Departing Employees, Data Theft, and Digital Forensics

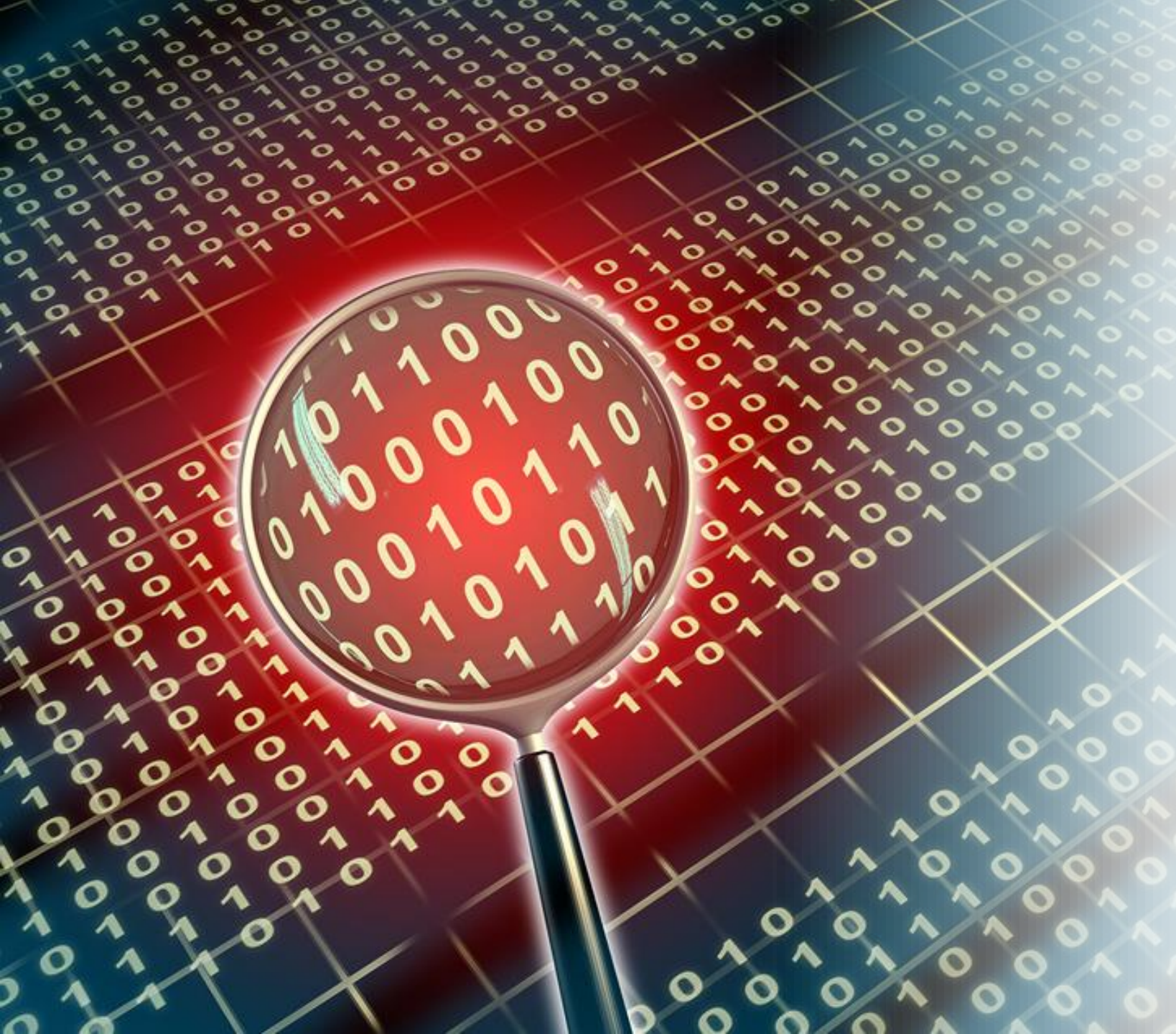
DC Bar – April 15, 2021

Presentation By: Michael Maschke and Brandon Barnes

Sensei Enterprises, Inc.

