

Path for Forensic Examiner Aces

Tuan Phan

Ohio Information Security Conference

March-2025



#Digital Forensics

Introducing: Tuan Phan

Tuan works for a big well-known Financial institute...



As an Assistant Vice President (AVP) of eDiscovery and Forensics Examiner Lead and has many years of hands-on technical experience, including EF/DF/DFIR, and Insider Threat Strategy.

He is a Principal Security Engineer for

ThreatReel

<https://threatreel.com>

Follow / contact Tuan:

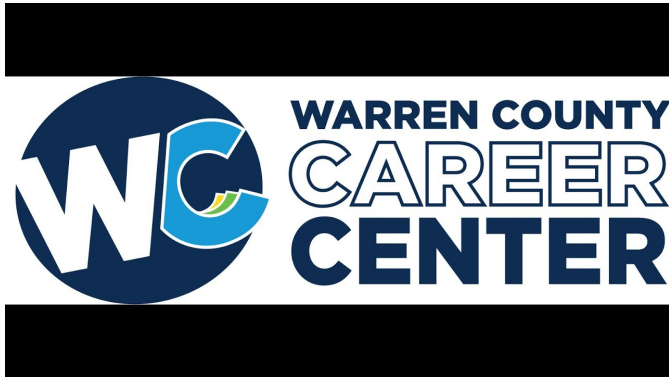
- <https://www.linkedin.com/in/tuanqphan>
- <https://github.com/phanrensic/slides>



Where I Volunteer...



Technical Mentor



Advisory Board Member

Disclaimer!

Yes, the presenter have day jobs. However...

Opinions expressed are based solely on his own independent security research and do not express or reflect the views of his employers.



Agenda

What is a Digital Forensics Examiner (DFE)

- Baseline knowledge required for DFE.
- Public vs Private
- Basic technical skills and the experience.
- Q&A

“Forensic”



White Lab Coat



Clean Room\Forensic Lab

Why This Talk?

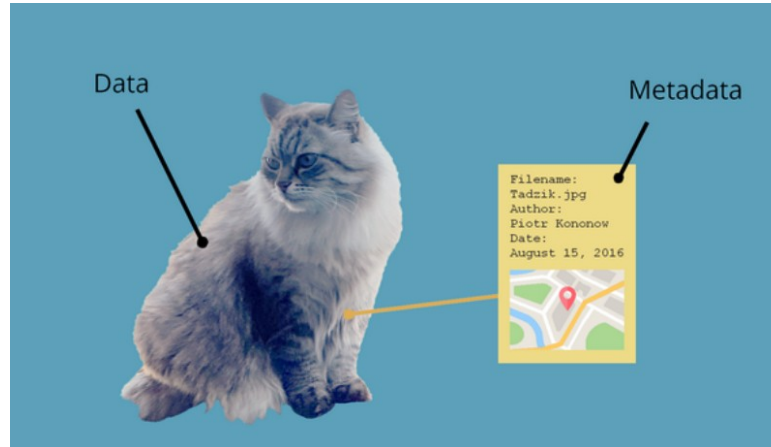
- This talk is inspired by job candidates I participated in interviewing.
- Help fill the knowledge, clear the confusion and skill gaps.
- Digital Forensics – Is this the career path for you?

Digital Forensics

- The process of identifying, collecting, preserving, extracting, analyzing, and presenting evidence.
 - Manner that is legally acceptable, presented in a Court of Law or other.
- Data is collected without alteration,
 - Every step can be traced for legal and compliance purposes.
- Reconstruction of events provide evidence of crimes or case of user misconduct.

- Data and Metadata

- Author\Owner
- Creation date
- Modify date
- Last Access date
- Printed date



Roles of DF\DFIR



- **Digital Forensics Examiner or Digital Forensics Incident Response (DFIR)**, both investigate security incidents, events, and alerts to answer the classic “Who?”, “What?”, “When?”, “Where?”, “Why?”, and “How?” questions.
- **DF** essentially the collection, **preservation**, and analysis of data.

