

NIST 800-86

# 사고 대응에 포렌식 기술을 통합하는 가이드

NIST : 국립 표준 기술 연구소  
(National Institute of Standards and Technology)

Karen Kent

Suzanne Chevalier

Tim Grance

Hung Dang

(Translation by ringga)

# 목 차

## 0. 요 약

### 1. 소개

#### 1.1 권위(Authority)

#### 1.2 목적과 범위

#### 1.3 대상 독자

#### 1.4 간행물 구조

## 2. 포렌식 역량 수립과 구성

### 2.1 포렌식의 필요성

### 2.2 포렌식 직원 채용(Staffing)(?)

### 2.3 다른 팀들과의 상호 작용

### 2.4 정책

#### 2.4.1 역할 및 책임 정의

#### 2.4.2 포렌식 도구 사용에 대한 지침 제공

#### 2.4.3 정보 시스템 수명 주기의 포렌식 지원

### 2.5 지침 및 절차

### 2.6 권고 사항

## 3. 포렌식 절차 수행

### 3.1 데이터 수집

#### 3.1.1 가능한 데이터 소스 식별

#### 3.1.2 데이터 수집

#### 3.1.3 사고 대응 고려사항

### 3.2 검사

### 3.3 분석

### 3.4 보고

### **3.5 권고 사항**

## **4. 데이터 파일들의 데이터를 사용**

### **4.1 파일 기본 사항**

#### **4.1.1 파일 저장 매체**

#### **4.1.2 파일시스템**

#### **4.1.3 미디어 상의 기타 데이터**

### **4.2 파일 수집**

#### **4.2.1 매체에서 파일 복사**

#### **4.2.2 데이터 파일 무결성**

#### **4.2.3 파일 수정, 액세스 및 생성 시간**

#### **4.2.4 기술적 문제**

### **4.3 데이터 파일 검사**

#### **4.3.1 파일 찾기**

#### **4.3.2 데이터 추출**

#### **4.3.3 포렌식 툴킷 사용**

### **4.4 분석**

### **4.5 권고 사항**

## **5. 운영 체제의 데이터 사용**

### **5.1 OS 기초**

#### **5.1.1 비휘발성 데이터**

#### **5.1.2 휘발성 데이터**

### **5.2 OS 데이터 수집**

#### **5.2.1 휘발성 OS 데이터 수집**

##### **5.2.1.1 포렌식 도구 준비**

##### **5.2.1.2 휘발성 OS 데이터 유형**

##### **5.2.1.3 데이터 수집의 우선 순위 지정**

#### **5.2.2 비 휘발성 OS 데이터 수집**

### 5.2.3 데이터 수집과 관련된 기술적 문제

### 5.3 OS 데이터의 조사와 분석

### 5.4 권고 사항

## 6. 네트워크 트래픽 데이터 사용

### 6.1 TCP/IP 기본 사항

#### 6.1.1 응용 계층

#### 6.1.2 전송 계층

#### 6.1.3 IP 계층

#### 6.1.4 하드웨어 계층

#### 6.1.5 네트워크 포렌식에서 계층의 중요성

### 6.2 네트워크 트래픽 데이터 출처

#### 6.2.1 방화벽 및 라우터

#### 6.2.2 패킷 스니퍼 및 프로토콜 분석기

#### 6.2.3 침입 탐지 시스템

#### 6.2.4 원격 액세스

#### 6.2.5 보안 이벤트 관리 소프트웨어

#### 6.2.6 네트워크 포렌식 분석 도구

#### 6.2.7 다른 출처들

### 6.3 네트워크 트래픽 데이터 수집

#### 6.3.1 법적 고려 사항

#### 6.3.2 기술적 문제

### 6.4 네트워크 트래픽 데이터 조사 및 분석

#### 6.4.1 관심있는 이벤트 식별

#### 6.4.2 데이터 출처 검사

#### 6.4.2.1 데이터 소스 값

#### 6.4.2.2 검사 및 분석 도구

#### 6.4.3 결론 짓기

#### **6.4.4 공격자 식별**

#### **6.5 권고 사항**

### **7. 응용 프로그램의 데이터 사용**

#### **7.1 응용 프로그램 구성 요소**

##### **7.1.1 구성 설정**

##### **7.1.2 인증**

##### **7.1.3 로그**

##### **7.1.4 데이터**

##### **7.1.5 지원하는 파일**

##### **7.1.6 응용 프로그램 아키텍처**

#### **7.2 응용 프로그램의 유형**

##### **7.2.1 이메일**

##### **7.2.2 웹 사용**

##### **7.2.3 대화형 통신**

##### **7.2.4 파일 공유**

##### **7.2.5 문서 사용**

##### **7.2.6 보안 응용 프로그램**

##### **7.2.7 데이터 익제 도구**

#### **7.3 응용 프로그램 데이터 수집**

#### **7.4 응용 데이터 검사 및 분석**

#### **7.5 권고 사항**

### **8. 여러 소스의 데이터 사용**

#### **8.1 의심되는 네트워크 서비스 월 감염**

#### **8.2 이메일 위협**

#### **8.3 권고사항**

### **부록 A**

### **부록 B**

**B.1 시나리오 질문**

**B.2 시나리오들**

**부록 C, D, E, F, G**

## 0. 요약

포렌식은 일반적으로 법에 과학을 적용하는 것으로 정의됩니다. 디지털 포렌식(컴퓨터 및 네트워크 포렌식이라고도 알려짐)에는 많은 정의가 있습니다. 일반적으로 정보의 무결성을 유지하면서 데이터에 대한 엄격한 관리 연속성(Chain of Custody)을 유지하면서 데이터 식별, 수집, 검사 및 분석에 과학을 적용하는 것으로 간주됩니다. 데이터는 특정 방식으로 형식이 지정된 디지털 정보의 고유한 부분을 나타냅니다. 조직은 많은 출처에서 점점 더 많은 양의 데이터를 보유하고 있습니다. 예를 들어, 데이터는 다른 소스들 중에서도 표준 컴퓨터 시스템, 네트워킹 장비, 컴퓨팅 주변 장치, 개인용 정보 단말기 (PDA), 소비자 전자 장치 및 다양한 유형의 미디어에 의해 저장되거나 전송될 수 있습니다.

다양한 데이터 소스로 인해 디지털 포렌식 기법은 범죄 및 내부 정책 위반 조사, 컴퓨터 보안 사고 재구성, 운영 문제 해결 및 실수로 인한 시스템 손상 복구와 같은 다양한 목적으로 사용될 수 있습니다. 실질적으로 모든 조직은 디지털 포렌식(이 가이드의 나머지 부분에서 포렌식이라고 함)을 수행할 수 있어야 합니다. 이러한 기능이 없으면 조직은 보호되고 민감한 데이터의 노출과 같은 시스템 및 네트워크에서 발생한 이벤트를 확인하는 데 어려움을 겪습니다. 이 안내서는 정책 및 절차의 개발을 포함하여 포렌식 능력 확립에 대한 자세한 정보를 제공합니다. 주로 컴퓨터 보안 사고 대응을 지원하기 위해 포렌식 기법을 사용하는데 중점을 두고 있지만 대부분의 자료는 다른 상황에도 적용됩니다.

서로 다른 조직이 서로 다른 법률 및 규정의 적용을 받기 때문에 이 문서를 디지털 포렌식 조사 를 수행하는데 사용하거나 법률 자문으로 해석하거나, 범죄 활동 조사의 기초로 사용해서는 안됩니다. 대신 조직은 해당 지침을 법률 자문위원, 법 집행 공무원 및 관리가 제공하는 광범위한 지침과 함께 포렌식 능력 개발을 위한 출발점으로써의 가이드로 사용해야 한다.

디지털 포렌식 수행 프로세스는 다음과 같은 기본 단계로 구성됩니다:

- 1) 수집(Collection) : 데이터의 무결성을 보존하는 절차에 따라 관련 데이터의 가능한 출처에서 데이터를 식별, 라벨링, 녹음 및 수집합니다.
- 2) 검사(Examination) : 자동 및 수동 방법의 조합을 사용하여 수집된 데이터를 포렌식적으로 처리하고 특정 데이터를 평가 및 추출하면서 데이터의 무결성을 보존합니다.
- 3) 분석(Analysis) : 합법적으로 정당한 방법과 기술을 사용하여 조사 결과를 분석하여, 수집 및 시험 수행에 대한 자극이었던 질문을 다루는 유용한 정보를 얻습니다.
- 4) 보고(Reporting) : 사용된 행위에 대한 묘사를 포함한 분석 결과 보고, 도구 및 절차 선택 방법 설명, 수행해야 할 작업 결정(예 : 추가 데이터 소스의 포렌식 검사, 확인된 취약성 보안, 기준 보안 개선) 절차, 도구 및 포렌식 프로세스의 다른 측면에 대한 개선을 위한 권장 사항을 제공합니다.

운영 체제, 네트워크 트래픽 및 응용 프로그램 등이 있습니다. 이 가이드는 각 범주의 데이터 소스의 기본 구성 요소와 특성을 설명하고, 각 범주의 데이터를 수집, 검사 및 분석하는 기술에 중

점을 둡니다. 또한, 이 가이드는 여러 데이터 원본을 함께 사용하여 이벤트를 더 잘 이해할 수 있는 방법에 대한 권장 사항을 제공합니다.

