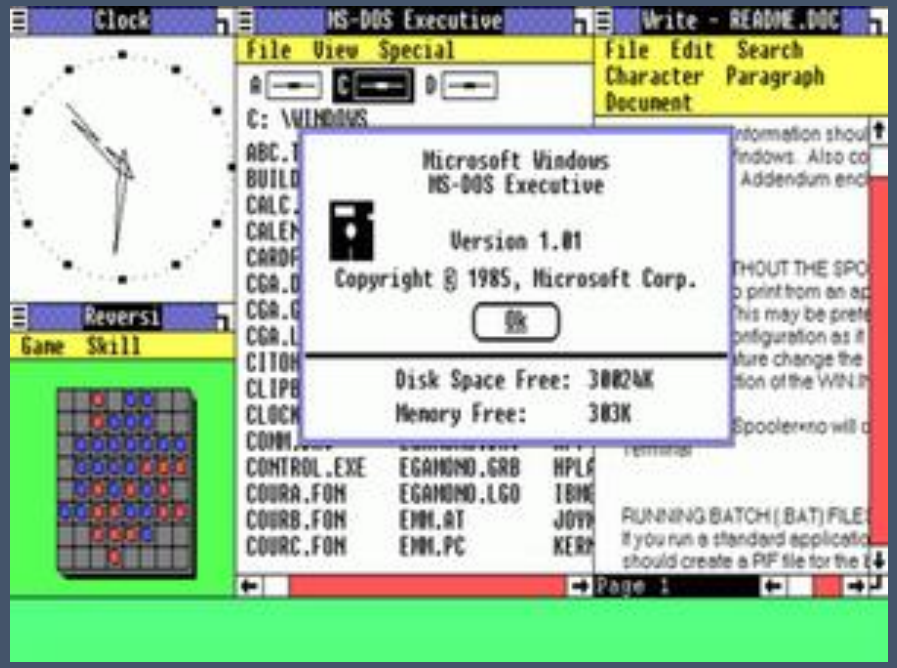
A Lawyers Guide to Windows 10 and Evolving Digital Forensics Techniques

Mike Maschke, CEO
Brandon Barnes, Digital Forensic Examiner
Sensei Enterprises, Inc.

