



# DIGITAL DISCOVERY & E-EVIDENCE



**VOL. 11, NO. 11**

**REPORT**

**NOVEMBER 1, 2008**

Reproduced with permission from Digital Discovery & e-Evidence, Vol. 11, No. 11, 11/01/2008. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

**BEST PRACTICES**

## Mapping Your Network Architecture: What Attorneys Must Know About Network and Data Management

By CHRIS KNOX AND STACY JACKSON

The landscape of legal discovery is changing. With the shift from paper-based to electronic information, lawyers no longer spend countless hours reviewing boxes of paper documents. Instead, most now spend their time collecting, managing, and reviewing electronic data.

Unlike paper-based discovery—which was a relatively static process—e-discovery is in a perpetual state of change as technology continuously evolves. The most recent changes result from amendments to the Federal Rules of Civil Procedure (FRCP) that compel attorneys to deal with electronic data early in the litigation pro-

cess through the meet and confer conference with opposing counsel. The FRCP changes also allow us to take advantage of the Safe Harbor provision if data is lost or destroyed, but only if we can show there is a good faith and routine operation of our computer systems.

There are many issues involved in managing electronically stored information (ESI) during litigation, but one aspect of which many attorneys are often unaware involves the location and nature of client data and data management procedures. Many attorneys see this information as too technical to address—they figure that all responsibility for data management lies with the IT department. This hands-off approach is a serious mistake.

Every attorney should have a thorough understanding of client data: the types of data a client produces and where to find it, how data flows through client systems, and how and when data is destroyed, altered, or overwritten. In other words, in order to represent the scope of e-discovery effectively, lawyers must enter the courtroom with a thorough understanding of a client's network architecture. Judges are making it abundantly clear that they expect attorneys to be able to knowledgeably discuss their client's data. One way to do this is to create a network map.

**Purpose.** A network map graphically represents the location and flow of an organization's ESI (See Figure 1). While the IT department may already have its own network map, a lawyer's network map serves a different purpose. From a legal perspective, the map should

*Stacy Jackson is corporate counsel with IE Discovery. She has managed IE Discovery's Legal Services team, working directly with client attorneys in charge of cases and coordinating project management to ensure quality deliverables. She can be reached at [SJackson@iediscovery.com](mailto:SJackson@iediscovery.com).*

*Chris Knox is Chief Information Officer at IE Discovery. He has 12 years of project and resource management experience and is responsible for the implementation of strategic initiatives and IT expenditures. He can be reached at [cknox@iediscovery.com](mailto:cknox@iediscovery.com).*

include information about the location and accessibility of data. It should also indicate the complexity of discovery and assist in executing any litigation holds. Optimally, the map will include user information, retention schedules, data accessibility, and the types of systems used throughout the organization.

Creating a network map can be a daunting project that involves a great deal of time from both the Legal and IT departments. But, it's better to plan ahead and have the map ready before litigation begins than to scramble to create one hastily in the middle of a lawsuit.

Following are the steps you should follow to ensure your network map is ready for meet and confers, litigation holds, and invoking a Safe Harbor defense.

## How to Map Network Architecture

Before instituting a litigation hold, counsel should know what information the litigation requires and who is likely to possess that information. A network map can help narrow the list of potential custodians to include in the hold, as well as more accurately target which types of documents to preserve and exempt from normal document retention policies.

- **E-mail Servers:** E-mail servers store the files employees send via e-mail and, sometimes, via PDA. These servers usually contain the largest volume of potentially relevant information, because most business communication—including file sharing—occurs online.

- **Database Servers:** As the name implies, database servers contain databases that are generally a key location for potentially relevant ESI.

- **File Servers:** File servers provide a centralized network repository where users store and share files that often contain relevant ESI.

- **Web Servers:** Web servers store the files that comprise an organization's Internet and intranet sites. Generally, Web servers are not a large source of discoverable information, unless the case revolves around an employee's inappropriate use of the Internet.