다음 권장 사항을 시행하는 것은 연방 부서 및 기관들을 위해 효율적이고 효과적인 디지털 포렌식 활동을 용이하게 할 것이다.

조직은 법 집행 기관에 연락하고 모니터링을 수행하고 포렌식 정책 및 절차에 대해 정기적으로 검토하는 등 모든 주요 포렌식 고려 사항을 다루는 명확한 진술을 정책에 포함해야 합니다.

높은 수준에서 정책은 권한이 부여된 직원이 적절한 상황에서 합법적인 이유로 시스템과 네트워크를 모니터링하고 조사를 수행 할 수 있도록 허용해야 합니다. 조직은 사건 처리자 및 포렌식적인 역할을 가진 다른 사람을 위한 별도의 포렌식 정책을 가질 수도 있습니다. 이 정책은 적절한 행동에 관한 보다 상세한 규칙을 제공합니다. 포렌식 정책은 조직의 포렌식 활동을 수행하거나 지원하는 모든 사람들과 외부 조직의 역할과 책임을 명확하게 정의해야 합니다. 이 정책은 다른 상황에 있는 내부 팀과 외부 조직에 누가 문의해야 하는지 명확하게 지시해야 합니다.

조직은 조직의 정책과 모든 적용 가능한 법률 및 규정을 기반으로 포렌식 작업을 수행하기 위한 절차 및 지침을 작성하고 유지 관리해야 합니다.

가이드 라인은 가능한 모든 상황에 맞는 포괄적인 절차를 개발하는 것이 현실적이지 않기 때문에 포렌식 기법을 사용하여 사건을 조사하기 위한 일반적인 방법론에 초점을 맞추어야 합니다. 그러나 조직에서는 일상적인 작업을 수행하기 위한 단계별 절차 또한 고려해야 합니다. 지침과 절차는 일관성 있고 효과적이며 정확한 조치를 용이하게 해야 하며, 특히 기소 또는 내부 징계 조치로 이어질 수 있는 사건에 중요합니다. 포렌식적으로 건전한 방식으로 증거를 처리하면 의사 결정권자는 자신이 필요한 조치를 취할 수 있는 입장에 놓이게 됩니다. 지침과 절차는 증거 수집 및 처리, 도구 및 장비의 무결성 유지, 관리 보관성(Chain of Custody) 유지, 적절한 증거 보관에 대한 정보를 포함하여 법적 절차에 대한 증거의 허용 가능성을 지원해야 합니다. 전자 기록 및 기타 기록을 변경하거나 달리 조작 할 수 있으므로, 조직은 해당 기록의 무결성을 입증하기 위해 정책, 지침 및 절차를 통해 준비되어야 합니다. 지침과 절차는 팀의 정책과 절차에 중대한 변경이 있을 때 뿐만 아니라 주기적으로 검토되어야 합니다.

조직은 정책과 절차가 포렌식 도구를 합리적으로 적절하게 사용하도록 보장해야 합니다.

조직의 정책과 절차는 다양한 상황에서 법의학 조치가 수행되어야 하는 것과 수행되어서는 안되는 것을 명확하게 설명하고 암호, 개인 데이터(예: 사회 보장 번호)나 전자 메일의 내용과 같은 포렌식 도구로 기록될 수 있는 민감한 정보에 대한 필요한 안전 장치를 설명해야 합니다. 법률 고문은 모든 포렌식 정책과 높은 수준의 절차를 주의 깊게 검토해야 합니다.

조직은 IT 전문가가 포렌식 활동에 참여할 준비가 되어 있는지 보장해야 합니다.

사고 처리자 및 기타 사고 대응자와 같은 IT 전문가는 포렌식을 위한 그들의 역할과 책임을 이

해하고 포렌식 관련 정책 및 절차에 대한 훈련과 교육을 받아야하며, 그들이 담당하는 기술이 사건이나 다른 사건의 일부일 때 다른 사람들과 협력하고 다른 사람들을 도울 준비가 되어 있어야 한다. IT 전문가는 수행해야 하는 작업과 수행하지 말아야 할 작업을 결정하는 것과 같은 포렌식 활동을 위한 일반적인 준비와 구체적인 포렌식 상황을 논의하기 위해 필요할 때마다 법률 고문과 긴밀히 상의해야 합니다. 또한, 경영진은 법의학 기능 지원, 법의학 정책 검토 및 승인, 업무 핵심 시스템을 오프라인 상태로 만드는 것과 같은 특정 포렌식 조치 승인에 대한 책임을 져야 합니다.

## 1. 소개

### 1.1 권위(Authority)

국립 표준 기술 연구소(NIST)는 2002년 연방 정보 보안 관리법(FISMA), 공법 107-347에 의거하여 법적인 책임을 증진하기 위해, 이 문서를 개발했습니다.

NIST는 모든 기관 운영 및 자산에 대해 적절한 정보 보안을 제공하기 위한 최소 요구 사항을 포함하여 표준 및 지침을 개발할 책임이 있습니다. 그러한 기준과 지침은 국가 보안 체계에는 적용되지 않는다. 이 지침은 관리 예산처(OMB) Circular A-130, Section 8b (3), Securing Agency Information Systems의 요구 사항과 일치합니다.—A-130, 부록 IV : 주요 섹션 분석에서 분석한 바와 같이— 보충 정보는 부록 A-130에 수록되어 있습니다.

이 가이드라인은 연방 기관에서 사용할 수 있도록 준비되었습니다. 비정부기구가 자발적으로 사용할 수 있으며, 저작자 표시가 필요하지만 저작권의 대상이 아닙니다. 이 문서의 어떤 내용도 법무부 장관이 연방 당국에 의무적으로 구속력을 갖는 표준 및 지침을 위배하지 않아야 하며, 이 지침은 현행 상무부 장관, OMB 관리자 또는 기타 연방 공무원이 기존 당국의 것을 변경하거나 대체하는 것으로 해석되어서는 안됩니다.

이 지침은 범죄 행위 조사와 관련하여 법 집행 요원에게 구속력을 행사해서는 안됩니다.

### 1.2 목적과 범위

이 간행물은 조직이 컴퓨터 및 네트워크 법의학 수행에 대한 실질적인 지침을 제공함으로써, 컴퓨터 보안 사고를 조사하고 일부 정보 기술(IT) 운영 문제를 해결하는데 도움을 주기 위한 것입니다. 이 가이드는 법 집행의 관점이 아닌, IT 관점에서 포렌식을 제시합니다. 특히, 해당 간행물은 효과적인 포렌식 활동을 수행하는 프로세스를 설명하고 파일, 운영 체제(OS), 네트워크 트래픽 및 응용 프로그램과 같은 다양한 데이터 소스에 대한 조언을 제공합니다.

해당 간행물은 디지털 포렌식 조사를 수행하거나, 법률 자문으로 해석되는 포괄적인 단계별 안내서로 사용해서는 안됩니다. 그 목적은 다양한 기술과 사고 대응이나 문제 해결 활동을 수행하는데 사용할 수 있는 잠재적인 방법을 독자들에게 알리기 위한 것입니다. 독자는 자신의 상황과 관련된 법률 및 규정(즉, 지방, 주, 연방 및 국제)에 대한 준수 여부를 경영진 및 법률 고문과 상의 한 후에 권장 사례를 적용하는 것이 좋습니다.

### 1.3 대상 독자

이 간행물은 수사, 사고 대응, 문제 해결 목적에 대한 포렌식 수행을 위해 책임을 져야 하는 사고 대응팀; 포렌식 분석가; 시스템, 네트워크 및 보안 담당자; 그리고 컴퓨터 보안 프로그램 관리

자를 위해 작성되었습니다.

이 가이드에서 권장하는 방법은 전자 증거의 처리 및 검사와 관련된 주요 원칙을 강조하기 위해 고안되었습니다. 전자 장치 및 소프트웨어, 포렌식 절차 및 도구의 끊임없이 변화하는 특성으로 인해, 독자는 이 가이드에 제시된 것보다 더욱 자세한 정보를 얻기 위해, 이 가이드에 나열된 리소스를 비롯한 다른 리소스를 참조해야 합니다.

## 1.4 간행물 구조

이 간행물의 나머지 부분은 7개의 주요 섹션으로 나뉩니다.

- 1) 2절에서는 컴퓨터 및 네트워크 포렌식에 대한 필요성을 논의하고 조직의 포렌식 기능을 수립하고 조직하는 방법에 대한 지침을 제공합니다.
- 2) 3절에서는 컴퓨터 및 네트워크 포렌식 수행과 관련된 기본 단계인 데이터 수집, 검사, 분석 및 보고에 대해 설명합니다.
- 3) 4절에서 7절은 3절에서 설명한 프레임 워크를 기반으로 다양한 데이터 소스의 데이터를 수집, 검토 및 분석하는 세부 정보를 제공합니다. 4절에서 7절에 설명된 데이터 소스 카테고리는 각각 데이터 파일, OS, 네트워크 트래픽 및 애플리케이션입니다.
- 4) 8절에서는 분석을 통해 여러 데이터 소스 간의 이벤트를 서로 연관시키는 방법을 보여주는 사례 연구를 제시합니다.

이 간행물에는 다음 자료가 포함된 여러 부록이 들어 있습니다.

