Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.585

활성 상태의 NAS 시스템 상에서 내부 데이터 수집 기법 연구*

서 형 민,† 김 도 현, 이 상 진‡
고려대학교 정보보호대학원

The Method for Data Acquisition on a Live NAS System*

Hyeong-Min Seo,† Dohyun Kim, Sang-Jin Lee‡
Center for Information Security Technologies(CIST), Korea University

요 약

최근 데이터의 대용량화로 인해 스토리지 시장이 커짐에 따라 디지털 포렌식 관점에서 클라우드 및 USB, 외장 하드와 같은 저장 매체에 대한 연구가 꾸준히 진행되고 있다. 하지만 TB 단위 이상의 대용량 데이터 저장이 가능하며 기업용 저장 장치 뿐만 아니라 개인용 저장 장치로도 많이 사용되고 있는 NAS에 대한 연구는 부족한 실정이다. 본 논문에서는 NAS 제품 중 국내의 시장에서 점유율이 높은 소형 NAS 두 개, 대형 NAS에서 한 개의 제품을 선정하여 활성 상태의 NAS에서 내부 데이터 수집을 위한 디지털 포렌식 조사 절차와 기법을 제안한다.

ABSTRACT

As the storage market has been expanded due to growing data size, the research on various kinds of storages such as cloud, USB, and external HDD(Hard Disk Drive) has been conducted in digital forensic aspects. NAS(Network-Attached Storage) can store the data over one TB(Tera Byte) and it is well used for private storage as well as for enterprise, but there is almost no research on NAS. This paper selects three NAS products that has the highest market share in domestic and foreign market, and suggests the process and method for data acquisition in live NAS System.

Keywords: NAS(Network-Attached Storage), Storage, Digital Forensics

I. 서 론

디지털기기의 발전으로 인해 사진, 동영상, 음악과 같은 많은 멀티미디어 컨텐츠들이 디지털 데이터의 형태로 저장 및 활용되고 있다. 이러한 멀티미디어 컨텐츠들은 고품질의 서비스를 추구하는 대중의 요구에 따라 데이터의 크기도 커지고 있다. 실제로 IT 시장조사 기관인 IDC와 스토리지 기업인 EMC의 '디지털 유니버스 보고서'에 따르면[1], 2013년에 생성된 디지털 데이터의 크기는 4.4조GB이며, 2020년에는 44조GB까지 폭발적으로 증가할 것으로 예상하였다.

하지만 멀티미디어 컨텐츠, 대용량 데이터를 사용하기 위해 주로 사용되는 PC나 스마트폰은 저장 장치의 크기가 작기 때문에 데이터 저장 장치 용도로는 한계를 가지고 있으며, 이에 따라 대용량 데이터를 로컬 저장 장치 대신 효율적으로 관리할 별도의 대용량 저장 장치에 대한 소요가 증가하고 있다.

IT 리서치 회사 가트너에 따르면 스토리지 시장에서 NAS(Network-Attached Storage)가 가장 높

접수일(2015년 2월 3일), 수정일(1차: 2015년 3월 23일, 2차: 2015년 3월 25일), 게재확정일(2015년 4월 8일)
* 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
† 주저자, sylar@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

은 성장세를 보였다. NAS는 그동안 주로 기업용 저장 매체로 인식되었지만 다양한 기능과 저렴한 가격의 소형 제품이 출시되면서 개인 사용자와 SOHO(Small Office Home Office)용으로도 많은 관심을 받으며 기업용 저장 장치 시장에서 개인용 저장 장치 시장으로까지 영역이 확대되었다.

NAS의 수요가 계속 증가함에도 불구하고 디지털 포렌식 관점의 연구는 미미하였다. NAS는 내부 데이터를 하드웨어 RAID(Redundant Array of Independent Disks) 방식을 사용하여 저장하며 제조사별로 자체 개발한 RAID 레벨을 사용하는 등 내부 RAID 구성이 다르기 때문에 NAS에서 저장 장치(HDD, SSD)만을 복제하여 수집하는 경우 볼륨 재구성과 내부 데이터 추출이 어렵다.

또한 형사소송법 106조 3항에 따르면 디지털 저장매체에서 정보를 압수할 경우 범위를 정해 출력하거나 복제하는 것을 원칙으로 한다. 따라서 방대한 데이터를 가지고 있는 NAS의 활성 상태에서 내부 데이터를 선별적으로 수집하는 기법에 대한 연구가 필요하다.

본 논문에서는 NAS 제품 중 전 세계 시장에서 점유율이 높은 'Netgear'와 'Synology' 社의 제품들[2][3]을 대상으로 활성 시스템에서 시스템의 관리자 권한을 획득하여 시스템 기본 정보와 휘발성 정보를 획득하는 방법과 파일이나 파티션 단위로 데이터를 수집하는 방법, 내부 데이터 선별 수집을 위한 메타데이터를 획득하는 방법을 제안하고, 활성 상태에서 NAS 데이터를 수집하는 자동화 도구 "NASExtractor"를 소개한다.

