How to Backup Active Directory: A Step-by-Step Guide

blog.netwrix.com/how-to-backup-active-directory

Microsoft Active Directory (AD) is the primary authentication service used by a majority of organizations worldwide (roughly 90 percent). It stores critical business information on domain controllers (DCs) like user accounts, their permissions, the number of computers in your organization's network, etc. In other words, it's critical infrastructure. However, many businesses still don't understand just how important it is to back up Active Directory. If an outage were to occur, your organization would lose an estimated $100,000 per day, according to the latest research findings. While those numbers are scary, they likely represent the impact of only the most severe Active Directory recovery scenarios. Still, these figures should be reason enough for your business to take AD backup seriously.

This guide will explore the ins and outs of how to back up Active Directory Domain Controller (AD DC). Learn about the best practices, tools and methods, and how to perform different types of backups.

Why is Active Directory Backup Important?

There are several factors that can lead to Active Directory DC becoming unavailable, which includes cyber attacks, human error, natural disasters, and power outages. AD outages caused by one or a combination of these factors can have several effects on your business. Apart from the immediate financial losses we mentioned initially, your business may also experience:

- **Data Losses:** Without efficient Active Directory backups, your business risks losing important AD data, such as user account information, permissions, and configurations. Without these pieces of information, important business processes may be severely affected.
- **Reputational Damage:** Delayed recovery efforts due to a lack of AD backups may end up affecting your organization's reputation, especially if the outage affects critical business functions and services that customers need.
- **Loss of Employee Productivity:** If employees can't access the resources they need to do their work, their productivity may decrease while waiting for the restoration of your organization's network.

Active Directory backups can help prevent all of the above by creating a copy of all the data stored in the AD that you can retrieve in case of an outage. These backups should be part of the larger recovery strategy that ensures Active Directory downtimes don't last too long or severely affect your operations.

Tools and Methods for Active Directory Backup

Below are the steps involved in conducting a Windows Server Backup.

Full Server Backup

A full server backup, commonly referred to as a full backup, aims to restore “everything.” It creates a copy of all the volumes or partitions on the server, including all the applications and operating systems, as well as the system state.

This AD backup allows for bare metal recovery (BMR), which allows you to transfer all the recovered data from a full server backup onto a new physical server or virtual machine (VM).

To perform a full AD backup, you can use two methods:

Method 1: Using Windows Server Backup GUI

1. Log in to the server with the appropriate administrative privileges.

2. On the Windows Start menu, search for the backup utility by typing “Windows Server Backup” and click on it to launch it.

3. On the left pane of the Windows Server Backup console, you’ll see two options: “Backup Once” and “Backup Schedule.” Since we’re performing a one-time backup, select “Backup Once.”

4. Choose the “Different options” radio button and click Next.

5. You’ll then have two options; “Full server (recommended)” and “Custom.” Select the “Full server (recommended)” button, then click Next.

6. Specify your backup destination by choosing between “Local drives” or “Remote shared folder.” For simplicity, let’s choose “Local drives” for this guide. Click Next.

7. On the Confirmation Screen, ensure everything is as you want, then click “Backup” to start the backup process.

Method 2: Using Windows Server Backup Command-line Tool (wbadmin.exe)

1. Launch the Command Prompt with administrative privileges.

2. Type the following command to perform a full server backup:

```
wbadmin start backup -backuptarget:\<Drive_letter_to_store_backup\>: -include:\<Drive_letter_to_include\>:
```

3. Press Enter to execute the command.

Handpicked related content:

[Free Guide] Active Directory Security Best Practices

Importance of a Full Server Backup

In the event of a catastrophic failure such as hardware malfunction, cyberattack, or natural disaster, a full server backup ensures that no matter what happens, a business has a fallback option that can restore its operations to the last backup point, minimizing the impact of data loss. Full server backups capture the entire system, including operating system files, applications, and data. This comprehensive snapshot ensures data integrity by preserving the relationships between files and their dependencies.

Backing up All Volumes/Partitions on a Server

By backing up all volumes or partitions, you ensure that all data, including system files, applications, and user data, is included in the backup. Having backups of all volumes or partitions simplifies the recovery process. Instead of restoring individual files or directories, you can restore entire volumes or partitions, reducing the time and effort required to recover from a backup.