- 1) '부록 A'는 이 간행물에서 제기된 주요 권고 사항을 제시합니다.
- 2) '부록 B'는 포렌식 기법이 유용할 수 있는 시나리오를 제시하고 독자에게 각 시나리오와 관련된 일련의 질문을 요구합니다.
- 3) '부록 C'와 'D'는 각각 용어집과 두문자어 목록을 포함합니다.
- 4) '부록 E'는 인쇄 리소스를 나열하고 '부록 F'는 포렌식 기능을 설정하거나, 포렌식 도구 및 기법을 이해하는데 유용한 온라인 도구 및 리소스를 나타냅니다.
- 5) '부록 G'에는 발행물에 대한 색인이 들어 있습니다.

## 2. 포렌식 역량 수립과 구성

데이터라는 용어는 특정 방식으로 형식이 지정된 디지털 정보의 고유한 부분을 나타냅니다. 전문적이고 개인적인 용도와 네트워킹의 보급에 대한 컴퓨터의 확장으로 인해 많은 출처에서 증가하는 양의 데이터를 기록하고 분석할 수 있는 도구가 필요했습니다. 예를 들어, 데이터는 표준 컴퓨터 시스템(예: 데스크톱, 랩톱, 서버), 네트워킹 장비(예: 방화벽, 라우터), 컴퓨팅 주변 장치(프린터), 개인용 정보 단말기(PDA), CD, DVD, 이동식 하드 드라이브, 백업 테이프, 플래시 메모리, 썬드라이브 및 점프 드라이브에 의해서 저장되거나 이동될 수 있습니다. 많은 전통적이지 않은 소비자 전자 장치(예: 휴대폰, 비디오 게임 콘솔, 디지털 오디오 플레이어, 디지털 비디오 레코더)를 사용하여 데이터를 저장할 수도 있습니다. 이렇게 다양한 데이터 소스가 증가하면서, 포렌식 도구와 기술 개발 및 개선에 박차를 가하는 것에 많은 도움이 되었습니다. 이러한 포렌식 도구의 발전은 범죄 수사, 컴퓨터 보안 사고 재구성, 운영 문제 해결 및 돌발적인 시스템 손상으로부터 복구와 같은 도구 및 기술을 다양한 목적으로 사용할 수 있다는 사실로 인해 야기되었습니다.

이 섹션에서는 조직의 포렌식 기능을 구성하는 몇 가지 측면에 대해 설명합니다. 그것은 포렌식에 대한 잠재적인 다양한 용도를 보여줌으로써 시작하고 포렌식 과정에 대한 높은 수준의 개요를 제시합니다. 섹션의 다음 부분에서는 포렌식 서비스가 일반적으로 제공되는 방법에 대해 설명하고 포렌식 태스크를 수행하는 데 필요한 기술을 구축하고 유지하는 방법에 대한 지침을 제공합니다. 또한, 법률 고문 및 물리적 보안 직원과 같은 다양한 팀을 포렌식(forensic) 활동에 포함시킬 필요성을 설명합니다. 이 절은 정책, 지침 및 절차에서 포렌식(예: 역할 및 책임 정의, 도구 및 기술의 올바른 사용법에 대한 지침 제공, 정보 시스템 수명주기에 포렌식 포함)을 다루는 방법을 논의함으로써 끝납니다.

이 가이드에 제시된 기술 및 프로세스는 디지털 포렌식의 원칙을 기반으로 합니다. 포렌식은 일반적으로 법에 과학을 적용하는 것으로 정의됩니다. 디지털 포렌식(컴퓨터 및 네트워크 포렌식이라고도 함)에는 많은 정의가 있습니다. 일반적으로 정보의 무결성을 보존하고 데이터에 대한 엄격한 관리 연속성(Chain of Custody)을 유지하면서 데이터 식별, 수집, 검사 및 분석에 과학을 적용하는 것으로 간주됩니다. 서로 다른 조직이 서로 다른 법률 및 규정의 적용을 받기 때문에, 이 서적을 디지털 포렌식 조사를 수행하는데 사용하거나 법률 자문으로 해석하거나 범죄 행위 조사의 기초로 사용해서는 안됩니다. 대신 조직에서는 법률 자문위원, 법 집행 공무원 및 관리가 제공하는 광범위한 지침과 함께 포렌식 기능을 개발하기 위한 출발점으로 이 가이드를 사용해야 합니다.

### 2.1 포렌식의 필요성

지난 10년 동안 컴퓨터 관련 범죄 건수가 증가하여 누가, 무엇을, 어디서, 언제, 어떻게 범죄를 저지를 수 있는지 컴퓨터 기반 증거를 사용하는 법 집행을 지원하는 회사 및 제품이 늘어났습니다. 결과적으로 컴퓨터 및 네트워크 포렌식은 컴퓨터 범죄 증거 데이터를 법원에 적절하게 제공

하도록 진화했습니다. 포렌식 도구 및 기법은 범죄 조사 및 컴퓨터 보안 사고 처리와 관련하여 가장 자주 고려됩니다. 의심스러운 시스템을 조사하고, 증거를 수집 및 보존하고, 이벤트를 재구성하고, 이벤트의 현재 상태를 평가하여 이벤트에 응답하는데 사용됩니다. 그러나 포렌식 도구 및 기법은 다음과 같은 여러 가지 유형의 작업에도 유용합니다.

- 1) 작동 문제 해결: 네트워크 구성이 잘못된 호스트의 가상 및 실제 위치 찾기, 응용 프로그램 기능 문제 해결, 현재 OS 및 호스트를 위한 응용 프로그램 구성 설정 기록 및 검토와 같은 많은 포렌식 도구 및 기법을 운영 문제 해결에 적용 할 수 있습니다.
- 2) 로그 모니터링: 로그 항목을 분석하고 여러 시스템에서 로그 항목을 상관시키는 등의 다양한 도구와 기술이 로그 모니터링을 지원할 수 있습니다. 이를 통해 사건 처리, 정책 위반 확인, 감사 및 기타 노력들을 지원할 수 있습니다.
- 3) 데이터 복구: 실수로 또는 의도적으로 삭제되었거나 수정된 데이터를 포함하여 시스템에서 손실된 데이터를 복구할 수 있는 수십 가지 도구가 있습니다. 복구할 수 있는 데이터의 양은 사례 별로 다릅니다.
- 4) 데이터 취득: 일부 조직에서는 포렌식 도구를 사용하여 재배치 또는 폐기되는 호스트의 데이터를 수집합니다. 예를 들어, 사용자가 조직을 떠나면 사용자 워크스테이션의 데이터를 수집하여 나중에 필요할 경우를 대비하여 저장할 수 있습니다. 그런 후, 워크스테이션 매체는 원래의 사용자 데이터를 모두 제거하기 위해 소독될 수 있습니다.
- 5) 의무 준수/규제 컴플라이언스: 기준 및 새롭게 등장한 규제에서는 많은 조직에서 민감한 정보를 보호하고 감사 목적으로 특정 기록을 유지해야 합니다. 또한, 보호된 정보가 다른 당사자에게 노출될 경우 조직은 다른 기관이나 영향을 받는 개인에게 통지해야 할 수 있습니다. 포렌식은 조직이 컴플라이언스를 실시하고 그러한 요구 사항을 준수하도록 도울 수 있습니다.

상황에 관계없이 포렌식 프로세스는 다음과 같은 기본 단계로 구성됩니다.

- 1) 수집: 이 프로세스의 첫 번째 단계는 데이터의 무결성을 보존하는 지침과 절차에 따라 관련 데이터의 가능한 소스에서 데이터를 식별하고 레이블을 지정하며 기록하고 획득하는 것입니다. 수집은 전형적으로 현재 네트워크 연결과 같은 동적 데이터를 잃을 가능성과 배터리 구동 장치(예: 휴대폰, PDA)에서 데이터를 잃을 가능성이 있으므로 시기 적절하게 수행됩니다.
- 2) 검사: 검사는 데이터의 무결성을 유지하면서 특정 관심 분야의 데이터를 평가하고 추출하기 위해 자동화된 방법과 수동 방법을 결합하여 대용량의 수집된 데이터를 포렌식적으로 처리합니다.
- 3) 분석: 이 과정의 다음 단계는 합법적으로 정당한 방법과 기술을 사용하여 조사 결과를 분석하여 수집 및 시험 수행을 위한 자극이었던 질문을 다루는 유용한 정보를 유도하는 것입니다.
- 4) 보고: 최종 단계에서는 분석 결과를 보고합니다. 여기에는 사용된 동작 설명, 도구 및 절차 선택 방법 설명, 수행해야 할 다른 작업 결정(예: 추가 데이터 소스의 법의학 검사, 식별된 취약성 보안, 지침, 절차, 도구 및 포렌식 프로세스의 다른 측면에 대한 개선 권고 사항을 제공합니다. 보고 단계의 형식은

상황에 따라 크게 다릅니다.

포렌식 과정에 대한 심층적인 토론이 3절에 제시되어 있습니다. 4절부터 7절까지는 다양한 유형의 포렌식 데이터를 수집, 검사 및 분석하는데 대한 추가 정보를 제공합니다.