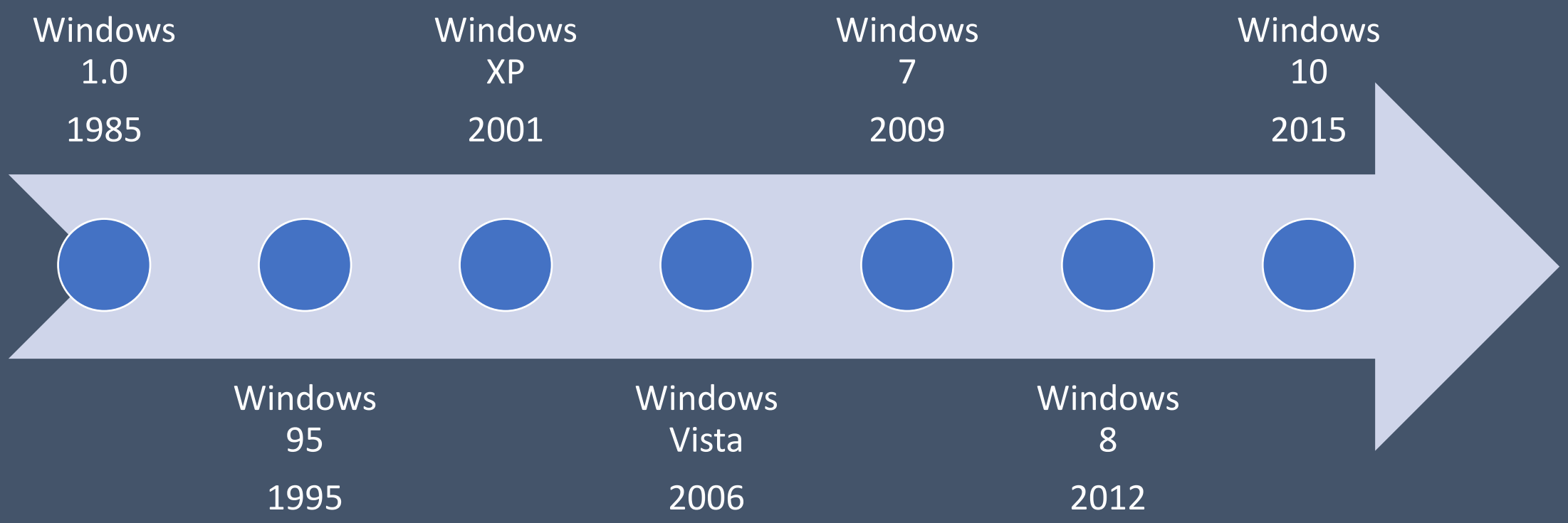
DC Bar
November 19th, 2020

Microsoft Windows

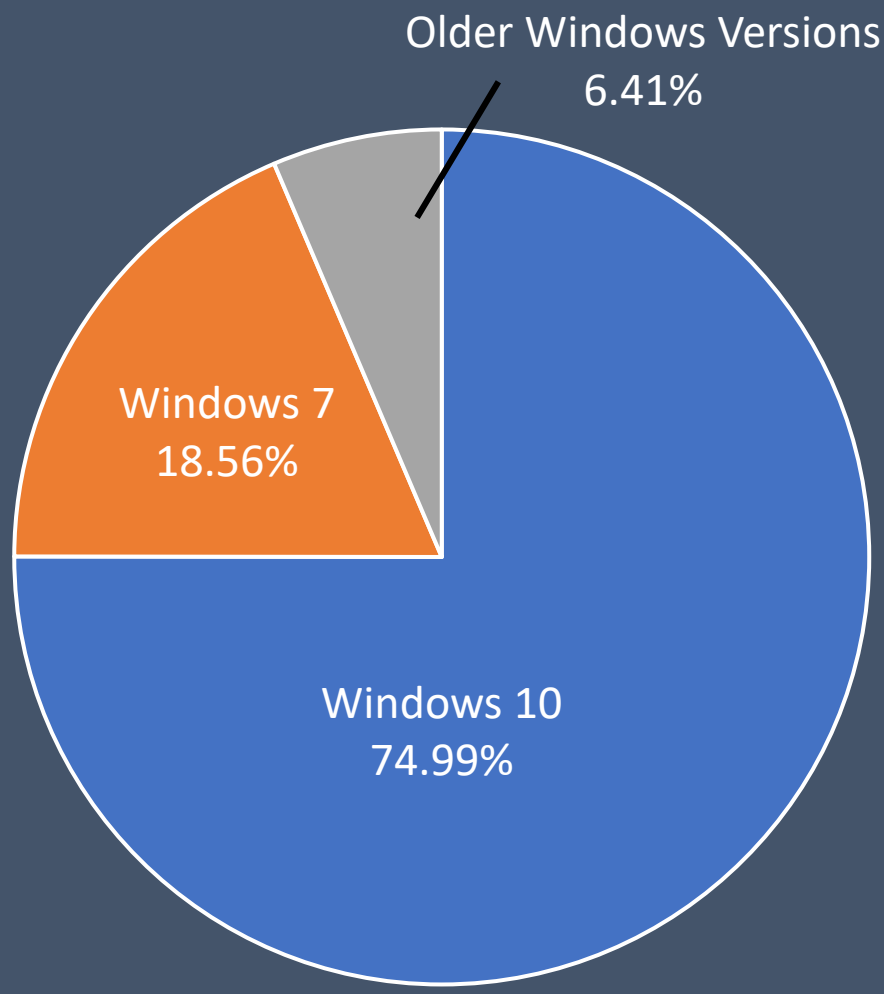
- Announced by Bill Gates on November 10, 1983
- First version released in 1985
  - Simplistic - features like calendar, notepad, calculator, and clock
- Future versions begin to introduce popular features such as Internet, downloadable applications, customizable settings



