Writeup 2
CS 373
James Tyler Ball

Advanced Forensics 1:

It looks like the lectures in part 1 will stress the analysis of an acquired piece of malware. This includes the initial response, how to set up an environment to examine the malware, looking for what has been affected of breached within the 'home' system.

Also important is how to go about analyzing a piece of malware without modifying it. Something on the lists of topics I didn't expect was "creating event timelines". I imagine this to be super useful when giving a report on how the effects of a piece of malware to management.

I am intrigued at the idea of analyzing memory. Professor Beek talked about a case in which it was suspicious that an offender had altered the MAC times stored in the memory of a machine.

"The Cuckoo's Nest" is an early book about chasing hacking and instant response.

The broad steps in Forensics are:

1. Evidence Acquisition
2. Investigation and Analysis
3. Reporting Results

and can be categorized in the following three fields:

- live forensics
- post-mortem based forensics
- network-based forensics

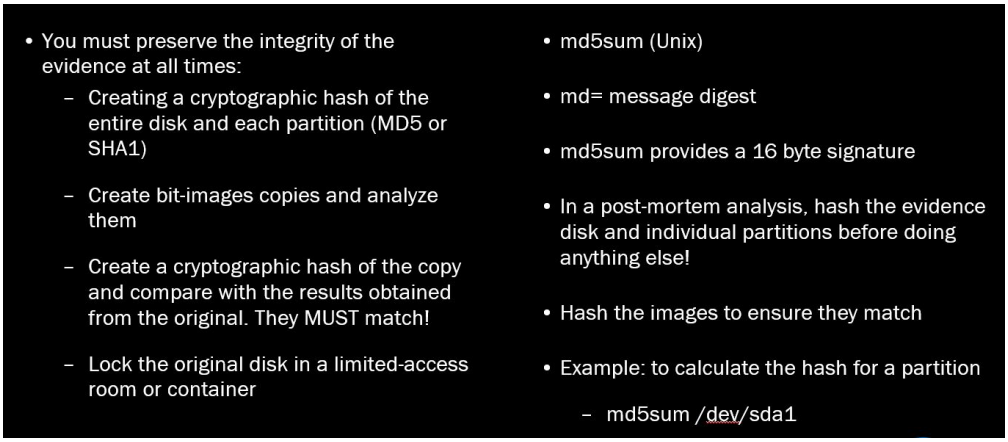
Nutshell notes:

- Note that it is not the responsibility of the forensics investigator to determine guilt, only what happens to a system.
- Generally a forensics team does not want to cut off network activity or "pull the plug" of an attacker unless safety is a concern.

- Post-mortem includes the analysis of gaming systems; communication can occur over these devices and their networks.
- Checksums can be used to analyze sensitive or illegal material without the forensics team actually having to expose themselves to that data
- A report should be reviewed and the key points near-airtight. The court system will try to drill the integrity of the forensics team. “Expert Witness” courses are advised for forensics investigators. Lawyer-esque sentence structure helps.

Remember when investigating to

1. Minimize Data Loss (pulling the plug can lead to data loss)
2. Record Everything. Make a backup of the evidence, log times, check watch vs system time. This can help to synchronize events across multiple machines. Always appoint one team member as the designated writer. Pen and paper adds to integrity.

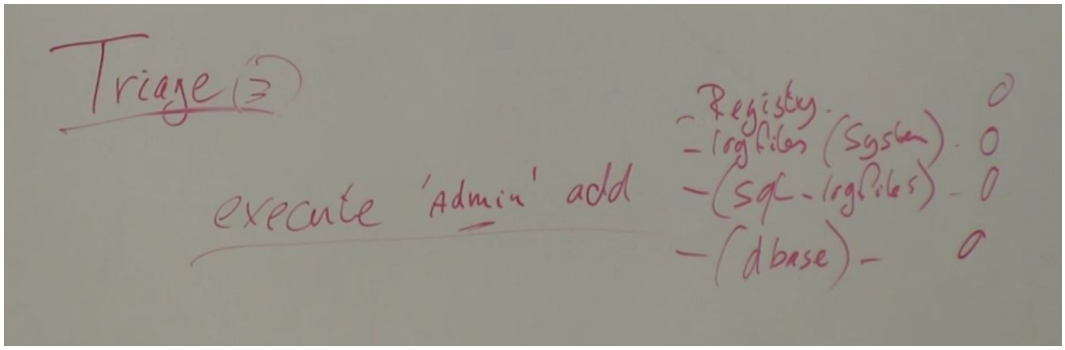


Compromise is part of the analysis. When you do compromise, write down the decision in great detail.

3. Analyze All Data. Learn how to extract data from different systems (GPS). Look for evidence in multiple layers:
    a. network
    b. OS
    c. database and apps
    d. peripherals
    e. removable media
    f. human testimony
4. Report Findings. A judge without an IT background will need to understand your findings.