## 2.2 포렌식 직원 채용(Staffing)(?)

실질적으로 모든 조직은 컴퓨터 및 네트워크 포렌식을 수행할 수 있는 능력이 있어야 합니다. 이러한 기능이 없으면 조직은 보호되고 민감한 데이터의 노출과 같은 시스템 및 네트워크에서 발생한 이벤트를 확인하는 데 어려움을 겪습니다. 이러한 필요성의 정도는 다양하지만 조직 내의 포렌식 도구 및 기법의 주 사용자는 일반적으로 다음 세 그룹으로 나눌 수 있습니다.

- 1) 수사관: 조직 내의 수사관은 OIG(Office of Inspector General) 사무국에서 가장 많이 제기되며, 그들은 부정 행위 혐의에 대한 조사를 담당합니다. 일부 조직의 경우 OIG는 범죄 활동과 관련된 것으로 의심되는 사건에 대한 조사를 즉시 인계 받습니다. OIG는 일반적으로 많은 포렌식 기법과 도구를 사용합니다. 조직 내의 다른 수사관들에는 법률 고문 및 인사부 직원이 포함될 수 있습니다. 법 집행 공무원 및 범죄 수사를 수행 할 수 있는 조직 외부의 사람들은 조직 내부의 수사관 그룹의 일부로 간주되지 않습니다.
- 2) IT 전문가: 이 그룹에는 기술 지원 직원과 시스템, 네트워크 및 보안 관리자가 포함됩니다. 이들은 일상적인 작업(예: 모니터링, 문제 해결, 데이터 복구) 중에 자신의 전문 분야에 특정한 소수의 포렌식 기법과 도구를 사용합니다.
- 3) 사건 처리자: 이 그룹은 권한이 없는 데이터 액세스, 부적절한 시스템 사용, 악의적인 코드 감염 및 서비스 거부 공격과 같은 다양한 컴퓨터 보안 사고에 대응합니다. 사고 처리자는 일반적으로 조사 중에 다양한 포렌식 기법과 도구를 사용합니다.

많은 조직에서는 포렌식 업무를 수행하기 위해 직원과 외부 당사자가 함께하고 있습니다. 예를 들어, 일부 조직에서는 표준 작업을 직접 수행하고 특수한 지원이 필요한 경우에만 외부자를 사용합니다. 모든 포렌식 작업을 수행하려는 조직 조차도 일반적으로 물리적으로 손상된 미디어를 재구성을 위해 데이터 복구 회사로 보내는 것과 같이 특별히 까다로운 작업을 아웃소싱하거나, 특별히 훈련된 법 집행 담당자 또는 컨설턴트가 비정상적인 소스(예: 셀 전화)로부터 수집된 데이터를 다루게 된다. 이러한 작업은 일반적으로 전문 소프트웨어, 장비, 시설 및 기술 전문 지식을 사용하지만, 이것이 대부분의 조직에서 인수 및 유지 보수 비용이 높아서 그렇다고 정당화 할 수는 없습니다. 3.1.2절에서 설명한 것처럼 조직은 사전에 법 집행 공무원이 수행해야 할 조치를 결정해야 합니다. 또한, 소송 절차를 위해 전문가의 증언이 필요하면 조직에서 외부 지원을 요청할 수 있습니다.

어떤 내부 또는 외부 당사자가 포렌식의 각 측면을 처리해야 하는지 결정할 때, 조직은 다음 요

소를 염두에 두어야 합니다.

- 1) 비용: 많은 잠재적인 비용이 있습니다. 데이터 수집 및 검사에 사용되는 소프트웨어, 하드웨어 및 장비는 상당한 비용(예: 구매 가격, 소프트웨어 업데이트 및 업그레이드, 유지 관리)을 수반할 수 있으며, 변경을 방지하기 위해 추가적인 물리적 보안 조치가 필요할 수 있습니다. 기타 중요한 비용에는 직원 훈련 및 인건비가 포함되며, 이는 전문 포렌식 전문가에게 특히 의미가 있습니다. 일반적으로 필요한 포렌식 조치는 외부인에 의해 비용 효율적으로 수행되는 경우는 드물며, 내부적으로 수행되는 것이 비용 효율인 경우가 많습니다.
- 2) 응답 시간: 현장에 있는 직원은 외부 전문가보다 더 빨리 컴퓨터 포렌식 활동을 시작할 수 있습니다. 지리적으로 분산된 물리적 위치가 있는 조직의 경우, 멀리 있는 시설 근처에 있는 외부 아웃소싱이 조직의 본사에 있는 직원보다 더 빨리 대응할 수 있습니다.
- 3) 데이터 감도: 데이터 민감성 및 개인 정보 보호 문제로 인해 일부 조직에서는 외부업체가 하드 드라이브를 이미지화하고 데이터에 대한 액세스를 제공하는 다른 작업을 수행하는 것을 꺼려할 수 있습니다. 예를 들어, 사건의 흔적이 있는 시스템에는 의료 정보, 재무 기록 또는 기타 중요한 데이터가 포함될 수 있습니다. 조직은 데이터의 개인 정보를 보호하기 위해 해당 시스템을 자체 통제하에 두는 것을 선호 할 수 있습니다. 반면에, 팀 내에 사생활 보호 문제가 있는 경우(예를 들어, 사고 처리 팀원과 관련된 것으로 의심되는 경우) 포렌식 조치를 수행하기 위해서는 독립적인 제 3자를 사용하는 것이 바람직합니다.

포렌식 작업을 수행하는 사고 처리자는 포렌식 원칙, 지침, 절차, 도구 및 기법, 데이터를 숨기거나 파괴할 수 있는 방도 도구 및 기법에 대해 합리적으로 포괄적인 지식을 갖추고 있어야 합니다. 또한, 이는 사고 처리자가 정보 보안 및 조직 내에서 가장 일반적으로 사용되는 OS, 파일 시스템, 응용 프로그램 및 네트워크 프로토콜과 같은 특정 기술 주제에 대한 전문 지식을 보유하고 있는 경우에 유리합니다. 이러한 유형의 지식을 보유하면 사건에 보다 신속하고 효과적으로 대응할 수 있습니다. 또한, 사고 처리자는 일반적이지 않은 응용 프로그램의 데이터를 검사 및 분석하는 것과 같은 특정 포렌식적 노력을 위해 기술 전문가를 제공하는데 적합한 팀과, 인력을 신속하게 결정할 수 있도록 시스템 및 네트워크에 대한 전반적이고, 폭넓은 이해가 필요합니다.

포렌식을 수행하는 개인은 다른 유형의 작업도 수행해야 할 수 있습니다. 예를 들어, 조사 결과가 법원에서 사용되는 경우, 사고 처리 담당자는 증언을 제공하고, 조사 결과를 뒷받침할 것을 요구 받을 수 있습니다. 사고 처리자는 기술 지원 직원, 시스템 및 네트워크 관리자 및 기타 IT 전문가에 대한 포렌식 교육 과정을 제공할 수 있습니다. 가능한 교육 주제에는 포렌식 도구 및 기술 개요, 특정 도구 사용에 대한 조언 및 새로운 유형의 공격 징후가 포함됩니다. 사고 처리자는 IT 전문가 그룹과의 대화식 세션을 통해 포렌식 도구에 대한 생각을 듣고 기존 포렌식 기능의 잠재적인 단점을 파악할 수도 있습니다.

사고 처리팀에서는 한 명 이상의 팀원이 팀원의 능력에 심각한 영향을 미치지 않도록 각자의 일반적인 포렌식 활동을 수행할 수 있어야 합니다. 사고 처리자는 포렌식 도구 및 기타 기술 및 절차 항목을 사용하여 서로를 교육 할 수 있습니다. 실습과 외부 IT 및 포렌식 교육 과정은 기술을

구축하고 유지하는 데 도움이 될 수 있습니다. 또한, 팀 구성원에게 새로운 도구 및 기술에 대한 시연을 선보이거나 실험실에서 포렌식 및 안티-포렌식 도구를 사용해 보는 것도 도움이 될 수 있습니다. 이는 사고 처리자를 휴대 전화 및 PDA와 같은 장치의 데이터 수집, 검사 및 분석과 관련하여 친숙해지게 하는데 특히 유용합니다. 사고 처리자는 새로운 포렌식 기술, 기법 및 절차를 최신 상태로 유지해야 합니다.

### 2.3 다른 팀들과의 상호 작용

한 사람이 조직 내에서 사용되는 모든 기술(모든 소프트웨어 포함)에 능숙하지는 않습니다. 따라서 포렌식 조치를 수행하는 개인은 추가 지원을 위해 필요에 따라 조직 내의 다른 팀 및 개인에게 연락을 취할 수 있어야 합니다. 예를 들어, 데이터베이스 관리자가 배경 정보를 제공하고 기술 질문에 대답하며 데이터베이스 설명서 및 기타 참조 자료를 제공 할 수 있는 경우에, 특정 데이터베이스 서버와 관련된 사건을 보다 효율적으로 처리할 수 있습니다. 조직은 IT 부서의 IT 전문가, 특히 사고 처리 담당자 및 사고 대응 담당자가 포렌식의 역할과 책임을 이해하고 포렌식 관련 정책, 지침 및 절차에 대한 지속적인 교육 및 교육을 받고 협력할 준비가 되어 있는지 확인해야 합니다. 그들이 책임지고 있는 기술이 사건이나 다른 사건의 일부일 때, 다른 사람들을 도울 수 있습니다.