Previous Windows Versions



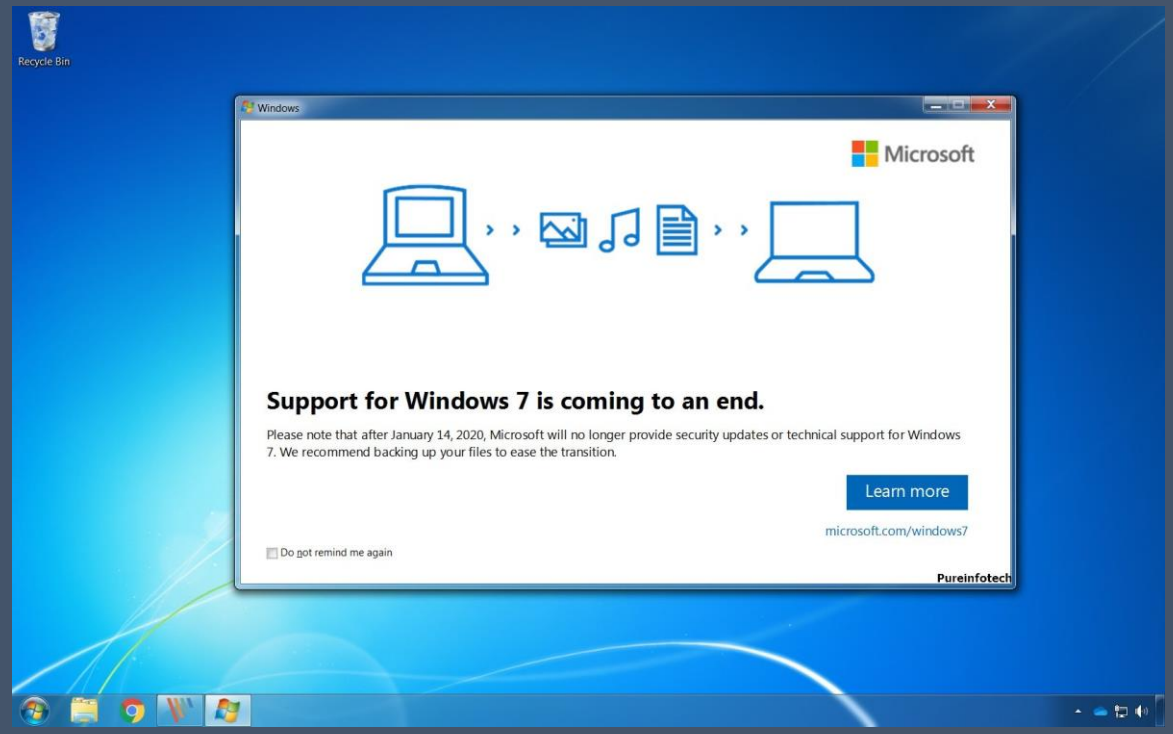
Windows Versions in Use in 2020



Statistics obtained from statcounter.com

Why Windows 10?

- Widely used Windows 7 support ended on January 14, 2020
  - Continuing to use older versions of Windows allows your PC to become more vulnerable to security risks