II. 관련 연구 및 NAS 소개

NAS는 네트워크로 연결된 데이터 저장 장치로서 다른 네트워크 클라이언트에 데이터의 접근 권한을 제공하며[4], 설치와 관리가 간편하고 저장 장치의 확장이 용이하다는 특징이 있다.

NAS는 여러 개의 HDD, SDD 등의 저장 장치를 하드웨어 또는 소프트웨어 RAID방식으로 구성하여 사용된다. RAID는 1987년 버클리 연구소의 David A Patterson 등[5]이 발표한 기술로 데이터 구성 등의 설정 방식에 따라 RAID 레벨을 나누고, RAID 레벨에 따라 NAS의 운영 형태를 정할 수 있다.

RAID에 대한 연구는 소프트웨어 RAID의 재구성에 대한 성능 확인 및 개선 방법만 미미하게 진행되었을 뿐 포렌식 관점에서는 이루어지고 있지 않다. 또한 EnCase와 X-Ways Forensics 등의 포렌식 도구에서 RAID 재구성 기능을 지원하나 표준 RAID만 지원하며, 실질적으로 재구성할 때 데이터 영역의 시작 오프셋을 알아야만 볼륨을 재구성할 수 있기 때문에 비활성 상태에서 NAS 데이터를 수집하기 어려운 실정이다. 따라서 활성상태에서 NAS 데이터를 수집하기 위한 접근 방법을 연구할 필요가 있다.

NAS에 저장된 데이터는 인터넷을 이용하여 웹 기반의 File Station을 통해 접근하거나 FTP, Telnet, SSH와 같은 쉘을 이용하여 접근할 수 있다.

NAS에서 제공하는 서비스는 제조사 및 제품별로 지원하는 방식이 다르다. 'Synology' 社에서는 웹 기반의 관리 페이지와 함께 DiskStation Manager(이하 DSM)이라는 클라이언트 프로그램을 제공한다. 'Netgear' 社에서도 마찬가지로 웹 기반의 관리 페이지와 함께 RAIDar라는 클라이언트 프로그램을 제공한다. 따라서 웹 기반의 관리 페이지와 각 NAS들의 클라이언트 프로그램을 통해서 파일을 관리 및 확인할 수 있다.

III. 활성 NAS 시스템의 내부 데이터 수집 기법

NAS를 대상으로 디지털 포렌식 조사를 할 경우에는 대상 데이터들이 방대하고 HDD, SDD 와 같은 저장 장치들이 RAID로 구성되어 있으며 서버 등으로 활용될 수 있음을 고려해야 한다. 또한 NAS 시스템에 영향을 최소화하며 내부 데이터를 수집할 수 있는 접근 방법을 선택해야 한다.

본 논문에서는 RFC3227(Guideline for Evidence Collection and Archiving)[6] 디지털 증거 수집 절차 표준의 기준과 NAS의 특성을 반영하여 [그림 1]과 같이 디지털 포렌식 관점에서 활성 상태의 NAS 시스템에 대한 내부 데이터를 수집하는 절차를 제안한다.

NAS는 다양한 RAID 레벨을 지원하며 제품군에 따라 파일에 접근하기 위해 지원하는 프로토콜이 다양하다. 따라서 디지털 포렌식 관점에서 내부 시스템을 조사하기 위해서는 우선 제품군과 시스템 정보를 파악해야 한다.

