Tool Name: Active Directory Explorer (AD Explorer)

Name: Suraj Balanagouda Nadagoudra

---

1. Introduction

What is Active Directory?

Active Directory (AD) is a directory service developed by Microsoft that stores information about users, computers, and other resources in a network. It allows administrators to manage permissions and access to networked resources.

In simple terms, Active Directory is like a database that keeps track of who is allowed to access what within a Windows-based network. It contains details like user names, passwords, groups, organizational units (OUs), and computers.

Why is it Important in Cybersecurity and Digital Forensics?

Active Directory plays a major role in security because: - It manages user authentication (logins). - It controls who can access which resources. - It logs activities that can help detect malicious behavior.

In digital forensics, AD can help trace: - Unauthorized access attempts - Privilege escalations - Insider threats

What is AD Explorer and Who Uses It?

AD Explorer (Active Directory Explorer) is a free tool developed by Microsoft Sysinternals. It allows users to: - Explore and navigate the structure of Active Directory. - Inspect objects and attributes. - Take snapshots of AD data. - Compare snapshots to see changes over time.

Who uses it? - Cybersecurity analysts - System administrators - IT auditors - Digital forensic investigators

2. Tool Overview

Developer Details

- **Developer:** Microsoft (Sysinternals Suite by Mark Russinovich)

Tool Type and Licensing

- **Type:** Free utility
- **License:** Freeware (for personal and commercial use)

Installation Method

- No installation required.
- It is a standalone executable file (portable tool).
- Simply download and run.

System Requirements

- Windows 7 or later
- .NET Framework is not required
- Administrative privileges may be required for full access

---

3. Detailed Features

Interface Overview

- Simple GUI with navigation pane on the left and details pane on the right.
- Top menu bar contains buttons for snapshots, search, and export.

AD Tree Browsing

- You can view the hierarchy of the domain.
- Includes Users, Groups, OUs, Computers, etc.
- Expandable nodes for easy navigation.

Object Attribute Inspection

- Click any object to see its attributes.
- Attributes include userPrincipalName, SID, groupMembership, etc.

Snapshots and Change Tracking

- Take a snapshot of the current AD state.
- Load snapshots later for offline viewing.

- Compare two snapshots to find differences.

LDAP Search Filtering

- Perform LDAP queries to find specific users or groups.
- Example: Find all members of a specific group.

Bookmarking

- Save frequently accessed objects for quick access later.

Exporting Data

- Export snapshot data to a file for further analysis.

Security of the Tool

- Read-only access by default.
- Does not modify any AD data.
- Safe for audit and investigation.

---

4. Step-by-Step Usage Guide

Step 1: Download and Run AD Explorer

1. Visit the official Sysinternals site.
2. Download **ADEXPLORER.EXE**.
3. Double-click the executable to run it.

Step 2: Connect to an AD Domain or Load a Snapshot

- **To connect to live domain:**
  - Go to **FILE > CONNECT**.
  - Enter domain controller address or select default.
- **To load a snapshot:**
  - Go to **FILE > LOAD SNAPSHOT**.
  - Browse to saved snapshot file.

Step 3: Take a Snapshot

1. Connect to the AD.
2. Go to **FILE > CREATE SNAPSHOT**.
3. Choose location to save **.DAT** snapshot file.

Step 4: Compare Snapshots

1. Load the first snapshot.
2. Go to **File > Compare to Snapshot**.
3. Select the second snapshot.
4. Tool shows added, removed, or changed objects.

Step 5: Search Using Filters

1. Click on **Search > Find** or **Ctrl+F**.
2. Enter LDAP filter (e.g., **(memberOf=CN=Domain Admins,DC=example,DC=com)**).
3. Click "Search" to see results.

Step 6: Export and Interpret Results

- Use **File > Save Snapshot As** to save AD data.
- Analyze the .dat file or export specific objects.
- Data can be used in reports, audits, or investigations.

5.Screenshots Section (Placeholders)

I have issue with my laptop, so I unable to take screenshots, I learned about this tool, In future I will change this activity pdf with uploaded screenshots.

---

6. Real-World Use Cases

Digital Forensics Investigation

- Investigate account logins, changes in group memberships.
- Compare before/after snapshots to detect unauthorized changes.

Insider Threat Detection

- Check if someone was added to privileged groups.
- Monitor changes in user account attributes.

Privilege Escalation Tracking

- Identify if a normal user was added to Domain Admins.
- Trace modification timestamps and object creators.

HR and IT Audits

- Verify employee access permissions.
- List all accounts with administrative privileges.

Disaster Recovery Analysis

- Restore configurations from snapshot references.
- Validate integrity of AD after a recovery.

---

7. When to Use the Tool

Timeline of an Investigation

- **Start:** Load AD Explorer to view current domain state.
- **Middle:** Take snapshots and compare.
- **End:** Export data for case documentation.

Before/After Critical System Changes

- Take snapshots before applying patches.
- Compare with post-update snapshot to ensure no AD corruption.

Regular Audit Checklists

- Weekly or monthly checks of group memberships.
- Review high-privilege accounts.

Incident Response Workflow

1. Take live snapshot.
2. Load old snapshot.
3. Compare for anomalies.
4. Export and report.

---

8. Who Should Use It?

- **Digital Forensic Analysts:** To investigate security incidents.
- **System Administrators:** To manage and monitor AD structure.
- **Security Auditors:** To verify compliance with security policies.
- **Blue Team / SOC Teams:** For post-attack analysis and monitoring.

---

9. Skill Requirements

- Basic knowledge of how Active Directory works.
- Familiarity with Windows Server environment.
- Understanding LDAP (Lightweight Directory Access Protocol).
- Ability to read AD object attributes and interpret them.

---

10. Limitations and Suggestions

Limitations

- No real-time monitoring or alerts.
- Cannot modify or fix AD data (read-only tool).
- Snapshot file is in proprietary format (.dat).
- No built-in report generation.

Suggestions for Improvement

- Add auto-snapshot scheduling.
- Allow exporting to JSON or CSV.
- Add integration with SIEM tools.
- Include visual graph of AD structure.

---

11. Comparison with Other Tools

Tool	Purpose	Strength	Weakness
AD Explorer	Read-only AD analysis	Simple UI, snapshot diff	No real-time data
ADUC	Admin tasks	Built-in Windows tool	No snapshot or comparison
PowerView	Red team enumeration	PowerShell automation	Complex for beginners
LDP.exe	Lightweight Directory Protocol client	Native AD testing	Technical and raw
Bloodhound	AD attack paths	Graph-based, powerful	Not beginner-friendly

---

12. Conclusion

AD Explorer is a powerful yet simple tool for understanding and investigating Active Directory environments. It's especially helpful in forensic investigations and audits, where it provides safe, read-only access to AD data.

For interns and beginners, it is an excellent starting point to learn: - How AD objects are structured - How to search and compare changes - How to prepare audit-ready reports

It's a must-learn tool for every cybersecurity enthusiast working in a Windows environment.

13. Appendix

Glossary of Terms

- **OU:** Organizational Unit
- **DN:** Distinguished Name
- **LDAP:** Lightweight Directory Access Protocol
- **SID:** Security Identifier

Example LDAP Queries

- **(OBJECTCLASS=USER)** – Find all users
- **(MEMBEROF=CN=DOMAIN ADMINS,DC=EXAMPLE,DC=COM)** – Find domain admins

References / Useful Links

- https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer
- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/
- https://www.ldapexplorer.com/en/ldap-attributes.htm