DF Lecture 5 Notes

Here’s a **comprehensively formatted version** of **Lecture 5: Operating System Forensics** by **Dr. Zunera Jalil**, exactly as per your request—**no wording changed**, just improved for better clarity and exam preparation:

Lecture 5 - Operating System Forensics

Dr. Zunera Jalil
Email: zunera.jalil@au.edu.pk
Date: 18th March 2025

Data Analysis for OS Forensics

- Forensic examiners perform data analysis to examine artifacts left by perpetrators, hackers, viruses, and spyware.
- They scan deleted entries, swap or page files, spool files, and RAM during this process.
- These collected artifacts can provide a wealth of information with regard to how malicious actors tried to cover their tracks and what they were doing to a system.

What is Operating System Forensics?

- The process of retrieving useful information from the Operating System (OS) of the computer or mobile device in question.
- The aim is to acquire empirical evidence against the perpetrator.
- The understanding of an OS and its file system is necessary to recover data for computer investigations.
- The file system provides an operating system with a roadmap to data on the hard disk & also identifies how hard drive stores data.

- There are many file systems introduced for different operating systems:
  - **FAT, exFAT, and NTFS** for Windows OSs
  - **Ext2fs, or Ext3fs** for Linux OSs

More on OS Forensics

- Data and file recovery techniques for these file systems include **data carving**, **slack space**, and **data hiding**
- Another important aspect of OS forensics is **memory forensics**, which incorporates:
  - Virtual memory
  - Windows memory
  - Linux memory
  - Mac OS memory
  - Memory extraction
  - Swap spaces
- OS forensics also involves web browsing artifacts, such as **messaging and email artifacts**
- Common Operating Systems: **Windows, Linux, Mac, iOS, Android**

Windows Forensics

Important Locations to Analyze:

1. **Recycle Bin**
   - Holds files that have been discarded by the user
   - Soft Deletion process – recovering files from recycle bin can be a good source of evidence
2. **Thumbs.db Files**
   - Contain images' thumbnails that can provide relevant information

3. **Browser History**
   - Web Browser generates history files
   - Microsoft Windows Explorer is the default
   - Other supported browsers: Opera, Mozilla Firefox, Google Chrome, Apple Safari

---

4. **Print Spooling**
   - When printing, a **print job** is created and queued until completed
   - Printer must be configured in **EMF mode** or **RAW mode**
     - RAW: straight graphic dump
     - EMF: converted to Microsoft Enhanced Metafile
   - EMF files can provide empirical forensic evidence

   Paths to EMF files:

   - Windows NT/2000: `Winnt\system32\spool\printers`
   - Windows XP to 10: `Windows\system32\spool\printers`
   - OS forensic tools can detect this path automatically

Registry Forensics

5. **Registry**
   - Holds a database of values and keys useful to forensic analysts
   - Contains policies, statuses, etc., as keys, subkeys, values
   - Tools: `regedit`, `reg` command-line tool
   - Registry contains **hives** under which subkeys are present – important for system function

---

Windows Artifacts

- Thumbcache
- Jump lists
- Recycle Bin
- Prefetch files
- ShimCache
- AmCache
- System Resource Usage Monitor (SRUM)
- MFT
- Windows 10 Timeline
- `$J`, `$Log file`
- Link file - Shortcut (.lnk)
- User Assist
- Word Wheel Query
- NTUSER.DAT
- ShellBags
- Background Activity Monitor (BAM)/DAM
- PowerShell

Windows Password Storage

- User passwords are stored in:
  1. **SAM (Security Account Manager)**
  2. **AD (Active Directory)**
- **SAM**
  - Used in Windows XP, Vista, 7
  - Stores user passwords for local and remote authentication
  - Uses cryptographic protection

- Passwords are **hashed** and stored in registry hive: `"%SystemRoot%/system32/config/SAM"`

Applications Password Cracking

- Programs used to gain unauthorized access or retrieve forgotten passwords
- **Methods:**
  - Brute force method
  - Dictionary searches
  - Rule-based attack
  - Password guessing
  - Rainbow attack

Explanation of Attacks

- **Brute Force Attack**
  - Tests all possible combinations
  - Time increases exponentially with password length
- **Dictionary Attack**
  - Tries strings from a list (dictionary)
  - Useful against weak passwords
- **Rule-Based Attack**
  - Uses known information to narrow search
  - Most powerful technique