시스템 정보를 파악한 후에는 휘발성 정보를 수집해야 한다. 관리자 비밀번호를 알 수 없는 상황에서

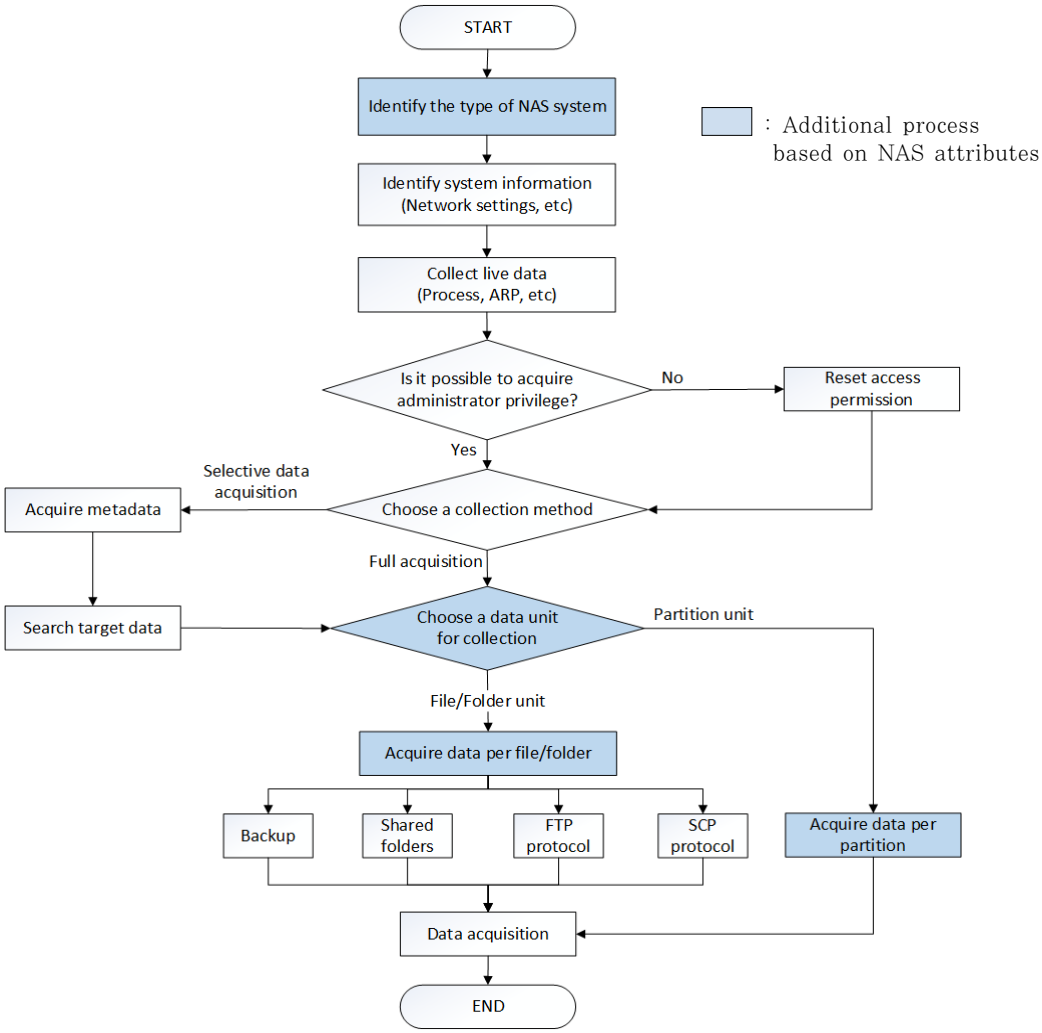

Fig. 1. Flow chart of data acquisition on a live NAS system

는 비밀번호를 초기화하는 과정에서 재부팅이 이루어질 수 있다. 따라서 관리자 권한을 획득하기 전에 휘발성 정보를 수집해야 한다.

제품에 대한 정보 파악과 휘발성 정보를 수집한 후에는 NAS 내부 데이터를 수집하기 위해 관리자 권한을 획득해야 한다. 관리자 권한을 획득하면 폴더 및 파일, 파티션 단위로 내부 데이터를 수집할 수 있다.

NAS는 주로 대용량 저장장치로 사용되기 때문에 일반적으로 내부 파티션의 크기가 매우 크다. 따라서 파티션 단위의 이미징을 수행하기 전에 파티션 내부 데이터들의 메타데이터를 먼저 수집하여 선별적으로 조사 대상 데이터를 수집하는 것이 효율적이다. 이러한 선별 수집단계를 거침으로써 내부 데이터 조사에 소요되는 시간을 줄일 수 있다.

수집 대상 데이터를 선별한 후에는 파티션 단위, 폴더 단위, 파일 단위 등으로 데이터 수집을 진행한다. 수집한 데이터들의 무결성을 훼손하지 않는 것은 중요하나 활성 상태에서 데이터의 무결성을 유지하는 것은 현실적으로 어렵다[7]. 따라서 활성 상태의 NAS에서 수집한 데이터들에 대해 각각 해쉬값을 생성하여 기록하고, 피조사자, 참관인 등 관련자의 확인 서명을 받는 수사 절차가 필요하다. 더불어 수집 시 데이터에 대한 훼손을 최소화하면서 데이터를 추출하여 분석하는 것이 중요하며, 데이터를 최소화하면서 수집하는 다양한 방법을 본 논문에서 제시한다.

3.1 시스템 정보 확인

활성 상태에서 NAS 내부 데이터를 수집하기에 앞서 제품군 확인과 함께 현재 NAS의 네트워크, Shell, 패스워드의 현재 상태와 RAID 레벨, chunk 크기 등의 RAID 및 시스템 정보를 획득해야 한다. 'Synology'와 'Netgear' 社의 NAS 제품들은 리눅스 운영체제를 사용하기 때문에 〔표 1, 2〕와 같은 명령어들을 통해 시스템 정보를 확인할 수 있다.

Table 1. Major internal file check for system information in NAS system

File name	Contents
/proc/cpuinfo	Information about the processor
/proc/devices	List of device drivers configured into the currently running kernel
/proc/diskstats	Displays the I/O statistics of block devices
/proc/filesystems	Filesystem supported by the NAS system
/proc/locks	Kernel locks
/proc/mdstat	Information about RAID
/proc/meminfo	Information about memory usage
/proc/mounts	Information about mounted filesystems
/proc/partitions	Table of partitions known to the system
/proc/slabinfo	Information about memory usage at the slab level
/proc/stat	Overall statistics about the system
/proc/swaps	Information about Swap space utilization
/proc/uptime	The time the system has been up
/proc/version	The kernel version
/etc/sysconfig/clock	Information about timezone
/etc/group	The configured user groups and who belongs to them
/etc/hosts	Information about the host
/etc/resolve.conf	Information about setup the DNS
/etc/crontab	Information about setup the automatic running of system routines

Table 2. Linux commands to check system information in NAS system

Command	Contents
mdadm	Information about RAID (Level, Disk Info.)
mount	Information about mounts a storage device or filesystems
df	Information of device name, total blocks, total disk space, used disk space, available disk space and mount points on a file system
fdisk	Partition table

〔표 1〕은 RAID 및 시스템 정보를 확인하기 위한 내부파일 중 주요 파일들을 나타낸다.

