Stephen Goldmeier, Public Information Attorney
Neal Gallucci, CFCE
Office of the Ohio Public Defender,
Forensic Training Unit
www.opd.ohio.gov/Forensics

A Digital Investigation from Beginning to End

June 2017

The field of digital forensics is always changing, and the case law regarding these issues is still emerging. This session is designed to encourage defense attorneys to think creatively about how old concepts could be applied to new digital realms. This document will provide an overview of the forensic-investigation process. It is our job as attorneys to find the problems with this process and ensure that it is not used unfairly against our clients.

1: The Investigator/Forensic Expert

Certifications, Qualifications, and Experience

In most forensic-examination cases, the forensic examiner (sometimes a police officer with forensic training) will be trained how to use forensic software, not in the underlying principles. Examiners that rely only on the software to derive their forensic conclusions might not understand the technical underpinnings of their results.

These types of examiners can be challenged, as they can sometimes draw inaccurate conclusions from an analysis. As such, it is important to verify their credentials of any examiners in a case. If the conclusions of the examination seem complicated or over-stretched, this may be a way to undermine those conclusions by highlighting the limitations of the examiner's training and certification. Also consult with your own expert to find problems with the State examiner's conclusions

Certifying Organizations

- IACIS - The International Association of Computer Investigative Specialists
- GIAC Computer Forensics
- SANS Computer Forensics
- Access Data (Vendor Specific)
- Encase (Vendor Specific)

Ways to Challenge Expertise

Expiring Credentials

Almost all forensic certifications expire over time and require a re-certification process to keep credentials active. This is especially important in the field of Digital Forensics, as the technology changes very quickly. Make sure the credentials/certifications of the

forensic examiner on your case are active by checking with the accrediting origination. If the expert's credentials are out-of-date, work with your expert to emphasize the newest aspects of the digital evidence at issue and of the examination process itself.

Limitations of Specific Certifications

Some certifications will only train an expert to perform certain examinations or use certain software. The expert's certification alone might not qualify them to render opinions on the results of the tools they use or to explain how the tools work. Cross-examine experts on any information they provide that is not covered by their training or their certification.

Limited Scope of Training

Beyond certifications, experts may assert that training in some areas qualifies them to testify in other areas. Raise questions about the expert's ability to testify regarding matters outside of their training, and bring in experts to explain why additional training is needed for certain opinions.

2: The Search Warrant

Limitations and Specificity

In a digital forensics case, the warrant for a search must specify which data is being examined. For instance, if a warrant covers text messages, but the examiner also uncovers items from internet history, that subsequent search might not be covered by the warrant. Try to exclude the "non-responsive" items (i.e. items not reasonably covered by the warrant and not related to the purpose of the original search). (See Kerr, Orin S., "Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data," available at http://ssrn.com/abstract=2628586).

The United States Supreme Court has made it clear that warrants for digital evidence are crucial, even if the device itself is seized pursuant to some other probable cause. (See *Riley v. California*, 573 U.S. ___, 134 S.Ct 2473, 189 L.Ed.2d 430 (2014)). Watch for warrants based on officers saying that "in their experience" certain crimes involve phones; this is likely not specific enough to support a mobile-phone warrant.

Also, one federal court has held that law enforcement keeping images of examined hard drives for later use is outside the scope of the original warrant. (See *U.S. v. Ganias*, 755 F.3d 125 (2d Cir. 2014)). Some warrants might even include a clause mandating destruction of a device after it is searched. In short, there are many opportunities to test the limits of warrants in digital forensics cases. This is also an area where defense attorneys can challenge the relevance of evidence found on a device and attempt to exclude images or messages that are prejudicial to the defendant.

Cloud Storage

Many applications will store data on a remote server, or "in the cloud," and the phone or computer will access this cloud data when it is running. This information is *not* stored on the

device itself. If a warrant allows a search of the contents of a phone, watch for evidence that is actually recovered from cloud storage, as items stored on a remote server might not be covered by the warrant.

Consent

If law enforcement asserts that they had consent to search a device, watch for who actually gave that consent. A third party's ability to consent to a search of a device could be limited by who actually owns the device, who uses it, and whether it is normally password-protected.