Linux works very well for analyzation tools, but this class is set up for windows so we don't have to switch OS. Database forensics is a field that needs more attention.

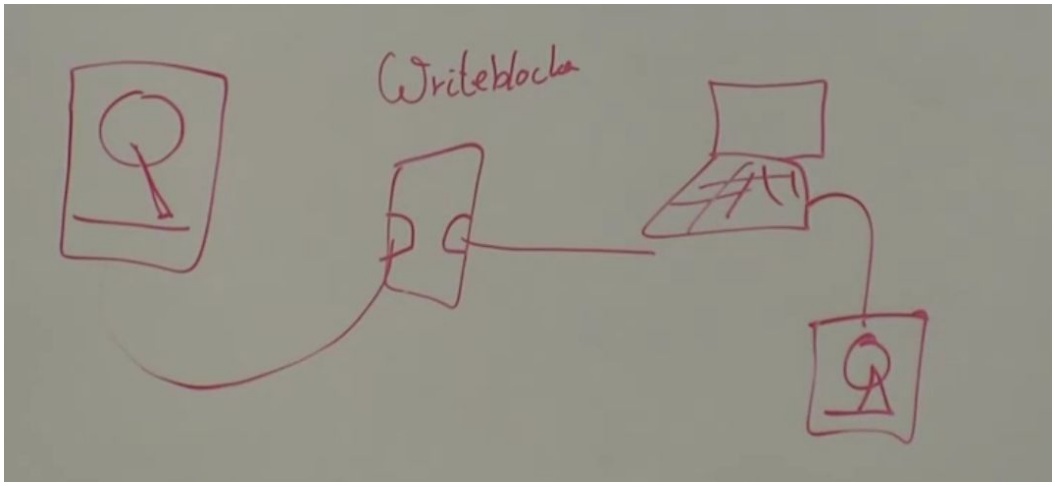
- Important term is a TRIAGE. Can you reach the same conclusion in different ways? Example: hacker trying to create an admin account on a database. Proven in multiple ways the hacker was unsuccessful:



Even when an investigator has physical access to a drive, there are several challenges when trying to analyze the data. This includes the size of a single drive, examining multiple drives on the same system.

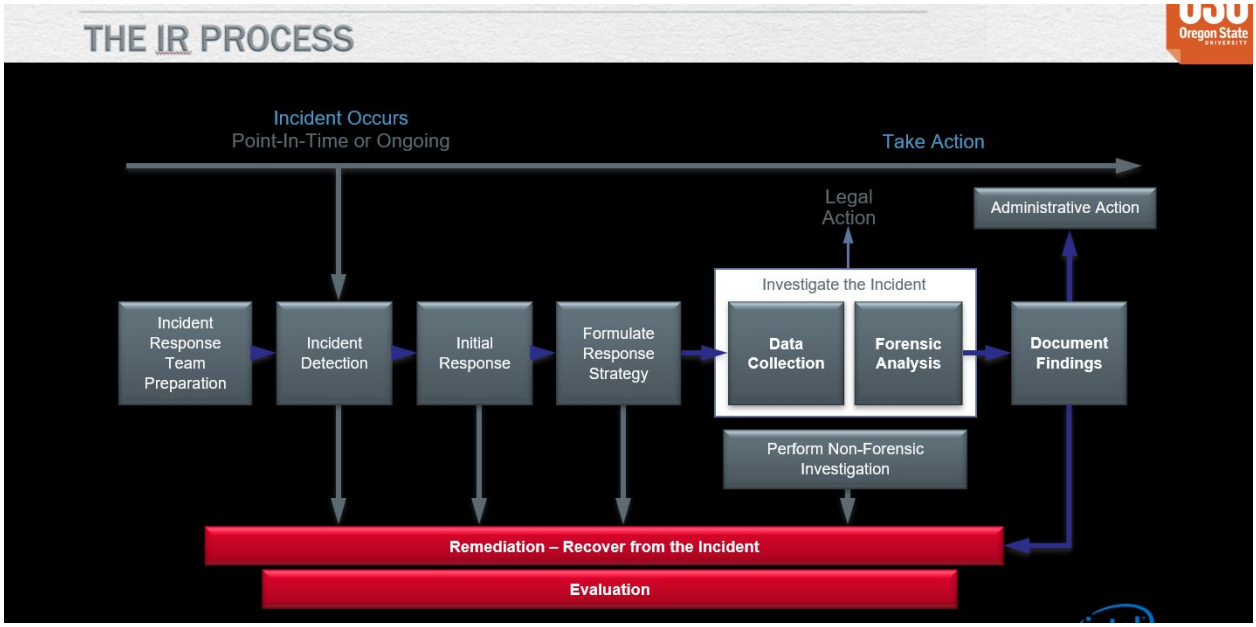
Something I hadn't thought about is how much an investigator risks by removing a suspect machine or drive from its original location (loss of RAM, loss of network traffic). I always pictured investigators yanking drives out of computers to take back to labs. This lecture has made me think more carefully about what an investigator needs to consider when encountering a new machine.