- **PDA Servers:** Technically, there is no such term as "PDA servers". However, attorneys should understand that all such devices access a back-end server such as Blackberry Enterprise Server (BES). Depending on how these back-end servers are configured, they could store e-mails that counsel may need to review for a discovery.

- **Virtual Servers:** Virtual servers are created by breaking a single physical server into multiple logical units to increase the server's utilization rate. Depending

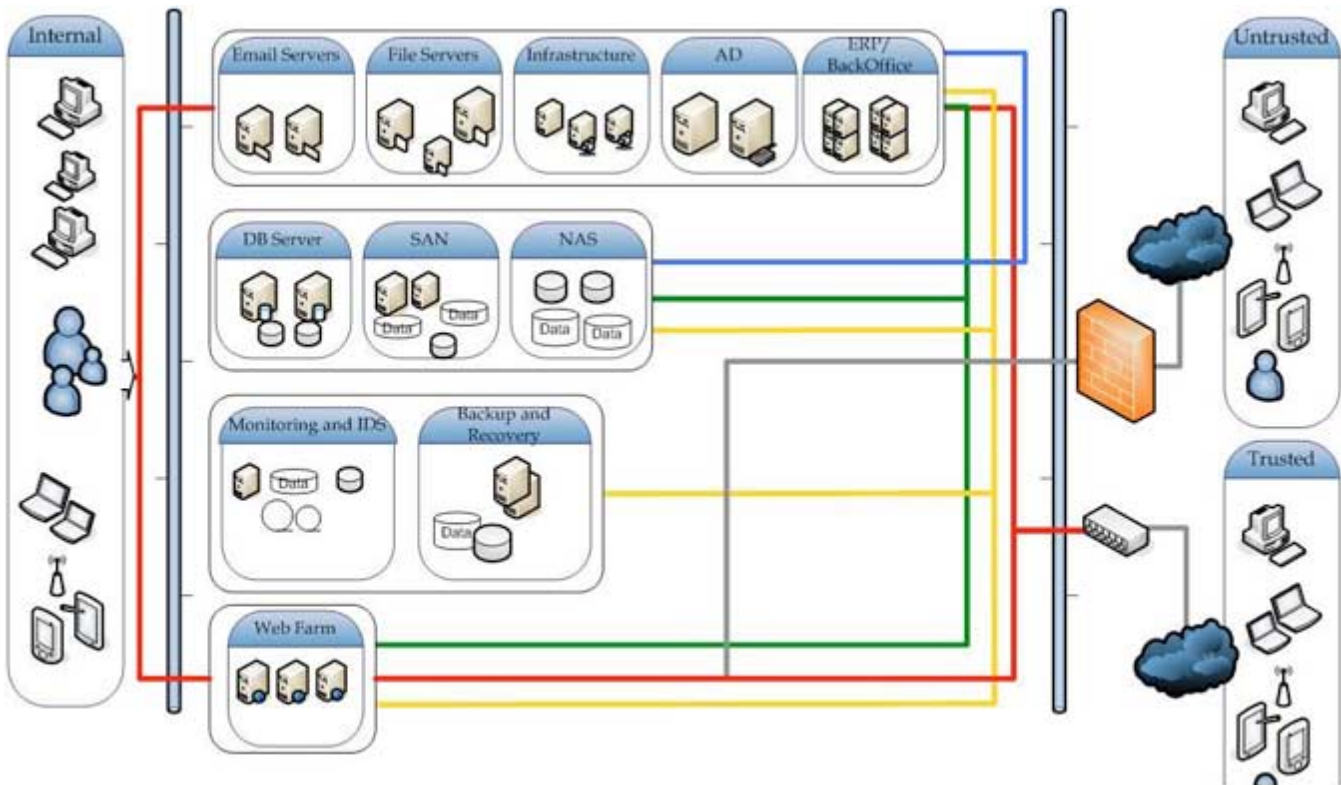


Figure 1 - Example of a Network Map

For many attorneys, delving into the world of network architecture involves learning a new language. Here are a few common technical concepts that every lawyer should understand.