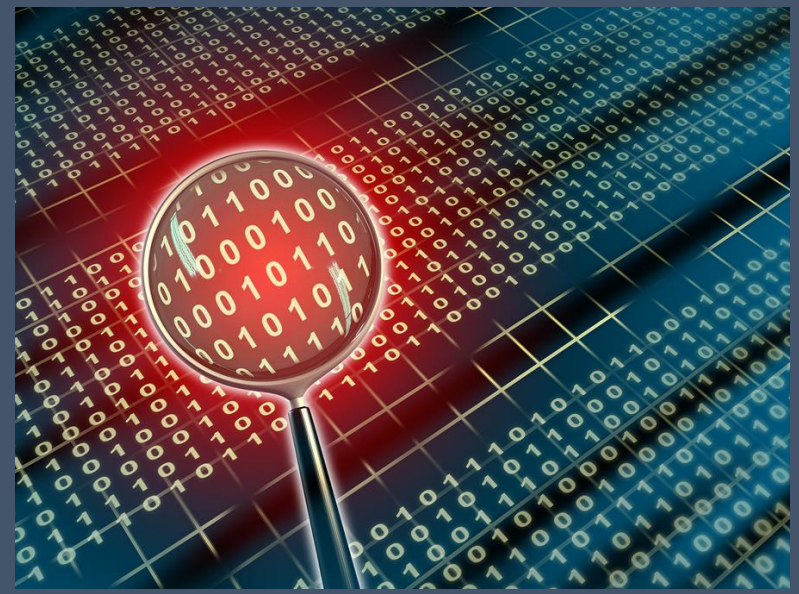


Windows 7 Vulnerabilities

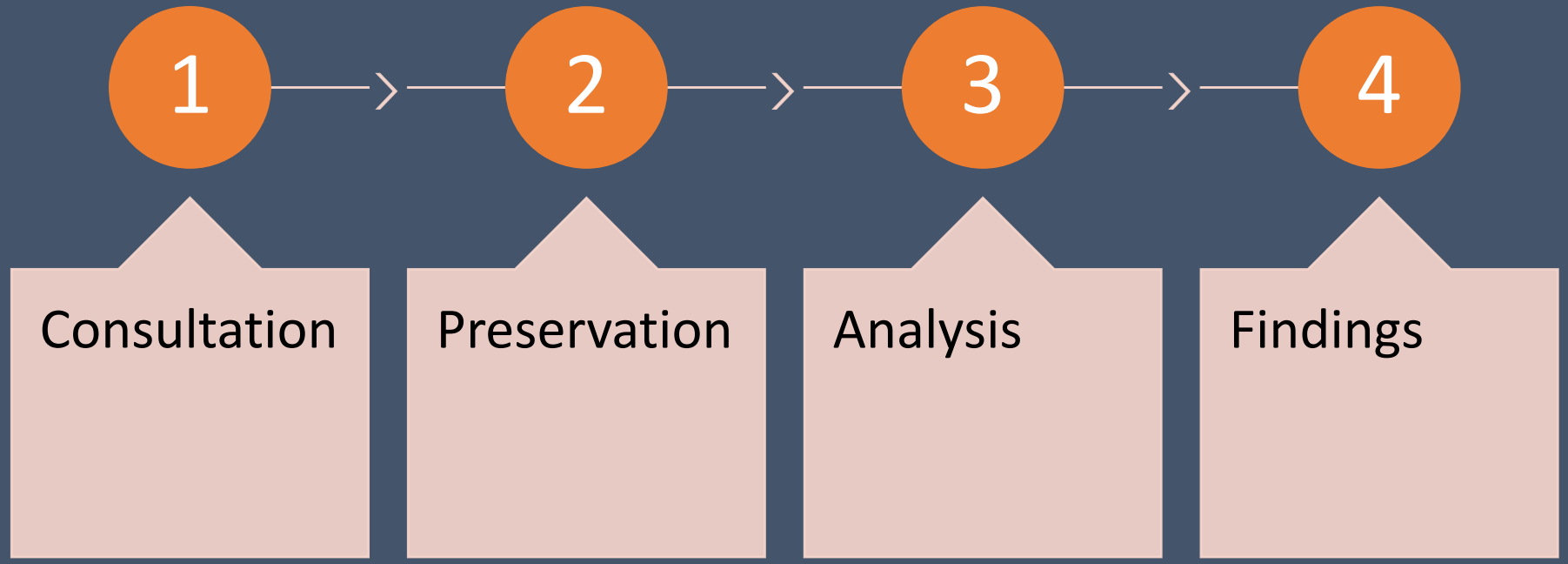
- Since Windows 7 is no longer supported, this means…
  - No new software releases by Microsoft
  - Risk of exploits by hackers increases
  - Organizations continuing to use Windows 7 are out of compliance