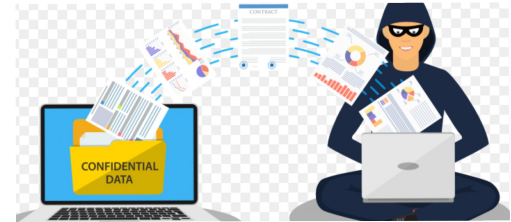
Aspiring DFE

- Retain a working level knowledge of the 5 steps of digital forensics.
 - 1) Identification
 - 2) Data collection\preservation
 - 3) Analysis & Examination
 - 4) Reporting\Presentation
 - 5) ***Documentation**

When Digital Forensic Starts

Tied to some kind of criminal or Cyber crime investigation.

- Any events that happen in your company's perimeter.
 - Inappropriate conduct\Fraud
 - Data being tampered\thief
 - Misuse of company resources
 - Someone getting access to something that they shouldn't have had or in a malicious way.
 - Mouse jiggler



What Does it Takes to be a DFE

- 1) **Analytical Thinking:** Ability to piece together clues and draw conclusion from complex data.
- 2) **Attention to Detail:** Precision is critical when handle and analyzing evidence.
- 3) **Communication Skills:** Teamwork and willingness to communicate and work well with others.
- 4) **May work long hours.**
- 5) **Ability to be good under pressure.**
- 6) ***Testify in court.**

Public vs Private

Public Sector

- Work with regional government bureaus
- Deal most with devices for evidence of criminal activities such as hacking, fraud, homicide, Drugs enforcement, Child abuse, and others.
- Goal is to provide evidence of crime.
- Lab Accreditation for ISO 9001

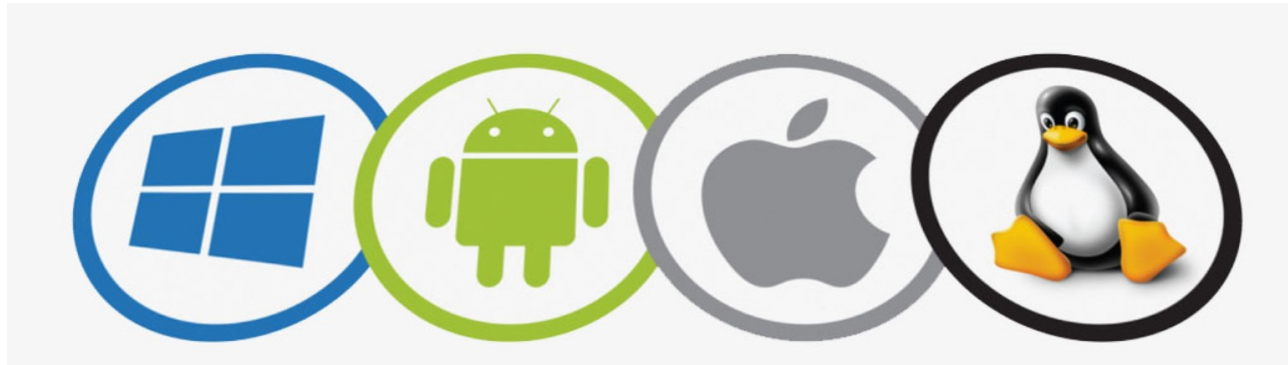
Private Organization

- Deal the same types of device analyses as public, but less intense in mobile volume.
- Email archives, SIEM, EDR, Compliance Portal, DLP, and other enterprise tools.
- Legal Right Hold (LRH)\eDiscovery -
 - FRCP Rule 37
- Goal is to solve the case of the user and prevent potential future threats.
- Not all lab are Accreditation for ISO 9001



OS Basic Skills

- **General knowledge of operating systems;**
 - Windows,
 - Linux & Mac
 - IOS
 - Android
 - Others



Basic Artifacts Skills

- **Windows:**

- Recycle Bin/Deleted data, Registry, Browser artifacts, File Activity, winevt, SRUM, and others.

