folder that might no longer exist on a system (due to deletion, or being located on a network/removable device).

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING SHELLBAGS

For Windows XP, shellbag artifacts are located in the NTUSER.dat registry hive at the following locations:

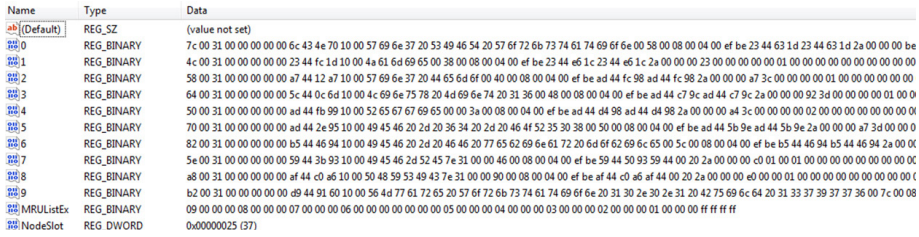
- HKCU\ Software\Microsoft\Windows\Shell
- HKCU\Software\Microsoft\Windows\ShellNoRoam

For Windows 7 and later, shellbags are also found in the UsrClass.dat hive:

- HKCR\Local Settings\Software\Microsoft\Windows\Shell\Bags
- HKCR\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

The shellbags are structured in the BagMRU key in a format similar to the hierarchy to which they are accessed through Windows Explorer with each numbered folder representing a parent or child folder of the one previous. Within each of those folders are the MRUListEx, NodeSlot, and NodeSlots keys:

- MRUListEx contains a 4-byte value indicating the order in which each child folder under the BagMRU hierarchy was last accessed. For example if a given folder has three child folders labelled 0, 1, 2, and folder 2 was the most recently accessed, the MRUListEx will list folder 2 first followed by the correct order of access for folders 0 and 1.
- NodeSlot value corresponds to the Bags key and the particular view setting that is stored there for that folder. Combining the data from both locations, investigators are able to piece together a number of details around a given folder and how it was viewed by the user.
- NodeSlots is only found in the root BagMRU subkey and gets updated whenever a new shellbag is created.



Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	7c 00 31 00 00 00 00 00 6c 43 4e 70 10 00 57 69 6e 37 20 53 49 46 54 20 57 6f 72 6b 73 74 61 74 69 6f 6e 00 58 00 08 00 04 00 ef be 23 44 63 1d 23 44 63 1d 2a 00 00 00 be
1	REG_BINARY	4c 00 31 00 00 00 00 00 23 44 fc 1d 10 00 4a 61 6d 69 65 00 38 00 08 00 04 00 ef be 23 44 e6 1c 23 44 e6 1c 2a 00 00 00 23 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00
2	REG_BINARY	58 00 31 00 00 00 00 00 a7 44 12 a7 10 00 57 69 6e 37 20 44 65 6d 6f 00 40 00 08 00 04 00 ef be ad 44 fc 98 ad 44 fc 98 2a 00 00 00 a7 3c 00 00 00 00 01 00 00 00 00 00 00
3	REG_BINARY	64 00 31 00 00 00 00 00 5c 44 0c 6d 10 00 4c 69 6e 75 78 20 4d 69 6e 74 20 31 36 00 48 00 08 00 04 00 ef be ad 44 c7 9c ad 44 c7 9c 2a 00 00 00 92 3d 00 00 00 00 01 00 0
4	REG_BINARY	50 00 31 00 00 00 00 00 ad 44 fb 99 10 00 52 65 67 67 69 65 00 00 3a 00 08 00 04 00 ef be ad 44 d4 98 ad 44 d4 98 2a 00 00 00 a4 3c 00 00 00 00 02 00 00 00 00 00 00 0
5	REG_BINARY	70 00 31 00 00 00 00 00 ad 44 2e 95 10 00 49 45 46 20 2d 20 36 34 20 2d 20 46 4f 52 35 30 38 00 50 00 08 00 04 00 ef be ad 44 5b 9e ad 44 5b 9e 2a 00 00 00 a7 3d 00 00 0
6	REG_BINARY	82 00 31 00 00 00 00 00 b5 44 46 94 10 00 49 45 46 20 2d 20 46 46 20 77 65 62 69 6e 61 72 20 6d 6f 62 69 6c 65 00 5c 00 08 00 04 00 ef be b5 44 46 94 b5 44 46 94 2a 00 0
7	REG_BINARY	5e 00 31 00 00 00 00 00 59 44 3b 93 10 00 49 45 46 2d 52 45 7e 31 00 00 46 00 08 00 04 00 ef be 59 44 50 93 59 44 00 20 2a 00 00 00 c0 01 00 01 00 00 00 00 00 00 00 0
8	REG_BINARY	a8 00 31 00 00 00 00 00 af 44 c0 a6 10 00 50 48 59 53 49 43 7e 31 00 00 90 00 08 00 04 00 ef be af 44 c0 a6 af 44 00 20 2a 00 00 00 e0 00 00 01 00 00 00 00 00 00 00 0
9	REG_BINARY	b2 00 31 00 00 00 00 00 d9 44 91 60 10 00 56 4d 77 61 72 65 20 57 6f 72 6b 73 74 61 74 69 6f 6e 20 31 30 2e 30 2e 31 20 42 75 69 6c 64 20 31 33 37 39 37 37 36 00 7c 00 08
MRUListEx	REG_BINARY	09 00 00 00 08 00 00 00 07 00 00 00 06 00 00 00 00 00 00 00 05 00 00 00 04 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00 ff ff ff ff
NodeSlot	REG_DWORD	0x00000025 (37)