해당 시스템 파일들을 통해 확인한 시스템 정보들 외에도 〔표 2〕와 같은 리눅스 명령어들을 통해 저장장치에 대한 정보를 확인할 수 있다.

해당 시스템 파일들을 통해 확인한 시스템 정보들 외에도 〔표 2〕와 같은 리눅스 명령어들을 통해 저장장치에 대한 정보를 확인할 수 있다.

3.2 휘발성 정보 수집

프로세스와 네트워크, 사용자 로그인 상태 등은 시스템 리부팅을 통해 정보가 삭제될 수 있다. 이러한 정보들을 휘발성 정보라 한다[8]. 휘발성 정보들은 침해 사고 의도를 이해하고자 할 때 매우 중요한 정보로 시스템의 "snap-shot"을 제공한다[9].

휘발성 정보를 수집할 수 있는 명령어는 〔표 3〕과 같다.

Table 3. Volatile information collection command

Command	Contents
ps	Active processes (Process name, PID)
who	Information about all users who are currently logged in
ifconfig -a	Network Interface Card Information
netstat -a	Network connection information
arp -a	Information about hosts in ARP cache table
route	Information about routing table

3.3 접근 권한 획득

일반적으로 NAS는 계정별로 파일 및 폴더에 대한 접근 권한을 부여한다. 따라서 NAS에서 공유하는 모든 파일 및 폴더와 시스템 정보, RAID 레벨 및 네트워크 정보를 확인하기 위해서 관리자 권한이 필요하다. 'Netgear' 제품은 초기 관리자 아이디와 비밀번호를 [표 4]와 같이 설정한다.

만약 관리자 비밀번호를 알 수 없는 상황이라면 비밀번호를 초기화하여 관리자 권한을 획득하여야 한다. 비밀번호를 초기화하더라도 사용자 데이터는 훼손되지 않는다. 비밀번호를 초기화 하는 방법[10]으로는 OS Reinstall, Tech Support 모드 부팅, NAS 펌웨어 업데이트가 있다.

'Synology' 제품에 대해서 관리자 비밀번호를 모르는 경우에는 제품 후면에 있는 RESET 버튼을 누름으로써 비밀번호를 재설정 할 수 있다[11]. 초기 관리자 로그인 아이디와 비밀번호는 [표 5]와 같이 비어 있으므로 아이디만 입력한 후 admin 계정으로 바로 로그인할 수 있다.

Table 4. Default ID and password for 'Netgear'

ID	Password
admin	Netgear1

Table 5. Default ID and password for 'Synology'

ID	Password
admin	-

3.4 데이터 수집

3.4.1 메타 데이터를 활용한 선별 수집

NAS에서 수집 대상 데이터의 선별 방법은 메타 데이터를 획득하는 방법과 리눅스 명령어를 활용하여 조사 대상 데이터를 검색하는 방법으로 나눌 수 있다.

메타 데이터 획득은 선별 수집 과정에서 대상 파일의 원활한 검색을 위해 꼭 필요한 과정이며, 이 과정에서 폴더 및 파일의 이름, 시간 정보, 크기 등의 정보를 획득한다.

메타 데이터는 NAS에서 지원하는 쉘에서 리눅스 명령어 'ls', 'tree'를 통해 획득할 수 있다. 해당 명령어의 옵션에 따라 폴더 및 파일 목록을 생성시간이나 접근시간, 수정시간으로 정렬하여 볼 수 있으며 숨김 파일에 대해서도 확인할 수 있다.

[그림 2]는 'ls -aceplR' 명령어로 파일 및 폴더를 생성시간 기준으로 정렬하여 출력한다. 'a' 옵션은 숨긴 파일을 표시해주며, 'c' 옵션은 파일 생성 시간 순으로 파일을 정렬해준다. 'l' 옵션은 파일 용량과 수정 시간 등의 파일 상세 정보를 보여주며, 'p' 옵션은 파일이 디렉터리일 경우 각 파일명의 뒤에 '/'를 써서 구분해준다. 'R' 옵션은 하위 경로와 그 안에 있는 모든 파일을 나열할 때 사용한다.

[그림 3]은 'ls -aueplR' 명령어로 파일 및 폴더를 접근시간 기준으로 정렬하여 출력한다. u 옵션은 파일의 최종 수정 시간 대신에 파일의 최종 접근 시간으로 보여준다.

[그림 4]는 'ls -aeplR' 명령어로 파일 및 폴더를 수정시간 기준으로 정렬하여 출력한 결과다.