Bare Metal Recovery Capabilities

Bare metal recovery is a backup type for restoring a server to a functional state after a catastrophic failure or when setting up a new server. BMR allows you to restore an entire server, including the operating system, system settings, applications, and data, from scratch. This is crucial in the event of hardware failure, corruption, or other disasters that render the server inoperable. BMR can significantly reduce the time required to recover a server compared to reinstalling the operating system and applications manually.

Restoring AD to a New Physical Server or Virtual Machine

Restoring Active Directory to a new physical server or virtual machine involves careful planning and execution to ensure a smooth transition without data loss or service interruptions. Below are the steps and best practices to restore AD to a new physical server or virtual machine.

- Evaluate the hardware or virtualization platform for the new server/VM to ensure it meets the requirements for running AD.
- Install the operating system (Windows Server) on the new server/VM, ensuring it is compatible with the version of AD you are restoring.
- Restore the AD to the new server/VM using most recent backup either using Windows server backup tool or third-party backup software.
- Once the new server/VM is operational and running AD, ensure that it replicates and synchronizes properly with the existing domain controllers.
- If the new server/VM is intended to replace an existing domain controller holding FSMO roles, transfer the FSMO roles (Schema Master, Domain Naming Master, RID Master, PDC Emulator, and Infrastructure Master) to the new server/VM.
- Use the “ntdsutil” or PowerShell commands to transfer the FSMO roles to the new server/VM.

- Perform thorough testing to ensure that AD functionality is restored and that users can authenticate, access resources, and perform domain-related tasks without any issues.
- Verify that Group Policies, DNS settings, and other AD-dependent configurations are functioning correctly.
- Document the steps taken during the restoration process for future reference and auditing purposes.

System State Backup

A system state backup creates a copy of just the essential components required to restore the Active Directory to a functional state. These components may include Active Directory database (NTDS), SYSVOL directory, system registry, boot files, performance monitor configuration files, etc. As such, a system state backup is very important for AD disaster recovery.

You can perform a system state backup in two ways:

Method 1: Using Windows Server Backup GUI

1. First, log in to the server with the appropriate administrative privileges.

2. On the Windows Start menu, search for the backup utility by typing "Windows Server Backup" and click on it to launch it.

3. On the left pane of the Windows Server Backup console, you'll see two options: "Backup Once" and "Backup Schedule." Since we're performing a one-time backup, select "Backup Once."

4. Choose the "Different options" radio button and click Next.

5. In the "Backup Once" page, select the "Custom" option, then click Next.

6. Under "Select Items for Backup," click "Add Items," then check the box next to "System State." Click "OK."

7. If using Windows Server 2008 R2 or Windows Server 2008, select the volumes to include in the backup. Optionally, enable system recovery to include critical volumes.

8. On the "Specify Destination Type" page, select either "Local drives" or "Remote shared folder," then click Next. If backing up to a remote shared folder, enter the path, select access control preferences, and provide user credentials for write access.

9. For Windows Server 2008 and Server 2008 R2, choose "VSS copy backup" on the "Specify Advanced Options" page. Click "Next."

10. Select the desired backup location on the "Select Backup Destination" screen.

11. Review the backup settings and click “Back up” to confirm and start the backup process.

Method 2: Using Windows Server Backup Command-line Tool (wbadmin.exe)

1. Launch the Command Prompt with administrative privileges by searching for “Command Prompt” in the Start menu, right-clicking it, and selecting “Run as administrator.”

2. Type the following command to initiate the system state backup, then press “Enter.”

```
wbadmin start systemstatebackup -backuptarget:<TargetDrive>
```

Replace <TargetDrive> with the destination where you want to store the backup.

Understanding System State Backup

System State Backup ensures that important system configurations, files, and databases are backed up and can be restored in case of system failure, corruption, or other issues. The Active Directory database is the most crucial component of System State backup, which contains information about the entire domain structure, including user and group policies, domain trusts, and security settings. System files, including critical operating system files, boot files, and files required for system startup and operation, are also included in a System State Backup.

Components Included in System State Backup

A System State Backup includes critical components necessary for system recovery. These components may vary slightly depending on the version of Windows Server, but they are typically the same. These components collectively ensure that critical system configurations, databases, and files are backed up.