- **Linux & Mac:**

- Trash Bin, File System Events, Browser artifacts, File Activity, *.plist, Recently Used Items, KnowledgeC: Application Focus, and others

- **Mobile devices (iOS\Android):**

- Geo-location, communication, application, media, web browser, and others

Filesystem Basic Skills

Knowing where things are supposed to be located on an endpoint\devices

Windows

- C:\Recycle.bin
- \Windows\System32\Config*registry
- \Windows\System32\sru\SRUDB.dat
- \Users\AppData\Local\ConnectedDevicesPlatform\<id>\ActivitiesCache.db

Linux\Mac

- /home/<USERNAME>
- /etc, /var/log, and /etc/passw
- *.plist

IOS

- /mobile/Library/Safari/
- /mobile/Library/SMS/sms.db
- /mobile/Library/CallHistoryDB/

Android

- /system/packages.list
- /system_ce/0/recent_images
- /data/system/usagestats/0

<https://www.sans.org/posters/windows-forensic-analysis/>

[illegible]

| Cloud Storage | | | |
|---|--|---|---|
| OneDrive | Google Drive for Desktop | Box Drive | Dropbox |
| Description OneDrive is installed by default on Windows 8 systems, although it must be manually authorized in order to sync Microsoft Cloud accounts. | Description Google Drive is the new name for the original Google Backup and Sync app, which is used to sync Google Drive content to a local drive. | Description Box Drive is a desktop application for Windows and Mac OS X that syncs Box content to a local drive. | Description Dropbox is a file sharing application for Windows, OS X, and Linux that syncs files to a local drive. |
| Location OneDrive is installed in the Windows 8 system folder (C:\Windows\System32\WindowsPowerShell\v1.0\). | Location Google Drive for Desktop is installed in the Windows 8 system folder (C:\Windows\System32\WindowsPowerShell\v1.0\). | Location Box Drive is installed in the Windows 8 system folder (C:\Windows\System32\WindowsPowerShell\v1.0\). | Location Dropbox is installed in the Windows 8 system folder (C:\Windows\System32\WindowsPowerShell\v1.0\). |
| Interpretation OneDrive is a cloud storage service that syncs files to a local drive. | Interpretation Google Drive for Desktop is a cloud storage service that syncs files to a local drive. | Interpretation Box Drive is a cloud storage service that syncs files to a local drive. | Interpretation Dropbox is a cloud storage service that syncs files to a local drive. |
| Usage OneDrive is used to sync files to a local drive. | Usage Google Drive for Desktop is used to sync files to a local drive. | Usage Box Drive is used to sync files to a local drive. | Usage Dropbox is used to sync files to a local drive. |
| Cloud Account Details | Users Accounts | Authentication Events | Logon Event Types |
| Description Microsoft Cloud Accounts store account information in the SAM file, including the user's address associated with the account. | Description Google Drive for Desktop stores account information in the SAM file, including the user's address associated with the account. | Description Box Drive stores account information in the SAM file, including the user's address associated with the account. | Description Dropbox stores account information in the SAM file, including the user's address associated with the account. |
| Location Microsoft Cloud Accounts are stored in the SAM file (C:\Windows\System32\config\SAM). | Location Google Drive for Desktop accounts are stored in the SAM file (C:\Windows\System32\config\SAM). | Location Box Drive accounts are stored in the SAM file (C:\Windows\System32\config\SAM). | Location Dropbox accounts are stored in the SAM file (C:\Windows\System32\config\SAM). |
| Interpretation The presence of this file indicates that a Microsoft Cloud account is present. | Interpretation The presence of this file indicates that a Google Drive for Desktop account is present. | Interpretation The presence of this file indicates that a Box Drive account is present. | Interpretation The presence of this file indicates that a Dropbox account is present. |
| Last Login and Password Change | Remote Desktop Protocol (RDP) Usage | Successful/Failed Logons | System Resource Usage Monitor (SRUM) |