수집된 메타 데이터는 [그림 5]와 같은 명령어를 통해 분석 시스템에 파일로 저장할 수 있다. 따라서

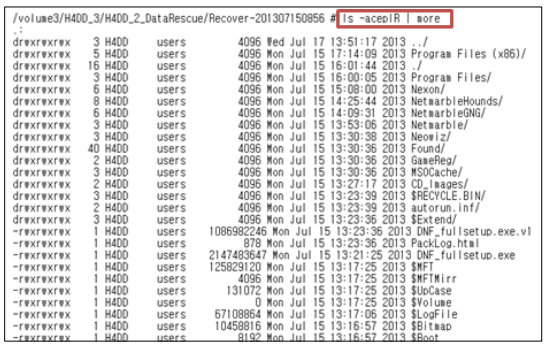

Fig. 2. Arrange by creation time (ls -aceplR)

Fig. 3. Arrange by access time (ls -aueplR)

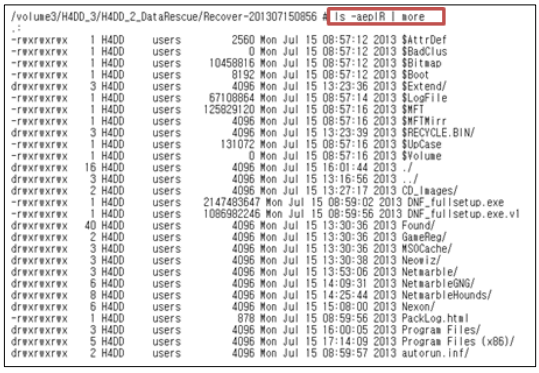

Fig. 4. Arrange by modified time (ls -aeplR)

분석 시스템에서 문서 뷰어 프로그램을 통해 [그림 6]과 같이 원하는 파일을 검색할 수 있다.

메타 데이터를 획득하여 분석 시스템에서 대상 파일을 검색하는 방법 이외에도 NAS에서 지원하는 쉘에서 리눅스 명령어, 'find'와 'grep'을 사용하여 [그림 7]과 같이 관련 파일을 검색할 수 있다.

3.4.2 파일 및 폴더 단위 데이터 수집

파일 및 폴더 단위로 데이터를 수집하는 방법으로는 NAS의 클라이언트 프로그램에서 제공하는 백업

```
ssh root@163.152.127.29 ls -alR / > C:₩output.txt
```

Fig. 5. Command to save a metadata file

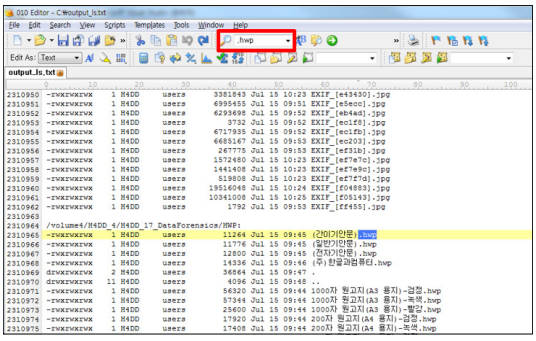

Fig. 6. Search of metadata

```
/volume1/H4DD_1 # find . -name *"한글"* -print
./H4DD_12_DataForensics/(주)한글과컴퓨터.hwp
./H4DD_12_PDR/ProgramData/Microsoft/Windows/Start Menu/Programs/한글과컴퓨터
./H4DD_15_DataForensics/HWP/(주)한글과컴퓨터.hwp
./TEST/TEST_한글
```

```
/volume1/H4DD_1/TEST # find . -type f | xargs grep "내용"
./TEST_English/test.txt:내용
```

Fig. 7. Find a file command

기능을 사용하는 방법과 공유 폴더 기능을 사용하는 방법, FTP/SCP 프로토콜을 사용하는 방법이 있다.

백업, 공유 폴더 설정, FTP 프로토콜을 사용할 경우 각 해당 설정파일이 수정되나, 해당 파일들은 사용자의 데이터가 존재하는 데이터파티션 영역(예: /volume1)에 존재하지 않는다. 따라서 사용자 데이터의 무결성을 최대한 보존할 수 있다.

또한 본 논문에서는 SCP 프로토콜을 소개함으로 파일 및 폴더 단위로 데이터를 수집할 때 포렌식 관점에서 가장 적합한 방법을 제시한다.

3.4.2.1 백업 기능

백업 기능을 통해 내부 데이터를 수집하기 위해서는 해당 NAS 제품이 지원하는 클라이언트 프로그램을 사용해야 한다. 'Netgear'와 'Synology'의 경우 관리자 페이지로 접속하면 백업 기능 메뉴를 확인할 수 있다. 다만 'Netgear ReadyNAS'에서 백업 기능을 사용할 경우 백업된 파일들의 메타데이터는 획득할 수 없는 한계점이 있다. 그러나 'Synology' 에서는 [그림 8]과 같이 메타데이터 백업 활성화 메뉴를 선택함으로써 백업 대상 파일들의 메타데이터를 수집할 수 있다. 수집된 메타데이터는 SQLite Database 포맷으로 저장된다.