IT 전문가 및 사고 처리자 외에도 조직 내의 다른 사람들은 기술 능력이 낮은 포렌식 활동에 참여해야 할 수도 있습니다. 예를 들면, 경영진, 법률 고문, 인사 담당자, 감사관 및 물리적 보안 직원이 포함됩니다. 관리는 포렌식 기능 지원, 법의학 정책 검토 및 승인, 특정 포렌식 조치 승인(예: 업무용 시스템을 하드 드라이브에서 데이터를 수집하기 위해 6시간 동안 오프라인으로 전환)을 담당합니다. 법률 고문은 모든 포렌식 정책과 높은 수준의 지침 및 절차를 신중하게 검토해야 하며 포렌식 조치가 합법적으로 수행되도록 하기 위해 필요한 경우 추가 지침을 제공할 수 있습니다. 인사부는 직원 관계 및 내부 사건 처리에 대한 지원을 제공할 수 있습니다. 감사원은 포렌식 활동 비용을 포함하여, 사건의 경제적 영향을 파악하는데 도움을 줄 수 있습니다. 물리적 보안 직원은 증거를 얻고 물리적으로 증거를 확보하는데 도움을 줄 수 있습니다. 이러한 팀이 포렌식 프로세스에서 중요한 역할을 하지는 않지만 이러한 팀이 제공하는 서비스가 도움이 될 수 있습니다.

팀간 의사 소통을 원활하게 하기 위해 각 팀은 하나 이상의 연락 지점을 지정해야 합니다. 이 개인은 각 팀원의 전문 지식을 알고 적절한 사람에게 도움을 요청할 책임이 있습니다. 조직은 필요한 경우 적절한 팀이 참조 할 수 있는 연락처 목록을 유지해야 합니다. 목록에는 표준(예: 사무실 전화) 및 긴급(예: 휴대 전화) 연락 방법이 모두 포함되어야 합니다.

### 2.4 정책

조직은 법 집행 기관에 연락하고 모니터링을 수행하고 포렌식 정책, 지침 및 절차에 대해 정기

적으로 검토하는 등 모든 주요 포렌식 고려 사항을 처리하는 명확한 진술을 정책에 포함해야 합니다. 높은 수준에서, 정책은 권한이 부여된 직원이 적절한 상황에서 합법적인 이유로 시스템과 네트워크를 모니터링하고 조사를 수행할 수 있도록 허용해야 합니다. 조직은 사고 처리자 및 포렌식적인 역할을 수행하는 다른 사람을 위한 별도의 정책을 가질 수도 있습니다. 이 정책은 적절한 행동에 대한 보다 자세한 규칙을 제공합니다. 그러한 요원은 정책을 숙지하고 이해해야 합니다. 법률 및 규정의 변경 및 새로운 법원 판결로 인해 여러 관할 구역에 걸쳐있는 조직의 경우 정책을 자주 업데이트해야 할 수 있습니다. 또한, 조직의 포렌식 정책은 개인 정보 보호에 대한 합리적인 기대와 관련된 정책을 포함하여, 조직의 다른 정책과 일관되어야 합니다. 2.4.1절부터 2.4.3절까지는 정책 관련 주제에 대해보다 자세히 논의합니다.

#### 2.4.1 역할 및 책임 정의

포렌식 정책은 조직의 포렌식 활동을 수행하거나, 지원하는 모든 사람들의 역할과 책임을 명확하게 정의해야 합니다. 여기에는 사고 처리 및 일상 업무(예: 시스템 관리, 네트워크 문제 해결)에서 수행되는 작업이 포함되어야 합니다. 정책에는 2.3절에 열거된 법 집행 노력에 참여할 수 있는 모든 내부 팀과 법 집행 기관, 외주업체 및 사고 대응 조직과 같은 외부 조직이 포함되어야 합니다. 이 정책은 다른 상황에 있는 내부 팀과 외부 조직에 누가 연락해야 하는지 명확하게 표시해야 합니다. 이 정책은 관할권 분쟁(복수의 법 집행 기관이 조사할 수 있는 여러 관할권을 포함하는 범죄)을 해결하고 해결 방법을 설명해야 합니다. 2.2절에서 언급했듯이, 일부 조직에는 부정행위 혐의에 대한 조사를 담당하는 감사관 사무국(Office of Inspector General, OIG)이 있습니다. OIG는 관할권 분쟁을 해결하는 데에도 적합 할 수 있습니다. 일부 조직에서는 범죄가 저질러졌을 경우, 즉시 OIG가 조사를 진행합니다.

#### 2.4.2 포렌식 도구 사용에 대한 지침 제공

사고 처리자; 시스템 및 네트워크 관리자와 같은 IT 전문가; 조직 내의 다른 사람들은 다양한 이유로 포렌식 도구와 기법을 사용합니다. 이 기술은 많은 이점을 가지고 있지만 실수로 또는 의도적으로 정보에 대한 무단 액세스를 제공하거나 사고의 증거를 포함하여 정보를 변경 또는 파괴하기 위해 오용 될 수 있습니다. 또한, 일부 상황에서는 특정 포렌식 도구 사용이 보장되지 않을 수도 있습니다.(예: 사소한 사건으로 인해 수십 시간의 데이터 수집 및 시험 노력이 필요하지 않음).

도구가 합리적이고 적절하게 사용되도록 하기 위해 조직의 정책, 지침 및 절차는 다양한 상황에서 포렌식 조치가 수행되어야 하는 작업과, 수행되지 않아야 할 작업을 명확하게 설명해야 합니다. 예를 들어, 네트워크 관리자는 정기적으로 네트워크 통신을 모니터링하여 작동 문제를 해결할 수 있어야 하지만, 권한이 부여되지 않은 사용자의 이메일은 읽지 않아야 합니다. 헬프 데스크 에이전트는 특정 사용자의 워크 스테이션에 대한 네트워크 통신을 모니터링하여 애플리케이션 문제

를 해결할 수는 있지만, 다른 네트워크 모니터링을 수행 할 수는 없습니다. 개별 사용자는 어떤 상황에서도 네트워크 모니터링을 수행할 수 없습니다. 정책, 지침 및 절차는 정상적인 상황(예: 일반적인 의무) 및 특수한 상황(예: 사건 처리)에서 적용 가능한 각 역할에 대해 허용되거나 금지되는 구체적인 행동을 명확하게 정의해야 합니다.

또한, 정책, 지침 및 절차는 또한 안티-포렌식 도구 및 기법의 사용을 다루어야 합니다. 4절에서 7절에 설명되어있는 안티-포렌식 소프트웨어는 다른 사람들이 액세스 할 수 없도록 데이터를 숨기거나 파괴하도록 설계되었습니다. 자선으로 기부할 컴퓨터에서 데이터를 제거하고 사용자의 개인 정보를 보호하기 위해 웹 브라우저에서 캐시된 데이터를 제거하는 것과 같이 안티-포렌식 소프트웨어에는 많은 긍정적인 용도가 있습니다. 그러나 포렌식 도구와 마찬가지로 안티-포렌식 도구는 악의적인 이유로 사용될 수 있습니다. 따라서, 조직에서는 이러한 도구를 사용할 수 있는 사용자와 상황을 지정해야 합니다.

포렌식 도구는 민감한 정보를 기록할 수 있기 때문에 정책, 지침 및 절차에도 정보를 위해 필요한 안전 장치를 설명해야 합니다. 또한, 사고 처리자가 암호나 환자의 의료 정보를 보는 것과 같이 민감한 정보의 부주의한 노출을 처리하기 위한 요구 사항이 있어야 합니다.

#### 2.4.3 정보 시스템 수명 주기의 포렌식 지원

포렌식 고려 사항이 정보 시스템 수명주기에 통합되면 많은 사건을 보다 효율적이고 효과적으로 처리 할 수 있습니다. 이러한 고려 사항의 예는 다음과 같습니다.

- 1) 특정 기간 동안 시스템의 정기 백업 수행 및 이전 백업 유지
- 2) 워크 스테이션, 서버 및 네트워크 장치에서 감사 활성화
- 3) 중앙 집중식 로그 서버를 보호하기 위해 감사 레코드 전달
- 4) 모든 인증 시도 기록을 포함하여, 감사를 수행하기 위한 중요 업무 응용 프로그램 구성
- 5) 공통 OS 및 응용 프로그램 배포 파일에 대한 파일 해시 데이터베이스 유지 관리 및 특히 중요한 자산에 대한 파일 무결성 검사 소프트웨어 사용
- 6) 네트워크 및 시스템 구성의 기록(예: 기준선) 유지
- 7) 시스템 및 네트워크 활동에 대한 과거 검토를 수행 지원을 위한 데이터 유지 정책 설정
- 8) 진행중인 소송 및 조사와 관련된 데이터를 보존하고, 더 이상 필요하지 않은 데이터를 삭제하라는 요청이나 요구 사항을 준수

이러한 고려 사항의 대부분은 조직의 정책 및 절차에서 기존 조항을 확장한 것으로 일반적으로 핵심 포렌식 정책 대신 관련 개별 문서에서 지정됩니다.

