Digital Forensics
Lecture Week 7

Windows Artifacts

Readings
Nelson Chapter 5

Objectives

- To understand Windows Artifacts
- To identify Volatile Forensic Data
- To identify non-Volatile Forensic Data
- To understand computer profiling

The Scenario

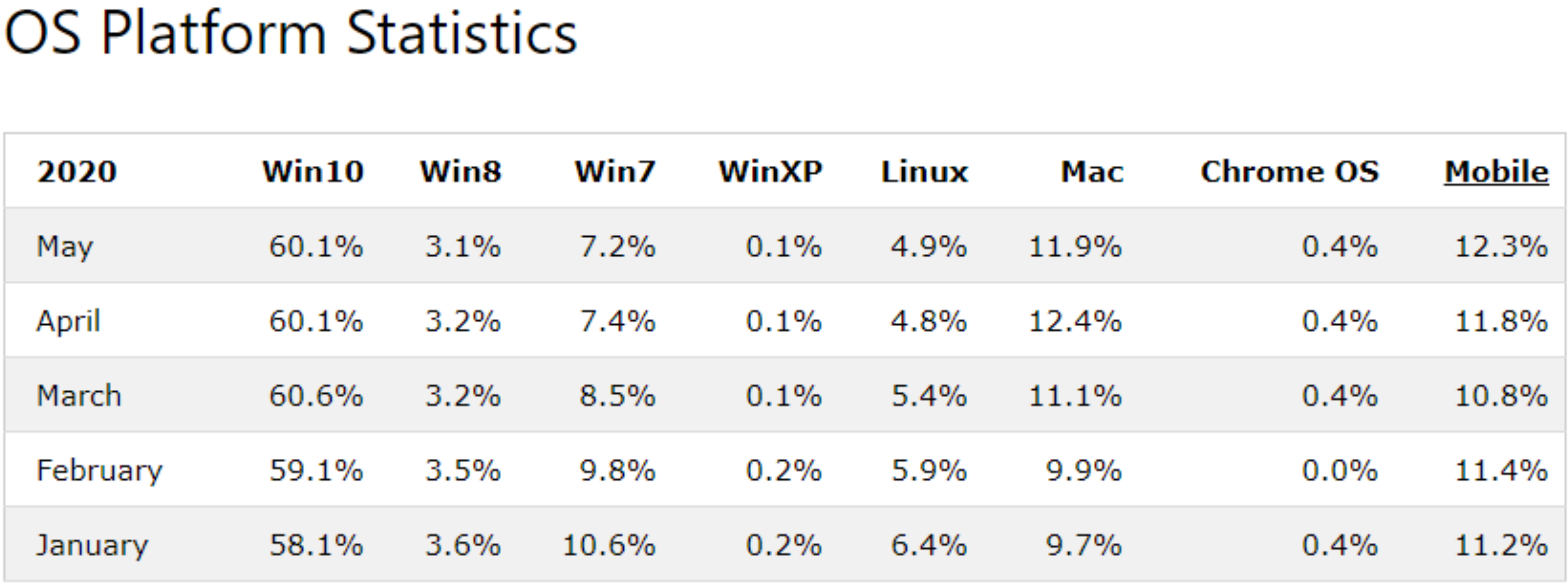
- We are asked to examine a digital device
- We suspect it has been involved in an attack
- We suspect there may be evidence left
  - And traces of any malware used
- We wish to capture the evidence immediately
- We will first capture the volatile evidence
- Then we will capture the non-Volatile evidence

Device Variation

- Each device has completely different artifacts
- Depends on the OS
  - Windows, Apple, MAC iOS, Android
- Depends on the Virtualisation
  - Native Host, Virtual Machine, Cloud based services
- Depends on the installed Apps
  - Browsers, Office, VPNs

Client Operating Systems

- What OS is the suspect likely to use?
- w3schools.com collect web browser statistics



OS Platform Statistics

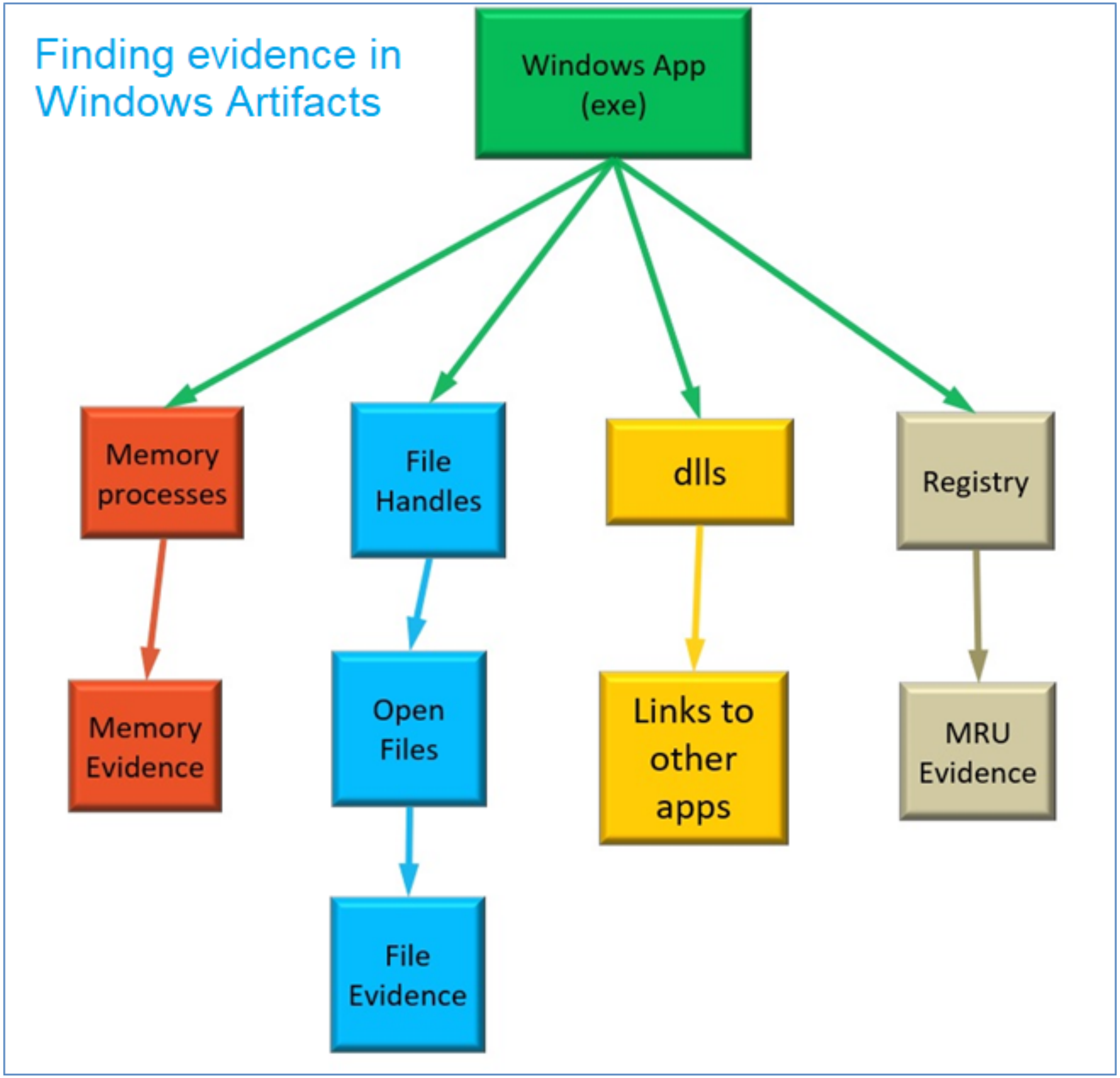
2020	Win10	Win8	Win7	WinXP	Linux	Mac	Chrome OS	Mobile
May	60.1%	3.1%	7.2%	0.1%	4.9%	11.9%	0.4%	12.3%
April	60.1%	3.2%	7.4%	0.1%	4.8%	12.4%	0.4%	11.8%
March	60.6%	3.2%	8.5%	0.1%	5.4%	11.1%	0.4%	10.8%
February	59.1%	3.5%	9.8%	0.2%	5.9%	9.9%	0.0%	11.4%
January	58.1%	3.6%	10.6%	0.2%	6.4%	9.7%	0.4%	11.2%

- We will look at Windows 10 now and later Linux

Windows Artifacts

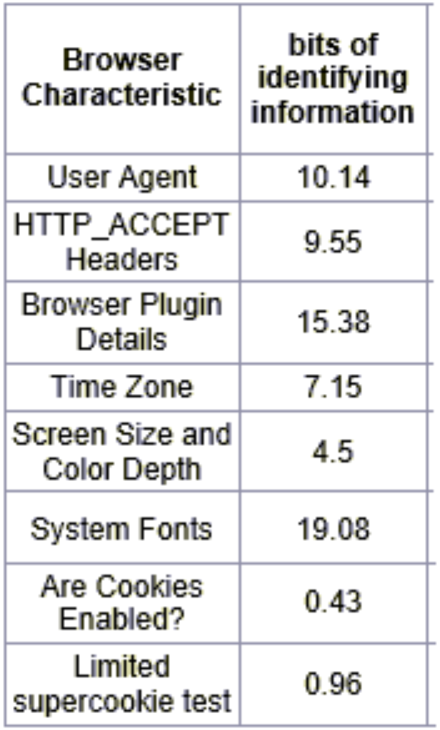
- The suspect uses a Windows device to:
  - Send and receive emails
  - Visit web sites and use social networking
  - Download and collect data
- By accident or design, there may be malware
- What does Windows collect about her activity?
  - Where will we find this information?
  - In what order should we search?