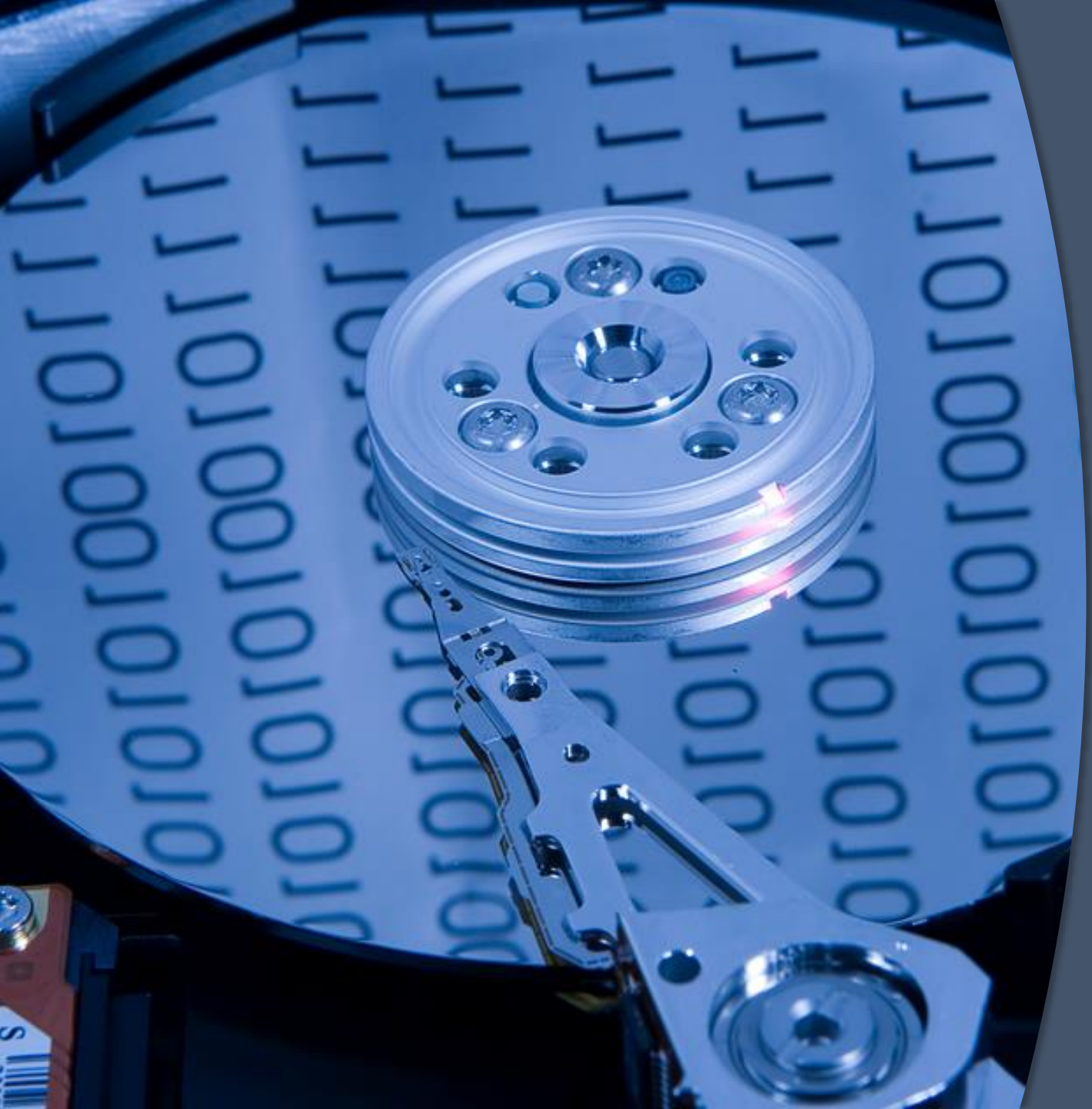
Digital Forensics Introduction

- Digital Forensics – involves the preservation and analysis of electronic devices
- May be used for a wide variety of matters, including civil and criminal
- Attempt to answer questions such as who, what, when, where, why, and how