**Servers.** Most organizations have a variety of servers that perform different functions. The most common servers include:

on the functions associated with an organization's virtual servers, they may contain discoverable data.

**Storage.** In addition to understanding server architecture, counsel must also be familiar with the client organization's storage implementation—including hard drives, network-attached storage (NAS), and storage

area networks (SAN)—in order to craft a thorough, yet not overbroad, litigation hold notice.

**Accessible v. Inaccessible Data.** The landmark series of rulings in *Zubulake* divided data into two categories: accessible information that must be produced during discovery and inaccessible that need not be. Under *Zubulake*, data that is active—such as that on a user’s desktop—is considered accessible, as is data that is stored in nearline or offline devices. Nearline storage includes removable media—devices like magnetic disks, CDs, and DVDs—that can be quickly accessed even though they are not directly integrated into a system. Offline storage refers to media—like magnetic tape and zip drives—that is separate from the network and requires more than a few seconds of human intervention (in other words, more effort than popping a CD into a desktop system) to access.

Inaccessible data refers to data that is created specifically for backup purposes, as well as erased and damaged data. Counsel should bear in mind that not every jurisdiction will necessarily consider backup data inaccessible if it is easy and inexpensive to access. Also, remember that as technology changes, data in formats that we currently consider inaccessible may be considered accessible in the future.

### STRUCTURE OF A TYPICAL IT DEPARTMENT

#### **Database Administrator (DBA)**

- Responsible for all aspects of the databases

- Includes recoverability, integrity, security, performance

#### **Help Desk Technician**

- Supports staff on corporate and desktop applications

- Liaison with IT – typically most ‘face time’ with corporate staff

#### **Network Engineer**

- Designs servers, network devices, storage, and security

- Source of network map

#### **Systems Administrator**

- Executes designs from the network engineer and technical architect

- Working knowledge of servers and applications

#### **Systems Analyst**

- Performance and design analysis on specific systems

- Expert in a few systems; big picture of overall architecture

#### **Technical Architect**

- Designs interaction between hardware, software, and network devices

- High-level map of applications and network infrastructure

#### **Developer**

- Implements specific applications

- Expert in a few systems; big picture of overall architecture

## Questions to Ask IT

Legal and IT should work together when creating a network map to develop standards and expectations about what to include. IT experts can answer many critical questions, including:

- **Physical Inventory:** The network map should include information about how many servers, laptops, and desktops the organization has, along with information about equipment such as PDAs and cell phones.

- **Application Inventory:** Counsel also needs to know *how many* applications the organization uses and *how* those applications are used. Don’t forget to include operating systems, spam-filtering systems, and third-party applications, such as virus checking programs and e-mail archiving systems.

- **Application Logging:** Counsel should also ask the IT department whether is currently in place. Application logging captures ephemeral data—data that changes or is quickly discarded by systems, like IP addresses—that the court may request depending on the nature of the case.

- **Accessibility:** Even small organizations often produce tremendous amounts of ESI, so counsel should understand how much of that data that is both accessible and inaccessible. The IT department can also explain how external access to your network is controlled and tracked.

- **Security:** Security features are another important aspect of network mapping, since issues like biometrics and data encryption can expand the boundaries of network architecture. Also, counsel should understand what regulatory compliances and certifications are currently in place, as adherence to these protocols may affect an organization’s data management strategy.

- **Non-Traditional Applications:** Many younger employees rely heavily on non-traditional applications like Instant Messaging (IM), and text messaging. Currently, there are few good ways to log this type of data, so it’s likely that an organization’s IT department isn’t currently capturing this potentially discoverable information.

- **Third-Party Applications:** Many organizations work with third-party vendors that utilize software as a service (SaaS) models in which applications containing organizational data are stored outside of the client network. Despite the fact that such data is stored offsite, it is still discoverable. Third-Party applications should raise two red flags for you: (1) what is the document retention policy, i.e. do they follow their policy or your policy; and (2) how will you implement a litigation hold and preserve the data held by the third-party.