Finding evidence in Windows Artifacts



Using the Web Client

- We use a browser to ident the device
- The http request string is an example
- This is called device fingerprinting
  - Remember Browserleaks.
- We use this to guide our investigation



Browser Characteristic	bits of identifying information
User Agent	10.14
HTTP_ACCEPT Headers	9.55
Browser Plugin Details	15.38
Time Zone	7.15
Screen Size and Color Depth	4.5
System Fonts	19.08
Are Cookies Enabled?	0.43
Limited supercookie test	0.96

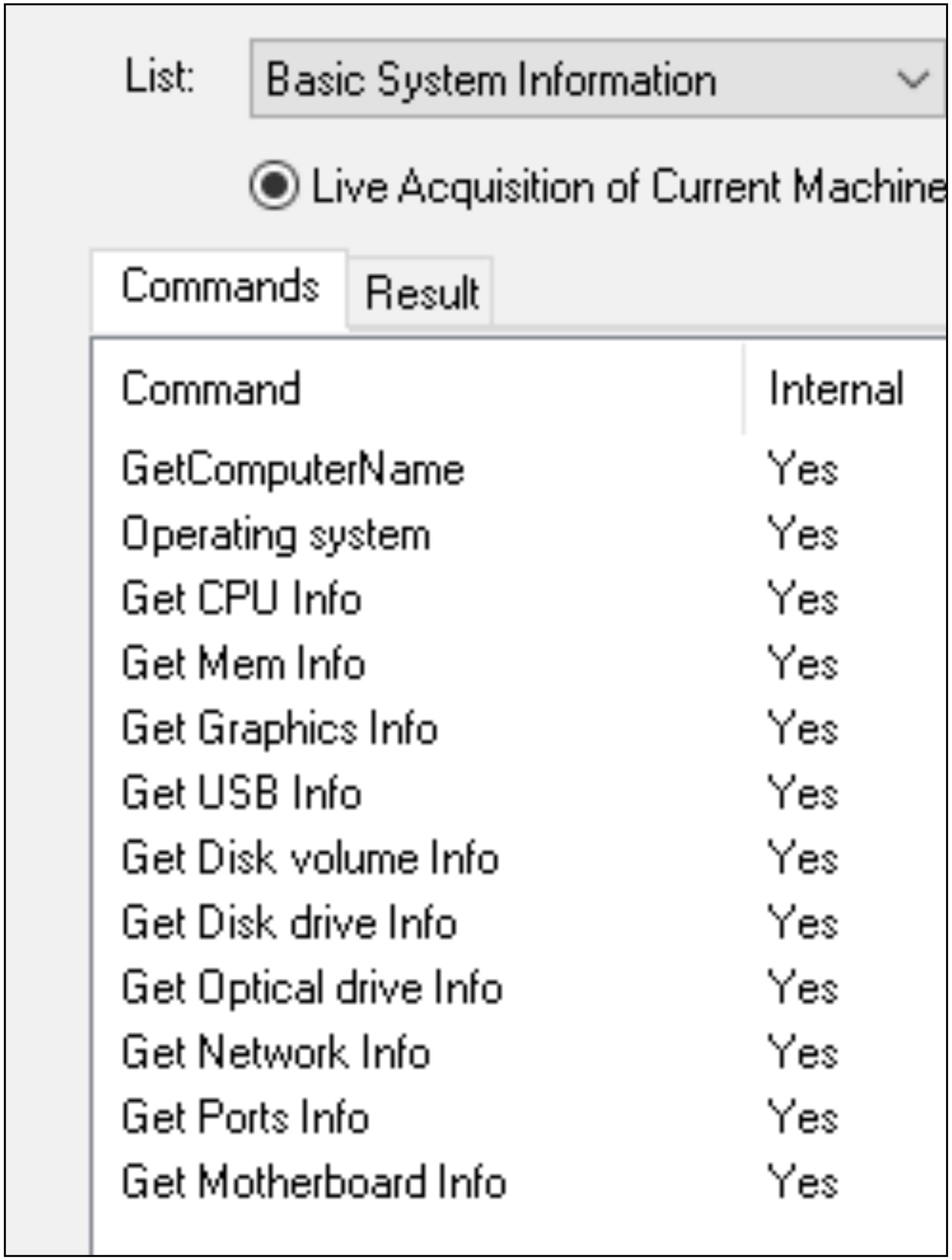
Windows Profiling

- An important forensics process
- We collect state information from normal behaviour
- We consider abnormal behaviour as being of forensic interest
- What is normal?
- We collect and average behaviour for a variety of combinations
- We vary browsers, applications, users, time of day, etc …
  - See later section on profiling

Windows Artifact tools

- We can use WMI to scan a PC to determine its configuration
- We can use python or Windows PowerShell to run commands
- We can use forensic tools
  - OSForensics
  - ProDiscover
  - Autopsy
  - Encase

OSForensics



List: Basic System Information

● Live Acquisition of Current Machine

Command	Internal
GetComputerName	Yes
Operating system	Yes
Get CPU Info	Yes
Get Mem Info	Yes
Get Graphics Info	Yes
Get USB Info	Yes
Get Disk volume Info	Yes
Get Disk drive Info	Yes
Get Optical drive Info	Yes
Get Network Info	Yes
Get Ports Info	Yes
Get Motherboard Info	Yes

Objectives

- To understand Windows Artifacts
- To identify Volatile Forensic Data
- To identify non-Volatile Forensic Data
- To understand computer profiling

Volatile Forensics

- Examiners use a routine in their initial investigation
  - Profile check to detect unusual artifacts
- We will do a cut down version today
  - Date and Time
  - Current Network sessions
  - Running Processes
  - Prefetch activity