| Description The last login and password change information is stored in the SAM file. | Description Remote Desktop Protocol (RDP) usage is tracked in the SAM file. | Description Successful and failed logon attempts are tracked in the SAM file. | Description System Resource Usage Monitor (SRUM) tracks system resource usage. |
| Location Last login and password change information is stored in the SAM file (C:\Windows\System32\config\SAM). | Location RDP usage is tracked in the SAM file (C:\Windows\System32\config\SAM). | Location Successful and failed logon attempts are tracked in the SAM file (C:\Windows\System32\config\SAM). | Location SRUM tracks system resource usage in the SAM file (C:\Windows\System32\config\SAM). |
| Interpretation The presence of this file indicates that a user has logged in. | Interpretation The presence of this file indicates that RDP is being used. | Interpretation The presence of this file indicates that a logon attempt was successful or failed. | Interpretation The presence of this file indicates that system resource usage is being tracked. |
| Service Events | Network History | Network Activity | Physical Location |
| Description Service events are recorded in the SAM file. | Description Network history is recorded in the SAM file. | Description Network activity is recorded in the SAM file. | Description Physical location is recorded in the SAM file. |
| Location Service events are recorded in the SAM file (C:\Windows\System32\config\SAM). | Location Network history is recorded in the SAM file (C:\Windows\System32\config\SAM). | Location Network activity is recorded in the SAM file (C:\Windows\System32\config\SAM). | Location Physical location is recorded in the SAM file (C:\Windows\System32\config\SAM). |
| Interpretation The presence of this file indicates that a service event has occurred. | Interpretation The presence of this file indicates that network history is being recorded. | Interpretation The presence of this file indicates that network activity is being recorded. | Interpretation The presence of this file indicates that physical location is being recorded. |
| Network History | Browser URL Parameters | WLAN Event Log | System Resource Usage Monitor (SRUM) |
| Description Network history is recorded in the SAM file. | Description Browser URL parameters are recorded in the SAM file. | Description WLAN event logs are recorded in the SAM file. | Description System Resource Usage Monitor (SRUM) tracks system resource usage. |
| Location Network history is recorded in the SAM file (C:\Windows\System32\config\SAM). | Location Browser URL parameters are recorded in the SAM file (C:\Windows\System32\config\SAM). | Location WLAN event logs are recorded in the SAM file (C:\Windows\System32\config\SAM). | Location SRUM tracks system resource usage in the SAM file (C:\Windows\System32\config\SAM). |
| Interpretation The presence of this file indicates that network history is being recorded. | Interpretation The presence of this file indicates that browser URL parameters are being recorded. | Interpretation The presence of this file indicates that WLAN event logs are being recorded. | Interpretation The presence of this file indicates that system resource usage is being tracked. |
| Network Activity | Physical Location | System Resource Usage Monitor (SRUM) | Physical Location |
| Description Network activity is recorded in the SAM file. | Description Physical location is recorded in the SAM file. | Description System Resource Usage Monitor (SRUM) tracks system resource usage. | Description Physical location is recorded in the SAM file. |
| Location Network activity is recorded in the SAM file (C:\Windows\System32\config\SAM). | Location Physical location is recorded in the SAM file (C:\Windows\System32\config\SAM). | Location SRUM tracks system resource usage in the SAM file (C:\Windows\System32\config\SAM). | Location Physical location is recorded in the SAM file (C:\Windows\System32\config\SAM). |
| Interpretation The presence of this file indicates that network activity is being recorded. | Interpretation The presence of this file indicates that physical location is being recorded. | Interpretation The presence of this file indicates that system resource usage is being tracked. | Interpretation The presence of this file indicates that physical location is being recorded. |