At some point when analyzing a system, you pull the plug. Take the hard disk in question, connect to a writeblocker (used to prevent compromising the disk). This is connected to the investigator's machine, which is again connected to a second disk.



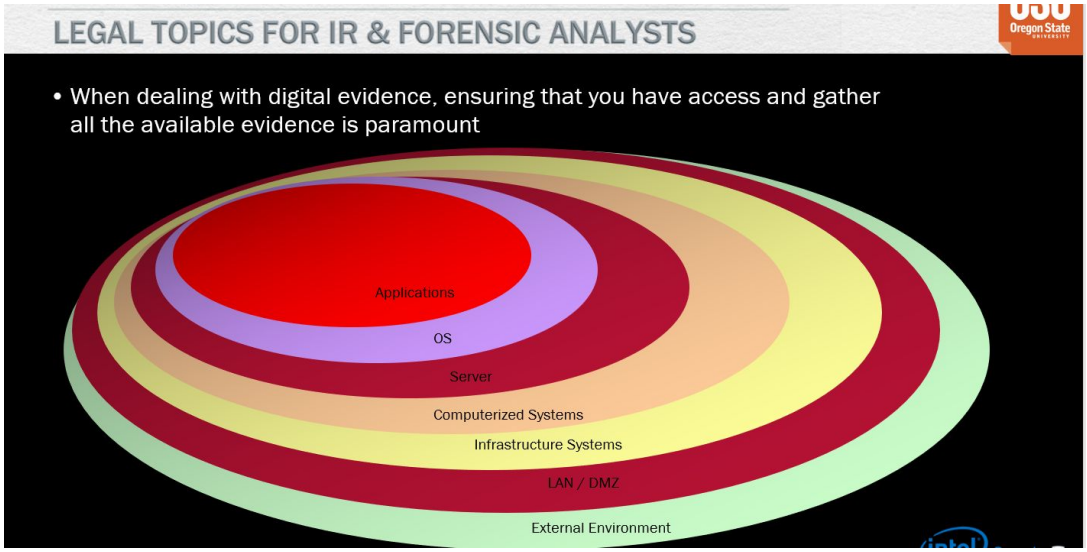
Just because an investigator has access to a suspect's personal information does not give the investigator the legal right to search through the suspect's email or similar information.

INSTANT RESPONSE PROCESS

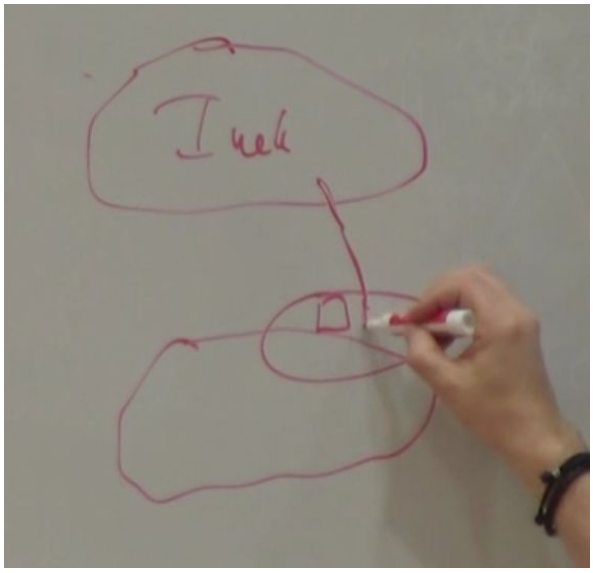


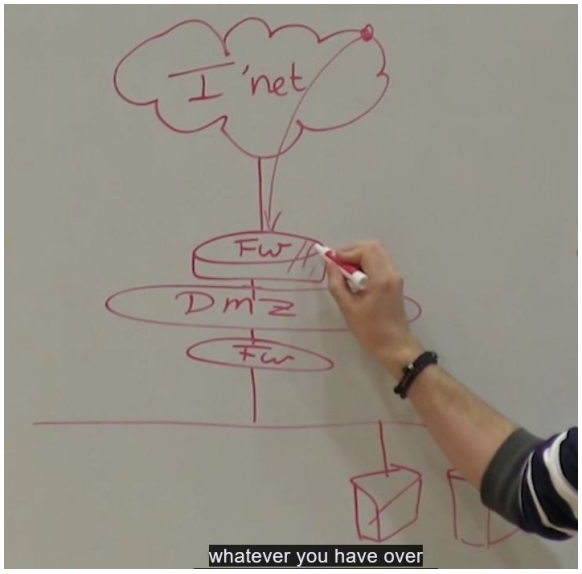
Note that there is not a clear path from start to finish. Each step must be processed carefully to determine the correct reaction.