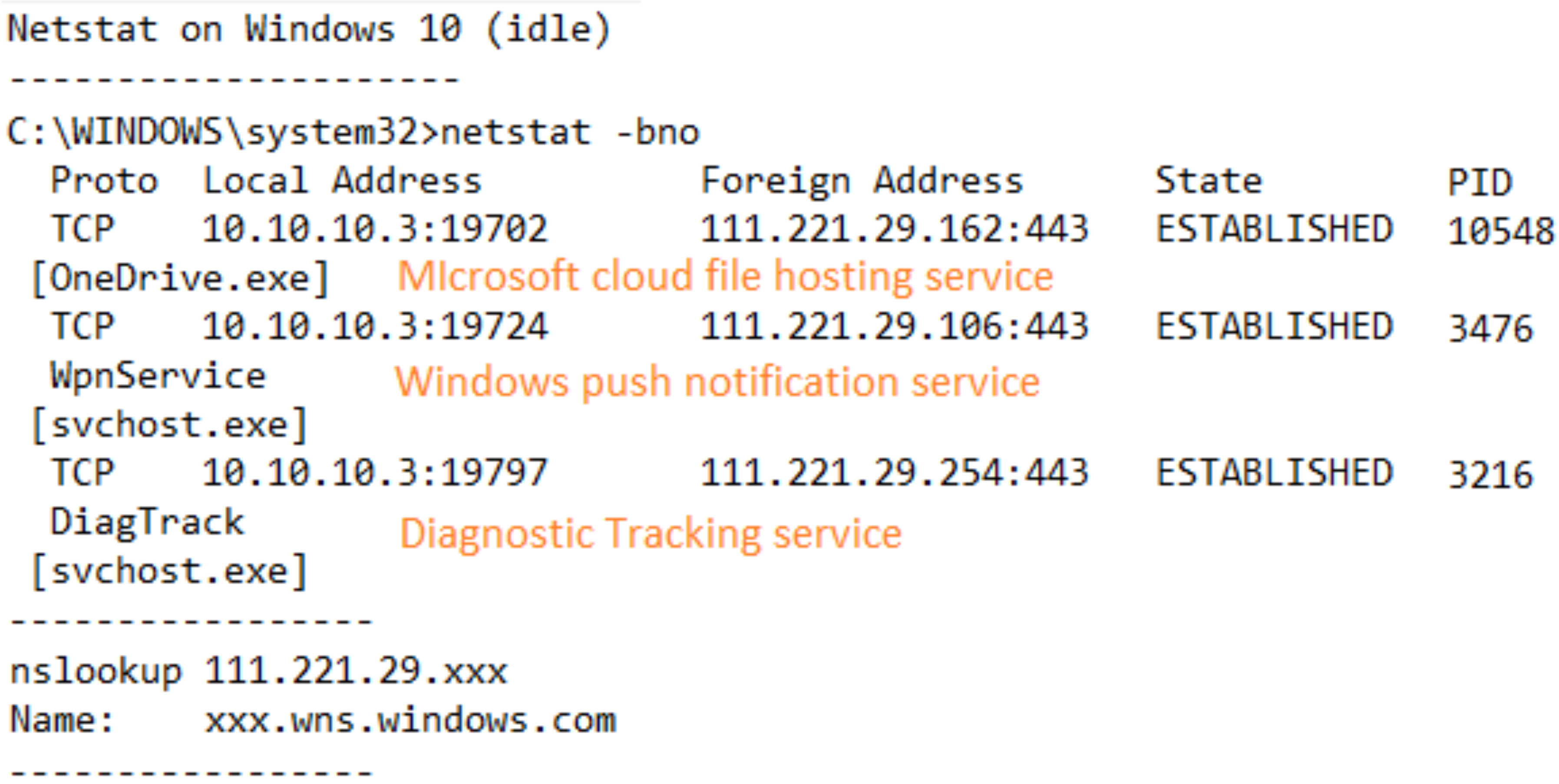
Volatile Evidence collection items

- Date and Time of our investigation
  - very important in a court of law
  - easy to obtain from built in Windows commands
  - Include the current time zone
- We check current network connections
  - Using the built-in netstat command
- We will see many connections
  - browsing and cloud services
  - How do we know which ones are normal?

Open tcp and udp ports

- Netstat shows open ports listening
- Listening for what?
- We use forensic tools to link the open ports to the executable program that launched them
- We examine the exes to see if they have been altered
- How?
  - We can look at the file publisher information
  - We can look at the published file hash sets
  - www.nsrl.**nist**.gov 4GB!
  - some forensic tools have a copy of these hashes in a SQLite db

Netstat on Windows 10
(idle, no user apps open)



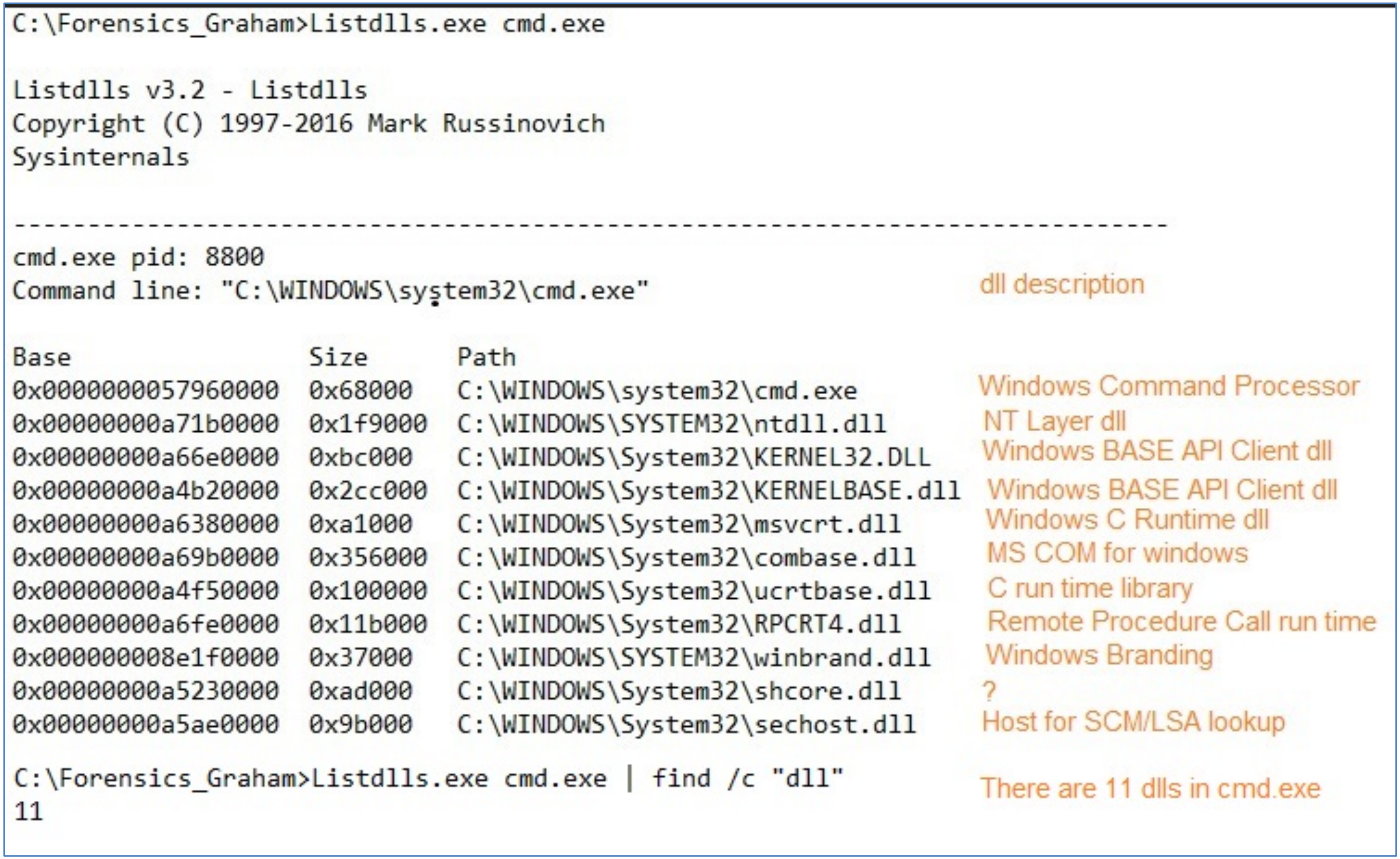
```
Netstat on Windows 10 (idle)
----------------------

C:\WINDOWS\system32>netstat -bno
  Proto  Local Address          Foreign Address        State           PID
  TCP    10.10.10.3:19702       111.221.29.162:443     ESTABLISHED     10548
 [OneDrive.exe]     MIcrosoft cloud file hosting service
  TCP    10.10.10.3:19724       111.221.29.106:443     ESTABLISHED     3476
  WpnService        Windows push notification service
 [svchost.exe]
  TCP    10.10.10.3:19797       111.221.29.254:443     ESTABLISHED     3216
  DiagTrack         Diagnostic Tracking service
 [svchost.exe]
-----------------
nslookup 111.221.29.xxx
Name:    xxx.wns.windows.com
-----------------
```

Processes, Services and dlls

- We met these in Week 6
  - See the CPU and Memory Lecture
- These are of forensic interest when chasing malware
- Use the pslist and listdlls tools
- Look for strange process names
- Look for strange exe locations

Viewing dlls



```
C:\Forensics_Graham>Listdlls.exe cmd.exe

Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals


------------------------------------------------------------------------------
cmd.exe pid: 8800
Command line: "C:\WINDOWS\system32\cmd.exe"

Base                Size      Path
0x0000000057960000  0x68000   C:\WINDOWS\system32\cmd.exe
0x00000000a71b0000  0x1f9000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x00000000a66e0000  0xbc000   C:\WINDOWS\System32\KERNEL32.DLL
0x00000000a4b20000  0x2cc000  C:\WINDOWS\System32\KERNELBASE.dll
0x00000000a6380000  0xa1000   C:\WINDOWS\System32\msvcrt.dll
0x00000000a69b0000  0x356000  C:\WINDOWS\System32\combase.dll
0x00000000a4f50000  0x100000  C:\WINDOWS\System32\ucrtbase.dll
0x00000000a6fe0000  0x11b000  C:\WINDOWS\System32\RPCRT4.dll
0x000000008e1f0000  0x37000   C:\WINDOWS\SYSTEM32\winbrand.dll
0x00000000a5230000  0xad000   C:\WINDOWS\System32\shcore.dll
0x00000000a5ae0000  0x9b000   C:\WINDOWS\System32\sechost.dll

C:\Forensics_Graham>Listdlls.exe cmd.exe | find /c "dll"
11
```

