DF Lecture 6 Notes

Here's a **well-formatted and structured version** of your notes for **Lecture 6 - Registry Forensics** by Dr. Zunera Jalil. No wording has been changed — only improved formatting, headings, and bullet points to make it easier to study for your exam:

Lecture 6 – Registry Forensics

Dr. Zunera Jalil
📧 *Email: zunera.jalil@au.edu.pk*

Windows Registry Overview

- Windows Registry holds a **database of values and keys** with useful forensic information.
- It keeps most of the **policy, status, and user-related data** in the form of:
  - Keys
  - Subkeys
  - Values
- Administrators can manage the registry using:
  - GUI tool: `regedit`
  - CLI tool: `reg`
- Registry consists of **hives**, under which subkeys are present.
- These hives are crucial to **overall system functioning**.

Registry Forensics Insight

- Registry keys and files encompass **user activities**.

- Can reveal details such as:
  - Time zone
  - Shared folders
  - Audit policies
  - Wireless SSIDs
  - Autostart locations
  - User login and activities
  - USB/removable/trusted devices
  - Cache, cookies, and history

Registry Structure & Functioning

General Behavior

- Upon installing software, hardware, or drivers:
  - **Initial configuration settings** are saved to the registry.
- On every startup:
  - Windows components retrieve and possibly **modify registry entries**.
- Data is sorted as:
  - **Computer-specific**
  - **User-specific**
- Supports **multiple user profiles**.

Registry Format

- Registry = **Hierarchical database**
- Tree structure:
  - Each **node** is a **key**
  - Keys can contain:
    - Subkeys

    - Data entries (*Values*)
- Keys and values are accessed by **applications**.
- A key may have **any number of values** in **any data format**.

Registry Hives

Common Hives

- `HKEY_CLASSES_ROOT`
- `HKEY_CURRENT_USER`
- `HKEY_LOCAL_MACHINE\SAM`
- `HKEY_LOCAL_MACHINE\SOFTWARE`
- `HKEY_LOCAL_MACHINE\SECURITY`
- `HKEY_LOCAL_MACHINE\SYSTEM`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG`

Hive Details

- Hive = Logical group of:
  - Keys
  - Subkeys
  - Values
- Has **supporting files** for data backup:
  - Stored in: `%SystemRoot%\System32\Config`

User Profile Hives

- Created each time a **new user logs in**
- Stored under: `HKEY_USERS`
- Contains:
  - App settings

  - Desktop/environment
  - Network connections

Permanent Hive Files

- Stored in:
  - `HKLM\SYSTEM\CurrentControlSet\Control`
  - Updated with each login
- Location: `systemroot\System32\Config`
- Hive keys & files:
  - `SAM` → `HKLM\SAM`
  - `SECURITY` → `HKLM\SECURITY`
  - `SOFTWARE` → `HKLM\SOFTWARE`
  - `SYSTEM` → `HKLM\SYSTEM`
  - `DEFAULT` → `HKEY_USERS\.DEFAULT`
  - Note: `HKLM\HARDWARE` is **not** stored as a file (recreated at startup)

Hives & Their Associated Files

Hive Location	Files
`HKEY_CURRENT_CONFIG`	System, System.alt, System.log, System.sav
`HKEY_CURRENT_USER`	Ntuser.dat, Ntuser.dat.log
`HKLM\SAM`	Sam, Sam.log, Sam.sav
`HKLM\SECURITY`	Security, Security.log, Security.sav
`HKLM\SOFTWARE`	Software, Software.log, Software.sav
`HKLM\SYSTEM`	System, System.alt, System.log, System.sav

Hive Location	Files
`HKEY_USERS\.DEFAULT`	Default, Default.log, Default.sav

Files in Windows NT and Later

- Six primary files:
  - `Ntuser.dat`
  - `System.dat`
  - `SAM.dat`
  - `Software.dat`
  - `Security.dat`
  - `Default.dat`

Volatile Hives (Created at Runtime)

- `HKEY_LOCAL_MACHINE\System\CurrentControlSet`
- `HKEY_CURRENT_USER`
- `HKEY_LOCAL_MACHINE\Hardware`

Registry File Paths

- `HKEY_CURRENT_USER`:
  → **NTUSER.DAT**
- `HKEY_LOCAL_MACHINE`:
  → **SAM, SYSTEM, SOFTWARE, SECURITY**

Forensically Interesting Artifacts

System & Application Settings

- Configuration & application settings
- Download directories
- Recently accessed files (images, movies, etc.)
- Autostart locations
- Applications started with minimal user interaction

Tracking Data

- USB devices (e.g., thumb drives, external HDDs)
- User activity MRUs
- Viewed documents/images
- UserAssist keys (installed/launched apps)