## 2.5 지침 및 절차

2.4절에서 언급했듯이 조직은 조직의 정책, 사고 대응 인력 모델 및 포렌식 활동에 참여한 다른 팀을 기반으로 포렌식 과제를 수행하기 위한 지침과 절차를 만들고 유지 관리해야 합니다. 활동이 외부 당사자에 의해 수행되더라도 조직의 내부 직원은 그들과 계속해서 상호작용하고, 외부 당사자들에게 지원에 대한 필요성을 통보나 시스템에 대한 논리적, 물리적인 접근 권한 부여나 수사관이 도착할 때까지, 사고 현장을 보호하는 등 몇몇 활동에 참가해야만 합니다. 내부 직원은 조직의 정책, 지침 및 절차를 이해하고 준수 할 수 있도록 외부 당사자와 긴밀히 협력해야 합니다.

조직의 포렌식 지침에는 가능한 모든 상황에 맞는 포괄적인 절차를 개발하는 것이 타당하지 않기 때문에 포렌식 기법을 사용하여 사건을 조사하기 위한 일반적인 방법론이 포함되어야 합니다. 그러나 조직에서는 하드 디스크 이미징, 시스템의 휘발성 정보 캡처 및 기록 또는 물리적 증거(예: 이동식 미디어) 확보와 같은 일상적인 작업을 수행하기 위한 단계별 절차를 개발하는 것도 고려해야 합니다. 지침 및 절차의 목적은 기소 또는 내부 징계 조치로 이어질 수 있는 사건에 대해 특히 중요하고 일관성 있고 효과적이며, 정확한 포렌식 조치를 용이하게 하는 것입니다. 전자 기록 및 기타 기록을 변경하거나 달리 조작할 수 있으므로 조직은 해당 기록의 무결성을 입증하기 위해 정책, 지침 및 절차를 통해 준비되어야 합니다.

정보는 모든 정보 자산이 전자 형태로 존재하는 형태로 빠르게 이동하고 있습니다. 공공 및 민간 부문 모두에서 특정 행동이나 결정의 수행이나 특정 정보 항목의 존재와 같은 전자 기록의 진위성, 신뢰성 및 확실성을 결정적으로 입증하는 것이 점차 중요 해지고 있습니다. 사업 기록은 일반적으로 원본과 동일하게 취급됩니다. 점점 법률 및 포렌식 공동체의 일부는 전자 기록을 생성, 변경 또는 조작할 수 있는 용이성에 관심을 기울이고 있습니다. 또한, 공공 및 민간 부문에서의 다양한 준수 방안은 전자 기록의 무결성을 입증하는 것을 점차 중요하게 만들고 있습니다.

이러한 문제들은 본 간행물의 범위를 훨씬 뛰어 넘는 명백한 경고와 함께, 법률 고문 및 고위 IT 담당자와의 논의가 필요하다는 것에 중요성을 부여하며, 다른 방법(예: 로그 보존 및 분석)과 결합된 건전하고 문서화된, 합리적으로 설명 가능한 포렌식 기법의 사용 및 의사 결정권자와 사고 처리자에게 중요한 리소스입니다.

포렌식 지침 및 절차는 조직의 정책 및 모든 관련 법률과 일치해야 합니다. 조직은 품질 보증 측정을 위한 수단으로서, 지침 및 절차 개발에 기술 전문가 및 법률 고문을 포함해야 합니다. 또한 경영진은 지침 및 절차 개발, 특히 모든 주요 의사 결정 요점을 문서화하고 의사 결정이 일관되게 이루어 지도록, 적절한 행동 과정이 정의되도록 보장해야 합니다.

가이드 라인과 절차는 적절한 증거 수집 및 처리, 도구 및 장비의 무결성 유지, 관리 연속성 (Chain of Custody) 유지 및 안전한 증거 보관에 대한 정보를 포함하여, 법적 절차에 대한 증거의 허용 가능성을 지원해야 합니다. 가능하지 않을 수도 있지만, 사고에 응하여 취한 모든 사건이나 행동을 기록하고, 취해진 주요 사건 및 조치에 대한 기록을 보관하여, 간과된 일이 없도록 하여야

사건 처리 방법을 다른 사람들에게 설명하는데 도움이 됩니다. 이 문서는 사례 관리, 보고서 작성 및 증언에 유용할 수 있습니다. 시스템을 복구하는 데 필요한 시간을 포함하여 사람들이 사건에 연루된 날짜와 시간을 기록하면 피해 비용을 계산하는데 도움이 될 수 있습니다. 또한, 포렌식적인 방식으로 증거를 처리하면 의사 결정권자에게 자신이 필요한 조치를 취할 수 있는 위치에 있도록 돕습니다.

또한, 가이드 라인과 절차를 작성한 후에도 정확한 상태로 유지하는 것이 중요합니다. 경영진은 지침과 절차를 얼마나 자주 검토해야 하는지 결정해야 합니다.(일반적으로 적어도 매년) 팀의 정책, 지침 및 절차가 중대한 변화를 겪을 때마다 검토를 수행해야 합니다. 지침 또는 절차가 업데이트되면 법적 절차에서 향후 사용을 위해 이전 버전을 보관해야 합니다. 지침 및 절차의 검토에는 그것의 창작에 참여한 같은 팀이 포함되어야 합니다. 검토를 수행하는 것 외에도 조직은 특정 지침 및 절차의 정확성을 검증하는 데 도움이 되는 연습을 수행할 수도 있습니다.

## 2.6 권고 사항

포렌식 능력을 수립하고 조직하는 주요 권장 사항은 다음과 같습니다:

- 1) **조직은 컴퓨터 및 네트워크 포렌식을 수행할 수 있는 능력이 있어야 합니다.** 포렌식은 범죄 및 부적절한 행동 조사, 컴퓨터 보안 사고 재구성, 운영 문제 해결, 감사 기록 유지 보수에 대한 실사 지원, 사고로 인한 시스템 손상 복구 등을 포함하여 조직 내 다양한 작업에 필요합니다. 이러한 기능이 없으면 조직은 보호되지 못하며, 중요한 데이터의 노출과 같은 시스템 및 네트워크 내에서 어떤 사건이 발생했는지 판단하기 어려울 것입니다. 또한, 포렌식적인 방식으로 증거를 처리하면 의사 결정권자는 자신이 필요한 조치를 취할 수 있는 위치에 있을 수 있게 됩니다.
- 2) **조직은 어느 측이 포렌식의 각 측면을 처리해야 하는지를 결정해야 합니다.** 대부분의 조직은 포렌식 작업을 수행하기 위해 자체 직원과 외부 당사자의 결합에 의존합니다. 조직은 기술과 능력, 비용, 응답 시간 및 데이터 민감도에 따라 어떤 작업을 해야 하는지 결정해야 합니다.
- 3) **사고 처리 팀은 강력한 포렌식 능력을 갖추어야 합니다.** 한 명 이상의 팀 구성원이 각각의 일반적인 포렌식 활동을 수행할 수 있어야 합니다. 실습과 IT 및 포렌식 교육 과정은 새로운 도구 및 기술을 시연할 수 있을 뿐만 아니라 기술을 구축하고 유지하는 데 도움이 될 수 있습니다.
- 4) **조직 내의 많은 팀이 포렌식에 참여해야 합니다.** 포렌식 조치를 수행하는 개인은 필요에 따라 추가 지원을 위해 조직 내의 다른 팀 및 개인에게 연락을 취할 수 있어야 합니다. 이러한 노력에 도움을 줄 수 있는 팀의 예로는 IT 전문가, 경영진, 법률 고문, 인사 담당자, 감사관 및 물리적 보안 직원이 있습니다. 이 팀의 구성원은 포렌식의 역할과 책임을 이해하고 포렌식 관련 정책, 지침 및 절차에 대한 훈련 및 교육을 받고 포렌식 조치와 협력하고 다른 사람들을 도울 준비를 해야합니다.
- 5) **포렌식 고려 사항은 정책에서 분명히 다루어져야 합니다.** 높은 수준에서 정책은 권한이 부여된 직원이 적절한 상황에서 합법적인 이유로 시스템과 네트워크를 모니터링하고 조사를 수행할 수 있도록 허용해야 합니다. 조직은 사고 처리자와 포렌식 역할을 가진 사람들을 위한, 적절한 행동에 대한 보다 자세한

규칙을 제공하는 별도의 포렌식 정책을 가질 수도 있습니다. 포렌식적 노력을 돋기 위해 부름을 받을 수 있는 사람은 모두 포렌식 정책을 숙지하고 이해해야 합니다. 추가 정책 고려 사항은 다음과 같습니다.

- 포렌식 정책은 조직의 포렌식 활동을 수행하거나 지원하는 모든 사람들의 역할과 책임을 명확하게 정의해야 합니다. 이 정책은 관련될 수 있는 모든 내외부 당사자를 포함해야 하며, 다른 상황에서 누가 어떤 당사자에게 연락해야 하는지 명확히 표시해야 합니다.
  - 조직의 정책, 지침 및 절차는 정상 및 특수 상황에서 포렌식 조치가 수행되어야 하는 것과 수행되어서는 안되는 것을 명확하게 설명하고, 안티-포렌식 도구 및 기법의 사용을 다루어야 합니다. 정책, 지침 및 절차는 또한 민감한 정보의 부주의한 노출 처리를 다루어야 합니다.
  - 포렌식 고려 사항을 정보 시스템 수명주기에 통합하면 많은 사건을 보다 효율적이고 효과적으로 처리할 수 있습니다. 예를 들어, 호스트에 대한 감사 수행 및 시스템 및 네트워크 활동에 대한 기록 검토 수행을 지원하는 데이터 보유 정책 수립이 포함됩니다.
- 6) **조직은 포렌식 과제를 수행하기 위한 지침과 절차를 만들고 유지 관리해야 합니다.** 지침에는 포렌식 기법을 사용하여 사건을 조사하기 위한 일반적인 방법론이 포함되어야 하며, 단계별 절차에는 일상 작업을 수행하는 방법이 설명되어 있어야 합니다. 지침과 절차는 법적 절차에 대한 증거의 허용 가능성 을 지원해야 합니다. 전자 기록 및 기타 기록은 변경되거나 달리 조작될 수 있으므로 조직은 정책, 지침 및 절차를 통해 그러한 기록의 신뢰성 및 무결성을 입증할 준비를 해야 합니다. 가이드 라인과 절차는 정기적으로 검토되어야 하며, 정확해야 합니다.

