📘 Lecture 9 — Windows Registry, Event Viewer & Malware Analysis

---

🧩 1. What is Windows Registry?

🔹 Definition:

The **Windows Registry** is a **central hierarchical database** in Windows that stores **configuration settings and options** for the operating system and all installed applications.
It tells Windows **how the system and applications should behave**.

🔹 Path:

%SystemRoot%\System32\Config

This is the folder where the registry's main files are physically stored.

🔹 Access:

Press **Win + R → type regedit → Enter**
This opens the **Registry Editor**, where you can view and modify registry keys.

🧠 2. Structure of Registry

The Registry is divided into **five main root keys**, each containing **subkeys and values**.

Root Key	Full Form	Function
HKEY_USERS	Holds user profiles	Stores settings for *all* users who have logged into the PC
HKEY_CURRENT_USER	Current logged-in user	Stores personalized settings like desktop, wallpaper, theme, etc.
HKEY_LOCAL_MACHINE	Local machine data	Contains OS configurations and software installation data
HKEY_CLASSES_ROOT	File association	Tells Windows which program should open which file type (e.g., .docx → MS Word)
HKEY_CURRENT_CONFIG	Current hardware configuration	Shows active drivers, display settings, etc., used in the current session

---

⚙️ 3. Why Registry is Important

- Every system action (installing software, changing wallpaper, setting network, etc.) updates the Registry.
- Registry defines how the **OS boots, performs, and behaves**.
- Hackers often modify registry entries to **create persistence**, **disable security**, or **auto-run malware**.

🧩 4. Registry Keys, Subkeys, and Values

Element	Description	Example
Key	A folder in registry containing subkeys or values	HKEY_LOCAL_MACHINE\SOFTWARE
Subkey	Nested folder inside a key	...\Windows\CurrentVersion\Run
Value	Data assigned to the key	"Path"="C:\Program Files\App\app.exe"

⚡ 5. Change System Settings via Registry

Example:

Disable “Set Time Zone Automatically” (Greyed Out Issue)

Steps:

1. Press **Win + R → regedit**
2. Navigate to:
3. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tzautoupdate
4. Select **Start** key → Double click → Set **Value Data = 0**
5. Restart your PC.

Explanation:
Setting this value disables the background timezone auto-update service.

🦠 6. Virus Detection Using Registry (Very Important for Interviews)

Hackers often configure malware to **auto-start** when Windows boots.
You can detect such malicious entries by checking these registry paths:

Registry Path	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Programs that start for **all users** at boot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Programs that run **only once** after reboot
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Programs that start for the **current user only**

🧠 **Tip:**
If you find unknown .exe files or random program names in these keys, they could be **malware startup entries**.

🔐 7. Windows Defender Settings via Registry

Path:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender Security Center\Virus and threat protection

Values Explanation (0–4)

Value Data	Meaning
0	Disable feature completely
1	Enable (default setting)
2	Limited functionality
3	Manual control required
4	Reserved / Advanced control by admin

Why use it:
System admins or attackers can control Defender's behavior through these registry values.

🌐 8. ElevenForum — Support Website

Website: https://www.elevenforum.com

Use:
This is a trusted Microsoft community where you can get step-by-step solutions for Windows errors, registry fixes, and update issues.

🧩 9. What is Event Viewer?

🔹 **Definition:**

Event Viewer is a Windows tool that records all **system, application, and security events/logs**.
It's used in **malware analysis** and **forensics** to trace what happened, when, and by which user.

🔹 **Access:**

Press **Win + R → type eventvwr.msc → Enter**

🔹 **Navigation:**

- Go to **Windows Logs → Application**
- To check errors: Click **Filter Current Log → Select Critical, Error**

🧠 10. Event Viewer in Malware Analysis

Uses:

- Track **when malware or crack software was installed**.
- See **system crashes, errors, and warnings** related to applications or drivers.
- Monitor **login times**, **system reboots**, **antivirus events**, etc.