Stages in a digital forensic investigation





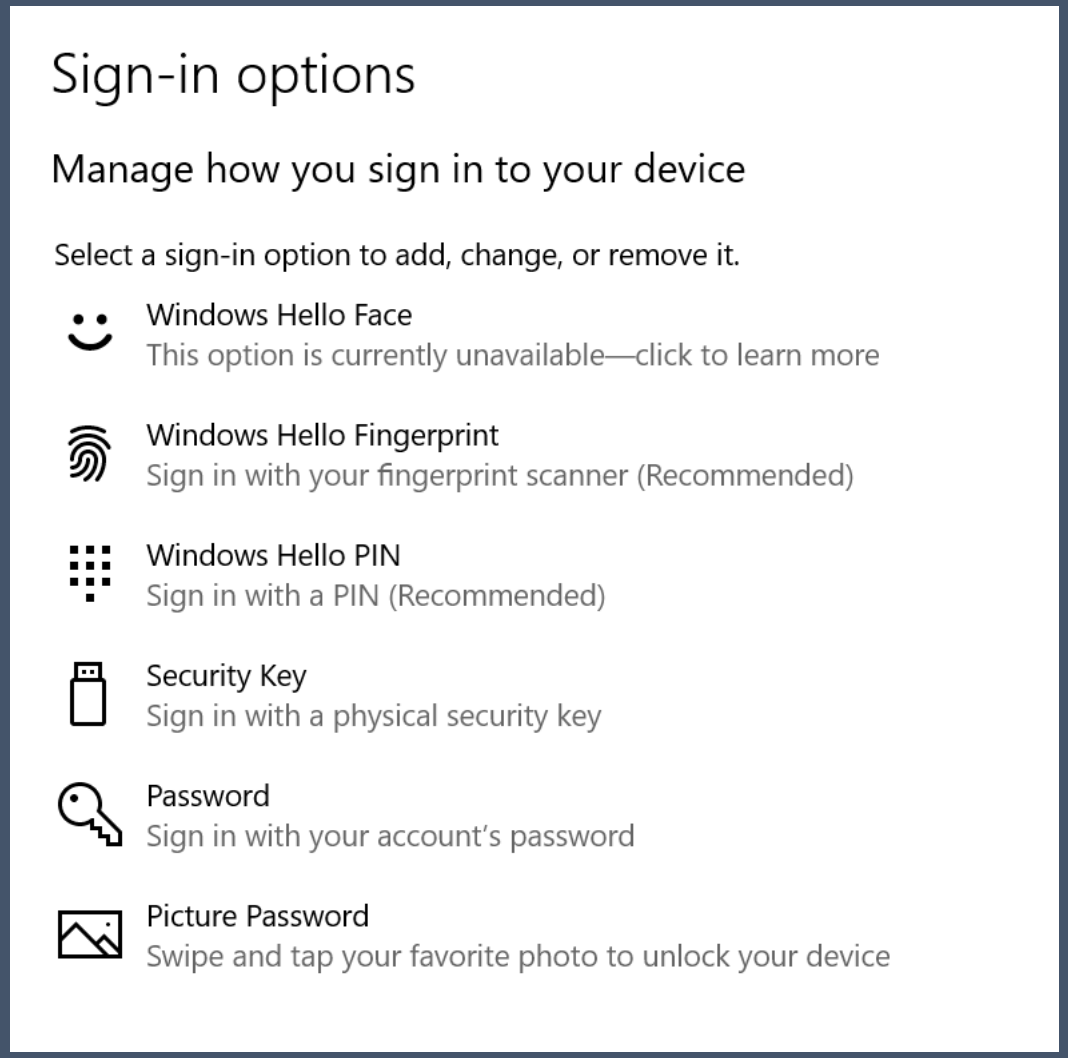
Data Preservation

- Process is also known as creating a forensic image (mirror copy)
- Involves making a bit by bit copy of the internal hard drive within the computer
- Ensures the data from the system has been preserved in its original form

Windows 10 Artifacts

Sign-In Options

- Windows 10 allows the user several different options for securing their device
- It’s important to note that none of these options encrypt the hard drive, a forensic image is still able to be produced



Sign-in Options (continued)

- Windows Hello Face – Face authentication using supported devices with specialized webcams
- Windows Hello Fingerprint – Fingerprint recognition software is used with supported devices
- Windows Hello Pin – Allows the user to sign in with a PIN code
- Security Key – User signs in with a physical key, such as an external USB drive containing the key
- Picture password – User chooses a preselected image to unlock the computer

Synched Data from other devices

- Windows 10 allows the user to link their cell phone to their computer
- Allows user to make and receive calls and texts, check notifications, and get instant access to the phone's photos and apps
- Also enables files such as Word, Excel, and PowerPoint documents to sync back and forth between devices
- This feature can be helpful when hoping to analyze cell phone data synched from the phone to the laptop

Windows Cortana

- With Windows 10's release, the virtual assistant Cortana is now available on computer systems
- Cortana can be used for various tasks, such as setting up reminders, searching the web, sending emails, and more
- By analyzing the Cortana databases stored on Windows 10 systems, a forensic analysis has the potential to uncover past Cortana activity

Windows Registry

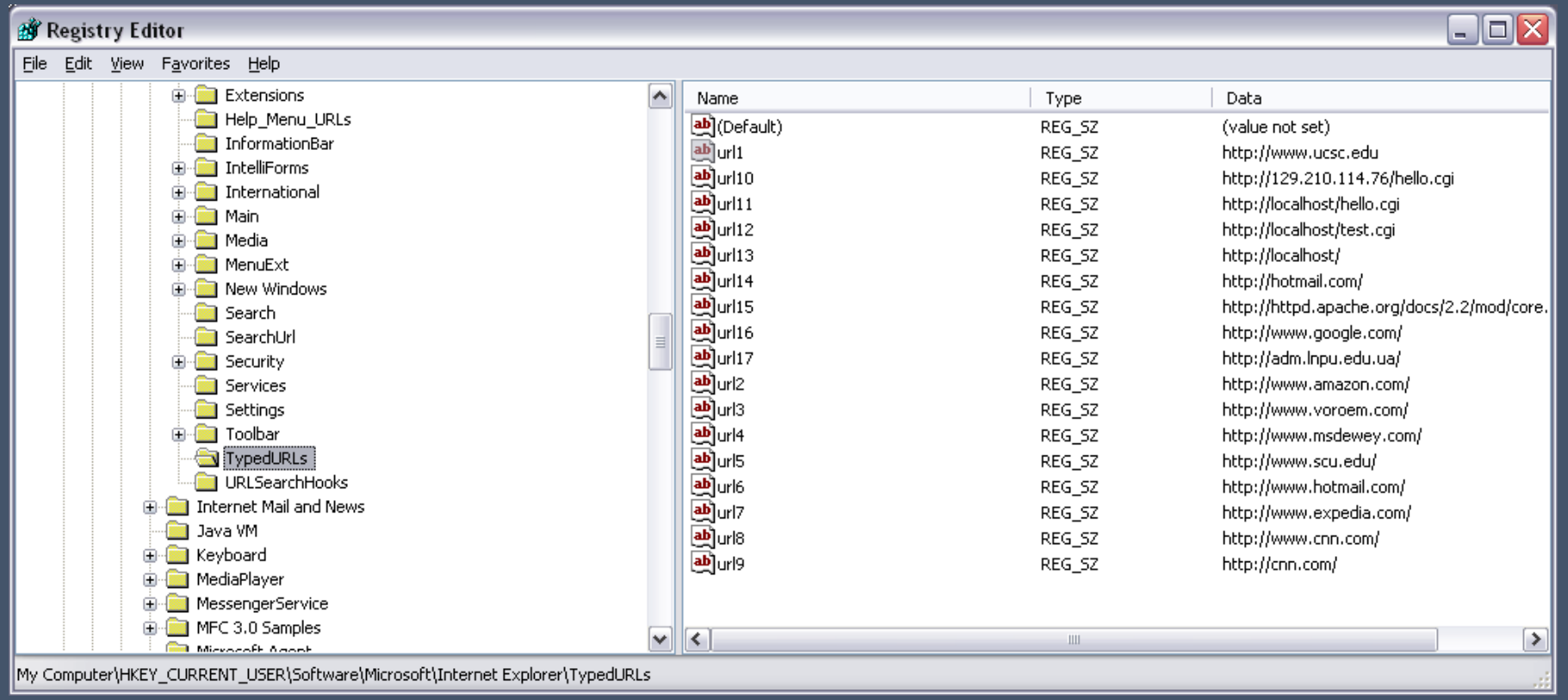
- Holds configurations settings and important records for the operating system
- Stores information and settings for software programs and hardware devices on the machine
- Can be described as the “DNA” of the Windows operating system