3: The On-Scene Investigation

Investigator Must Control the Scene and Document Everything

The first thing a computer forensics analyst is trained to do when arriving is to control the scene. This includes both controlling physical access to the device (for instance by setting up boundaries) AND controlling network access to the device (for instance by disabling all network connections, including putting mobile devices in airplane mode, or by placing mobile devices in Faraday bags designed to block incoming signals). This will prevent the device from being accessed remotely during the acquisition.

The analyst will be trained to document the scene to memorialize which devices are present and how they are arranged before being examined. The analyst should also document all actions taken, and the reasons for those actions, while on the scene. Either a lack of documentation or incorrect assumptions included in the documentation can be a source for cross-examination.

Investigator Must Follow Protocols for Interacting with Devices

An analyst is trained to attempt to access a device that is already running by waking it out of sleep mode. Once this is done, the analyst will look for encryption or lock screens, which will affect the collection techniques the analyst uses. Any use of a device alters it, so an analyst should document this process carefully. An analyst can also capture the device's more volatile data, like RAM, while it is powered on, because RAM is cleared once the device is powered off. Once that is done, the device will be powered off and collected for processing into evidence (unless encrypted; see below). However, if the device is already off, the analyst will leave it off, either to remove the relevant storage media or to power the device on in a more controlled environment. If the storage media is unable to be removed, then the analyst will have to turn the device back on in order to capture the information. This procedure requires even more documentation.

Legal Challenges

Be sure to cross-examine experts if it appears that they did not follow these protocols. In digital forensics, any interaction with a device can alter its contents, so any part of the process that is not carefully documented can be a point where doubt creeps in. Also, as with all forensic evidence, watch for the chain of custody, which is even more critical when dealing with a device that can change states or contents any time it is turned on or mishandled.

4: Encryption

About Encryption

All information on a computer or phone is stored as binary, or a series of ones and zeros, that, when interpreted, make up everything the device does and contains. Encryption is the process of transforming these bits, using an algorithm, to make them unreadable to anyone except those who possess a special key. Everything from individual files to an entire device can be encrypted.

Usually, an encryption key (or a password) must be used to decode the data. There are some software tools that can "crack" encryption by systematically trying every possible password combination until one works. However, using encryption cracking software is not feasible with modern encryption standards as it would take thousands of years to "crack" a password given the high amount of combinations. If one of these is used, make sure the analyst can explain how these tools work and how the analyst ensures that nothing is altered in the process.

Encryption and Mobile Devices

Mobile Devices usually have an option for a lock or passcode to prevent unwanted users from accessing the device. The lock screen *is* a form of encryption; as long as it is in place, the contents of the device are encrypted. And, most devices prevent brute-force attacks by requiring a delay after failed passcode attempts, or even wiping the device's data after too many failed attempts. Users can also slow brute force attacks by using longer passwords and special characters.

Encrypted devices cannot be imaged and analyzed unless the forensic analyst is able to unlock the phone. With current technology, this is almost impossible without the passcode itself. Mobile device companies are increasingly removing "back-door access" methods that allow someone to bypass encryption. Apple removed back-door access with the release of iOS 8.

Recently, law enforcement was attempting to decrypt a phone owned by the shooter in the San Bernardino terrorist attack. The phone was eventually unlocked, and the details of how this was accomplished are classified. It is likely that gaining access to the phone required enlisting third party professional hackers for possibly millions of dollars. This situation is not representative of the norm, as in almost every non-terrorism scenario, law enforcement will not invest as much time and money to gain access to a device.

Unlocking Phones and the 5th Amendment

It is an unsettled question as to whether police can force an individual to provide their passcode to unlock and decrypt their phone. Some courts have held that forcing a defendant to unlock a phone with a fingerprint is not "testimony" and therefore not protected by the 5th Amendment the way, say, forcing someone to reveal a password might be. This question is currently before courts around the country, and the law is evolving rapidly, so be sure to search for the most up-to-date information if this issue arises in one of your cases.

5: Preservation and Collection

Investigator Identifies and Collects Media

An analyst must first determine the type of media present before collecting evidence.

Removable Media

Most things we think of when we think of computers are removable media: flash drives, CDs, DVDs, memory cards, and even whole hard drives. If the storage device that contains the computer's data can be removed, then the analyst can attach the original media directly to the imaging machine (for example ImageMaster Solo, FRED, or Tableu Forensic Bridge). Such machines include a "write blocker," which ensures that the original media does not get altered during the collection.