### 3. 포렌식 절차 수행

포렌식을 수행하는 가장 일반적인 목표는 해당 이벤트와 관련된 사실을 찾아 분석하여 관심 이벤트를 더 잘 이해하는 것입니다. 2.1절에서 설명한 것처럼 법적 절차 및 내부 징계 조치에 대한 증거 수집, 맬웨어 사고 및 비정상적인 운영 문제 처리와 같은 다양한 상황에서 포렌식이 필요할 수 있습니다. 필요에 관계없이 포렌식은 [그림 3-1]에 표시된 4단계 프로세스를 사용하여 수행해야 합니다. 이러한 단계의 정확한 세부 사항은 포렌식에 대한 구체적인 필요성에 따라 달라질 수 있습니다. 조직의 정책, 지침 및 절차는 표준 절차로부터의 변화를 지시해야 합니다.

이 절에서는 포렌식 프로세스의 기본 단계인 수집, 검사, 분석 및 보고에 대해 설명합니다. 첫 단계인 수집에서는, 특정 이벤트와 관련된 데이터를 식별, 레이블 지정, 기록 및 수집하고 무결성을 보존합니다. 두 번째 단계에서, 포렌식 도구와 기술은 수집된 데이터 유형에 따라 확인을 실시하고 그것의 무결성을 보호하면서 수집된 데이터로부터 관련된 정보를 추출하는 것을 총족해야 한다. 검사는 자동화된 도구와 수동 프로세스의 조합을 사용할 수 있습니다. 다음 단계인 분석에서는, 수집 결과를 분석하여 수집 및 검사 수행에 대해 자극이 되었던 질문에 대한 유용한 정보를 얻습니다. 최종 단계인 보고에서는, 수행된 작업을 설명하고, 수행해야 할 필요가 있는 다른 작업들을 결정하고, 정책, 지침, 절차, 도구 및 포렌식 프로세스의 다른 측면에 대한 개선을 권고하는 등 분석 결과를 보고해야 합니다.

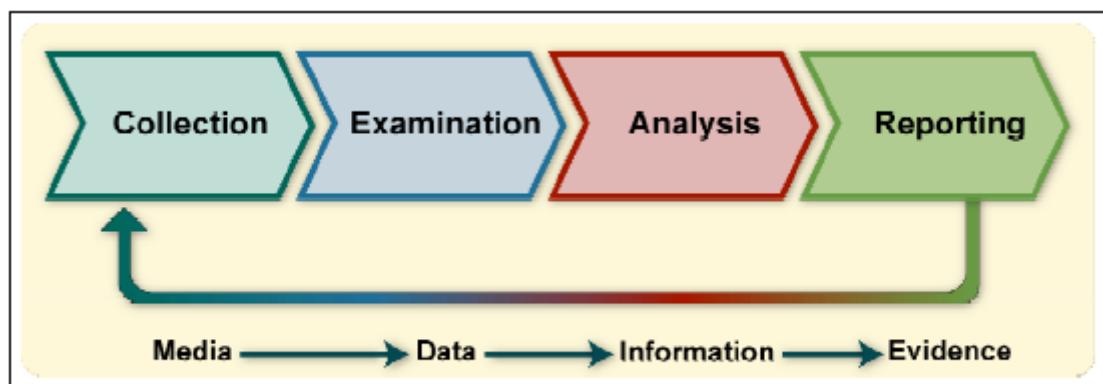


Figure 3-1. Forensic Process

[그림 3-1 : 포렌식 절차]

[그림 3-1]의 하단에 표시된 것처럼 포렌식 프로세스는 법 집행이나 조직의 내부 사용에 증거가 필요한지 여부에 관계없이 미디어를 증거로 변환합니다. 특히, 수집된 데이터를 검사할 때, 첫 번째 변환이 발생합니다. 그리고 미디어에서 데이터를 추출하여 포렌식 도구로 처리할 수 있는 형태로 변환합니다. 둘째로, 데이터는 분석을 통해 정보로 변환됩니다.

마지막으로, 증거로 변환된 정보는 지식을 행동으로 이동시키는 것과 유사합니다.—보고 단계에

서 하나 혹은 그 이상에서 분석에 의해 생성된 정보를 실제로 사용하는 것— 예를 들어, 특정 개인을 기소하는 데 도움이 되는 증거나, 일부 활동을 중단 또는 완화하는데 도움이 되는, 소송을 초래할 수 있는 정보 또는 사례에 대한 생성에 대한 지식으로 사용될 수 있습니다. 예를 들어, 그것은 특정 개인을 기소하는 증거 혹은 일부 활동을 중단 또는 완화하는 곳에 기소할 수 있는 정보로 도움이 되는 사항을 제공할 수 있으며, 법정에서 새로운 국면으로 리드할 수 있는 지식으로 사용될 수 있다.

### 3.1 데이터 수집

포렌식 프로세스의 첫 번째 단계는, 잠재적인 데이터 소스를 식별하고 데이터 소스를 획득하는 것입니다. 3.1.1절은 사용 가능한 다양한 데이터 소스를 설명하고 포렌식 목적으로 진행중인 데이터 수집을 지원하기 위해 조직이 수행할 수 있는 작업에 대해 설명합니다. 3.1.2절은 법적으로 또는 내부 징계 절차를 지원하는데 필요한 추가 작업을 포함하여 데이터 수집을 위한 권장 단계를 설명합니다. 3.1.3절에서는 수집 프로세스에 대한 조직의 비용과 영향에 대해 수집된 데이터의 가치를 가늠할 필요성을 강조하면서 사고 대응 고려 사항을 논의합니다.

#### 3.1.1 가능한 데이터 소스 식별

전문적이고 개인적인 목적으로 디지털 기술이 널리 보급됨에 따라 풍부한 데이터 소스가 만들어졌습니다. 가장 확실하고 일반적인 데이터 원본은 데스크톱 컴퓨터, 서버, 네트워크 저장 장치 및 노트북입니다. 이러한 시스템은 일반적으로 CD 및 DVD와 같은 미디어를 수용하는 내부 드라이브를 가지고 있으며 외부 데이터 저장소(예: USB, Firewire, PCMCIA-Personal Computer Memory Card International Association-) 미디어 및 장치를 부착 할 수 있습니다. 데이터 소스가 될 수 있는 외부 저장 장치의 예로는, 썬 드라이브(USB), 메모리 및 플래시 카드, 광학 디스크 및 자기디스크가 있습니다. 표준 컴퓨터 시스템은 일시적으로(즉, 시스템이 종료되거나 재부팅될 때까지) 사용 할 수 있는 휘발성 데이터도 포함합니다. 컴퓨터 관련 장치 외에도 많은 유형의 휴대용 디지털 장치(예: PDA, 휴대폰, 디지털 카메라, 디지털 녹음기, 오디오 플레이어)에는 데이터가 포함될 수 있습니다. 분석가는 사무실과 같은 물리적인 영역을 조사하고 가능한 데이터 소스를 인식할 수 있어야 합니다.

분석가들은 다른 장소에 있는 가능한 데이터 소스에 대해서도 생각해야 합니다. 예를 들어, 6절과 7절에서 설명했듯이 네트워크 활동 및 응용 프로그램 사용과 관련하여 조직 내에 많은 정보 소스가 있습니다. 인터넷 서비스 공급자(ISP)의 네트워크 활동 로그와 같은 것을 다른 조직에서도 기록 할 수 있습니다. 분석가는 각 데이터 소스의 소유자와 이것이 데이터 수집에 미칠 수 있는 영향을 염두에 두어야 합니다. 예를 들어, ISP 기록 사본을 얻으려면 일반적으로 법원 명령이 필요합니다. 또한, 분석가는 조직의 외부 시설(예: 직원의 개인 노트북 또는 계약자의 노트북)에 관한

법적 고려 사항뿐만 아니라 조직의 정책을 인식해야 합니다. 재택 근무자의 본사에 있는 컴퓨터와 관련된 사건과 같이 조직 외부의 위치가 관련되면 상황이 훨씬 더 복잡해 질 수 있습니다. 때로는 기본 데이터 소스에서 데이터를 수집하는 것이 불가능합니다. 따라서 분석가는 동일한 데이터의 일부 또는 전부를 포함 할 수 있는 대체 데이터 소스를 알고 있어야 하며, 얻을 수 없는 소스 대신 이러한 소스를 사용해야 합니다.