Windows Registry (continued)

- A lot of important artifacts in forensic investigations reside in the Windows registry:
  - Time zone information
  - Files accessed
  - Programs run
  - Web Browsing activity
  - USB devices
  - Passwords

Windows Registry Example

- Here is an example of a Windows registry entry for Typed URL's. This location can be helpful in determining visited websites in the past.



Windows Event Logs

- Windows 10 automatically keeps a detailed record of system, security, and application changes within event logs
- These system logs can assist investigators in determining certain events that were recorded by the machine
- These event logs include user logins, application installations, security management, system setup operations, and problems or errors

Types of Windows Event Logs

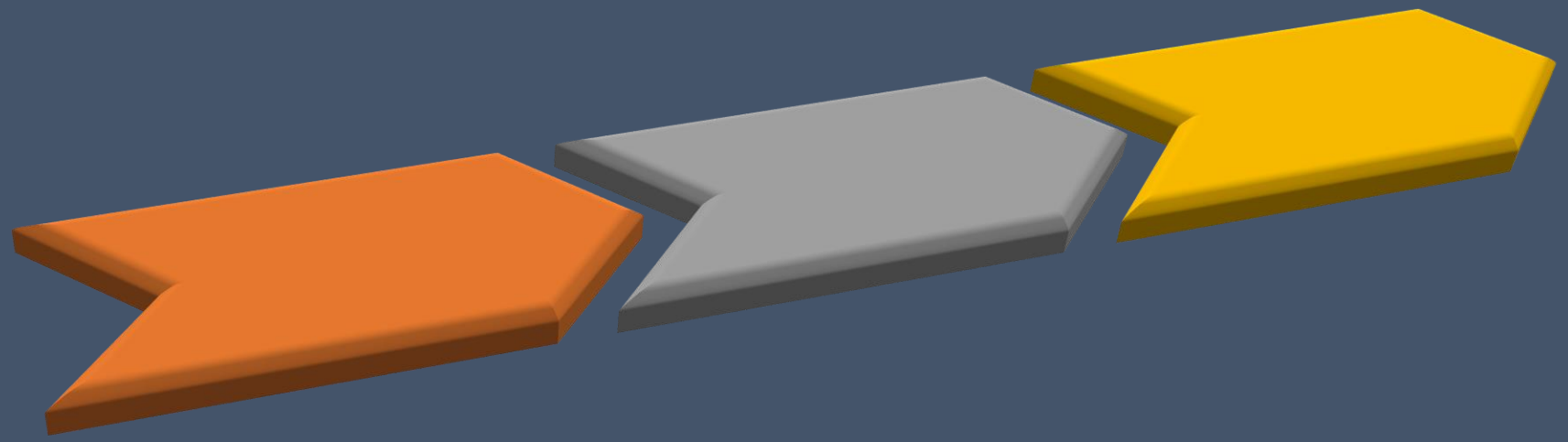
- **System logs** – Contain changes to hardware, device drivers, system changes, and all activities related to the machine. These logs are a great place to look for threats against networks and systems

- **Security logs** – Contain the login and logoff activity for the operating system. These logs can be analyzed to investigate attempted or unauthorized logins.