- **Active Directory Database (NTDS).** This component contains the Active Directory database, which stores information about users, groups, computers, and other objects in the domain.
- **System Registry.** The Windows Registry stores system and application settings. System State Backup includes a snapshot of the registry, allowing for the restoration of registry settings to a previous state if necessary.
- **System Files.** Critical system files, including those required for system startup and operation, are included in the System State Backup. These files ensure the proper functioning of the operating system and applications.
- **COM+ Class Registration Database.** This component contains information about Component Object Model (COM) components and their configuration. COM+ provides a framework for building and deploying distributed applications on Windows platforms.

- **Boot Files.** System State Backup includes boot files required for system startup, such as the Boot Configuration Data (BCD) store, boot manager files, and other boot-related components.
- **Certificate Services Database.** If Certificate Services (PKI) is installed, the Certificate Services database is included. This database stores information about issued certificates, certificate revocation lists (CRLs), and other PKI-related data.
- **SYSVOL Directory.** SYSVOL is a shared directory which stores the server copy of the domain’s public files. It includes Group Policy settings, scripts, and other essential components for domain controllers.
- **Cluster Service.** In clustered environments, the System State Backup includes components related to the Cluster service, which manages high-availability clusters.
- **Internet Information Services Metabase.** If Internet Information Services (IIS) is installed, the IIS Metabase is included in the System State Backup. The Metabase stores configuration settings for IIS websites and applications.
- **Active Directory Certificate Services.** If Active Directory Certificate Services (AD CS) is installed, its database is included. This database stores information about issued certificates and other PKI-related data.

Importance of System State Backup for AD Disaster Recovery

A System State Backup includes critical components of your operating system, the AD database, and ensures that the directory structure and data integrity are preserved during recovery. In the event of a domain controller failure, System State Backup allows you to restore the entire server, including AD, to a previously known good state. System State Backup also serves as a critical component of disaster mitigation strategies, providing a reliable mechanism for restoring the AD database to a consistent and healthy state in the event of database corruption such as hardware failures, software bugs, or improper shutdowns.

Handpicked related content:

Tutorial: Learn the Basics of Active Directory

Third-Party Backup Solutions

Third-party backup solutions offer additional features and flexibility compared to native backup tools and centralized management consoles, allowing IT administrators to manage backup policies, schedules, and recovery operations across multiple servers and endpoints from a single interface. They often incorporate advanced backup techniques such as incremental backups, differential backups, and block-level backups, and typically offer granular recovery options, allowing administrators to restore individual files, folders, applications, and AD objects, such as user accounts, groups, organizational units (OUs), and Group Policy objects (GPOs), or even specific database records without having to perform a full server restore.

Below are some third-party Active Directory backup solutions, each offering unique features and capabilities to meet organizations’ diverse needs.

- Netwrix Recovery for Active Directory
- Veeam Backup & Replication
- Quest Rapid Recovery
- Acronis Backup
- NetBackup by Veritas
- Backup Exec by Veritas
- Dell (formerly Quest) Active Directory Recovery Manager
- Adaxes

Automation of Active Directory Backups

It’s important to automate AD backups as much as possible, as this ensures critical directory data is protected against data loss or corruption. Automated backups require selecting a backup solution that supports automation and setting up a backup schedule within the backup solution to automatically perform AD backups at regular intervals, e.g., daily, weekly, or at other intervals.

Active Directory Backup Best Practices

Even after you back up Active Directory, there are several things you can do to ensure that the restoration process goes smoothly. Some Active Directory backup best practices include:

- Schedule regular backups of Active Directory to ensure that you have up-to-date copies of directory data.
- Configure backup schedules to perform backups at times when AD activity is low to minimize disruptions and ensure consistent backups.
- Perform full server backups or system state backups of domain controllers, as they include critical AD components such as the AD database (NTDS.dit), system registry, SYSVOL directory, and other essential system files.
- Maintain multiple backup copies at separate locations to protect against data loss due to hardware failures, disasters, or ransomware attacks.
- Regularly verify the integrity of AD backups by performing test restores and validation checks.
- Ensure that backup files are not corrupted and can be successfully restored in case of a recovery scenario.
- Store backups both onsite and offsite for redundancy and disaster recovery purposes. Securely store backup files in encrypted and access-controlled storage locations to prevent unauthorized access or tampering.
- Choose backup solutions that offer granular recovery options, allowing you to restore individual AD objects, attributes, or containers without needing to perform a full AD restore.
- Define a backup retention policy to manage backup storage efficiently and comply with regulatory requirements.