The examiner will then create a backup of the device before proceeding with analysis. This is commonly referred to as the "forensic copy" or "clone." This is a bit-by-bit direct copy of the original device. The original media should be sealed and stored, and the forensic copy/clone media should be the media used for forensic processing.

Encrypted Media

Because encrypted media is unreadable when powered off, a forensic analyst may have to create an image of the device while it is live. The results of this "live image" process will be stored on an external hard drive. This imaging process does not create a forensic copy. Instead it directly creates a "forensic evidence file" for further processing (discussed below). Verified forensic imaging software has write blocking built into the software. Examples of imaging software: FTK Imager, Encase Forensic Imager, ImageX, Linux 'dd', and SNS Sift.

Non-Removable Media

Some devices, particularly thin laptops (like the Surface or the MacBook), do not allow the hard drive to be removed from the device without the device being destroyed. This makes the devices thinner and lighter.

To image non-removable media, an analyst will boot up the device through imaging software running through a USB Flash Drive/CD-DVD, access the internal media, and export the media onto an external hard drive. Again, this creates a "forensic evidence file" (discussed below), not a copy, and verified forensic imaging software will have write blocking built into the software.

The Target Drive, and Using Sterile Media

The target media (the device the data is being forensically copied to) must be not only empty, but "sterile," meaning every individual bit is reset to zero (or some other identifiable pattern). This ensures that evidence from the case does not get mixed with pre-existing data on the target media source.

Overall Legal Challenges to Collection

Whichever method is used, the examiner must document every step of the process. If documentation is missing, cross-examination can reveal flaws in the process. The expert should be able to confirm that a write-blocker was used and that the software they use has been validated. Ask for documentation that the examiner's write blocking equipment is working as intended. Just like any hardware, physical write blockers have the possibility of going bad. Software-based write blockers could be installed and configured incorrectly, causing them to malfunction. Forensic examiners need to keep up-to-date logs as proof that tall their equipment is working up to forensic standards. If not, one could challenge the validity of the forensic images.

Also ask the examiner for verification that the target media contained no information before the forensic copy or forensic evidence file was placed onto the target media. If this documentation does not exist, the examiner cannot be certain that the suspect material came from the defendant's device.

Review all reports and lab notes carefully, and try to spot the missing links or missing documentation for cross-examination. Also have your expert watch carefully for any points where non-sterile media could have interfered with the evidence in the case.

Investigator Creates a Forensic Evidence File

The last step is that the forensic copy (the image generated through this process) is converted into a "forensic evidence file." This is a compressed computer file (with file extensions like .AD1, .E01, and .DD) of the original media which still contains the binary information. This file is what is actually processed within forensic programs.

For discovery purposes, make sure you get the forensic evidence file. This is the file your expert will want to examine in order to find anything overlooked by the State expert, and also to watch for any modified files after the evidence was seized. Above all else, in digital forensics cases, do not accept printouts or PDFs of the relevant material. Ask for the native files.

Native files also provide you and your expert access to metadata. For instance, with a native file of a digital photograph, you can learn the date the photograph was taken, what kind of camera was used, and possibly even where the photo was taken. This information is not available if you accept printed or edited files. Consider due process or *Brady* arguments for cases in which native files might provide exculpatory information.

Hash Values

In computer forensics, hashing is a way to represent a piece of digital evidence with a unique number generated from an algorithm. You might see the name of the algorithm the examiner used in the resulting report (such as MD5, SHA-1, or SHA-256, the strongest of the three). The hash value is like a DNA profile for the whole drive, and it can be used to establish if two drives are the same as each other.

An examiner should run the "hashing algorithm" (i.e. create a unique hash value for the drive) on the original media before creating an image of the drive. This way, the hash value of the drive from after the imaging and acquisition process can be compared to the original, to ensure that no data was altered during the course of the forensic acquisition.

Individual File Hashing

Individual files and folders can be hashed as well to determine if two files are exactly identical. This can be particularly important when the State is attempting to show where someone procured a certain file; if the hash values do not match, they are not the same file. Discrepancies can provide fuel for cross-examination.