<https://www.sans.org/posters/dfir-advanced-smartphone-forensics/>

[illegible][illegible]

*Important Skill: Logs

- The bedrock and starting point of most security investigations begins with any available logs.
- Private vs Public



Native Logs

Understanding where logs exist on various endpoints is vitally important

- **Windows Logs**

- %System32%\winevt\Logs

- **Linux Logs**

- /var/log/syslog

- **Server Logs**

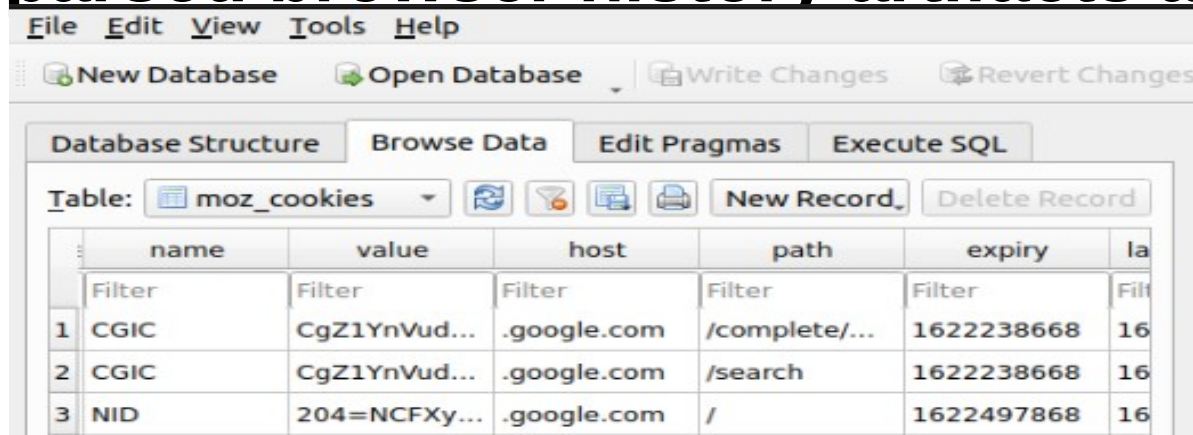
- %SystemDrive%\inetpub\logs\LogFiles

- **Application Logs**

- Depends on applications, some may stored in centralized management

SQL Basics Skills

- Understand “Structured Query Language” (SQL) to parse browser history artifacts and other *.DB



The screenshot shows a database browser window with a menu bar (File, Edit, View, Tools, Help) and buttons for 'New Database', 'Open Database', 'Write Changes', and 'Revert Changes'. Below these are tabs for 'Database Structure', 'Browse Data', 'Edit Pragmas', and 'Execute SQL'. The 'Browse Data' tab is active, showing a table named 'moz_cookies'. The table has columns: name, value, host, path, expiry, and last access time (partially visible as 'la'). The table contains three rows of data, all with a 'Filter' label in the first column.

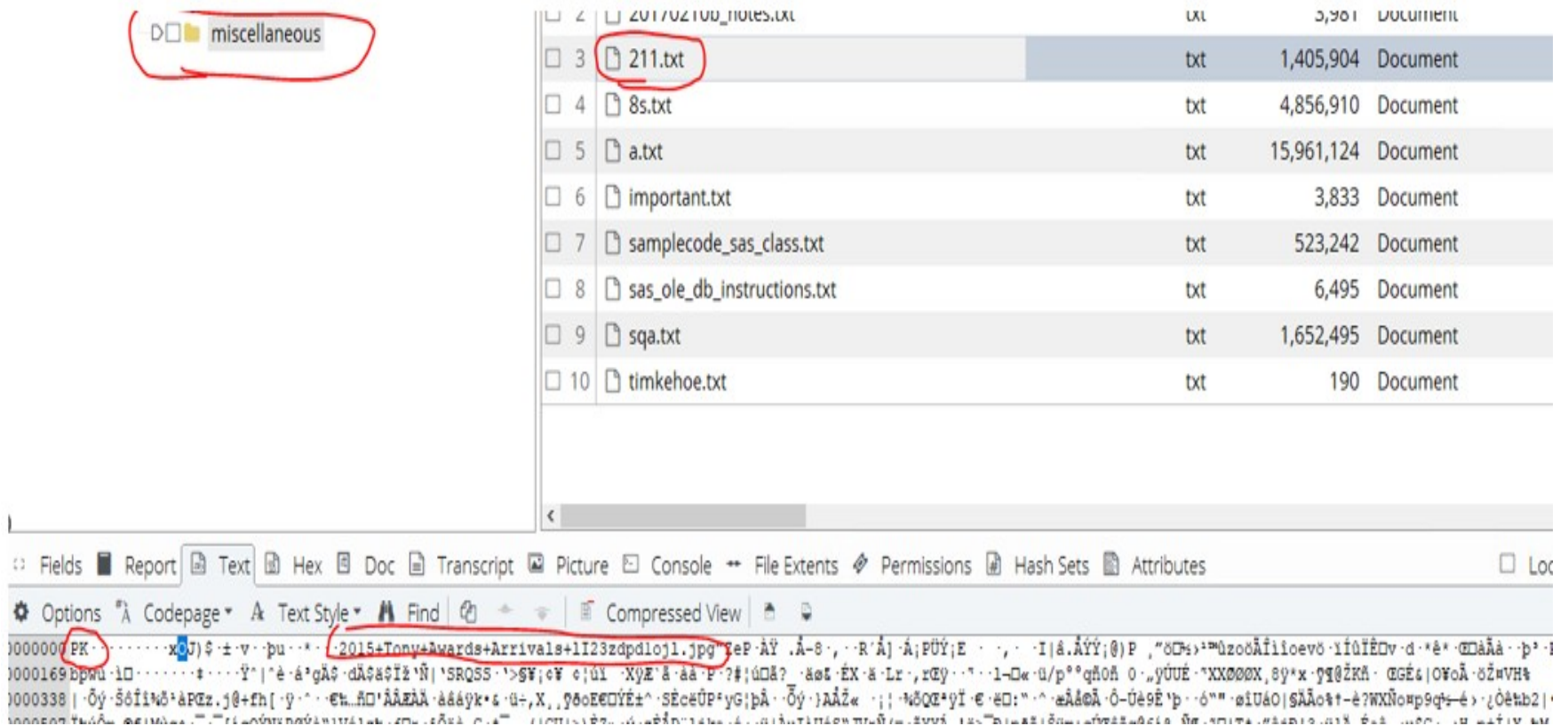
| | name | value | host | path | expiry | la |
|---|--------|--------------|-------------|---------------|------------|------|
| | Filter | Filter | Filter | Filter | Filter | Filt |
| 1 | CGIC | CgZ1YnVud... | .google.com | /complete/... | 1622238668 | 16 |
| 2 | CGIC | CgZ1YnVud... | .google.com | /search | 1622238668 | 16 |
| 3 | NID | 204=NCFXy... | .google.com | / | 1622497868 | 16 |