dll description

Windows Command Processor

NT Layer dll

Windows BASE API Client dll

Windows BASE API Client dll

Windows C Runtime dll

MS COM for windows

C run time library

Remote Procedure Call run time

Windows Branding

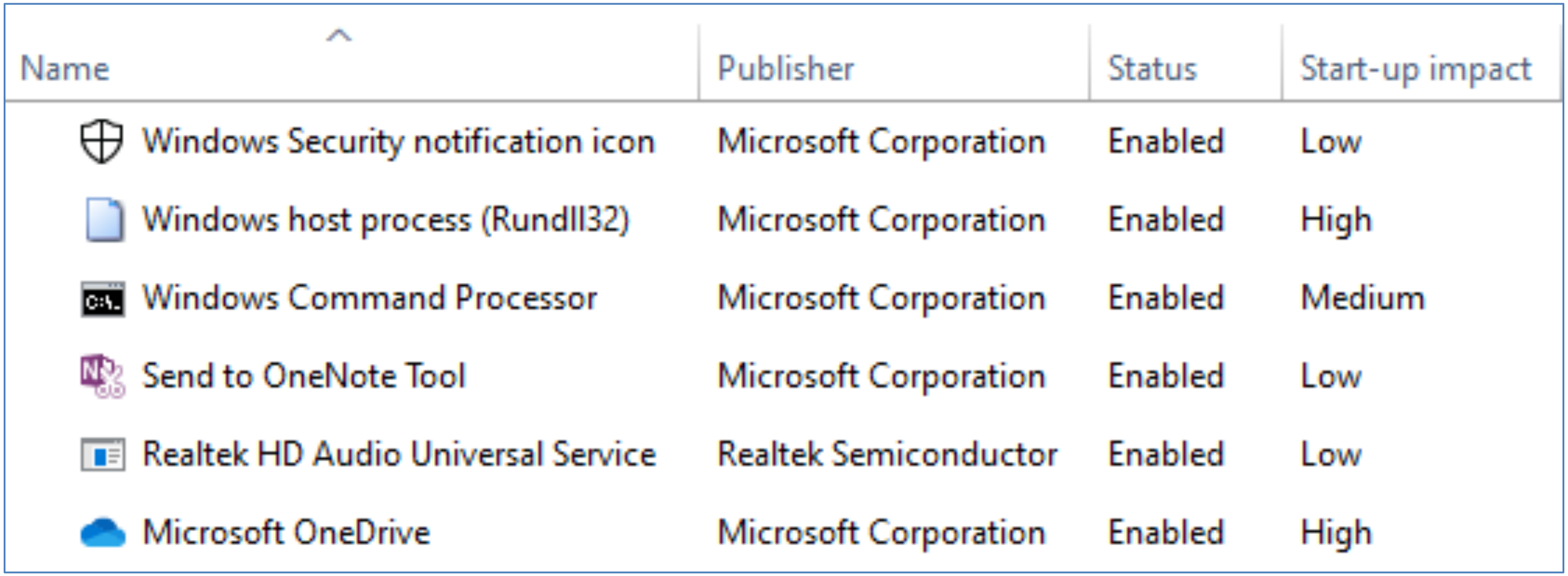
?

Host for SCM/LSA lookup

There are 11 dlls in cmd.exe

AutoStart/Autorun #1

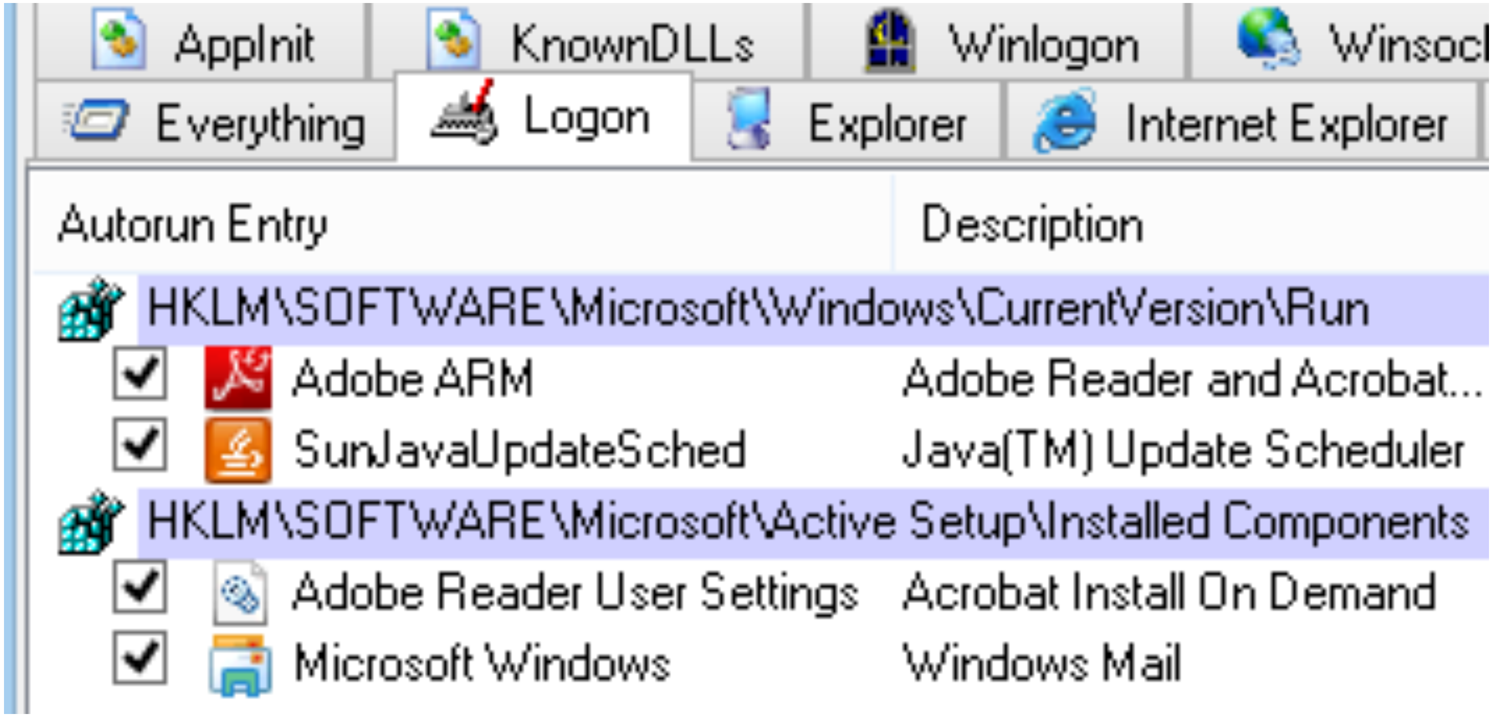
- Covered in Week 6



Name	Publisher	Status	Start-up impact
Windows Security notification icon	Microsoft Corporation	Enabled	Low
Windows host process (Rundll32)	Microsoft Corporation	Enabled	High
Windows Command Processor	Microsoft Corporation	Enabled	Medium
Send to OneNote Tool	Microsoft Corporation	Enabled	Low
Realtek HD Audio Universal Service	Realtek Semiconductor	Enabled	Low
Microsoft OneDrive	Microsoft Corporation	Enabled	High

AutoStart/Autorun #2

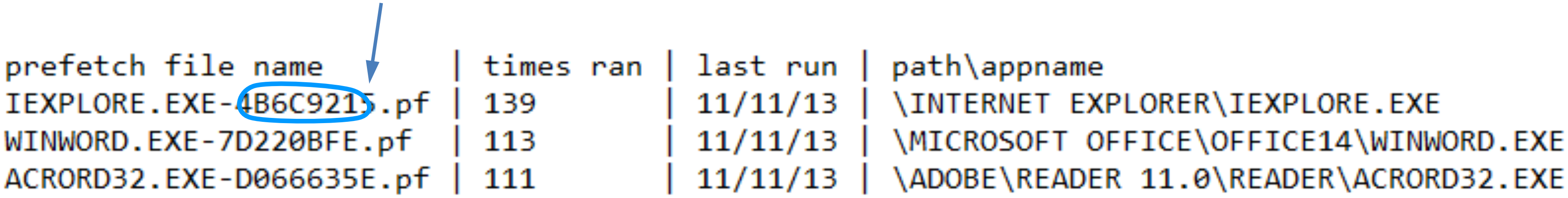
- Use the SysInternals Autoruns tool



Autorun Entry	Description
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	
☑ Adobe ARM	Adobe Reader and Acrobat...
☑ SunJavaUpdateSched	Java(TM) Update Scheduler
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	
☑ Adobe Reader User Settings	Acrobat Install On Demand
☑ Microsoft Windows	Windows Mail

Prefetch

- When an app runs, it needs various objects loaded into memory.
- Prefetch collects this information and preloads these objects for the next time the app starts.
  - Kept in C:\Windows\prefetch
  - the hash includes the name, date and file path.



```
prefetch file name       | times ran | last run | path\appname
IEXPLORE.EXE-4B6C9215.pf | 139       | 11/11/13 | \INTERNET EXPLORER\IEXPLORE.EXE
WINWORD.EXE-7D220BFE.pf  | 113       | 11/11/13 | \MICROSOFT OFFICE\OFFICE14\WINWORD.EXE
ACRORD32.EXE-D066635E.pf | 111       | 11/11/13 | \ADOBE\READER 11.0\READER\ACRORD32.EXE
```

- Provides evidence of when an app was used.
- Also how often it was opened.