- **Application logs** – Contain records of application related events that are installed on the system. Analyzing these logs can assist in troubleshooting specific software problems on the machine.

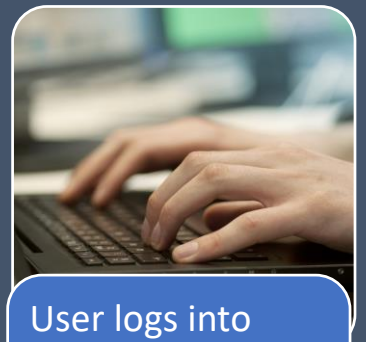
Timeline Analysis

- Process of using timestamps stored within data on a computer system to construct a timeline of events
- Windows operating systems record a variety of events within log files, allowing for detailed information to be recorded regarding computer events



Timeline Example

- Let's say you are interesting in learning everything available about a photo of interest, named "IMG_100.jpg"
- By analyzing the artifacts left behind by Windows 10, a digital forensic examiner could put together the following:



User logs into computer

- Sunday, February 1st, 2020 at 7:55 AM
- Determined from Windows Event Logs

IMG_100.jpg is downloaded from the Internet

- Sunday, February 1st, 2020 at 8:05AM
- Determined from Browser History

IMG_100.jpg is sent via Email

- Sunday, February 1st, 2020 at 8:20AM
- Determined from Emails stored on hard drive

IMG_100.jpg is deleted

- Sunday, February 1st, 2020 at 8:30AM
- Determined from data recovered from hard drive

Email

- It is possible to recover email artifacts during a forensic investigation
- May be stored within databases for popular email clients (Outlook, Thunderbird, etc.)
- Artifacts may also be stored in web history, in cached images or saved usernames and passwords

USB Devices

- Often, when USB devices are plugged into computers, the serial number of the device and the date and time of the access is recorded within the Registry
- An analysis of past USB devices plugged into the computer may be helpful in data theft investigations
- Determine important dates of USB activity (first plugged in date, last connected date)

Evidence of File Access

- May be contained within browser history
- Also may be stored within miscellaneous Windows 10 artifacts such as:
  - LNK Files- Evidence of file access
  - Shellbags- Evidence of folder access
  - Jump Lists- Evidence of file access/program execution

Internet / Browsing History

- Browser history is often a critical artifact in forensic examinations
- By default, Windows 10 keeps a detailed log of browser activity
- Some of the artifacts you can expect to be contained on a Windows 10 computer system:
  - Navigation history: what websites were visited and when
  - Bookmarks: what websites were favorited for easier access
  - Cached information: data saved from visited websites
  - Logins: login credentials for visited websites
  - Downloads: files downloaded to the system from the Internet

File Deletion and Data Recovery

- An important feature of Windows 10 is the ability for forensic examiners to tell what files have been deleted from the system and attempt to recover them
- The likelihood of recoverability depends on a couple factors, such as the amount of time since the deletion and the amount of new activity on the computer since the deletion

Data Theft

- When companies experience data theft, it can occur from internal or external sources
- Digital forensics is used to analyze important artifacts on Windows 10 systems to determine what happened and if there is evidence of stolen or misappropriated data

Employee Data Theft

- Previous employees can steal company data to start their own firm or use the data as an advantage
- By analyzing the artifacts left behind in Windows 10 systems, it is often possible to determine:

- USB device activity, including possible file transfer
- Sent and received emails, including email forwarded to personal accounts
- Dropbox and file sharing websites
- Activity prior to departure
- Recoverable deleted files
- Internet history and searches

Keyword Search

- Digital forensic software allows examiners to search across the entirety of the information stored on Windows 10 systems
- Keyword searching allows you to search through evidence looking for a word or combination of words
- Can be useful in locating:
  - Names of interest
  - Communications
  - Internet activity

Conclusion

- Windows 10 systems track a lot of information between log files, databases, and registry entries
- There is a potential wealth of information available with a forensic review
- If computer evidence is part of your case, it is recommended to first consult with a digital forensic examiner to determine what data may be available

Questions?

703-359-0700

mmaschke@senseient.com

bbarnes@senseient.com