- **Hybrid Attack & Password Guessing**
  - Based on dictionary attack

  - Combines known password with symbols
  - Uses commonly used passwords
- **Rainbow Attack**
  - Utilizes **precomputed tables** to reverse cryptographic hashes
  - Used to recover passwords, credit card numbers, etc.
  - Attacks hashed password databases

Password Recovery Tools

- **Office Password Recovery Toolbox**
  - Recovers lost Microsoft Office document passwords
- **Passware Kit Enterprise and Forensics**
  - Can recover passwords of 150+ file types

Other OSs Forensics

Linux Forensics

- Linux is open-source, Unix-like, used in many devices
- Uses **ext2, ext3, ext4** file systems
- Key directories:
  - `/etc` – system configurations
  - `/var/log` – application/security logs
  - `/home/$USER` – user data
  - `/etc/passwd` – user account information
- Tools: Dmesg, Insmod, NetstatArproute, Hunter.O, DateCat, P-cat, NC
- **Helix** (Knoppix Live CD) – supports Linux forensics

Mac OS X Forensics

- UNIX-based, uses Mach 3 microkernel + FreeBSD subsystem
- Forensic technique: **Target Disk Mode**
  - Use Firewire cable to create disk duplicate

Apple iOS Forensics

- UNIX-based mobile OS
- Used in iPhone, iPod Touch, iPad
- Can be rich source of evidence

Android Forensics

- Google’s open-source mobile OS
- Linux-based kernel
- Uses **Android Debug Bridge (ADB)** over USB for forensic access

---

Assignment 2

- **Tasks:**
  1. Explore assigned topic in detail
  2. Perform hands-on activities (take screenshots)
  3. Prepare **15–20 page report** explaining topic & findings

  - **Deadline:** Submit on **GCR by 27th March 2025**

Groups:

- Group A – Apple iOS Forensics
- Group B – Linux Kali Forensics

- Group C – Unix Forensics
- Group D – Mac OS X Forensics
- Group E – Android Forensics
- Group F – Windows Server
- Group G – Embedded and IoT OS
- Group H – Linux Ubuntu Forensics

Quiz Announcements

- **Quiz 2:**
  - **Date:** 25th March 2025
  - **Covers:** Lecture 4 and 5
- **Quiz 3:**
  - **Date:** 8th April (After Eid Holidays)
  - **Covers:** EC Council Modules 1, 2, 3, 4

Home Tasks / References

- **Chapter 5** (Textbook)
- Coursera Course:
  - Windows OS Forensics (Coursera)
- Articles:
  - GeeksForGeeks – Windows Forensic Analysis
  - Infosec Institute – OS Forensics
  - LinkedIn Learning – OS Forensics

ANY QUESTIONS?

Let me know if you'd like this as a PDF, printable version, or flashcards for revision.

Here’s a concise one-line description for each **Windows artifact** to help you with your notes:

1. **Thumbcache** – Stores thumbnail images for faster previewing of media files.
2. **Jump Lists** – Tracks recently opened files and folders for quick access in taskbar apps.
3. **Recycle Bin** – Holds deleted files temporarily; useful for recovering soft-deleted data.
4. **Prefetch Files** – Speeds up app loading by storing info about previously run programs.
5. **ShimCache** – Logs executables that have been run; useful for tracking execution history.
6. **AmCache** – Stores metadata of executed applications, including installation info.
7. **System Resource Usage Monitor (SRUM)** – Records app usage and network activity.
8. **MFT (Master File Table)** – Contains detailed metadata of every file on an NTFS drive.
9. **Windows 10 Timeline** – Logs user activity across time, apps, and devices.
10. **$J, $Log file** – NTFS metadata files; track file changes and transactional logs.
11. **Link file (.lnk)** – Shortcut files that reveal paths and metadata of accessed files.
12. **User Assist** – Stores info on programs run via the Start Menu or desktop.
13. **Word Wheel Query** – Tracks search terms entered in Windows Explorer.
14. **NTUSER.DAT** – Registry file storing user profile configuration and preferences.
15. **ShellBags** – Maintains folder view settings and folder access history.
16. **Background Activity Monitor (BAM)/DAM** – Logs background activity and app runtime data.
17. **PowerShell** – Command-line tool that stores history and script execution logs.

Let me know if you want this in table format or PDF!