Forming a team is not a clearly defined process either. A team is tailored to the available evidence at hand:



DMZ: demilitarized zone or safety zone:





use firewalls (put honeypot here)

Where do we look for evidence? Usually memory-dump, registry, prefetch-files. Installation, command and control. Spam alert. We face several challenges looking for more evidence:

- the large amount of data
- the company's normal operations may be impeded
- time! synchronization! Different machines have different log formats and are often incompatible
- need skilled investigators (remember that investigators need to be able to report their findings effectively)

INVESTIGATION

Locard's Exchange Principle: when two objects/systems are in contact, evidence is left behind. You cannot interact with a system without affecting it. This is part of why documentation of the process is important. In some cases, this can barr the evidence from appearing in court.

Remember that an attacker can still be using a machine remotely.

ORDER OF VOLATILITY (RFC 3227 -- the order of how you gather evidence)

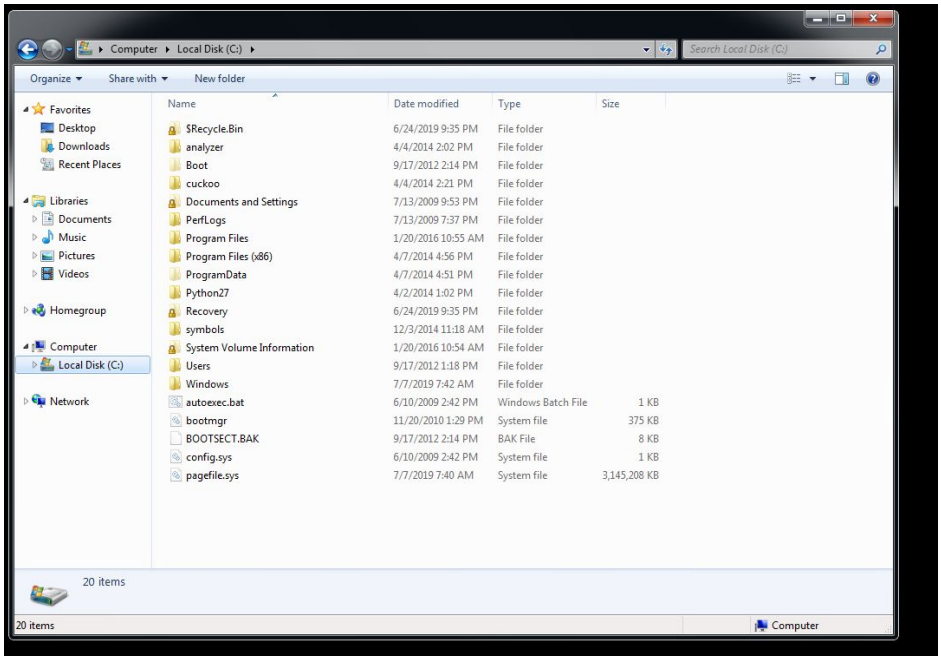
1. system memory
2. temp sytem files
3. process table, network connections (swap file, paging file)

    a. hibernation file - memory of the device state. Even if someone pulls the plug, we can take the hibernation files to analyze the state of the system.
    b. smartphone shot of the screen in some cases
4. network info - the sooner we gather this info the better
5. NOW WE REMOVE THE DRIVE -- forensics
    a. can we also find camera footage?
6. remote logging and monitoring data
7. phys config + network topology
8. backup files

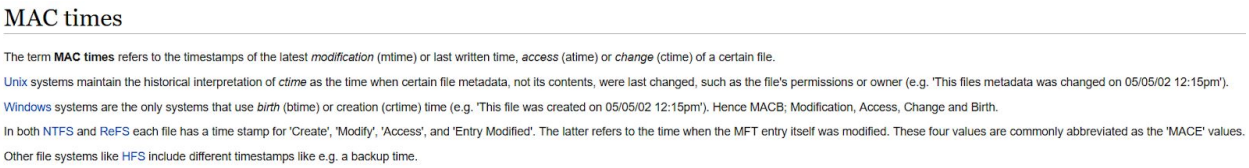
Note that volatile data will be lost on shutdown

SPECIAL NOTES FOLLOWING ALONG WITH LAB 1

Note I could not find FTK Imager on my C drive. As of Saturday night in the Slack channel I know I'm not the only one with this issue.



- As a responder, you usually carry a write-protected device with your trusted tools on it. Never install your forensics tools on a suspect's machine -- this compromises evidence.
- MAC times can be used to verify your actions -- as per the student's question.
- *What are MAC times? This is the second time in the lecture I've heard MAC times referred to, and I don't think it refers to Apple products. A quick google leads me to the following summary on ForensicsWiki:*



MAC times

The term **MAC times** refers to the timestamps of the latest *modification* (mtime) or last written time, *access* (atime) or *change* (ctime) of a certain file.

Unix systems maintain the historical interpretation of *ctime* as the time when certain file metadata, not its contents, were last changed, such as the file's permissions or owner (e.g. 'This files metadata was changed on 05/05/02 12:15pm').