Objectives

- To understand Windows Artifacts
- To identify Volatile Forensic Data
- To identify non-Volatile Forensic Data
- To understand computer profiling

Non-Volatile Forensics

- Examiners use a routine in their initial investigation
  - Profile check to detect unusual artifacts
- We will do a cut down version today
  - OS Patch level
  - Browser Add-ons
  - User accounts
  - Time Lines
  - MRUs
  - Registry
  - Restore points
  - Logs

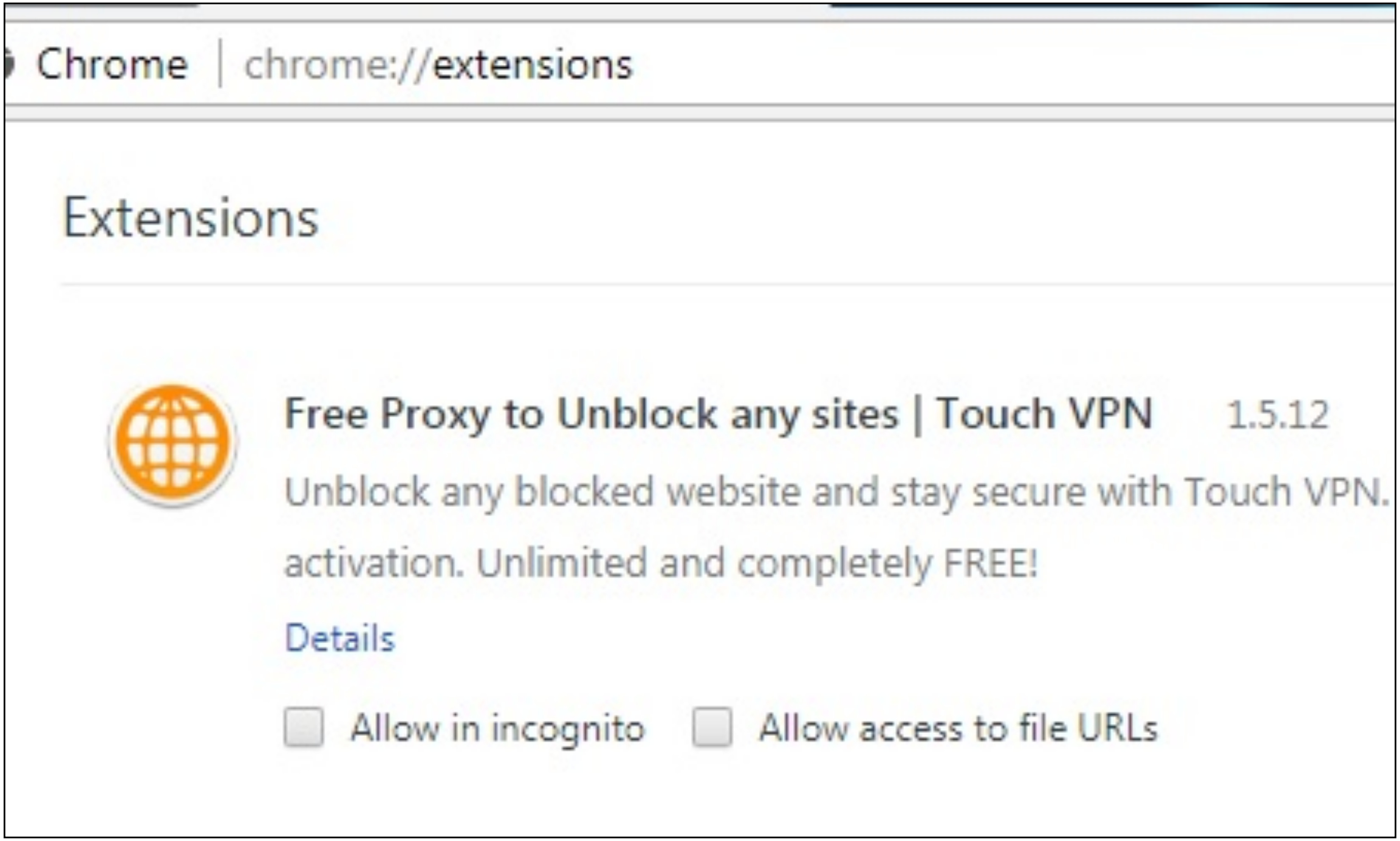
Collecting System Data

- Checking for Malware:
- The attacks possible on a device depend heavily on which OS patches have been applied
- We need to collect the patch level of the OS
- This includes patches for applications
  - Browsers
  - Office
  - Adobe, etc …
- We use the Forensic tool PsInfo or similar

Browser add-ons

- Customised browsers can reveal a lot about the suspect
- The chosen add-ons or extensions reveal a lot
- Found on Google or Apple store
- Check for:
  - anonymous proxies
  - VPNs
  - TOR

Chrome extensions



Chrome | chrome://extensions

Extensions

Free Proxy to Unblock any sites | Touch VPN 1.5.12

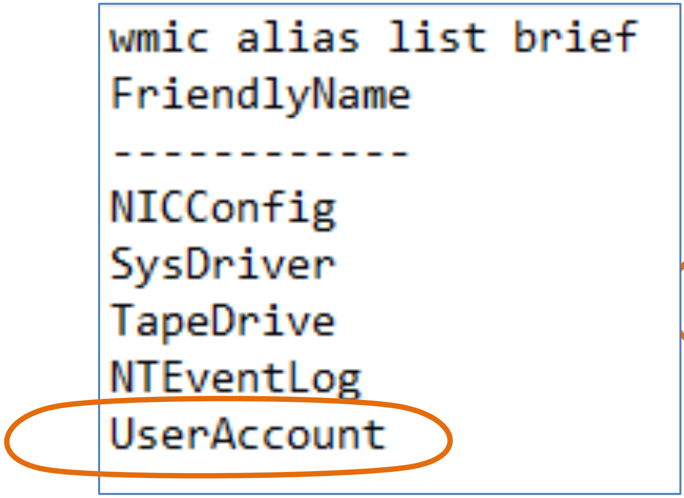
Unblock any blocked website and stay secure with Touch VPN.
activation. Unlimited and completely FREE!

Details

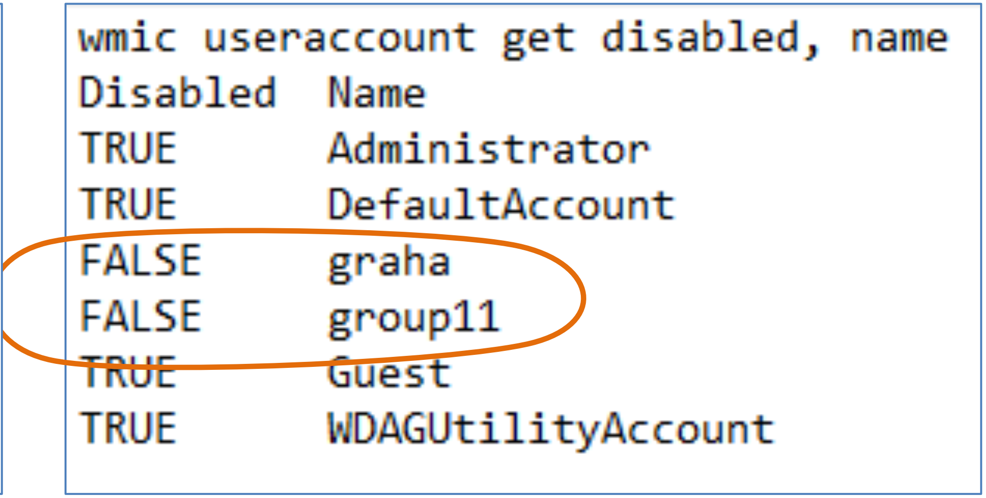
□ Allow in incognito □ Allow access to file URLs

Viewing User Accounts with WMIC

- Windows Management Instrumentation Command (WMIC)
- Can see Windows Internals
- wmic alias list brief – show all available commands
- wmic useraccount list brief – show common item headings
- wmic useraccount get disabled, name – show selected items



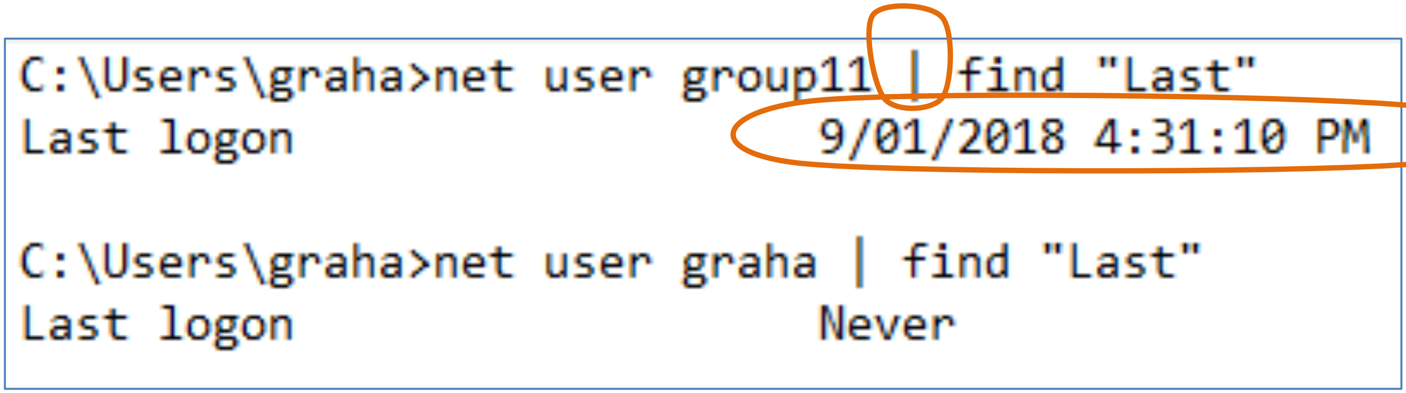
```
wmic alias list brief
FriendlyName
------------
NICConfig
SysDriver
TapeDrive
NTEventLog
UserAccount
```



```
wmic useraccount get disabled, name
Disabled  Name
TRUE      Administrator
TRUE      DefaultAccount
FALSE     graha
FALSE     group11
TRUE      Guest
TRUE      WDAGUtilityAccount
```