Data Theft by Former Employees

- An organization's intellectual property can be compromised by employees who attempt to take company data
- A study by InfoSecurity Magazine in 2019 found that 72% of former employees admitted to taking company data upon departure
- With the current work from home environment, employee data theft may be easier to accomplish



Digital Forensics

- *Digital Forensics* – branch of forensic science involving the recovery and analysis of digital devices and electronic evidence
- There are often many different routes data can be exfiltrated on employer provided devices
  - Luckily, those trained in digital forensic techniques can often provide answers on what data was taken and when

Presentation Overview

Identifying when a data theft investigation may be necessary

Discussing common steps and procedures used by digital forensic examiners analyzing suspected data theft by a former employee

Highlighting useful artifacts on devices that may provide evidence of employee data theft

Presenting overall recommendations and useful tips for dealing with employee data theft investigations

Retaining an Expert

- When employee data theft is suspected, you will likely need to work with a reputable digital forensics company
- It is important to ensure the company retained for the matter is skilled in performing this type of review and who is also knowledgeable on best practices when dealing with digital data

When to Perform an Investigation

- Depends on the specifics of the situation
- Some common reasons to perform a review of previous employee's devices include:
  - An abrupt depart from the company
  - New employment with a competitor
  - Reasons to be believe files have been copied, transferred, shared, or deleted

Data Preservation

Involves making a forensic image, or a complete copy, of the work provided device in its current state

This practice ensures all available data has been collected in a manner admissible in court

If the device is not preserved and is reallocated to another employee, important information regarding the previous employee's actions may be overwritten

Electronic Evidence Preservation

Depending on what systems the former employee had access to, common electronic evidence gathered in employment matters includes:

Cloud Accounts

Mobile Devices

Computers

Common Artifacts of Interest

- Most of the artifacts in this presentation are from the Windows registry or databases stored on the computer
- *Windows Registry* – holds configurations settings and important records for the operating system. Can be described as the "DNA" of the Windows operating system
- There is no centralized registry on Mac systems, instead there are a series of files across the computer that store user preferences

Database Files

- Store user data from certain installed applications
- Popular database files examine in employee data theft matters include:
- Web Browser databases such as Chrome, Safari, Firefox, Edge
- File Sharing Applications such as Dropbox

Popular Artifacts

Attached USB Devices

- A common route for data theft is using external storage devices, commonly referred to as USB’s or thumb drives
- Several artifacts left on computers system can help locate evidence of data theft through USB ports

USB Device Activity

- The registry file keeps track of attached USB devices
  - Determines USB devices plugged into the system, and by which user
- Additional analysis may show evidence of file transfers to USB devices

Sample USB Device History Report

Device Name	Serial Number	First Install Date/Time	Last Insertion Date/Time	Last Removal Date/Time	Associated User
SanDisk Cruzer Glide USB Device	5055670504585	2/25/21 2:35 PM	3/1/21 5:05 PM	3/1/21 5:35 PM	Mike
Western Digital External Hard Drive	83732745322	5/5/20 11:06 AM	8/10/20 7:06 PM	8/11/20 1:50 PM	Mike
PNY USB Device	588726584456	1/26/21 12:05 PM	1/28/21 3:45 PM	1/28/21 4:05 PM	Brandon

Email Review

- Former employees may use a work email, or a personal account, to facilitate theft of company data
- A review of email artifacts often includes:

  - Search and review of sent, received, and deleted emails
  - File transfers via email to personal accounts
  - Deleted emails
  - Communications prior to departure

Local Email vs Sever Email Analysis

Locally Stored Email

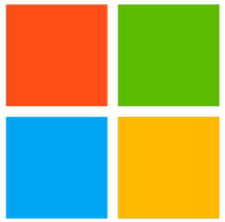
Examples:
Outlook Application,
Mozilla Thunderbird,
Mac Mail