'Synology'의 경우 '/var/log/synolog' 경로에 자체적인 로그파일들을 저장하고 있으며, 'synobackup.log' 파일에서 백업한 디렉터리와 시간 등의 정보를 확인할 수 있다.

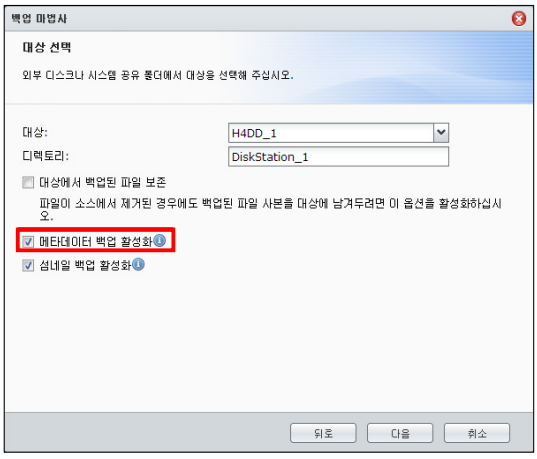

Fig. 8. Metadata backup activation menu in 'Synology'

3.4.2.2 공유 폴더

백업 기능과 마찬가지로 공유 폴더 설정도 해당 제품의 관리자 페이지를 통해서 지정할 수 있다. 또한 Telnet이나 SSH 프로토콜을 이용하여 설정하는 방법도 가능하다.

Telnet 또는 SSH 프로토콜을 이용하여 공유 폴더를 설정하기 위해서는 Samba 서비스 관련 파일을 수정해야 한다. Samba 서비스는 SMB(Server Message Block) 프로토콜을 통해 LAN 환경에서 UNIX-like 서버와 윈도우 클라이언트 간에 파일이나 프린터를 공유할 수 있도록 하는 서비스를 말한다. 따라서 SMB 프로토콜을 통해 분석 PC(윈도우)에서 NAS 시스템을 네트워크 드라이브로 연결할 수 있다. 〔표 6〕은 제품 별 SMB 프로토콜 관련 파일로 설정 시 해당 정보가 수정된다.

Table 6. The relevant file of SMB

Product name	File name	Details
Netgear ReadyNAS	/etc/front-view/Samba/smb.conf	Setup information about shared folder path and access authority
Synology DS412 Plus	/usr/syno/smb.conf	
Synology RS10613xs+	/usr/syno/etc/smb.conf	

3.4.2.3 FTP

FTP(File Transfer Protocol)는 TCP/IP 프로토콜을 가지고 서버와 클라이언트 사이에서 파일을 전송하기 위한 프로토콜로 HTTP와 달리 명령 연결과 데이터 전송용 연결의 2가지 종류가 존재한다. 명령 연결은 먼저 제어 포트인 서버 21번 포트로 사용자 인증 후 명령을 위한 연결이 만들어지면 해당 포트를 통해 클라이언트에서 지시하는 명령어를 전달한다. 데이터 전송용 연결은 실제 파일이 전송될 때 새로운 연결이 이루어지며, 능동과 수동모드 두 가지로 지원한다.

FTP의 활성화 여부는 관리자 페이지에서 확인할 수 있으며, Telnet이나 SSH 프로토콜을 통해서도 확인 및 설정할 수 있다. 〔표 7〕은 제품 별 FTP 프로토콜 관련 파일로 설정 시 해당 정보가 수정된다.

Table 7. The relevant file of FTP

Product name	File name	Details
Netgear ReadyNAS	/etc/front-view/proFTPd/Shares.conf	Shared list
Synology DS412 Plus	/etc/synoinfo.conf	Activation availability, Setup information
Synology RS10613xs+		

3.4.2.4 SCP

SCP(Secure Copy Protocol)는 SSH와 동일한 매커니즘의 파일 전송을 지원하는 프로토콜로 송신 데이터의 신뢰성 및 기밀성을 보장한다.

FTP 프로토콜을 사용하여 다수의 파일을 전송할 경우에는 파일명을 모두 기입해야 하는 불편함이 있는 반면, SCP는 '-r' 옵션을 통해 하위 폴더를 포함하여 디렉터리 전체를 전송할 수 있다. 또한 이전 수집 방법들과는 달리 설정 파일을 수정할 필요 없이 SSH 데몬을 실행함으로써 SCP 프로토콜을 이용할 수 있다. 따라서 시스템에 가장 적은 영향을 미치기 때문에 위의 방법들 중 가장 바람직한 수집 방법이라고 할 수 있다.

3.4.3 파티션 단위 데이터 수집

파티션 단위의 데이터 수집은 분석 시스템 또는 다른 대용량 저장장치로 할 수 있다. 수집할 때는 블록 단위로 파일을 복사 및 변환 해주는 dd 명령어와 SSH 프로토콜(혹은 Telnet 프로토콜)을 사용한다. 윈도우 시스템에서는 SSH 프로토콜을 사용하기 위해서 'PuTTY[1]', 'Xshell[2]'과 같은 별도의 프로그램이 필요하다.