Legal Challenges

Make sure to watch for differing hash values between the evidence recovered on the scene and the evidence used against a client. Such differences could show that the collection and examination process tainted the original evidence, or the original evidence was different from what was actually examined.

Known File Filters

A forensic examiner can create or obtain a list of unique hash values of known files, known as a File Hash List, and quickly run the list against a forensic image to identify known files. Internet Crimes Against Children (ICAC) maintains a list of the hash values of known child-pornography images, and this technique is often used to find these images on a drive as a first step in investigation.

A Note on Hashing and Solid State Drives

Solid State Hard Drives (SSD) are more commonly used now, and will soon be the dominant type of hard drive on the market. SSDs are found in thin laptops, tablets, phones, and high-end computers. SSDs have new features that help make the hard drives perform better by constantly moving data around on the drive. While individual file hashing is not affected, these features can change the hash value of the whole drive itself, even if the contents are still the same and nothing was altered. Also, unlike traditional hard drives, an SSD's special features will make deleted files unrecoverable almost minutes after deletion (discussed below). This is why documentation is so important during a forensic examination. A forensic examiner should document if they received different hash values on the same media in order to establish that the difference was the result of these SSD features, not mishandling of forensic evidence.

6: Desktops and Laptops

<u>Registry</u>

The Registry is a place within the operating system where system information is stored. Examiners will comb the registry for evidence against your client, and your expert can also inspect the registry to get a better picture of how the device was used.

Note: The below information is mostly applicable to the Windows Registry, which will be relevant to the majority of cases.

Device/OS Information

When an analyst is examining a device, the first thing he/she will do is determine the operating system (OS) of the device. The type of OS will determine which forensic artifacts could be left behind on the computer and which tools to use. The most common computer operating systems are Windows and OS X. These versions might change as time goes on, and you might have to learn the quirks of any operating systems relevant to a case. For now, the vast majority of forensic investigations on desktops/laptops occur on Windows devices.

Time Zone Information

The Registry stores the time zone Information, which tells the operating system which time zone to record dates and times in. In cases where the timeline is critical, it is important to determine which time zone all the information is being displayed in, as mistakes can compromise a defense (or provide fodder for cross-examination).

Domain / Network Information / Network History

The Registry also stores the network history of a device. This includes what domain the device is on (most relevant to corporate networks), the wireless networks the device has connected to, and IP addresses the device has previously used. Again, this can provide grounds for cross-examination. Also, watch for cases based on IP address information. The process of assigning IP addresses to users is very complex, and the State might have to call witnesses from the defendant's internet service provider or provide additional documentation to use this evidence. Work with your expert to see what might be missing from the State's case.

USB / Removable Media History

The Registry also stores detailed history on removable media devices, such as USBs, cameras, phones, etc., that have been connected to the device. However, the Registry only maintains the first time the removable device was connected, so it can be difficult to use this information in establishing timelines. Confer with your expert regarding these limitations if an examiner makes any time assertions regarding these removable devices.

Law enforcement may use the USB/Removable Media History information to secure a warrant allowing them to search for additional storage devices. Look for ways to challenge the warrant. For instance, the investigator might not have looked at the Removable Media History yet when the warrant was secured.

Installed Software

Using Registry information, a forensic examiner should be able to provide a detailed report of all the software installed or previously installed on the computer. A defense

expert could, for instance, determine that no file-sharing applications have been installed on a computer.

Date and Time Analysis

Mobile phones receive date and time information from carriers, which makes this information more standard and reliable for mobile devices. And, date and time settings can be controlled by system administrators in a business environment. Even if a user changes the time zone for a device, this only changes the hour adjustment; it does not change the times recorded in the operating system's logs.

However, for home computers, dates and times are a lot less reliable, largely because the primary user will also be the administrator. The computer's owner can easily use their administrator privileges to modify the dates and times within an operating system, as well as hide any evidence that those modifications occurred. For instance, in some versions of Windows, the system records a log when an administrative user changes date and time information, but the same administrator would be able to clear those log entries, too.

For instance, in a home with two roommates, one roommate could set the system time to five hours earlier, engage in illegal activities, and reset the time afterward. If the other roommate was using the computer five hours earlier, it could appear that the other roommate was the one engaging in the illegal activities. A skilled examiner might find minor artifacts that show what actually happened, but in general, this is why date and time evidence is uncertain and possibly unreliable for home computers.