Email Stored on a Server

Example:
Accessing email by web browser: Yahoo, Gmail, AOL

Microsoft 365 Log Analysis

- Microsoft's Audit Log Feature
- Various user events are detailed within the Microsoft audit logs
  - Sent, received, forwarded, and deleted emails
  - Downloaded attachments
  - Viewed Emails
  - Search terms
  - Sign in's and sign off's
  - Most logs kept 90 days, few 1 year



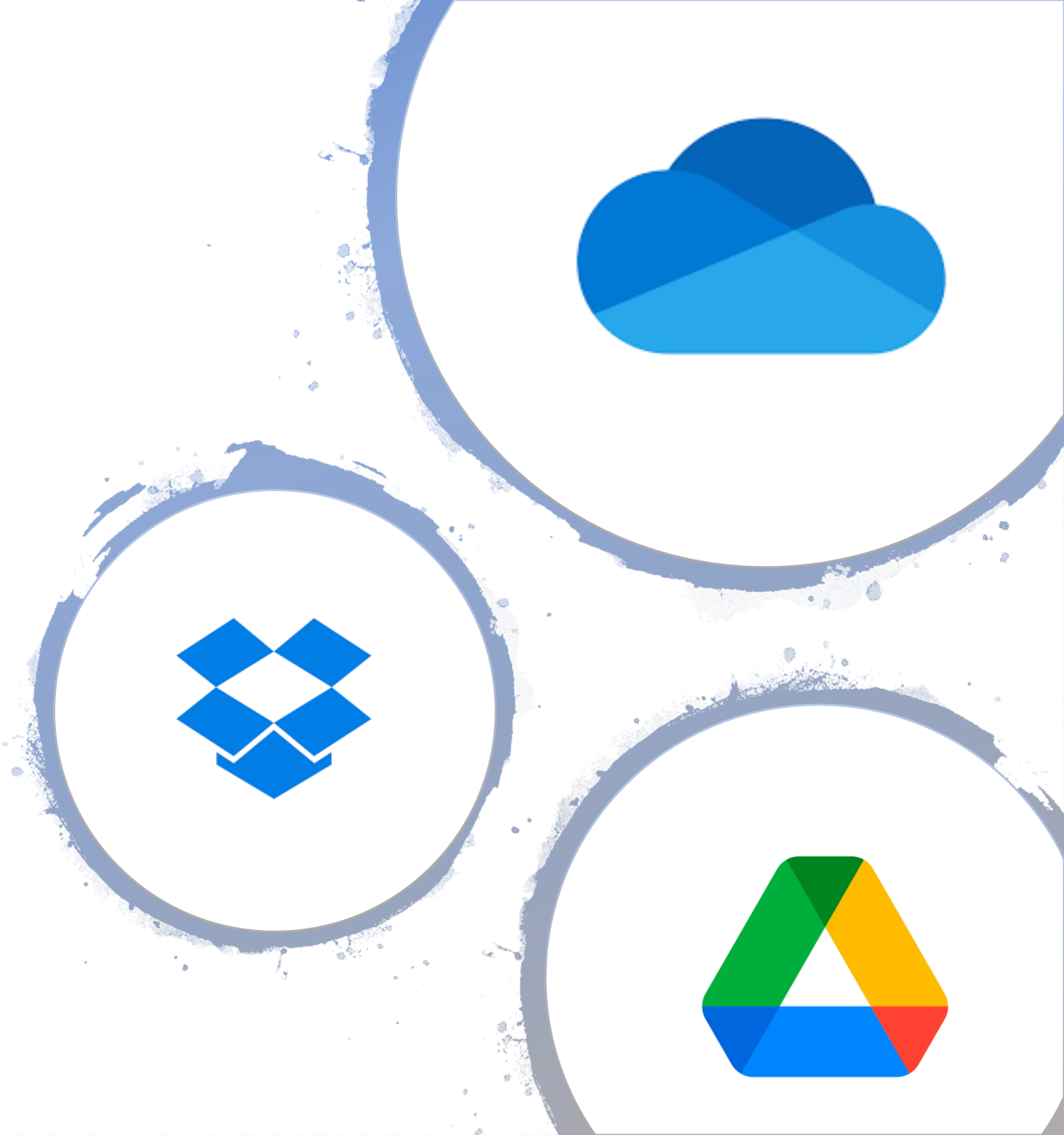
Microsoft

File Sharing Websites

- Reasons to use a file sharing website:
- Sending large files
- Access files from anywhere with an Internet connection
- File synchronization across multiple devices
- Collaboration with coworkers and clients