Windows systems are the only systems that use *birth* (btime) or creation (crtime) time (e.g. 'This file was created on 05/05/02 12:15pm'). Hence MACB; Modification, Access, Change and Birth.

In both NTFS and ReFS each file has a time stamp for 'Create', 'Modify', 'Access', and 'Entry Modified'. The latter refers to the time when the MFT entry itself was modified. These four values are commonly abbreviated as the 'MACE' values.

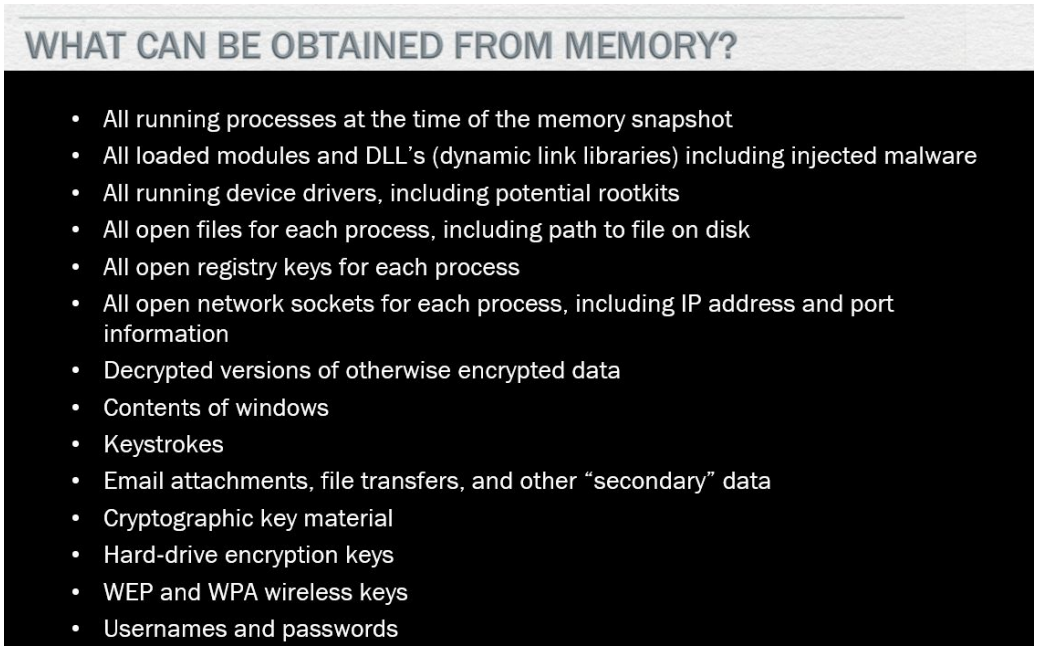
Other file systems like HFS include different timestamps like e.g. a backup time.

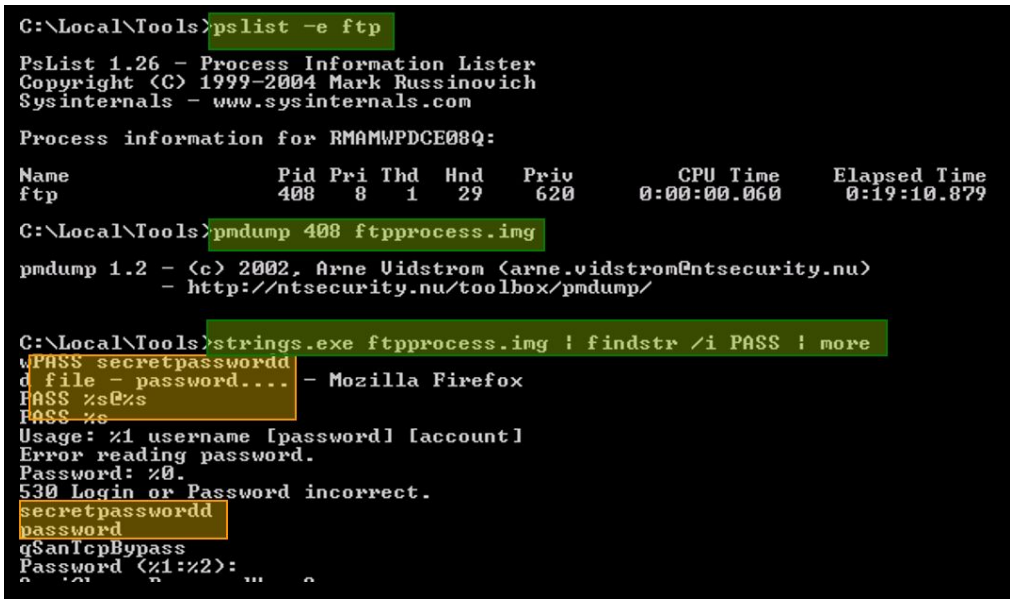
- Store your memory dump on external media. Note that we're continuing to work NOT to compromise the suspect's machine.
- Note FTK Imager has a large fingerprint in memory. FastDump is a small command line tool. Again, we run into the issue of compromise and "tainting" our suspect machine by the act of analyzing it.
- Always look for the master file table (export file if needed).
- ~99% of Police Forces are using EnCase as a forensics tool.
- A student's question touches again on the idea that you can't avoid some degree of tampering due to analyzing the data.
- There are options to encrypt dumped data.