Windows User Information

In addition to operating-system-wide information, Windows also stores specific information for each user on a computer.

Last Activity

A computer forensic examination can determine that last activity on the device before it was seized. The examination can even determine the last activity of each user in case there are multiple users. If the last activity is after the date of seizure, this might show that the examiner did not use a write-blocker, or it could reveal any number of other problems with the forensic-examination process.

Most Recently Used (MRU)

Microsoft Office products (Words, Excel, PowerPoint, etc.) maintain the 50 most recently accessed files for each program within the Windows Registry. Adobe products also store some information regarding recent file access.

Lnk Files

A .Lnk file is a file that contains a "link" or "pointer" to another actual file. Windows uses these files to provide quick access to frequently/recently used files and programs. By default, Windows will automatically create a .Lnk file somewhere almost every time a

file is accessed. A forensic analyst can easily search for all .Lnk files and generate a report showing what files were accessed by a user and when.

A .Lnk file does not contain the actual file, rather a historic reference of the file access. (The same is true for items in the MRU list, above.) Cross-examine on this limitation if the evidence against your client is based on suspicious file names in this list, not on actual files discovered on the device.

Windows 7 introduced a new type of .Lnk file, called "Jump Lists." These are lists of every file that a user has opened (or even attempted to open) with a particular application. For example, when you right click on an application from your task bar, you can see a list of files recently accessed by that application.

Internet History

By default, all internet browsers maintain detailed internet history within the user's profile. Internet history can include websites visited, downloads, favorites, cookies, and cached files (or temporary storage). A detailed internet history report can show what was accessed, when, and how many times. Internet history is too complex to examine manually, so examiners will usually rely on forensic tools to decipher and accumulate this information, which can create avenues for challenges when examiners draw conclusions without considering the underlying information.

Internet Evidence Finder

The most widely used internet evidence processing tool is Magnet Forensics' Internet Evidence Finder (IEF). An examiner can load a forensic evidence file into IEF, and with a click of one button, all active and deleted internet artifacts are identified.

Clearing History or Changing Settings

Anyone using a web browser can alter the time-frame for stored internet history or clear their internet history altogether. Windows does not record the action of clearing internet history or changing settings, so it is hard to prove that someone did so. Consult with your expert if an examiner asserts that he/she can tell your client cleared incriminating internet history.

Private Browsing

Almost all website browsers have some sort of "private browsing" feature. When this is activated, internet history is not recorded. Google Chrome refers to this as Incognito Mode.

User Assist Registry Key

Every user profile has a unique User Assist registry entry which records a history of all the programs a user has executed. The User Assist key provides information such as when the program was run and how many times. Forensic studies have shown the User

Assist key is reliable for determining which programs have been executed, but not determining when and how many times a program has been used, so cross-examine thoroughly if it is misused.

Explaining Deleted information

Note: The following examples are based on modern Microsoft Windows technology, though the general principles could apply to other devices and technologies.

When a file is created, two things happen. One, a "file table record" is added to the Master File Table (MFT), which is a list of files on a drive and their actual locations. Two, the actual data of the file is written to the hard drive somewhere else. When a file gets "deleted," nothing is actually deleted. Instead, the "file table record" that points to the actual data of the file is marked as "unallocated," meaning they can both be reused. Then, when a new file is created, it will use the next available "unallocated" space in the MFT and on the drive itself. This means that *the data isn't actually deleted until it is overwritten by another file*. Files from this "unallocated" space that have not yet been overwritten might be used as evidence against a client.

This is a complex process, so if a forensic examiner tries to use deleted files against a defendant, press the examiner on how this works. Because some forensic examiners are not computer scientists and are instead specialized law enforcement officers, examiners will often not fully understand how deleted files work. Additionally, many forensic examiners do not know how to manually recovery deleted files and rely on software to produce this information for them. Press if an examiner asserts that something is missing from the evidence because your client deleted it; deleted files may leave a trace, so if an examiner found no such trace, this could cast doubt on their assertion.

Deleted Information with Multiple Users

When a deleted file is recovered, most of the time it cannot be matched with its "file table record." Without this, it is nearly impossible to determine where the file came from on the system. When a system has multiple users, the expert may be unable to determine if the file was associated with your client.