Information of Interest in Registry

- Basic system information:
    - Computer Name
    - Time of Last Shutdown
    - Product Name, Build version
    - Time zone
    - Wireless SSIDs
    - USB Device connections
    - MRUs

Detailed Artifacts

Computer Name

- Assigned once during setup

- Useful for tracking user activity over network

Last Shutdown Time

- Helps analyze user status and timeline of events

Shared Folders/Apps

- Locally or remotely created
- Can help track:
    - Data sharing
    - File access history

Audit Policies

- Indicates events/logs of interest

Wireless SSIDs

- Assist in tracing IP and investigating unauthorized access

USB Devices

- Registered by **Plug and Play (PnP) Manager**

Most Recently Used (MRU) Lists

- Maintained by many applications
- Include:
    - Recently opened/created files
    - Search history
    - Connected systems
- Can reflect the **user's mindset** or actions before a crime

---

System Restore Points

- Show backup activity and system status over time

Windows Password Storage

Two Main Locations

1. **SAM (Security Account Manager)**
    - Stores passwords in hashed format
    - Location: `%SystemRoot%\System32\config\SAM`
    - For local and remote user authentication
2. **AD (Active Directory)**
    - For remote user authentication

Forensically Interesting Registry Spots

- Areas to analyze include:
    - Password files
    - Hive files
    - User activity entries
    - USB history
    - Autostart programs
    - MRU lists

Quiz References

- **Quiz 2**: *[5-minute quiz]*
    - CLO No. 1
    - *What will be the capacity of this drive?*

- **Quiz 3**: *Scheduled for 8th April (After Eid Holidays)*
    - Based on: **EC Council Modules 1, 2, 3, 4**

References

- Hackers Arise – Windows Registry Forensics
- ScienceDirect – Windows Registry Forensics
- Google Books – Windows Registry Forensics

Let me know if you want this in **PDF**, or want me to create a **mind map**, **flashcards**, or a **summary sheet** for faster revision.

Here's a **consolidated and organized table** of all the Windows Registry hives mentioned in the lecture, including their **associated files**, **paths**, and **descriptions** based on the content of Lecture 6:

✅ Consolidated Table of Windows Registry Hives

Registry Hive	Path	Associated File

HKEY_CLASSES_ROOT	N/A	Merged view fr
		`HKLM\Software`
		and
		`HKCU\Software`

HKEY_CURRENT_USER	`%SystemRoot%\Users\<username>\NTUSER.DAT`	`Ntuser.dat`, `Ntuser.dat.lo`

Registry Hive	Path	Associated File
HKEY_LOCAL_MACHINE\SAM	`%SystemRoot%\System32\Config\SAM`	`Sam` , `Sam.log` , `Sam.sav`
HKEY_LOCAL_MACHINE\SECURITY	`%SystemRoot%\System32\Config\Security`	`Security` , `Security.log` , `Security.sav`
HKEY_LOCAL_MACHINE\SOFTWARE	`%SystemRoot%\System32\Config\Software`	`Software` , `Software.log` , `Software.sav`

HKEY_LOCAL_MACHINE\SYSTEM	`%SystemRoot%\System32\Config\System`	`System` , `Syste`
		`System.log` ,
		`System.sav`

Registry Hive	Path	Associated File
HKEY_LOCAL_MACHINE\HARDWARE	N/A (volatile)	Not stored on d

HKEY_USERS	`%SystemRoot%\System32\Config\Default` (for `.DEFAULT`)	`Default`, `Defa`
		`Default.sav`

HKEY_CURRENT_CONFIG	Linked to HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current	`System`, `Syste`
		`System.log`,
		`System.sav`

HKEY_USERS.DEFAULT	`%SystemRoot%\System32\Config\Default`	`Default`, `Defa`
		`Default.sav`

🧠 Additional Notes on Registry Hives:

- **Volatile Hives** (not stored on disk):
    - `HKEY_LOCAL_MACHINE\Hardware`
    - `HKEY_LOCAL_MACHINE\System\CurrentControlSet`
    - `HKEY_CURRENT_USER`
- **Hive Files Storage Directory**:
    - `%SystemRoot%\System32\Config`
- **File Types in Registry**:
    - `.dat`, `.log`, `.sav` — used to store, update, and back up registry data.
- **Registry File Locations (Quick View)**:

File	Path
`NTUSER.DAT`	`%SystemRoot%\Users\<username>\`
`SAM`, `SECURITY`, `SOFTWARE`, `SYSTEM`, `DEFAULT`	`%SystemRoot%\System32\Config\`

Let me know if you'd like this exported to PDF, a table in Word, or formatted for flashcards!