PHYSICAL MEMORY

"memory" refers to RAM. It is important to capture this memory because it is generally temporary: the information "decays" when the machine is disconnected from power. RAM also contains important information on processes that are running at a given time.

A multitude of key and sensitive data can be acquired from RAM:





passwords acquired from RAM, many applications store passwords unencrypted in RAM

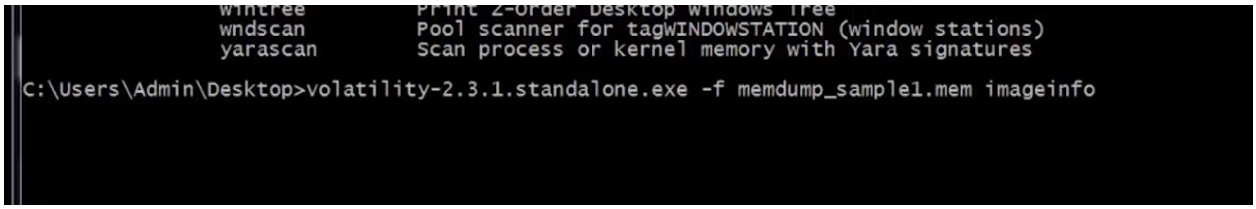
Remember to look for easy to read strings in memory dumps for hints as to what the processes are doing.

Volatility is expanding across different operating systems. Yara (mentioned in the instructions for the write-ups) can make signatures for malicious behaviors be software. Combining Yara and Volatility can compare active processes against those in a database to better understand threats.

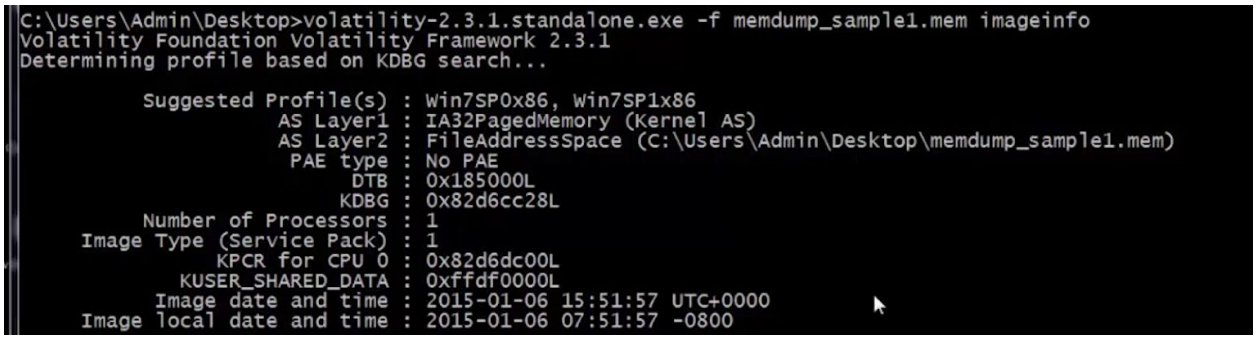
SPECIAL NOTES FOLLOWING ALONG WITH LAB 2

As mentioned above, I was unable to acquire the appropriate file from FTK.

Volatile analyzes a memory dump. The first plugin run was <imageinfo>:



After some time, the output was printed:



Running <psscon> revealed such processes as evil.exe. Process IDs are also displayed. It is possible to draw a map of the running processes in memory.

Professor Beek also wanted students to run “dlllist -p <pid>”, “netscan”, “Deskscan”, and “Getsids”. Some of this explanation was inaudible, but netscan looks for network activity, deskscan looks for activity on the desktop, and getsids can look at which users have the malware running.

```
C:\Users\Admin\Desktop>volatility-2.3.1.standalone.exe -f memdump_sample1.mem --profile=Win7SP0x86 dlllist -p 1216
Volatility Foundation Volatility Framework 2.3.1
************************************************************************
evil.exe pid:   1216
Command line : "C:\Users\Admin\Desktop\malware\MalwareBasics\Class1\Lab2\Replication\Sample1\evil.exe"
Service Pack 1

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000     0x8000     0xffff C:\Users\Admin\Desktop\malware\MalwareBasics\Class1\Lab2\Replication\Sample1\evil.ex
0x76ee0000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
0x76cd0000    0xd4000     0xffff C:\Windows\system32\kernel32.dll
0x750b0000    0x4a000     0xffff C:\Windows\system32\KERNELBASE.dll
0x72940000   0x153000     0xffff C:\Windows\system32\MSVBVM60.DLL
0x75650000    0xc9000     0xffff C:\Windows\system32\USER32.dll
0x75390000    0x4e000     0xffff C:\Windows\system32\GDI32.dll
0x754c0000     0xa000     0xffff C:\Windows\system32\LPK.dll
0x76db0000    0x9d000     0xffff C:\Windows\system32\USP10.dll
0x755a0000    0xac000     0xffff C:\Windows\system32\msvcrt.dll
0x754d0000    0xa0000     0xffff C:\Windows\system32\ADVAPI32.dll
0x767b0000    0x19000     0xffff C:\Windows\SYSTEM32\sechost.dll
0x76700000    0xa1000     0xffff C:\Windows\system32\RPCRT4.dll
0x76b70000   0x15c000     0xffff C:\Windows\system32\ole32.dll
0x76e50000    0x8f000     0xffff C:\Windows\system32\OLEAUT32.dll
```