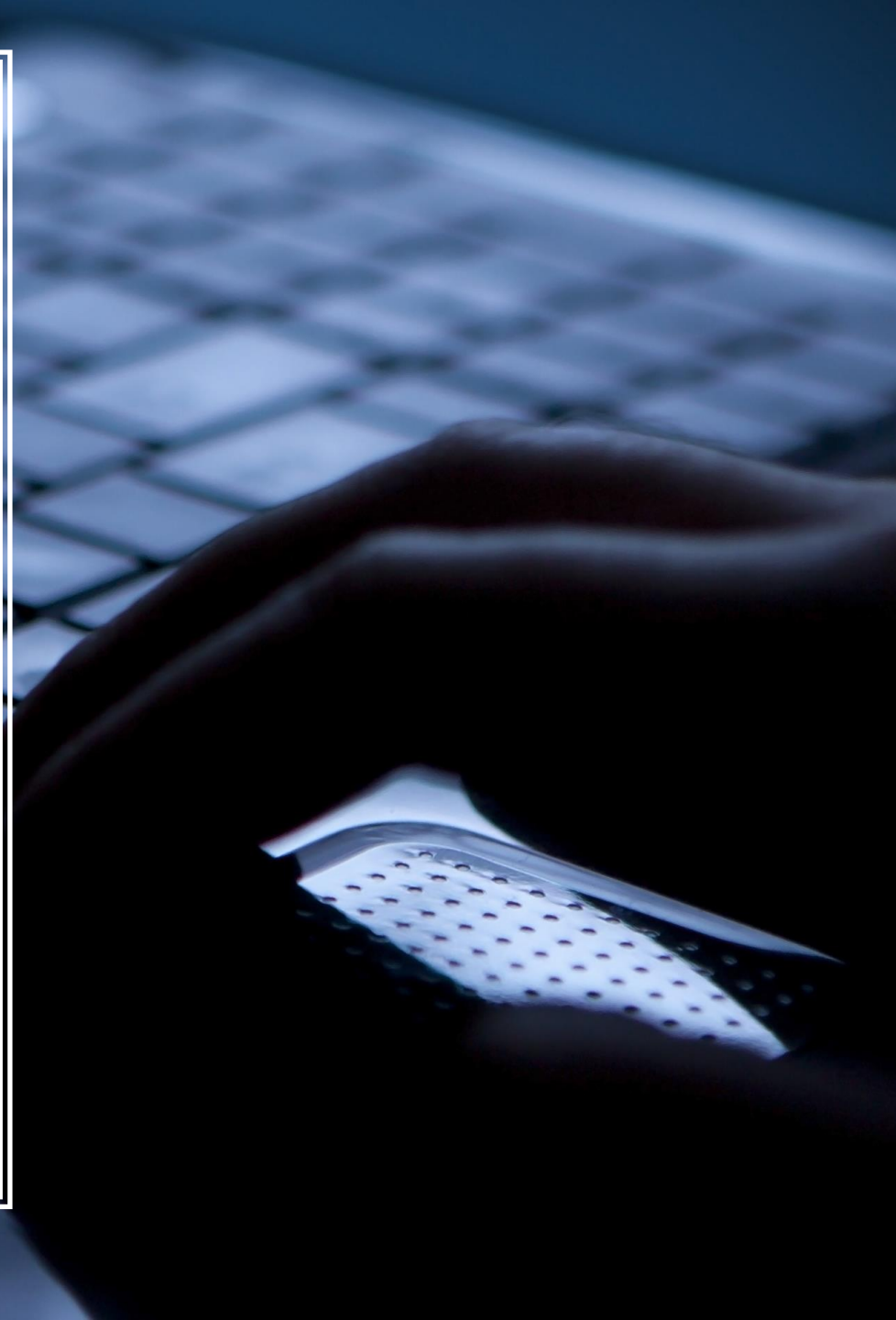
File Sharing Websites

- Popularity of file sharing websites has increased
- Dropbox – Hosted by Dropbox Inc., one of the most popular file sharing websites
- Google Drive – Hosted by Google, comes preinstalled on all modern Android devices
- OneDrive - Hosted by Microsoft, default save location for files in Windows 10
- iCloud – Hosted by Apple Inc., comes preinstalled on all modern Apple devices



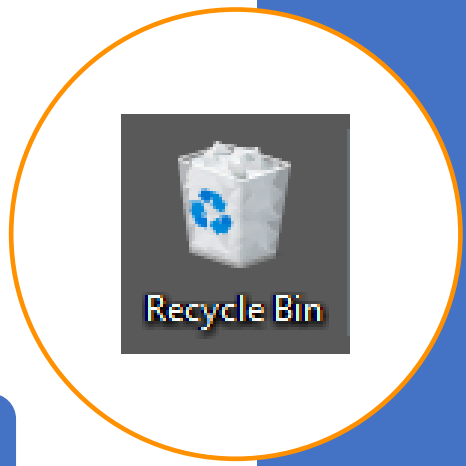
File Sharing Websites Review

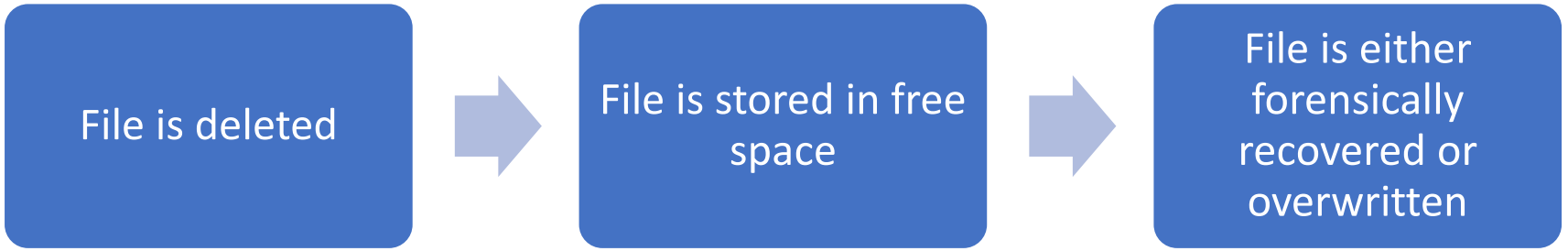
- Important artifacts can be uncovered when file sharing has occurred on devices belonging to former employees
- Web browser history, including active and deleted records
- Conduct a review of available logs from file sharing applications
- Keyword search for popular file sharing websites and applications



Deleted File Recovery

- Forensic software may have the capability to locate and restore previously existing files





Process of file deletion in most computers and mobile devices

Factors that affect recoverability

- There are a couple of factors that determine the likelihood of file recovery:
  - Amount of time that has passed since the deletion
  - Amount of new activity that has occurred since the deletion