Fragmentation

The way that files are managed on a drive could render deleted data very difficult to recover. Files are managed in units called "blocks" or "clusters." When files are added, removed, or changed, the space available for new files could be non-continuous, or "fragmented." When a new file is written, the operating system puts the new data in the first available blocks of data (which may not all be next to each other). New files are therefore usually in non-contiguous data blocks, rendering the file "fragmented."

The file table record tells the computer which blocks of data on the media are being used for that specific file. Without that file table record, if the data blocks are fragmented, the file is unable to be fully recovered, and in most cases, is unreadable.

And, as mentioned earlier, SSDs have features that fragment the files even if the file is not changed, moved, or deleted, making deleted files unrecoverable.

Viruses and Malicious Code

A forensic examination should always include a report of an anti-virus/malware scan of the analyzed media. There are malicious viruses and malware that will place illegal digital contraband, such as child pornography images, on a computer. Cross-examine the analyst if he/she cannot rule this out as a possible source of illicit images. RANSOMWARE

7: Mobile Device Analysis

Analyzing a mobile device (such as cell phones, tablets, and Ultrabooks) is generally very similar to analyzing a desktop or laptop computer. However, below are some peculiarities of a mobile device examination. (Note: the most common mobile operating systems are Android and iOS, but some mobile devices run Windows, just as a laptop or desktop computer would. For those devices, refer to the section on laptops and desktops, above.)

Different Software

Mobile forensic analysis uses different software tools. These include Cellebrite, Access Data's Mobile Phone Examiner (MPE), Internet Evidence Finder Plus, Encase Smartphone Examiner, and Lantern. This software will provided detailed reports on the device information, call history, text history, contacts, images, and application data.

Complications of Imaging

When imaging a mobile device, an examiner will follow a similar process to imaging a normal desktop or laptop. However, mobile phones change frequently, so mobile forensic tools must keep up with new mobile device connectors and operating systems. Generally, forensic software manufactures consistently update their systems to keep up with these changes.

Some devices cannot be imaged. For instance, "burner phones" or disposable cell phones often cannot be imaged. As mentioned earlier, the lock screen of a mobile device is a form of encryption, so without the lock screen passcode, an encrypted device also cannot be imaged.

Application Data

Just as some data on a computer is stored in the "cloud," a vast majority of information on a phone is "application data." Courts are currently grappling with the question of how the Federal Stored Communications Act applies to application data, specifically communications made through Facebook. Getting your own client's application data is easy, but getting another user's information is more difficult. An example of the complexities of this issue: a New York court has held that Facebook cannot object to a warrant for user information, but the users themselves might be able to suppress the results of the search. (See *In re 381 Search Warrants Directed to Facebook, Inc.*, --- N.Y.S.3d ---- (2015), available at http://online.wsj.com/public/resources/documents/2015_0721_facebook_warrants.pdf). Be aware that there are no such concerns with law enforcement using any publicly available social-media information.

8: File Transfer Technology

The most popular way of trading in illegal files from the internet is to use peer to peer or torrent technologies. This is because these technologies offer wide varieties of available files, speed, and (at least supposed) anonymity. This section will cover how these technologies work, which popular software use these technologies, and how they are used in forensic examinations.

Understanding IP Addresses

Internet services providers (e.g. Time Warner, AT&T, and WOW) assign a unique number to each device connected to the network. This number is a string of numbers separated by periods, and it's called an IP address. Because of their uniqueness, IP addresses can be used to determine who is accessing a specific website and where they are located. Some services and devices will use the same IP address over a long period of time. In most cases, IP addresses can change frequently. Either way, most internet service providers keep logs of IP address assignments for up to six months, so even if the IP address changes, the provider can usually connect it with a subscriber if they still have the records.

When a user accesses the internet, the computer on the other end can see and log their IP address. When law enforcement investigates a specific website or internet service, they start with the list of IP addresses that have accessed that illegal content.

Sophisticated computer users sometimes mask their IP address by using a Proxy Server. A Proxy Server acts as an intermediary, providing a different IP address to the website they are accessing. Because the website has a fake IP address listing, investigators cannot trace that IP address back to its source. Proxy technology is the main way users ensure their anonymity on the internet.