- Free online training
 - <https://www.sqlcourse.com/beginner-course/>
 - <https://www.sqlcourse.com/advanced-course/>

File Type Identification Skills

- **Understand file signatures, file headers, or whatever you prefer to call them...**
 - Because file extensions can be altered or removed
- **https://www.garykessler.net/library/file_sigs.html**

File Type Case Study



Identify File Execution

- Understand how to know if a file executed on a Windows endpoint
 - Some Examples for the registry key:
 - **UserAssist**
 - **RecentApps**
 - **ShimCache**
 - **CurrentVersion**
 - **Prefetch** - %windir%\Prefetch

File Execution Case Study

- UserAssist

- How many times was the File Explorer launched? (26)

Registry hives (1) Available bookmarks (31/0) Values UserAssist

Enter text to search... Find

Key name

Enter text to search... Find

Drag a column header here to group by that column

| Program Name | Run Counter | Focus Count | Focus Time | Last Executed |
|---|-------------|-------------|--------------------|---------------------|
| UEME_CTLCUACount:ctor | = | = | 0 0d, 0h, 00m, 00s | |
| {Common Programs}\Accessories\Snipping Tool.lnk | 9 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:14:34 |
| UEME_CTLSESSION | 54 | 0 | 0d, 0h, 00m, 00s | |
| {Common Programs}\Accessories\Paint.lnk | 7 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:14:34 |
| {Programs}\Accessories\Notepad.lnk | 6 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:14:34 |
| {User Pinned}\TaskBar\File Explorer.lnk | 26 | 0 | 0d, 0h, 00m, 00s | 2021-12-01 13:02:43 |
| {Programs}\Windows PowerShell\Windows PowerShell.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:37:24 |
| {User Pinned}\TaskBar\Firefox.lnk | 2 | 0 | 0d, 0h, 00m, 00s | 2021-12-01 12:32:34 |
| {Common Programs}\Accessories\Remote Desktop Connection.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 03:59:55 |
| {User Pinned}\TaskBar\Opera Browser.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-25 04:10:02 |
| {Common Programs}\Accessories\Notepad.lnk | 1 | 0 | 0d, 0h, 00m, 00s | 2021-11-30 10:55:21 |