Real Example:

If someone says, "I got a virus even after installing antivirus,"
→ You can open Event Viewer and **check the exact time of attack vs antivirus installation** to analyze sequence of events.

⚙️ 11. Reading Error Logs (Example Breakdown)

Error example from your lecture:

Faulting application name: ShellHost.exe, version: 10.0.26100.6725, time stamp: 0xcebbddf3

Faulting module name: ucrtbase.dll, version: 10.0.26100.6725, time stamp: 0xb17dff17

Exception code: 0xc0000409

Fault offset: 0x00000000000a4ace

Faulting process id: 0x1F18

Faulting application path: C:\Windows\System32\ShellHost.exe

Faulting module path: C:\WINDOWS\System32\ucrtbase.dll

Report Id: 32923feb-9dca-44ac-905b-5c4f8de5be10

Explanation:

Field	Meaning
Faulting application name	The program that crashed (ShellHost.exe = part of Windows Shell)
Faulting module name	The DLL responsible for the crash (ucrtbase.dll = Microsoft C runtime library)
Exception code 0xc0000409	Stack buffer overrun error – indicates memory corruption or exploit attempt
Fault offset	Memory address where crash occurred
Process ID / Start time	Helps correlate with other logs or events
Paths	File location (can verify integrity or infection)

📘 **Use Case in Forensics:**
If a DLL like ucrtbase.dll keeps crashing, it may be **replaced or hooked by malware**.

🛠️ 12. Checking System Logs

Path:

Event Viewer → Windows Logs → System

- Displays system-level warnings and errors (e.g., driver failure, hardware malfunction, service crash).
- Helps identify whether malware has corrupted a system service.

🛡️ 13. Checking Windows Defender Logs

Path:

Event Viewer → Applications and Services Logs → Microsoft → Windows → Windows Defender → Operational

Here you can check:

- When Defender scanned files
- Detected threats
- Quarantined or removed malware

👥 14. Checking User Login Logs

Path:

Event Viewer → Windows Logs → Security

Event IDs to remember:

Event ID	Description
4624	Successful login
4625	Failed login attempt
4634	User logged off
4647	User initiated logoff

Use Case:
If you suspect unauthorized access, check **4624** and **4625** entries for suspicious login times or IP addresses.

🧠 15. Why Event Viewer is Important in Cybersecurity

- Tracks **malware behavior and installation time**.
- Helps correlate **user activity** and **system errors**.
- Used in **digital forensics** and **incident response**.
- Can prove **if malware entered before or after antivirus installation**.

✅ Summary Table

Topic	Description	Tool/Path
Registry	Central configuration database of OS	regedit
Virus Detection	Detect startup malware entries	Run, RunOnce keys
Windows Defender Registry	Control Defender settings	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender...
Event Viewer	Analyze logs, errors, malware installs	eventvwr.msc
Application Error	Shows software crashes	Windows Logs → Application

Topic	Description	Tool/Path
System Log	Shows OS-level issues	Windows Logs → System
Security Log	Tracks user login/logout	Windows Logs → Security
Defender Logs	Tracks threat detections	Applications and Services Logs → Microsoft → Windows Defender
ElevenForum	Fix Windows-related issues	elevenforum.com

🧩 Visual Concept Summary (Flow)

Registry (Settings & Startup Config)

↓

Malware may modify keys (Run/RunOnce)

↓

Windows Defender monitors in real time

↓

Event Viewer logs every change or crash

↓

Analyst reviews logs (Application, System, Security)

↓

Traces malware behavior or infection source

✅ 📘 LECTURE 9 — COMPLETE SUMMARY

1. Windows Registry

The Windows Registry is a **central database** that stores:

- System configuration
- Application settings
- User preferences
- Hardware details

Location:
%SystemRoot%\System32\Config

Open using:
regedit

Anything you install or modify (software, drivers, wallpaper, services) updates the Registry.

---

2. Registry Structure (5 Root Keys)

1. HKEY_USERS (HKU)

Stores data for **all user profiles**.