- **Disaster Recovery/Business Continuity:** Almost every organization these days has a disaster recovery and business continuity plan. These plans should be thoroughly and routinely tested, and they should include external data centers that are on stand-by in case of an emergency.

- **Records Retention:** When it comes to records retention, IT has different goals than Legal. Counsel should ensure that IT is in full compliance with the corporate retention plan and that it includes a routine maintenance schedule.

- **Patch Management:** Security patches are an issue that most attorneys leave to the IT experts; however, counsel should understand that patches can alter the

way that operating systems work, affecting data movement and storage.

■ **Future Plans:** Attorneys must communicate regularly with the IT department about future technology plans. The Legal department needs to know about new technologies the IT department is considering, including any outsourcing initiatives, new backup technologies, different e-mail archiving methods and business continuity planning. The legal department should also be aware of how future trends—such as the adoption of social engineering technologies, virtual environments, and cloud and grid computing—could change the network map. Finally, Legal should be involved in any technical contract negotiations to ensure consistency with the corporate legal strategy.

### Preventing Sanctions Through A Documented, Routine Process

Under the Safe Harbor clause in the FRCP, the court cannot impose sanctions for spoliation on ESI that is lost during the “routine, good-faith operation of an electronic information system.” However, organizations cannot take advantage of the Safe Harbor clause if they cannot clearly demonstrate the implementation of routine processes. *Doe v. Norwalk Community College*, 2007 WL 2066496 (D. Conn. July 16, 2007).

Counsel should understand the organization’s backup procedures, including how backup materials are stored, how often tapes are destroyed or reused, whether material is backed up completely or incrementally, and whether any backup tapes are in a legacy format. Counsel should also confirm that IT consistently adheres to the backup plan.

### Security Considerations for Sharing a Network Map

Creating a network map that is appropriate for use in litigation is a balancing act. If the map is too high-level, the court may view it as unresponsive because it lacks enough information. On the other hand, if the map is too detailed, it may enable opposing counsel to easily identify and challenge holes in the client’s electronic information systems.

Additionally, very detailed network maps are difficult to maintain due to ongoing incremental changes. Ideally, a network map should contain an overview of technical systems that is just detailed enough to be highly readable at first glance with enough information for opposing counsel to determine the “buckets of information” that you have.

### What to Look for in Your Opponent’s Network Map

When viewing your opponent’s network map, consider how it compares to yours. Does it include the

same general information? If not, those gaps could hide potentially relevant information.

If the map is highly detailed, study it carefully throughout the discovery process to determine whether your opponent has, indeed, produced all potentially relevant information from the sources that you know exist. Remember that if the map is too general, you may have an indication that your opponent will be unresponsive during litigation.

#### UNDERSTANDING IT STAFF

##### **Executive Level**

- Best source for strategic-level discussions
- Understands the interdependencies of the various disciplines
- Most likely very little hands-on understanding

##### **Management Level**

- Best source for detailed discussion within their functional specialty
- Detailed understanding of independent disciplines
- Likely to understand all functions of staff-level operations (hands-on)

##### **Staff Level**

- Best source for detailed discussion specific to task-level activity
- Likely very little understanding of interdependencies of systems even within their own discipline
- Likely to be responsible for collecting data during discovery

### Final Thoughts

When mapping your network architecture, it’s important to keep the end result in mind: a successful discovery. Goals to consider throughout the entire the process include:

- Understanding how information flows through the client organization;
- Knowing what routine maintenance is performed on client systems;
- Knowing who you need to talk to in IT;
- Understanding high-level technical terminology;
- Discussing future trends in IT that will affect data discovery; and
- Going in with a plan.

Remember that mapping network architecture is not a speedy, one-time project. It takes a considerable amount of time and resources to create a comprehensive and accurate network map. Also, since technology constantly evolves, network architecture mapping is a dynamic process that you should revisit with IT on a regular basis.