Identify File Activity Skill

- Understand how to know if a file was accessed.
 - This activity is tracked under the following registries below:
 - Jump Lists
 - RecentDocs
 - LastVisitedMRU – last path file opened\executed
 - OpenedSavedPidMRU
 - LNK files
 - ShellBags
 - etc

File Activity Case Study

- RecentDocs

| Registry hives (1) | | | | Available bookmarks (21/0) | | | | | | |
|-------------------------|----------|-----------|----------------------|----------------------------|--|--|--|--|--|--|
| Enter text to search... | | | | Find | | | | | | |
| Key name | # values | # subkeys | Last write timestamp | | | | | | | |
| HKEY_CURRENT_USER | = | = | = | | | | | | | |
| FeatureUsage | 1 | 3 | 2020-09-29 15:35:01 | | | | | | | |
| FileExts | 0 | 185 | 2020-09-29 17:27:01 | | | | | | | |
| HideDesktopI... | 0 | 1 | 2020-09-29 15:07:50 | | | | | | | |
| LagoonStats | 2 | 0 | 2020-09-29 15:04:53 | | | | | | | |
| LowRegistry | 0 | 0 | 2020-09-29 15:04:55 | | | | | | | |
| MenuOrder | 0 | 1 | 2020-09-29 15:04:55 | | | | | | | |
| Modules | 0 | 3 | 2020-09-29 15:24:27 | | | | | | | |
| MountPoints2 | 0 | 3 | 2020-09-29 15:24:31 | | | | | | | |
| Package Inst... | 1 | 0 | 2020-09-30 14:32:10 | | | | | | | |
| RecentDocs | 5 | 3 | 2020-09-30 14:40:31 | | | | | | | |
| Ribbon | 2 | 0 | 2020-09-29 15:24:21 | | | | | | | |
| RunMRU | 0 | 0 | 2020-09-29 15:24:29 | | | | | | | |
| SearchPlatform | 0 | 1 | 2020-09-29 15:04:52 | | | | | | | |
| Shell Folders | 31 | 0 | 2020-09-29 15:04:56 | | | | | | | |
| Shutdown | 1 | 0 | 2020-09-30 14:43:30 | | | | | | | |

| Values | | | | | | |
|---|-------------------|-------------------|----------------------------------|--------------|---------------------|-----------------------|
| Recent documents | | | | | | |
| Drag a column header here to group by that column | | | | | | |
| Extension | Value Name | Target Name | Lnk Name | Mru Position | Opened On | Extension Last Opened |
| HKEY_CURRENT_USER | HKEY_CURRENT_USER | HKEY_CURRENT_USER | HKEY_CURRENT_USER | = | = | = |
| RecentDocs | 3 | temp | temp.lnk | 0 | 2020-09-30 14:40:31 | 2020-09-30 14:40:31 |
| RecentDocs | 2 | users.txt | users.lnk | 1 | | 2020-09-30 14:40:31 |
| RecentDocs | 0 | The Internet | The Internet.lnk | 2 | | |
| RecentDocs | 1 | kglicheck/ | ms-gamingoverlay--kglicheck-.lnk | 3 | | |
| Folder | 1 | temp | temp.lnk | 0 | 2020-09-30 14:40:31 | |
| Folder | 0 | The Internet | The Internet.lnk | 1 | | |
| .txt | 0 | users.txt | users.lnk | 0 | 2020-09-30 14:40:31 | |

Identify USB Activity Skill

- **Understand how to know if a USB was connected.**
 - **The majority of USB-related artifacts are located within the Windows Registry**
 - SYSTEM\CurrentControlSet\Enum\USBSTOR
 - SYSTEM\MountedDevices
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
 - **Windows Event Logs:**
 - System event logs may contain entries related to USB device insertions and removals.
 - Event Viewer path: Applications and Services Logs\Microsoft\Windows\DriverFrameworks-UserMode\Operational