- Monitor backup jobs regularly to ensure they complete successfully, implement alerting mechanisms to notify administrators of backup failures.
- Document backup procedures, schedules, and recovery processes to ensure consistency and facilitate troubleshooting.
- Regularly test backup and recovery processes to validate their effectiveness and identify any potential issues or shortcomings.
- Leverage Microsoft Volume Shadow Copy Service, a technology which takes manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use.

Microsoft Volume Shadow Copy Service (Microsoft VSS)

Microsoft Volume Shadow Copy Service is a technology in Microsoft Windows operating systems which allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use. These snapshots can be used for creating consistent backups of data, allowing users to restore files to previous versions or recover from data loss situations.

VSS operates at the block level of the file system and creates a point-in-time copy, or shadow copy, of the volume on which the data resides. This copy is made while the system continues to write to the original volume. It ensures data consistency by temporarily freezing the state of the volume, capturing a snapshot, and then allowing ongoing write operations to resume. VSS is commonly used by many backup solutions to create backups of data without needing to take systems offline or interrupt ongoing operations.

The primary components of VSS include.

- **VSS Service**: This is a Windows service responsible for managing the shadow copy creation process. It coordinates the activities of various VSS components.
- **VSS Requestor**: This is an application or service that initiates the process of creating or restoring a shadow copy.
- **VSS Writer**: This is a component within applications or services that maintain data on the volume. Writers ensure that data is in a consistent state before a shadow copy is created.
- **VSS Provider**: This is a system component that interacts directly with the volume and creates the shadow copies.

Handpicked related content:

[Free Guide] Active Directory Tutorial for Beginners

Recommended Backup Strategy for Active Directory

A comprehensive backup strategy for Active Directory is important; it not only safeguards against data loss but also ensures quick recovery in case of corruption, accidental deletions, or malicious attacks. Below, we outline a recommended backup strategy tailored specifically for Active Directory environments. Below is our recommended backup strategy for Active Directory.

Understand Business Requirements for AD backup

Evaluate the organization's AD environment to understand its complexity, size, and criticality. Identify the number of domains, domain controllers, forests, and any specialized configurations or integrations. Define clear goals and objectives for AD backup. These may include minimizing downtime, meeting regulatory requirements, and supporting disaster recovery efforts. Document detailed requirements for AD backup, including below.

1. Frequency of backups (e.g., daily, weekly)
2. Types of backups (e.g., full, incremental)
3. Storage requirements (e.g., on-premises, cloud)
4. Encryption and security measures
5. Backup retention policies
6. Monitoring and reporting capabilities
7. Integration with existing backup infrastructure
8. Disaster recovery procedures

Determine Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

Consider the impact of system downtime on the business. How much revenue would be lost per hour of downtime? What are the potential costs associated with data loss? Assess the technical capabilities of your backup and recovery infrastructure. Some backup solutions may offer faster recovery times or more frequent backups than others.

Recovery Point Objective (RPO)

RPO refers to the acceptable amount of data loss in the event of a disaster or outage. Determine how frequently data needs to be backed up to meet business requirements. For example, if the RPO is one hour, it means that in the event of a failure, the organization can afford to lose up to one hour's worth of data changes.

Recovery Time Objective (RTO)

RTO refers to the maximum acceptable downtime for a system or service in this case AD. Determine how quickly systems or services need to be restored after a failure. Factors to consider include the time it takes to detect the failure, initiate the recovery process, and restore operations. For example, if the RTO is four hours, it means that systems should be restored and operational within four hours of a failure.

Consider the cost implications of achieving specific RPOs and RTOs. More aggressive RPOs and RTOs typically require more sophisticated and expensive backup and recovery solutions. Document the agreed-upon RPOs and RTOs in your disaster recovery plan.