Find the last login for a user

- Use a pipe (|) to pass the output of net user into find



```
C:\Users\graha>net user group11 | find "Last"
Last logon                   9/01/2018 4:31:10 PM

C:\Users\graha>net user graha | find "Last"
Last logon                   Never
```

- What If the answer is Never?
  - the user logged in using a Microsoft cloud account

Timelines

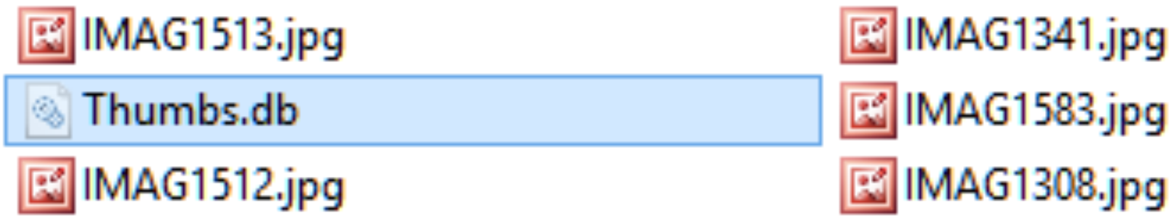
- Timelines track the Incident events step by step.
- You may find suspicious events in a log file.
- Other evidence may point to the suspect’s activity around this time.
- It is of forensic interest to assemble all activity around this time.
  - On the PC, network and phones
  - You must allow for different server Time Zones
- See Forensic toolkits for timeline reconstruction.

Collecting a Time Line

- Previous investigations will reveal the date and time of attacks.
- We can collect date and time information about every file on the device.
- We can then examine the files in use during the attack.
- There are three dates for each file
  - Created, Modified, Opened
- We use a Linux utility called find to examine file data
- (this is **not** the same as the Windows find used earlier)
- We export this to Excel for sorting

Thumbnail Caches

- Windows can create a Thumbs.db of image files in each directory for quick viewing

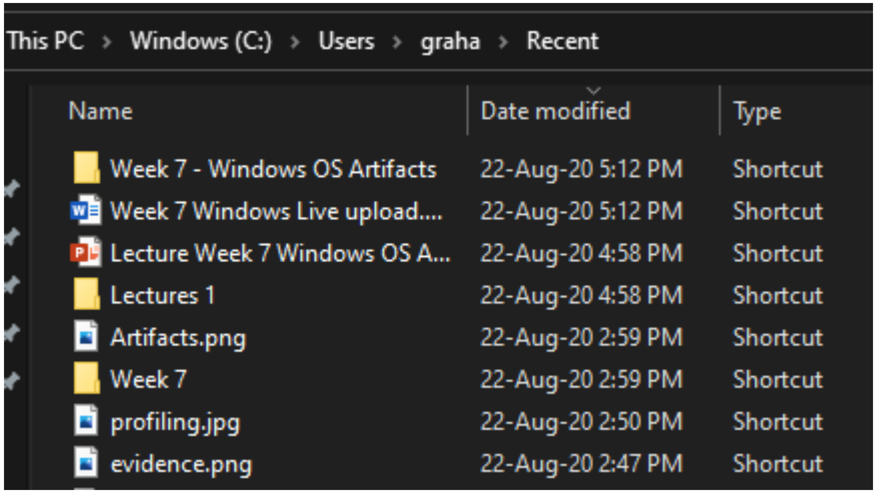


IMAG1513.jpg
Thumbs.db
IMAG1512.jpg
IMAG1341.jpg
IMAG1583.jpg
IMAG1308.jpg

- Deleting an image does not delete its entry in thumbs.db

Recent Files

- A list of recently opened data files and folders can be found in C:\Users\xxx\Recent
- To see recently used apps use UserAssist
  - See next slide



This PC › Windows (C:) › Users › graha › Recent

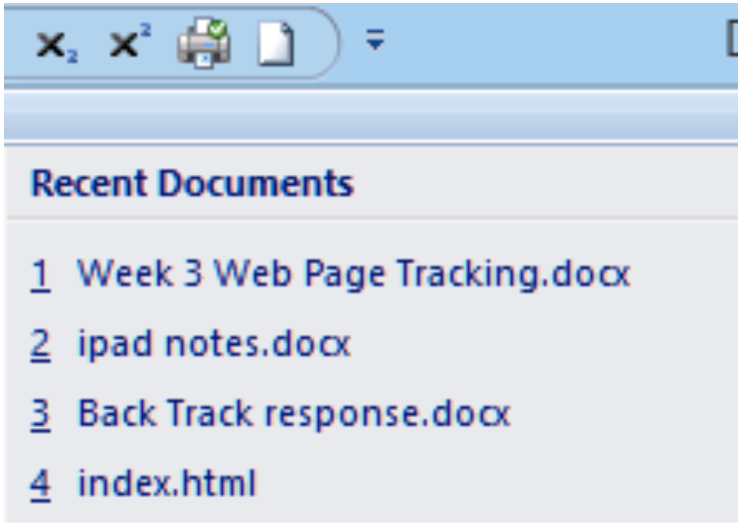
Name	Date modified	Type
Week 7 - Windows OS Artifacts	22-Aug-20 5:12 PM	Shortcut
Week 7 Windows Live upload....	22-Aug-20 5:12 PM	Shortcut
Lecture Week 7 Windows OS A...	22-Aug-20 4:58 PM	Shortcut
Lectures 1	22-Aug-20 4:58 PM	Shortcut
Artifacts.png	22-Aug-20 2:59 PM	Shortcut
Week 7	22-Aug-20 2:59 PM	Shortcut
profiling.jpg	22-Aug-20 2:50 PM	Shortcut
evidence.png	22-Aug-20 2:47 PM	Shortcut

The Windows Registry

- Covered in Week 6
- Contains many items of forensic interest
- AutoStart/AutoRun
- UserAssist – Records the number of uses of exes
- USBStore - Records USB devices used
- Lists of Most Recently Used items (MRUs)
  - See next slide

MRUs

- Windows keeps several Most Recently Used lists (MRUs)
- Files opened
- Apps started
- Web Pages visited
- Office docs opened