USB Activity Example

- **USBSTOR:**

- SYSTEM\CurrentControlSet\Enum\USBSTOR

- **Things to Record:**

- Device S/N:
 - Vendor:
 - Product:
 - Service:
 - Container Id:

| Value Name | Value Type | Data | Value Slack |
|---------------|------------|--|-------------------|
| %c | %c | %c | %c |
| DeviceDesc | RegSz | @disk.inf, %disk_devdesc%;Disk drive | 00-00-00-00 |
| Capabilities | RegDword | 16 | |
| Address | RegDword | 2 | |
| HardwareID | RegMultiSz | USBSTOR\Disk_USB____SanDisk_3.2Gen11.00 ... | 00-00-00-00 |
| CompatibleIDs | RegMultiSz | USBSTOR\Disk USBSTOR\RAW GenDisk | |
| ClassGUID | RegSz | {4d36e967-e325-11ce-bfc1-08002be10318} | 00-00-00-00-00-00 |
| Service | RegSz | disk | 00-00 |
| Driver | RegSz | {4d36e967-e325-11ce-bfc1-08002be10318}\0001 | 00-00-00-00 |
| Mfg | RegSz | @disk.inf, %genmanufacturer%;(Standard disk d... | 00-00-00-00-00-00 |
| FriendlyName | RegSz | USB SanDisk 3.2Gen1 USB Device | 00-00 |
| ConfigFlags | RegDword | 0 | |
| ContainerID | RegSz | {3deb34e4-837d-5c67-b987-c26b48b8df68} | 69-00-63-00-65-00 |

Understand Order of Volatile

- **Collect and Protect information relating to an incident**
 - Many different data source and protection mechanisms
- **RFC 3227 – Guidelines for Evidence Collection and Archiving**
 - A good set of best practices
- **How Long Does data stick around?**
 - Some media is much more volatile than others
 - Gather data in order from most to less
 - registers, cache
 - routing table, arp cache, process table, kernel statistics, memory
 - temporary file systems
 - disk
 - remote logging and monitoring data that is relevant to the system in question
 - physical configuration, network topology
 - archival media

Forensics Tools for skill building

- Many tools can be used to perform data analysis on different Operating Systems.
- Forensic toolkit for Win/Linux
 - Kali, Helix, DEFT, Autopsy Sleuth-kit, SIFT
 - FTK imager, Nirsoft
- Mobile Forensics
 - SAFT, Autopsy, Belkasoft



Ways to build Forensic skills

- **Follow Cyber Security Linkedin group free training and webinars.**
 - CYBER SECURITY FORUM INITIATIVE – CSFI
 - Forensic Focus
 - Belkasoft
 - Sleuth Kit Labs
- **Follow and watch YouTube Digital Forensics Channel**
 - TEDx Talks
 - SANS
 - Google Career Certificates
 - Others
- **Check out ENISA**
 - <https://www.enisa.europa.eu/>

Just Some of the Challenges

- Rapidly changing technology and Data volumes
- System & Application update
- Mental health
- Ongoing education
- Unsupported devices
- Encryption\Security Features



Certifications

- **Some well-known forensic certifications include the following:**
 - CISSP – Certified Information Systems Security Professional
 - CCE – Certified Computer Examiner
 - CFCE – Certified Forensic Computer Examiner
 - GIAC – Certified Forensic Analyst (GCFA)
 - CompTIA A+, Network+, Security+

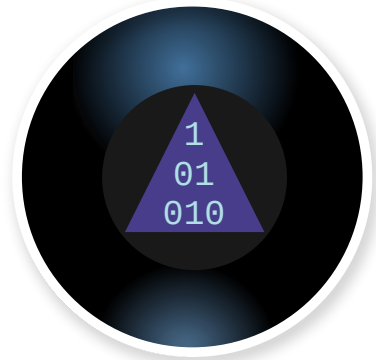
Salary & Benefits

- **The starting salary for a computer forensics professional depends on various factors.**
 - Whether you're employed in the public or private sector.
 - Degree (s) vs Certification (s)
 - # of years of experience
 - Location

Questions



Who?
What?
When?
Where?
Why?
How?



Thank you for Attending!



Tuan Phan

March 2025



*****<https://github.com/phanrensic/slides>*****