파티션 단위로 데이터를 수집하기에 앞서 수집 대상 파티션을 확인해야 한다. 수집 대상 파티션은 〔그림 9〕처럼 리눅스 명령어 df를 사용하거나 〔그림 10〕과 같이 '/proc' 경로에 존재하는 partitions 파일을 통해 확인할 수 있다.

1) http://www.chiark.greenend.org.uk/~sgtatham/putty/
2) http://www.netsarang.co.kr/download/down_xsh.html

```
~ # df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/md0               2451064    619808   1728856  26% /
/tmp                    506804       656    506148   0% /tmp
/dev/md2             3841041872 1739955416 2100984056  45% /volume1
/dev/md3             3841041872  63679208 3777260264   2% /volume2
/dev/md4             3841041872 148843736 3692095736   4% /volume3
/dev/md5             3841041872 405770472 3435169000  11% /volume4
```

Fig. 9. The 'df' command

```
~ # cat /proc/partitions
major minor  #blocks  name

   8        0 3907018584 sda
   8        1    2490240 sda1
   8        2    2097152 sda2
   8        3 3902297440 sda3
   8       16 3907018584 sdb
   8       17    2490240 sdb1
   8       18    2097152 sdb2
   8       19 3902297440 sdb3
   8       32 3907018584 sdc
   8       33    2490240 sdc1
```

Fig. 10. The 'cat /proc/partitons' command

3.4.3.1 분석 시스템으로의 데이터 수집

분석 시스템에서 'ssh root@NAS_IP_주소 dd if=해당파티션 | dd of=저장경로' 명령어를 〔그림 11〕과 같이 입력하면 해당 NAS의 파티션에 대한 이미지 파일이 저장된다. 저장된 이미지 파일은 〔그림 12〕와 같이 포렌식 도구로 확인할 수 있다.

3.4.3.2 대용량 저장 장치로의 데이터 수집

NAS 시스템은 대용량 저장장치로 보통 테라바이트(TB) 급의 데이터가 저장되어 있다. 따라서 분석 시스템으로 데이터를 수집하기에는 시스템 파티션을 저장하지 않는 이상 저장 공간의 문제점이 생긴다.

```
C:₩Users₩JHCHOI>ssh root@163.152.127.30 dd if=/dev/md0 | dd of=c:₩md0.dd
rawwrite dd for Windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL.  See copying.txt for details
Could not create directory '/home/JHCHOI/.ssh'.
The authenticity of host '163.152.127.30 (163.152.127.30)' can't be established.

RSA key fingerprint is c7:74:bc:44:a5:b0:27:b7:9f:80:9b:1d:a6:cb:c7:0b.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/JHCHOI/.ssh/known_hosts
).
root@163.152.127.30's password:
Error reading file: 109 파이프가 끝났습니다
8386536+0 records in
8386536+0 records out
8386536+0 records in
8386536+0 records out
4293906432 bytes (4.3 GB) copied, 378.016 seconds, 11.4 MB/s
```

Fig. 11. Data collection command in the analysis system

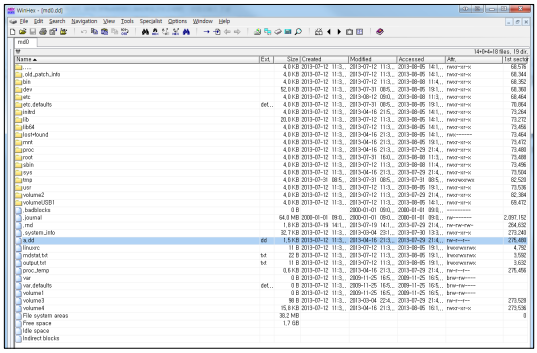

Fig. 12. Confirm the .dd file

따라서 〔그림 13〕과 같이 데이터를 수집하고자 하는 NAS 장비에서 다른 NAS로 해당하는 파일을 전송하는 과정이 필요하다.

분석 시스템에서 수집하고자 하는 활성 상태의 NAS 장비에 접근한 후 〔그림 14〕와 같이 명령어를 사용하면 해당 파티션의 이미지 파일을 다른 NAS 장비에 저장할 수 있다.

Fig. 13. Configuration of data acquisition in the mass storage device

```
~ # dd if=/dev/md0 | ssh root@163.152.127.30
    dd of=/md0.dd
root@163.152.127.30's password:
```

Fig. 14. Data collection command of as a mass storage device

IV. 활성 NAS 내부 데이터 수집 도구 소개

현재까지 확인한 주요 시스템 정보 및 수집 기법을 바탕으로 보다 사용이 용이하도록 C#을 이용하여 윈도우 폼으로 수집 도구를 〔그림 15〕와 같이 개발하였다.