Much of this data is stored in a raw hex format and needs to be formatted to understand the path and any additional details. You will need to collect data from each value in the hierarchy to piece together the path of the folder and then use data found in the Bags key to find additional details on the icons, position, and timestamp details. Finally, the last write time of the key can be used in conjunction with the MRUListEx to determine the last access time for a given folder.

ADDITIONAL WINDOWS SYSTEM ARTIFACTS

Windows system artifacts provide a huge array of information about activity on a suspect's operating system. Overall, these artifacts contain a wealth of information around the Windows system that can be quite valuable to you, as an investigator, and also help you gain insight into details about the system's users. Other Windows system artifacts can include jump lists, user accounts, event logs, timezone information, network shares, and OS and file system information.

WHY ARE WINDOWS SYSTEM ARTIFACTS IMPORTANT TO YOUR DIGITAL FORENSICS INVESTIGATION?

The Windows system artifacts mentioned above can be used by investigators together with other artifacts from browsers, email, and chat applications to piece together a suspect's actions on a system. While they might not contain the smoking gun like other artifacts, they are essential to understanding the activities on a system and how it was used in the commission or in support of a crime or incident.

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING WINDOWS SYSTEMS ARTIFACTS

JUMP LISTS

Jump lists were added to Windows 7 and later systems to provide a list of recently accessed files and documents associated with a given

application. Previously examiners only had access to a short list of recently accessed files, but jump list artifacts provide details on recent files for each application giving investigators a lot more information and timestamps around what the user was doing on a system.

Jump list details can be found in two primary locations, the automaticDestinations-ms and customDestinations-ms files providing details around the application, recent files, timestamps, as well as several other items of potential forensic value.

One unique artifact included in jump lists is the AppID, which is a CRC64 hash of the application path (for more information on calculating AppID values see a great write up from the Hexacorn blog here: http://www.hexacorn.com/blog/2013/04/30/jumplists-file-names-and-appid-calculator/)).

USER ACCOUNTS

User account information is stored in the SAM registry hive and lists all of the default and user created accounts for a given system: SAM\Domains\Account\Users\.

From here, investigators can collect account name, account type, groups, login count, timestamps around last login, last password change, and last incorrect password login, whether the account is disabled or a password is required.

An additional registry key to mention is the ProfileList key under the SOFTWARE hive: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList.

While the SAM hive stores login information for all local accounts, the ProfileList key stores information on all users who have logged into a system, including domain users, which can be valuable for examiners investigating intrusions or compromised accounts over a network.

EVENT LOGS

Windows event logs store a wealth of information about a system and its users. Depending on the logging level enabled and the version of Windows installed, event logs can provide investigators with details about applications, login timestamps for users, and system events of interest.