Recent Documents

1 Week 3 Web Page Tracking.docx

2 ipad notes.docx

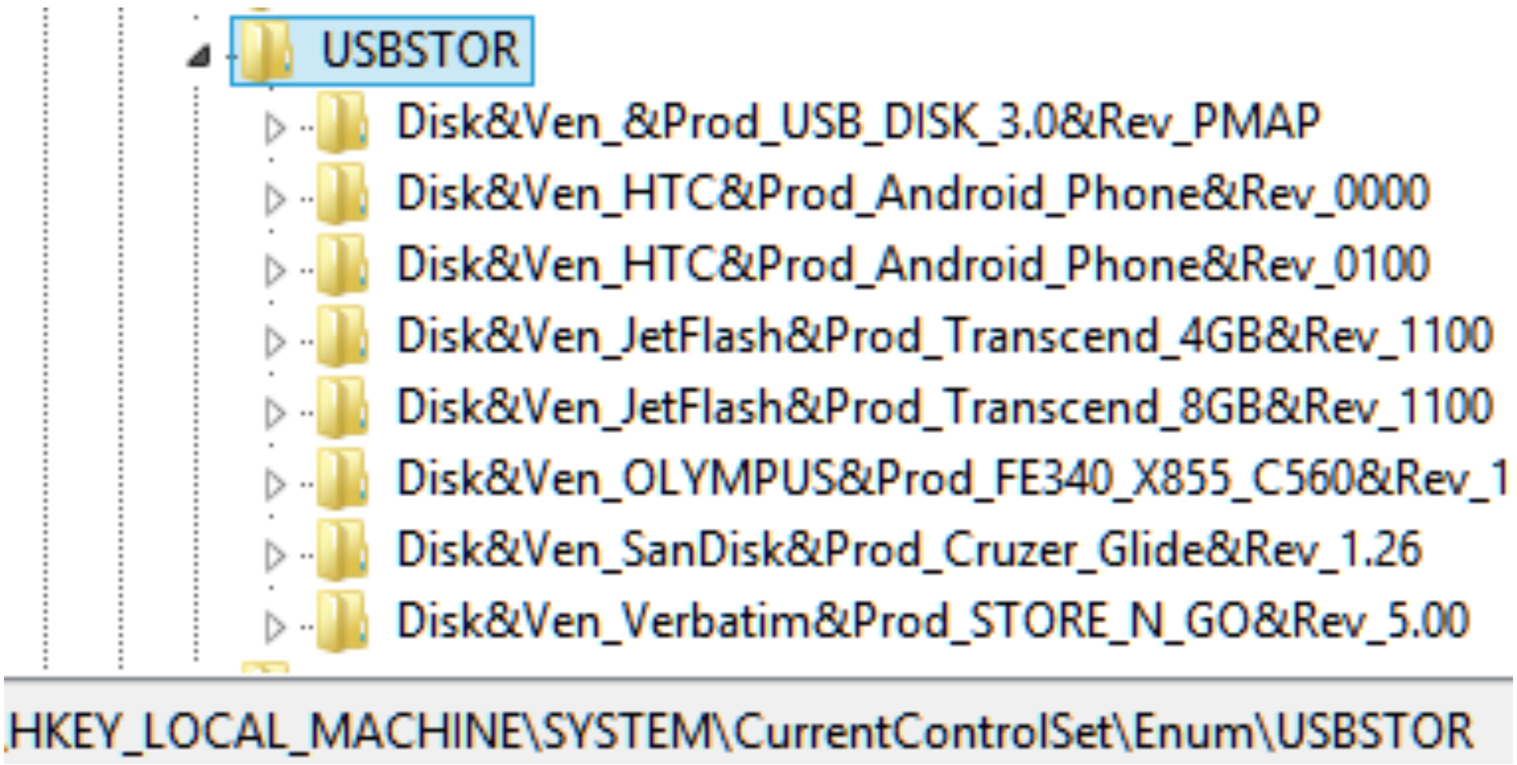
3 Back Track response.docx

4 index.html

- These all indicate what the suspect did recently
- https://www.nirsoft.net/utils/recent_files_view.html

The USBStor Key

- Records every device connected by USB
- Backed up at each restore point - see week 6



USBSTOR

Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP

Disk&Ven_HTC&Prod_Android_Phone&Rev_0000

Disk&Ven_HTC&Prod_Android_Phone&Rev_0100

Disk&Ven_JetFlash&Prod_Transcend_4GB&Rev_1100

Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_1100

Disk&Ven_OLYMPUS&Prod_FE340_X855_C560&Rev_1

Disk&Ven_SanDisk&Prod_Cruzer_Glide&Rev_1.26

Disk&Ven_Verbatim&Prod_STORE_N_GO&Rev_5.00

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

USB Oblivion

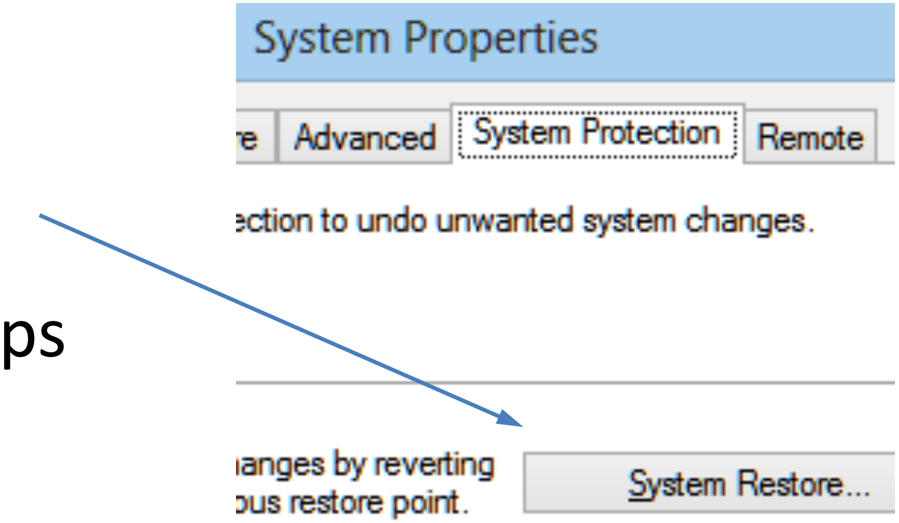
- Removes (most) traces of USB usage from the registry
- The act of running this tool is forensic evidence

- http://www.cherubicsoft.com/en/projects/usboblivion#.VefLVjZ--Hs

Restore Points

- Save a snapshot of registry and system configs
- Used before trying something dangerous

- Can rollback if something goes wrong
- Find Restore in System Properties
- Can recover deleted apps and registry keys



System Properties

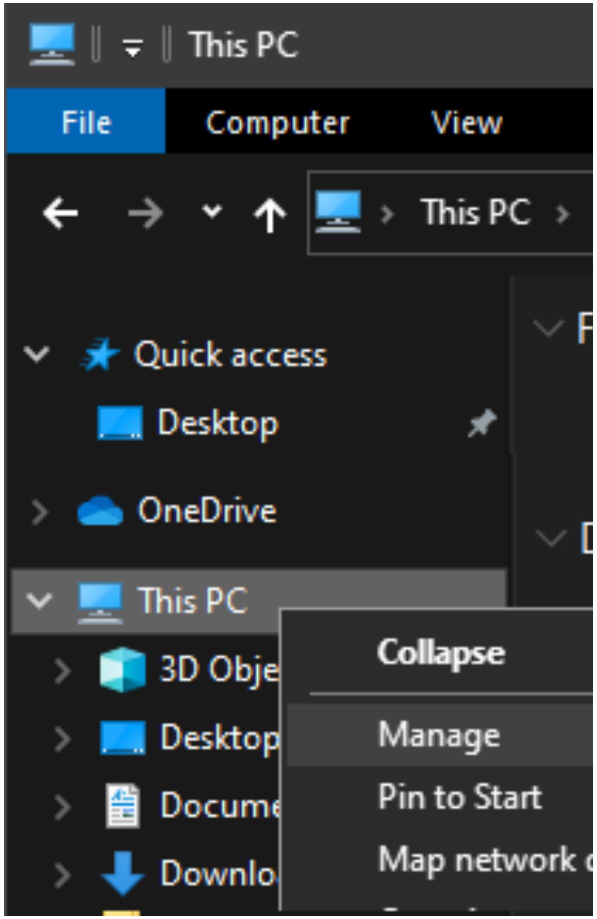
ection to undo unwanted system changes.

anges by reverting
ous restore point.

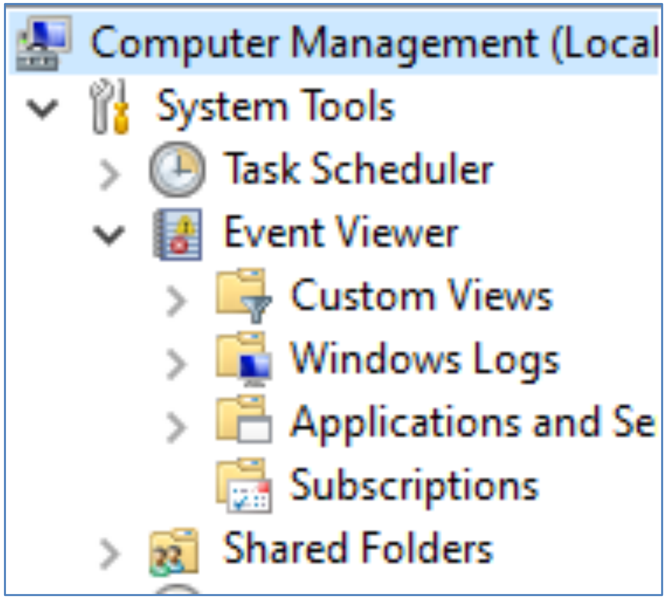
Windows logs

- Integrated into the Operating System
- Come with their own GUI Viewer
- Runs as the Event Viewer snap–in for the MMC
  - Microsoft Management Console (MMC)
- You can open the Event Viewer three ways
  - From the command line run eventvwr
  - From File Explorer select This PC, right click and select manage
  - From the Control Panel, select Administrative Tools, Event Viewer