2. HKEY_CURRENT_USER (HKCU)

Stores settings for the **currently logged-in user** (wallpaper, theme, desktop).

3. HKEY_LOCAL_MACHINE (HKLM)

System-wide configurations such as:

- Installed apps
- Drivers
- Services
- Security configs

4. HKEY_CLASSES_ROOT (HKCR)

Controls **file associations** (e.g., .mp3 opens in VLC).

5. HKEY_CURRENT_CONFIG (HKCC)

Stores **active hardware profile** settings.

---

3. Why Registry is Critical

- Controls OS startup
- Defines system performance
- Stores security configurations
- Hackers modify it to gain **persistence**
- Malware creates **startup entries** inside registry keys

---

4. Registry Keys → Subkeys → Values

- **Key** = Folder
- **Subkey** = Subfolder
- **Value** = Actual data

Example:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

---

5. System Modification via Registry (Example)

To fix “Time Zone Automatically” greyed-out:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tzautoupdate

Start = 0

---

6. Malware Detection Using Registry

Malware commonly adds itself to these locations:

Registry Path	Meaning
HKLM...\Run	Autostart for ALL users

Registry Path	Meaning
HKLM...\RunOnce	Runs once after reboot
HKCU...\Run	Autostart for current user

Suspicious unknown EXE = Malware indicator

---

7. Windows Defender Registry Control

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender Security Center\Virus and threat protection

Value Data Meaning:

- **0 = Disabled**
- **1 = Enabled (default)**
- **2 = Limited**
- **3 = Manual**
- **4 = Advanced**

Admins and attackers both use these.

---

8. ElevenForum

Trusted site for:

- Registry solutions
- Windows updates
- Troubleshooting guides

---

9. Event Viewer

Tracks EVERY important activity in Windows.

Open with:

eventvwr.msc

Logs:

- Application
- System
- Security
- Windows Defender
- Installation logs

---

10. Event Viewer for Malware Analysis

Used for:

- Detecting malware installation time
- Checking application crashes
- Tracking unauthorized logins
- Seeing defender alerts
- Correlating events to understand the attack timeline

---

11. Reading Application Error Logs

Sample fields:

- Faulting application
- Faulting module (.dll)
- Exception code
- Path of affected file
- Process ID

Example exception:
0xc0000409 = Buffer overrun → possible exploit attempt

---

12. System Logs

Located in:
Windows Logs → System
Shows:

- Hardware errors
- Driver failures
- Service crashes

Useful for root-cause analysis.

---

13. Windows Defender Logs

Path:
Applications and Services Logs → Microsoft → Windows → Windows Defender → Operational

Shows:

- Threat detected
- Removed
- Quarantined
- Blocked behaviors

---

14. User Login Security Logs

Event IDs:

Event ID	Meaning
4624	Successful login
4625	Failed login
4634	User logged off
4647	User initiated logoff

Used to detect:

- Unauthorized access
- Brute-force attempts
- Suspicious login times

---

15. Why Event Viewer is Essential in Cybersecurity

- Tracks malware footprints
- Helps reconstruct attack timeline
- Detects persistence mechanisms
- Shows user activities
- Helps verify if Defender blocked or missed an attack

✅ **CONCLUSION**

Lecture 9 explains the backbone of Windows OS internals:

✓ **Registry**

Controls system behavior. Malware modifies registry keys for persistence.

✓ **Event Viewer**

Tracks EVERYTHING — errors, logs, attacks, user activity. Critical for digital forensics.