Handpicked related content:

[Free Guide] How to Create Strong Password Policies for Better AD Security

Backup Frequency and the 3-2-1 Backup Rule

How often you should perform backups of your data refers to the backup frequency. Consider how frequently your data changes. Data that changes frequently may require more frequent backups to minimize data loss in the event of a disaster. The RPO is the terminology that determines the maximum acceptable amount of data loss. Backup frequency should be aligned with the RPO to ensure that backups capture changes within the acceptable window. Assess your storage capacity and available resources for performing backups. More frequent backups may require additional storage space and computational resources.

The 3-2-1 backup rule is a best practice for data backup and disaster recovery. It suggests creating multiple copies of your data and storing them in different locations to ensure redundancy and protection against various failure scenarios.

3: Maintain at least three copies of your data. This includes the original data and two backup copies.

2: Store the backup copies on at least two different types of storage devices or media. For example, you might use a combination of external hard drives, network-attached storage, tape drives, or cloud storage.

1: Keep at least one backup copy in a different physical location from the primary data and other backups or offsite. This provides protection against disasters such as fires, floods, or theft that could affect all copies stored in the same location.

When determining backup frequency and implementing the 3-2-1 backup rule, it is important to regularly review and adjust your backup strategy based on changes in data volume, business needs, and technological advancements. Regular testing of backups is also important to ensure their reliability and effectiveness in restoring data when needed.

Choosing a Secure Backup Storage Solution

It’s important to do your research when selecting a backup storage solution. Below are some considerations.

- Choose backup solutions that support encryption both in transit and at rest. This ensures that your data is protected from unauthorized access, whether it’s being transferred over the network or stored on backup media.
- Implement access controls to restrict who can access and manage backups. Use strong authentication mechanisms such as multi-factor authentication (MFA) and role-based access control (RBAC) to prevent unauthorized access.

- If using on-premises storage solutions, ensure that physical access to backup servers and storage devices is restricted to authorized personnel only. Consider using locked server rooms or data centers with strict access controls.
- Choose backup solutions that offer redundancy and fault tolerance to ensure high availability of your data. Implementing redundant storage architectures such as RAID or distributed storage systems helps mitigate the risk of data loss due to hardware failures.
- Store backup copies offsite or in a different geographical location to protect against local disasters such as fires, floods, or theft. Consider using cloud-based backup solutions or rotating backup media to offsite locations regularly.

Implementing Backup Testing Procedures

Implementing backup testing procedures ensures the reliability and effectiveness of your backup and recovery strategy. These objectives may include verifying backup integrity and assessing recovery time. Consider the below points when implementing backup testing procedures.

- Create detailed test plans that outline the specific scenarios, procedures, and criteria for testing backups. Include information such as the types of backups to be tested, the frequency of testing, and the expected outcomes.
- Establish a schedule for conducting backup tests regularly. Consider testing both incremental and full backups. Test various recovery scenarios, including full system restores, individual file restores, and application-specific restores.
- Evaluate whether the recovery time objectives are met and identify any bottlenecks or inefficiencies in the recovery process.
- Test the backup scheduling, notification mechanisms, and error handling procedures.
- Document the results of backup tests, including any issues encountered, deviations from expected outcomes, and areas for improvement.
- Ensure that backup testing procedures remain aligned with organizational goals and industry best practices.
- Monitor backup performance metrics, such as backup success rates and recovery times, to identify trends and potential issues proactively.

How Netwrix Can Help

While native Windows tools offer basic backups, Netwrix Recovery for Active Directory, part of the Netwrix AD security and ITDR solutions portfolio, empowers organizations to achieve a more robust AD disaster recovery strategy.. Key features include:

- Recovery of deleted user and computer objects, fully reanimated with all attributes restored
- Quick and flexible rollback of unwanted changes to any recorded state
- DNS rollback and recovery to any recorded state, preventing spoofing and data loss due to accidental change or malicious attack

- Domain controller backup for AD forest recovery
- Customizable snapshot scheduling to meet recovery point objectives (RPOs)
- Role-based Access Control (RBAC)

Conclusion and Recommendations

Active Directory is a critical component of many organizations' IT infrastructure, managing permissions and access to network resources. Ensuring that you have a backup strategy for AD can prevent the issues that might arise from data loss, corruption, or accidental deletion.