Peer to Peer

Peer to peer technology is mostly used for transferring files and hosting files anonymously. Peer to peer transfer is exactly what it sounds like: direct computer to computer transfer of a file. One person has the file, so they post that the file somewhere, and another person downloads that file. There are many ways of engaging in peer to peer transfer, some more anonymous than others:

Direct Transfer over the Internet and Newsgroups

Most simply, a user can upload files to a website and allow people to download the files directly from the website's server. This method is mainly useful for individual small files, not for large transfers. There are a number of websites where files can be shared this way, but the most common is the "newsgroup."

Newsgroups have been around since the earliest days of the internet. Newsgroups are organized by subject area, and they are meant to provide users a place to discuss common interests. Users typically need a subscription to gain premium access in order to download posted files from the forum. Newsgroups are very old, but new

technologies can make them more searchable and accessible, so they continue to be used today. They are used in many legal and productive ways, but of course some newsgroups specialize in sharing illegal material.

Peer to Peer Software

Users can also bypass the website and instead share files directly between one another using specialized software. Users can share a folder from their computer to the peer to peer program, which in turn makes the contents of that folder publicly visible and searchable. Another user can then log into the software and search for files. If the program finds the file the user is looking for, it then connects the two users' computers together, copying the file from the source computer and writing it to the destination computer. Again, this method is used primarily for smaller single files.

Examples of peer to peer software include Kazaa, BearShare, Limewire, and eDonkey.

Torrenting

Torrenting is the most common method used for obtaining pirated and otherwise illegal material. Torrenting involves using a file distribution network that identifies the locations of all users who are currently sharing a particular file and allowing other users to download that file from all of those different locations at once. Torrenting is essentially the same as the peer to peer software discussed above, except that it downloads from multiple users at the same time. That is what makes torrent files so popular for illegal file sharing: users can download multiple large files at very fast rates by downloading bits and pieces of a file from multiple people at the same time.

The "torrent" file itself is the tracker file that coordinates this complex web of people sharing the same file. The torrenting software uses the tracker to associate these users with each other and facilitate sharing files.

Torrent tracker files can be found on an array of websites, including Demonoid, ThePirateBay, and KickAssTorrents (KAT). KAT and Demonoid were recently closed down, as the vast majority of the torrents they were providing were for illegal content. Once a user finds a torrent file, they must run it using torrenting software, for example uTorrent, Vuze, BitTorrent, or FrostWire.

TOR – The Dark Web

The TOR network is a group of proxied servers (discussed above) that allows people to remain private on the internet. TOR technology is very complex, but put as simply as possible, a user's identity on the TOR network is masked because of TOR's complex proxy network. This way, users can still share information over public networks, but without compromising their privacy. TOR lets users publish web sites and other services without needing to reveal the location of the server hosting the material. This anonymity is, of course, ideal for illegal activity. (See http://www.torproject.org.)

Legal Challenges

When downloading files such as movies or images from the internet, often the files do not complete or get interrupted. These incomplete files are useless and are unable to be opened by the operating system. A forensic investigators might claim that a defendant accessed illegal material based on a file name, but if the download is incomplete, an illicitly named file is actually no evidence of contents. It is important to make sure that all the files identified by the forensic examiner can actually be opened within Windows. The same is true for torrent trackers; having illicitly named torrent trackers may be circumstantial evidence that illegal activity may have occurred, but it is not actually illegal material by itself. Make sure to review the file types of all the files the forensic examiner points out in the analysis to make sure they are actual media files.

Explaining the recent FBI Child Porn Sting

Recently, United States law enforcement officers were able to track down the location of a server hosting a website of child pornography material over the TOR network. The FBI seized the site, but they also continued to allow the website to operate while rerouting traffic through FBI servers. This allowed the FBI to monitor the activity to the server containing the illicit images and, after receiving a warrant, install hacking software on the computers who downloaded illicit material from the server.

This hacking software reported the user's IP address and computer information to the FBI, which the FBI then used to identify the actual people who accessed the material and issued search warrants for their individual devices. This story illustrates the kinds of new investigative techniques that no seminar can prepare us for. That is why it is important to understand general concepts and big ideas to apply in new, creative ways in our cases.