✓ **Malware Analysis**

Uses Registry + Event Viewer to find:

- When malware entered
- How malware ran
- What files were affected
- What user triggered it
- If antivirus reacted

Learning these concepts makes you capable of:

- Troubleshooting
- Detecting malware
- Performing basic forensics
- Securing Windows systems

🧠 **MINDMAP (Text Format)**

LECTURE 9

```
|
├── Windows Registry
|     ├─ Location: %SystemRoot%\System32\Config
|     ├─ Edit via: regedit
|     ├─ 5 Root Keys
|     |     ├─ HKU
|     |     ├─ HKCU
|     |     ├─ HKLM
|     |     ├─ HKCR
|     |     └─ HKCC
|     ├─ Keys → Subkeys → Values
|     └─ Malware modifies Run / RunOnce keys
|
├── Windows Defender Registry Control
|     ├─ Enable/Disable features
|     └─ Admin & attackers use same keys
|
├── Event Viewer (eventvwr.msc)
|     ├─ Application Logs
```

```
|     ├─ System Logs
|     ├─ Security Logs (4624, 4625, 4634, 4647)
|     └─ Defender Logs
|
├── Malware Analysis
|     ├─ Check Run/RunOnce paths
|     ├─ Check crash logs
|     ├─ Correlate timestamps
|     └─ Validate file paths & DLL integrity
|
└── Tools
      ├─ ElevenForum
      └─ Registry Editor
```

🎯 MOST IMPORTANT INTERVIEW QUESTIONS + DETAILED ANSWERS

---

1. What is the Windows Registry?

Answer:
Windows Registry is a central database that stores configuration settings for the operating system, hardware, users, and installed applications. It controls how Windows behaves.

---

2. Where is the Registry physically stored?

Answer:
In this folder:

%SystemRoot%\System32\Config

These files cannot be edited directly — they are edited through regedit.

---

3. Name the 5 root keys of the Registry.

Answer:

1. HKEY_USERS
2. HKEY_CURRENT_USER
3. HKEY_LOCAL_MACHINE
4. HKEY_CLASSES_ROOT
5. HKEY_CURRENT_CONFIG

Each root key stores different system and user data.

---

4. Why do attackers modify registry keys?

Answer:
Attackers modify registry keys to:

- Maintain persistence
- Auto-run malware after reboot
- Disable Windows Defender
- Disable security services
- Modify system behavior

Run/RunOnce keys are the most commonly misused.

---

5. Which registry keys are used to detect malware persistence?

Answer:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\...\RunOnce

Unknown executables here may indicate malware.

---

6. What is Event Viewer?

Answer:
Event Viewer is a Windows tool that logs system events such as:

- Application crashes
- Security logins
- System warnings
- Malware detections
- Driver failures

Used for troubleshooting and forensics.

---

7. How do you open Event Viewer?

Answer:
Press **Win + R** → type **eventvwr.msc** → Enter.

---

8. What are the main log categories in Event Viewer?

Answer:

- **Application**
- **System**
- **Security**
- **Windows Defender logs**
- **Setup logs**

---

9. Which Event IDs are used to check logins?

Answer:

- **4624** – Successful login
- **4625** – Failed login
- **4634** – Logged off

- **4647** – User initiated logoff

---

10. How does Event Viewer help in malware analysis?

Answer:

- Shows the exact time malware executed
- Shows which DLLs crashed
- Shows installation attempts
- Shows Defender detection logs
- Helps correlate user behavior
- Identifies persistence mechanisms

---

11. What does Exception Code 0xc0000409 mean?

Answer:
This code means **Stack Buffer Overrun**, often caused by:

- Memory corruption
- Exploit attempts
- Malware manipulating memory

---

12. How do you check Windows Defender logs in Event Viewer?

Path:

Applications and Services Logs

→ Microsoft

→ Windows

→ Windows Defender

→ Operational

---

13. Why is the Registry dangerous to modify?

Answer:
Because incorrect registry edits can:

- Break system boot
- Disable important services
- Crash Windows
- Make system unstable

Therefore, edits must be done carefully.

---

14. What is HKLM used for?

Answer:
HKLM stores:

- System-wide configuration
- Drivers
- Installed applications
- Security policies
- Windows services

Applies to every user.

---

15. What is HKCU used for?

Answer:
HKCU stores personal settings for the **current logged-in user** such as:

- Wallpaper
- Themes
- Software preferences