For Windows 2000, XP and 2003, event logs are stored as .evt files in the ROOT\Windows\system32\config folder and are typically grouped into three categories: application, system, and security. Versions of Windows beyond Vista handle event logs differently; they are now stored as XML files with an .evtx extension at ROOT\Windows\system32\winevt\Logs. Vista also introduced several new event logs in addition to the application, system and security logs found in Windows XP/2003. Now the logs are separated into two categories: Windows logs and Applications and Services logs.

Under the Windows logs, there are two new logs available to examiners: setup and forwarded events. Under Applications and Services logs, Windows will store a number of additional logs for various applications installed on the system.

TIMEZONE INFORMATION

One simple yet very important artifact is the system timezone information stored in the Windows registry. Windows stores a number of timestamps in both local and UTC time. Understanding which timestamp is which and how they relate to the timezone set by the system is essential to understanding the timeline of events of an incident. Timezone information is stored at the following key in the SYSTEM hive: HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation.

NETWORK SHARES

This information is pulled from a user's NTUSER.dat registry hive and will reveal any network shares that are or have previously been mounted by the user along with the associated drive letter if available. The first location it will check is the Map Network Drive MRU: HKCU\ Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU.

This location stores a list of network drives the user has mapped through the "Map Network Drive Wizard" in Windows. The last write time of this key will reveal the date in which the user mapped the drive.

The next location that stores valuable network share data is also stored in the NTUSER.dat under Network: HKCU\Network\.

This location stores a sub-key for every network share mounted to a particular drive letter. The RemotePath value will provide the investigator with the path that was mapped to that drive letter.

Finally, the MountPoints2 key also stores a wealth of information about any network shares mounted by the user: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2.

This key will list a number of additional folders mounted by the user. Note that the key will replace any of the backslashes (\) with pounds (#) displaying a share normally mounted as \\192.168.1.1\share as ##192.168.1.1#share.

OPERATING SYSTEM INFORMATION

As with the other system artifacts discussed here, most forensic examiners will be familiar with the artifacts associated to the operating system installation information stored at the registry keys stored below:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKLM\SYSTEM\CurrentControlSet\Control\Windows

OS details such as name, version, Product ID and Keys, which service pack is installed, as well as the installed and last shutdown timestamps associated to a given Windows installation are found in these locations.

Two artifacts of note are the install date and last shutdown time which can be valuable to investigators trying to gauge a timeline of events around the date Windows was installed and the last time the system was shutdown. Some examiners might notice that the last logon time for a user is sometimes after the last shutdown time noted in the registry. There are a number of scenarios that could make this occur; most often the system was simply powered off or unplugged without going through the proper Windows shutdown process, preventing the system from writing the new time to the ShutdownTime value.

FILE SYSTEM INFORMATION

Most forensic investigators are familiar with the common file systems and their storage structures that enable investigators to analyze and recover data. The File System Information artifact from Windows systems gives you additional details about the installed file system for all volumes and partitions found on their drive or the image

being analyzed. Details include the file system type, volume serial number, capacity, sector, and cluster information, including several other indicators that might be of value in your examination.

Most forensic tools will automatically organize file system details and apply the appropriate sector and cluster sizes to parse a given file system, but sometimes it's necessary to dig a little deeper and perform some manual analysis. These details are essential for the analysis and recovery of any files stored within.

FINDING IMPORTANT BUSINESS APPLICATIONS & OS ARTIFACTS WITH INTERNET EVIDENCE FINDER (IEF)

At Magnet Forensics, we're constantly updating and adding new capabilities to our digital forensics software, Internet Evidence Finder (IEF), to allow you to find more evidence on computers, smartphones, and tablets with a single, automated search. This is why we've added recovery capabilities for all of the important Business Applications & OS Artifacts included in this guide!

While IEF's roots are grounded in the recovery of Internet-based artifacts like browser history, webmail, social networking, and chat apps, we recognize that Internet artifacts are only a subset of the potential evidence that can be found on mobile devices and computers. The ability to get a holistic view of what a suspect has been up to by recovering more kinds of digital evidence with one tool is what today's investigator needs.

Curious about how Internet Evidence Finder can help you find, analyze, and present evidence for your computer and mobile investigations? Join us for a demo, and we'll show you why thousands of forensics professionals around the world have made IEF a part of their toolkit.

JOIN A DEMO
http://www.magnetforensics.com/register-for-an-ief-demo/

For more information call us at 519-342-0195
or email sales@magnetforensics.com