Importance of Crafting a Comprehensive Backup Strategy

An effective backup strategy involves a thorough analysis of your organization's data to prioritize backup efforts. This includes identifying the most critical data, understanding its frequency of change, and considering regulatory compliance requirements. In crafting such a strategy, it's important to implement a combination of regular and consistent backups using varied methods such as full, incremental, and differential backups. This approach ensures that the latest data is continuously and securely captured, minimizing potential data loss.

Recommendations for Protecting AD Infrastructure

Protecting your AD infrastructure requires a multi-layered approach that encompasses technical measures, comprehensive policies, and continuous vigilance. Regularly reviewing and updating your security strategy in line with evolving threats and best practices is vital for maintaining a secure and resilient AD environment. By implementing the recommendations below, organizations can strengthen the security posture of their Active Directory infrastructure and better protect against potential threats and vulnerabilities.

- Use strong access controls and role-based access.
- Keep AD servers and OS up to date with patches.
- Monitor and audit AD activity for suspicious changes.
- Implement multi-factor authentication for added security.
- Deploy network security measures like firewalls and antivirus software.
- Back up AD data regularly and test the recovery plan.
- Educate staff on security best practices and potential risks.
- Leverage built-in AD security features like Kerberos and BitLocker.
- Segregate and secure AD administration duties and tools.
- Consider advanced security solutions like Privileged Access Management (PAM) and SIEM systems for added protection.

Importance of Regular Reviews and Update of Backup Strategy

Your current backup strategy might cover all the essentials as of now, but with the rapid rate of digital transformation, will it still be as effective six months down the line? Regularly reviewing and updating your backup strategy ensures that it remains relevant and adaptable to the evolving needs and challenges of your organization. Embrace changes in technology, business requirements, and industry best practices to stay ahead of potential threats. You can mitigate the risk of data loss and operational disruptions.

Handpicked related content:

- Everything You Need to Know About AD Ransomware Attacks

FAQ

How do I back up my Active Directory?

You can back up Active Directory by performing a full server backup or system state backup. To do this, you can either use the Windows Server GUI or command-line tool.

How many types of backup are there in Active Directory?

There are two main ways you can backup Active Directory: full server backup and system state backup.

How do I back up Active Directory users and computers?

You cannot backup Active Directory users and computers (ADUC); it is a tool to manage AD objects. AD users and computers will back up when you perform a full server backup, however.

How do I back up Azure Active Directory?

AD provides backup features for only object-related backups and only for 30 days. There are other Azure Backup features for several other tasks, but not for backing up Azure AD.

How do I back up the Active Directory 2008?

You can use the Windows Server Backup feature to back up Active Directory 2008.

How do I recover Active Directory without backup?

While challenging, it is possible to recover AD without backup. You can leverage several options including the Active Directory Recycle Bin if enabled, rebuilding the AD environment, or using third-party object recovery tools.

How do I restore Active Directory backup in Windows 2003?

Boot into Directory Services Restore Mode (DSRM), open the command prompt, and use the Ntdsutil.exe utility to perform an authoritative restore from a recent backup.

How do I restore Active Directory backups?

You can either do this manually or with the help of third-party recovery tools. Manually, you must boot into DSRM on the domain controller.

What are the three types of backups?

Below are three main types of backups.

Full Backup: A full backup captures an entire dataset, including all selected files, folders, databases, or systems.

Incremental Backup: Incremental backups only capture changes made since the last backup, whether it was a full back up or an incremental backup.

Differential Backup: Differential backups capture changes made since the last full backup.Unlike incremental backups, which only capture changes since the last backup (whether full or incremental), differential backups capture changes since the last full backup.

What are the four types of backup systems?

The four types of backup systems include full, incremental, differential, and copy backup.

What is a full backup?

A full backup, also known as a full server backup, creates a copy of AD data, including the state system, with the aim of restoring AD to its original functionality.

What is a backup method?

A backup AD method refers to how you choose to perform the backup, with there being two primary ways. You can either use the Windows Server Manager or the command-line tool.

What is the best practice for Active Directory backup?

There are several best practices for Active Directory Backup you can implement, including backing up AD regularly, testing to ensure you can restore the backups, and enforcing stringent security measures on the storage.

Where are Active Directory backups stored?

The storage location for AD backups depends on your preference. You can choose to store the backups on local drives, cloud storage, external drives, etc.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University

of Pennsylvania.