Accessing Windows Logs

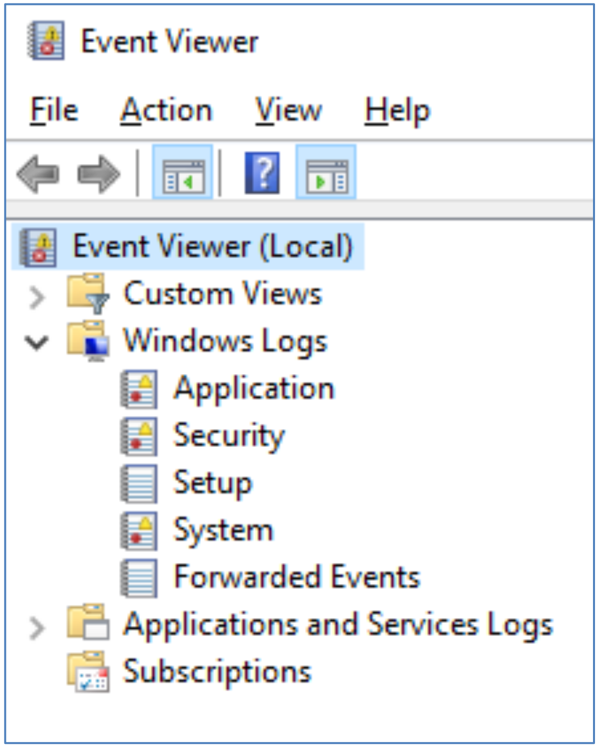


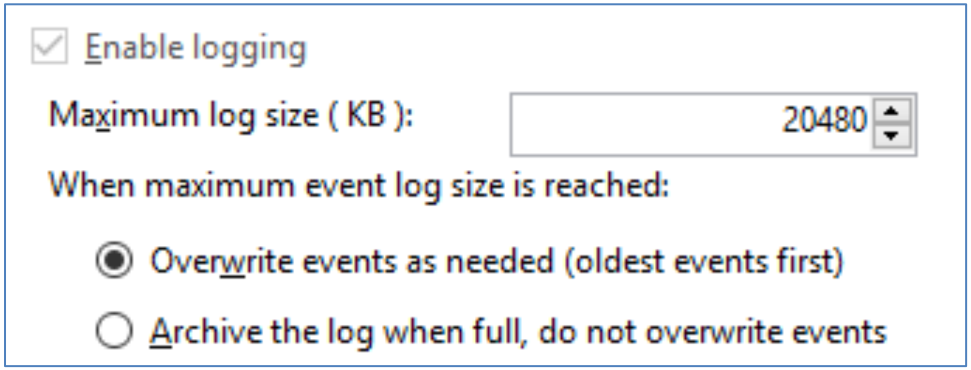
- File Explorer
- Right click on This PC
- Select Manage
- Select Event Viewer



Windows Logging

- There are three main logs
  - Application
  - Security
  - System
- Not all logging is enabled by default
- Logs default to 20MB and then roll over
  - Right click and select properties





☑ Enable logging

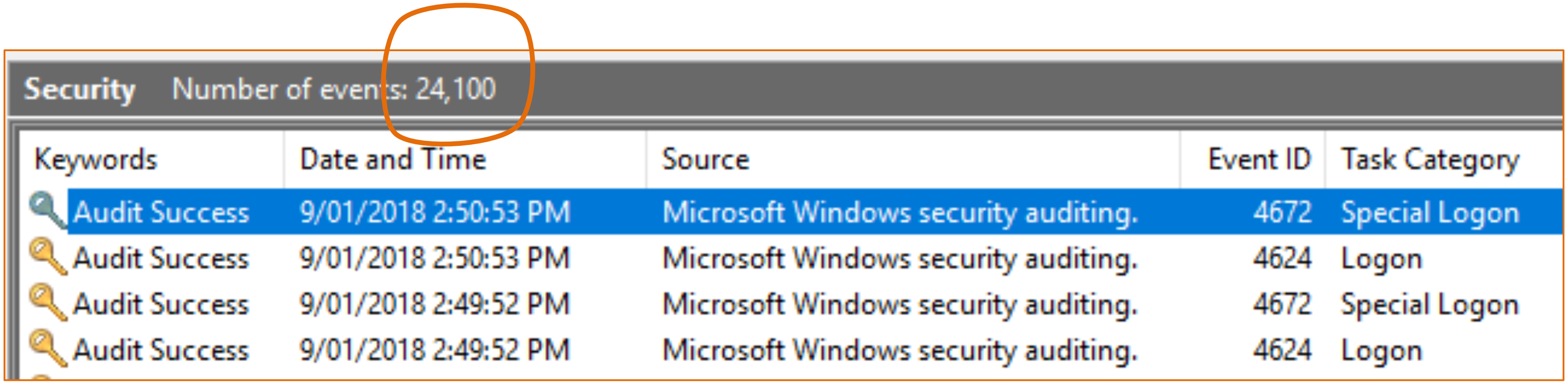
Maximum log size (KB): 20480

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

Event List



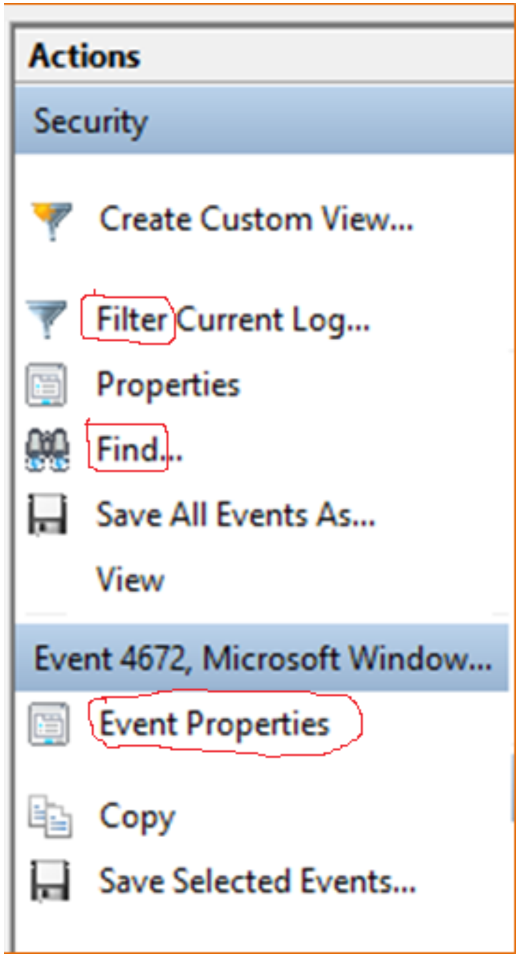
Security Number of events: 24,100

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	9/01/2018 2:50:53 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/01/2018 2:50:53 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/01/2018 2:49:52 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/01/2018 2:49:52 PM	Microsoft Windows security auditing.	4624	Logon

- Many MBs of Events in each of the three main logs
- We can Sort, Search and Filter the list

Log viewer Control Pane

- Use to Sort, Search and Filter the list



Objectives

- To understand Windows Artifacts
- To identify Volatile Forensic Data
- To identify non-Volatile Forensic Data
- To understand computer profiling

Computer Profiling

- Once we have examined a device’s artifacts and its forensics data we can reconstruct the user’s activity.
- From this activity we can abstract a view of the user.
- This is called computer profiling.
  - (This is NOT a user profile as used in social media)
- This is a user level view of the device
- We use this computer profile to confirm or deny allegations about the user.
- When we have a new device to examine we can use previous profiles to focus on key areas of investigation.

Hypothesis testing

- Using the computer profile, the investigator hypothesises an action by the subject.
- For example, downloading a pornographic image.
- She then tests this hypothesis using forensic examination.
- She is trying to attribute the download to one particular person.
- (See attribution week 2)

Some computer profiles

- Innocent (apparently)
  - Nothing to see, ‘as new’ install.
- Media professional
  - Image manipulation, heavy social media activity
- IT Professional
  - Use of Linux, VMs and VPNs.
- Hiding from forensics
  - Use of the dark web, metadata scrubbing, secure deletion.

Some artifacts used in profiling

(examples in braces)

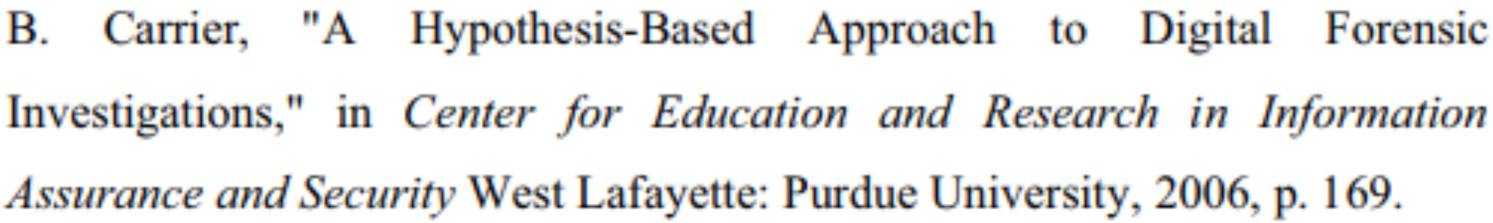
- Logons detected
  - Private (home), work (company), educational (uni), restricted (dark web). Other users.
- Other people – non login
  - Contacts. (Friends in divorce investigations), (Customers in illegally obtained data sales).
- Apps installed
  - Photo manipulation (photoshop, GIMP)
- Incognito Browsers and search engines used
  - (Chrome Incognito), (duckduckgo), (tor browser)
- Linux VMs installed
  - (Ubuntu, Kali)
- Use of VPNs
  - (Openvpn, TOR)

References

OS Support for Students by an expert in the field

http://www.computersciencestudent.com/

Background in forensic profiling



B. Carrier, "A Hypothesis-Based Approach to Digital Forensic Investigations," in *Center for Education and Research in Information Assurance and Security* West Lafayette: Purdue University, 2006, p. 169.

FIN