Overwritten data is unrecoverable

Internet History and Searches

- Web browser history may play a helpful part in determining activity prior to departure
- An examination of this artifact can uncover the following:
- Visited websites, date and time of visit
- Recovery of deleted web browser history and searches
- File access records within Internet history
    - Shows what files were accessed, date and time, and from what location

Internet History Sample Report

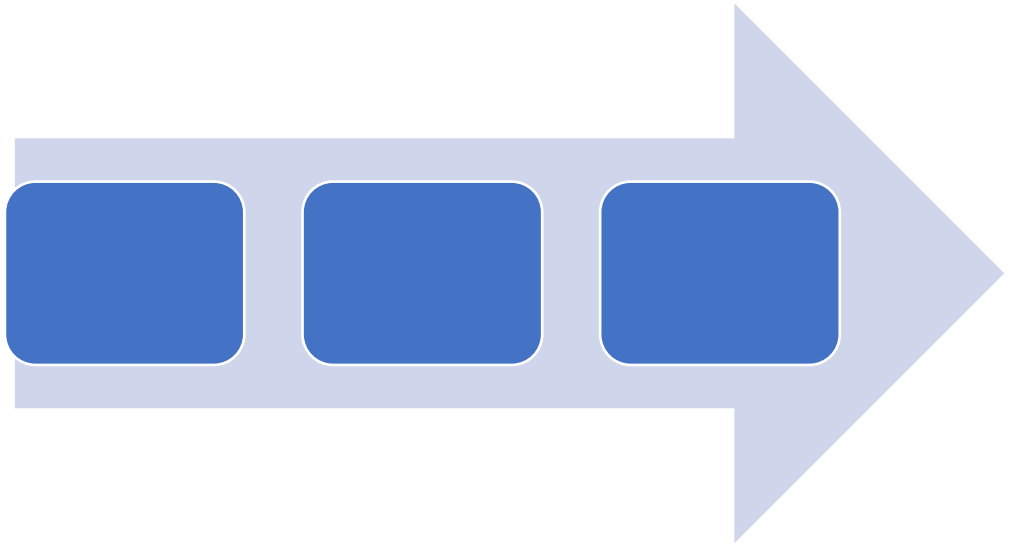
	Entry Type	Date Visited	URL	Search Term	Logon User	Path
1	File History	1/25/21 1:05 PM	https://www..google.com/search?q=gmail+signin	gmail signin	bbarnes@senseient.com	
2	File History	1/25/21 1:07 PM	https://mail.google.com/mail/u/0/#search/company+client+list	company client list		
3	File Download	1/25/21 1:07 PM	https://mail.google.com/mail/u/0/#inbox/FMfcgxwLtQMfdhu3ShQFGRkghtgTDdSRSnJkZMR			C:\Users\Brandon\Downloads\Company Client List.pdf
4	File Access	1/25/21 1:10 PM	E:\Work Documents\Company Client List.pdf			

Device Activity Prior to Departure

- This type of analysis can help determine what the user did on the device prior to leaving the company
- Evidence of file deletion
- Program installation and removal
- Device communications
- Internet history

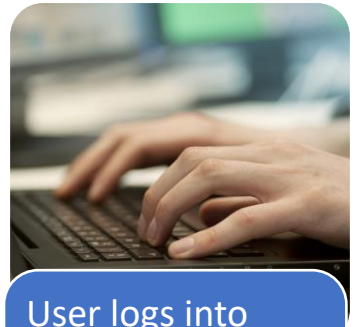
Windows Timeline Analysis

- 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 document of interest, named "ClientList.docx"
- 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

ClientList.docx is downloaded from the Internet

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

ClientList.docx is sent via Email

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

ClientList.docx is deleted

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

Recommendations

- Ensuring proper chain of custody and best practice is followed
- Avoid overwritten evidence or self-collection
- Consult with electronic evidence specialist
- Engage a digital forensics company to perform a forensic analysis

Questions?

Contact us:

- mmaschke@senseient.com
- 703.359.0700