해당 도구는 4개의 영역으로 나누어 구현하였다. 관리자 권한을 획득하기 위해 ①번 영역에서 해당 NAS 장비의 아이피 주소와 아이디, 패스워드를 입력한다. 입력이 완료되면 ③번 영역에서 RAID 레벨과 같은 주요 정보들을 확인할 수 있다. ②번 영역에서는 해당 파티션을 이미징 할 수 있는 기능과 검색

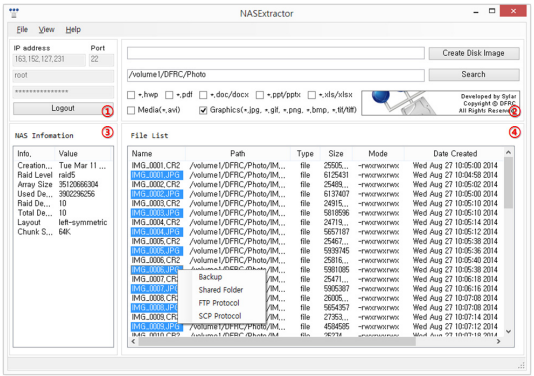

Fig. 15. Data acquisition tool on a live NAS system

기능을 제공한다. 검색 기능을 통해서 선별 수집이 가능하며, 검색 결과는 ④번 영역에서 확인 가능하다. 수집할 대상의 파일들을 선택하고 마우스 오른쪽 버튼을 누르면 수집할 방법들이 표시된다. 가능한 수집 방법을 선택하고, 저장 경로를 선택함으로써 파일을 수집할 수 있다. 수집한 파일들에 대해서는 SHA-1, SHA-256, MD5 해쉬 함수를 통해 해쉬 값을 생성하고 해당 값을 텍스트 파일로 저장한다.

V. 결 론

본 논문에서는 대용량 저장장치 NAS에 대해 활성 상태에서 데이터를 수집하는 절차를 디지털 포렌식 관점에서 연구하였다. 활성 상태에서 NAS에 저장된 데이터 수집 방법으로 메타데이터 및 파일 · 폴더 단위 선별 수집과 대용량 데이터의 수집 방법을 소개하고, 이 연구 결과를 바탕으로 활성 상태의 NAS에서 데이터를 수집하는 도구를 개발하였다.

클라우드와 같이 NAS에서 제공하는 서비스의 형태가 다양해짐에 따라 향후에는 해당 서비스의 아티팩트들을 분석하고 도구에 적용할 예정이다. 또한 RAID 구성 방법에 따른 수집 및 분석 방법 연구를 바탕으로 활성 상태뿐만 아니라 비활성 상태에서의 데이터 수집 및 분석 방법에 대해서도 추가 연구할 계획이다.

References

[1] EMC Inc, "The Digital Universe of Opportunities," http://korea.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf, Apr. 2014.

[2] Howard Miller, "Network-Attached Storage Market Study," Academia.edu, pp. 3-8, Nov. 2012.

[3] NAS Ranker, http://www.smallnetbuilder.com/tools/rankers/nas/ranking/RAID5/rev4/39

[4] NAS Wikipedia, http://en.wikipedia.org/wiki/Network-attached_storage

[5] David A Patterson, Garth Gibson, and Randy H Katz, "A Case for Redundant Arrays of Inexpensive Disks," SIGMOD Conference, vol. 1, pp. 109-116, Jun. 1988.

[6] RFC3227, "Guidelines for Evidence Collection and Archiving," http://www.faqs.org/rfcs/rfc3227.html, Feb. 2002.

[7] Matthew J. Decker, "Dispelling Common Myths of Live Digital Forensics," Digital Forensics Certification Board, White Papers, Sep. 2011.

[8] Hwang Hyun-Uk, Kim Min-Soo, Noh Bong-Nam, and Lim Jae-Myung, "Computer forensics: The trend and technology of system forensics," Journal of The Korea Institute of information Security & Cryptology, vol. 13, no. 4, pp. 1-14, Aug. 2003.

[9] KISA, "Guide to computer emergency analysis procedure," KISA guide 2010-8, pp. 24-25, Jan. 2010.

[10] NETGEAR Inc, "ReadyNAS NVX Business Edition User Manual," http://www.readynas.com/download/documentation/UM/ReadyNASnvx_UMv1.1_12Feb09.pdf, pp. 28-29, Feb. 2009.

[11] Synology Inc, "Synology NAS User's Guide Based on DSM 4.2," https://ukdl.synology.com/download/Document/UserGuid

e/DSM/4.2/Syno_UsersGuide_NAServe
r_enu.pdf, p. 100, May. 2013.

〈저자소개〉

서 형 민 (Hyeong-Min Seo) 학생회원
2013년 3월: 광운대학교 전자정보공과대학 컴퓨터소프트웨어학과 공학사
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 디지털 포렌식, 정보보호

김 도 현 (Do-Hyun Kim) 학생회원
2011년 2월: 서울과학기술대학교 정보통신대학 컴퓨터공학 공학사
2011년 3월~2013년 8월: 고려대학교 정보보호대학원 정보보호학과 공학석사
2013년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 디지털 포렌식, 모바일 포렌식

이 상 진 (Sang-jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수