dlllist output

```
C:\Users\Admin\Desktop>volatility-2.3.1.standalone.exe -f memdump_sample1.mem --profile=Win7SP0x86 netscan
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Proto    Local Address                  Foreign Address      State            Pid      Owner          Crea
0x3e409d90 TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        488      services.exe
0x3e40d788 TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        488      services.exe
0x3e40d788 TCPv6    :::49155                       :::0                 LISTENING        488      services.exe
0x3e410c88 TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x3e410c88 TCPv6    :::445                         :::0                 LISTENING        4        System
0x3e5271e0 TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        504      lsass.exe
0x3e5289f8 TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        504      lsass.exe
0x3e5289f8 TCPv6    :::49156                       :::0                 LISTENING        504      lsass.exe
0x3e99ce58 TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        872      svchost.exe
0x3e99ce58 TCPv6    :::49154                       :::0                 LISTENING        872      svchost.exe
0x3e9b68b0 TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        700      svchost.exe
0x3e9c11c8 TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        700      svchost.exe
0x3e9c11c8 TCPv6    :::135                         :::0                 LISTENING        700      svchost.exe
0x3e9c73e0 TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        396      wininit.exe
0x3e9c8b80 TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        396      wininit.exe
0x3e9c8b80 TCPv6    :::49152                       :::0                 LISTENING        396      wininit.exe
0x3e9ec750 TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        784      svchost.exe
0x3e9ed470 TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        784      svchost.exe
0x3e9ed470 TCPv6    :::49153                       :::0                 LISTENING        784      svchost.exe
0x3eb371d0 TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        872      svchost.exe
```

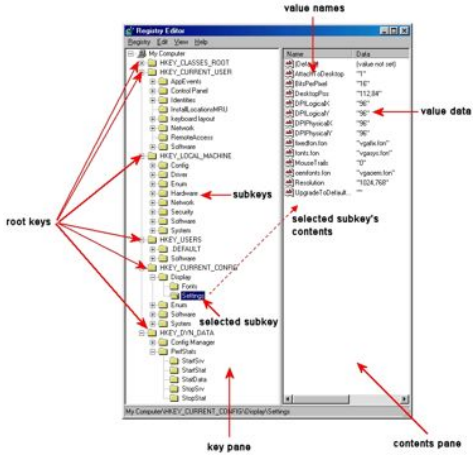
netscan output

```
C:\Users\Admin\Desktop>volatility-2.3.1.standalone.exe -f memdump_sample1.mem --profile=Win7SP0x86 deskscan
Volatility Foundation Volatility Framework 2.3.1
************************************************
Desktop: 0x3e5201b8, Name: msswindowstation\mssrestricteddesk, Next: 0x0
SessionId: 0, DesktopInfo: 0xfe400578, fsHooks: 0
spwnd: 0xfe400618, Windows: 20
Heap: 0xfe400000, Size: 0x80000, Base: 0xfe400000, Limit: 0xfe480000
************************************************
Desktop: 0x3e93ef20, Name: WinSta0\Default, Next: 0x8653ba28
SessionId: 0, DesktopInfo: 0xfe800578, fsHooks: 32
spwnd: 0xfe800618, Windows: 14
Heap: 0xfe800000, Size: 0xc00000, Base: 0xfe800000, Limit: 0xff400000
 2764 (spoolsv.exe 1368 parent 488)
 2784 (spoolsv.exe 1368 parent 488)
 2776 (spoolsv.exe 1368 parent 488)
 2772 (spoolsv.exe 1368 parent 488)
 1416 (spoolsv.exe 1368 parent 488)
 1372 (spoolsv.exe 1368 parent 488)
 476 (csrss.exe 336 parent 320)
```

deskscan output

Advanced Forensics 2:

Next to memory, one of the most important parts of a computer to a forensics investigator is the Registry. Nearly every operation in windows is recorded in the Registry.



Regripper can be used to analyze a dump of the Registry. Most information is contained in HKU (HKEY_USERS) and HKLM (HKEY_LOCAL_MACHINE). HKU can be used to find browsing history.

AutoRun is one of the most common targets to install malware. Malware wants to survive a reboot.

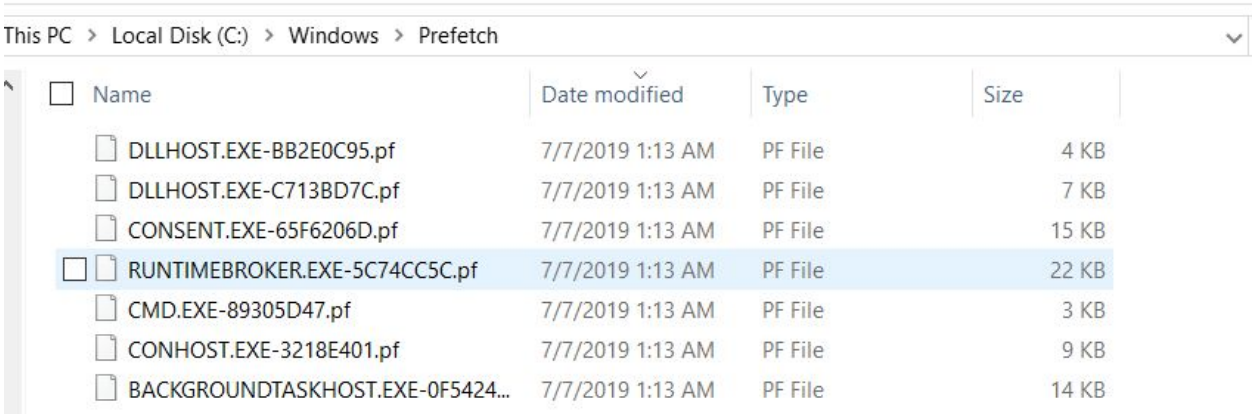
It is re-emphasized that creating a well documented timeline is very important in your analysis, relating to both actions taken by investigators and activity related to the malware in question. The Registry contains information like what files were modified when, which can help to fill out a picture of what activity occurred on the suspect's machine.

The tools discussed this week (Volatility, Master File Table, Reg-Ripper) can help an investigator to build a reliable timeline, which often becomes the center of an investigative process.

Professor Beek then uses two new command within Volatility:

- timeliner: used to create an overview of processes of network connections with times attached.
- mftparser: looks into memory dump and views the master file table, outputs data into a text document. Naturally this document will be much larger than the one created by timeliner

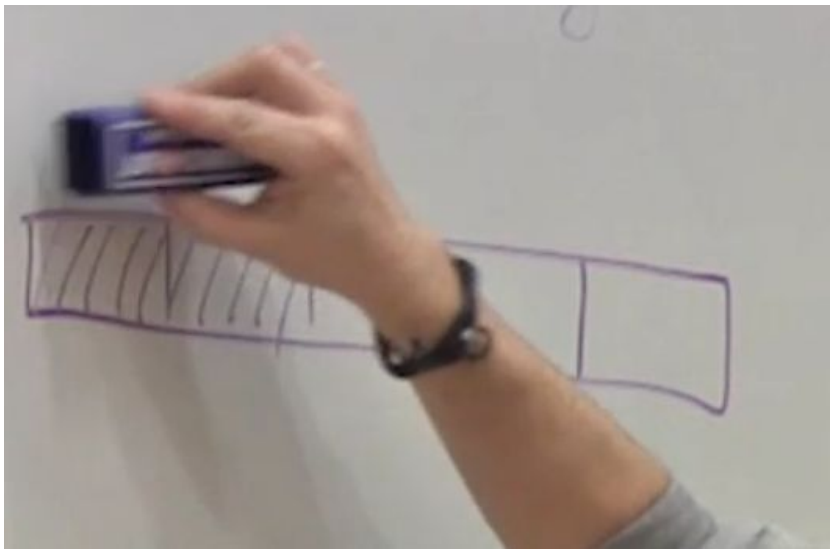
You can also look for information in the Prefetch directory in Windows, which contains the last 128 files run:



examining Prefetch on my local machine

Professor Beek then brought up the idea of looking at system restore points to see if an attacker left any crucial information that might have been deleted or removed later.

The next tool we're looking at is DataCarving. This is used to recover deleted data. This works because data isn't always removed from storage upon deletion, only no longer flagged.



visual representation of "flags" being removed

Phones are a huge vulnerability. SMS messages and other sensitive data can be recovered from old devices. We can search for specific file types be examining signatures are estimated

sizes to extract ‘deleted’ data. Sometimes programs will look for a header and footer, sometimes they look for a given file structure.

To use Photorec in the VM, go to Tools->testdisk-6.14. Select the drive with the deleted content and specify where you want PhotoRec to put the recovered files.

The final video in the lecture goes over an in-class challenge. The students download a file and have to answer six questions based on the information they extract from the file. Remember to try and translate any foreign language encountered to get a better idea of what the files might do.