조직은 포렌식 목적에 유용할 수 있는 데이터를 수집하기 위해 지속적으로 사전 대책을 강구 할 수 있습니다. 예를 들어, 5.1.1절에서 설명한대로 대부분의 OS는 정상 작동의 일부로 인증 시도 및 보안 정책 변경과 같은 특정 유형의 이벤트를 감사하고 기록하도록 구성할 수 있습니다. 감사 레코드는 이벤트가 발생한 시간과 이벤트의 출처를 포함하여 중요한 정보를 제공할 수 있습니다.

또 다른 유용한 조치는, 중앙집중식 로깅을 구현하는 것이며, 그것은 특정 시스템과 응용 프로그램이 로그 사본을 안전한 중앙 로그 서버에 전달하는 것을 의미합니다. 중앙집중식 로깅은 권한이 없는 사용자가 로그를 변경하거나 안티-포렌식 기법을 사용하여 분석을 방해하는 것을 방지합니다. 정기적인 시스템 백업을 수행하면 분석자가 특정 시간에 시스템의 내용을 볼 수 있습니다. 또한, 6절 및 7절에서 설명한 것처럼 침입 탐지 소프트웨어(IDS), 바이러스 백신 소프트웨어 및 스파이웨어 탐지 및 제거 유틸리티와 같은 보안 모니터링 제어는 공격 또는 침입이 발생한 시기와 방법을 보여주는 로그를 생성할 수 있습니다.

또 다른 사전예방적 데이터 수집 조치는 특정 시스템의 키보드 사용을 기록하는 키스트로크 모니터링과 같은 사용자 동작 모니터링입니다. 이 방법은 가치 있는 활동 기록을 제공할 수 있지만 사용자가 조직 정책 및 로그인 배너를 통해 이러한 모니터링을 수행할 것을 권고하지 않는 한 개인 정보 침해가 될 수 있습니다. 대부분의 조직에서는 의심되는 사건에 대한 추가 정보를 수집할 때를 제외하고 키스트로크 모니터링과 같은 기술을 사용하지 않습니다. 그러한 모니터링을 수행하는 권한은 법률 고문과 논의하고 조직의 정책에 명확하게 문서화되어야 합니다.

### 3.1.2 데이터 수집

잠재적인 데이터 소스를 식별한 후에 분석가는 소스에서 데이터를 수집해야 합니다. 데이터 수집은 3단계 프로세스를 사용하여 수행해야 합니다. 즉, 데이터 수집 계획 수립, 데이터 수집 그리고 수집된 데이터의 무결성 확인입니다. 다음 항목은 이 세 단계의 개요를 제공하지만, 2단계 및 3단계의 세부 정보는 수집되는 데이터 유형에 따라 다릅니다. 4.2, 5.2, 6.3절 및 7.3절은 각각 데이터 파일, OS 데이터, 네트워크 트래픽 데이터 및 애플리케이션 데이터의 무결성 확보 및 검증에 대한 보다 자세한 설명을 제공합니다.

1. **데이터 수집 계획을 세웁니다.** 여러 가지 잠재적인 데이터 소스가 있기 때문에 계획을 세우는 것이 대부분의 경우 중요한 첫 번째 단계입니다. 분석가는 소스를 우선 순위화하여

데이터를 수집해야 하는 순서를 정하는 계획을 수립해야 합니다. 우선 순위 지정을 위한 중요한 요소는 다음과 같습니다.

- **가능성이 높은 가치.** 분석가는 상황에 대한 이해와, 비슷한 상황에서의 이전 경험을 바탕으로 잠재적인 각 데이터 소스의 상대적 가치를 예측할 수 있어야 합니다.
- **휘발성.** 휘발성 데이터는 컴퓨터의 전원이 꺼지거나 시간이 흐른 후에 손실된 라이브 시스템의 데이터를 나타냅니다. 휘발성 데이터는 시스템에서 수행된 다른 작업의 결과로 손실될 수도 있습니다. 많은 경우 휘발성 데이터를 수집하는 것이 비휘발성 데이터보다 우선되어야 합니다. 그러나 비휘발성 데이터는 본질적으로 다소 동적일 수 있습니다.(예: 새 이벤트가 발생 할 때, 덮어 쓰이는 로그 파일)
- **필요한 노력의 양.** 다른 데이터 소스를 확보하는데 필요한 노력의 양은 크게 다를 수 있습니다. 이러한 노력에는 분석가 및 기타 기관(법무 고문 포함)이 소비한 시간뿐만 아니라 장비 및 서비스 비용(예: 외부 전문가)도 포함됩니다. 예를 들어, 네트워크 라우터에서 데이터를 수집하는 것은 ISP에서 데이터를 수집하는 것보다 훨씬 적은 노력을 필요로 합니다.

분석가는 잠재적인 각 데이터 소스에 대해, 이 세가지 요소를 고려하여 데이터 소스 획득의 우선 순위 결정 및 먼저 획득할 데이터 소스 결정에 대해서 정보에 근거한 결정을 내릴 수 있습니다. 어떤 경우에는, 너무 많은 가능한 데이터 소스가 있기 때문에 모든 데이터 소스를 얻을 수는 없습니다. 조직은 데이터 소스 획득 우선 순위 결정의 복잡성을 신중하게 고려해야 하며, 분석가가 우선 순위 지정을 효과적으로 수행하는데 도움이 되는 작성 계획, 지침 및 절차를 개발해야 합니다.

2. **데이터를 수집합니다.** 보안 도구, 분석 도구 또는 기타 수단을 통해 데이터를 아직 수집하지 않은 경우, 데이터를 수집하는 일반적인 프로세스에서는 포렌식 도구를 사용하여 휘발성 데이터를 수집하고, 비휘발성 데이터 원본을 복제하여 데이터를 수집하여 원본 데이터를 보호합니다. 수집은 로컬 또는 네트워크를 통해 수행될 수 있습니다. 시스템과 데이터에 대해 더 많은 지배권을 가지기 때문에 로컬에서 데이터를 습득하는 것이 선호될 수 있지만, 로컬 데이터 수집은 항상 할 수 있는 것이 아닙니다.(예를 들어, 잠긴 룸의 시스템, 다른 위치의 시스템) 네트워크를 통해 데이터를 수집할 때는 수집할 데이터의 유형과 사용하려는 노력의 양을 결정해야 합니다. 예를 들어, 여러 네트워크 연결을 통해 여러 시스템에서 데이터를 수집해야 하거나, 하나의 시스템에서 논리 볼륨을 복사하는 것으로 충분할 수 있습니다.
3. **데이터의 무결성을 확인하십시오.** 데이터를 수집한 후에는 무결성을 확인해야 합니다. 분석가가 법적인 이유로 디지털 데이터가 필요할 경우 데이터가 변조되지 않았음을 증명하는 것이 특히 중요합니다. 데이터 무결성 확인은 일반적으로 도구를 사용하여 원본 및 복사된 데이터의 메시지 디제스트를 계산한 다음 디제스트를 비교하여 이들이 동일한

지 확인합니다.

또한, 몇 가지 다른 단계를 수행해야 합니다. 프로세스 전반에 걸쳐 프로세스에서 사용되는 각 도구에 대한 정보를 포함하여 데이터를 수집하기 위해 취해진 모든 단계에 대한 자세한 로그를 보관해야 합니다. 이 문서를 통해 다른 분석가가 필요할 경우 나중에 프로세스를 반복할 수 있습니다. 또, 컴퓨터 설정 및 주변 장치를 시각적으로 알리기 위해 증거를 촬영해야 합니다. 또한 실제로 시스템을 만지기 전에 분석가는 모니터에 표시된 사진, 문서, 실행중인 프로그램 및 기타 관련 정보를 기록하거나 메모해야 합니다. 화면 보호기가 활성화되어 있으면 암호로 보호될 수 있기 때문에 문서화해야 합니다. 만약, 가능하다면 현장의 한 사람이 증거 보관 담당자로 지정되어야 하며, 수집된 모든 품목을 사진, 기록 및 라벨링을 할 책임이 있으며 작업 수행자와 함께 취한 모든 조치를 기록해야 합니다. 증거가 법적 절차를 위해 오랜 시간 동안 필요하지 않을 수 있기 때문에, 적절한 문서화를 통해 분석가는 데이터 수집을 위해 수행된 작업을 정확하게 기억할 수 있으며, 잘못된 취급에 대한 주장을 논박하는 데 사용할 수 있습니다.

분석가는 증거 수집을 돋기 위해 포렌식 워크 스테이션, 백업 장치, 빈 미디어 및 증거 처리 용품(예: 하드-바운드 노트북, 관리 연속성(Chain of Custody) 포맷, 증거 저장 봉투 및 태그, 증거 테이프, 디지털 카메라 등)를 미리 준비해야 합니다. 경우에 따라, 증거의 무단 액세스 및 변경을 방지하기 위해 현장을 물리적으로 보호해야 합니다. 이것은 물리적 보안 직원이 방을 지키는 것처럼 간단 할 수 있습니다. 또한, 법률 집행 담당자가 법적인 이유로 데이터 수집을 처리해야 하는 상황이 있을 수도 있습니다. 여기에는 ISP 레코드를 얻고 외부 컴퓨터 시스템 및 비정상적인 장치 및 미디어에서 데이터를 수집하는 것이 포함되지만 이에 국한되지는 않습니다. 법률 고문의 지침에 따라 조직은 사전에 법 집행 공무원에 의해 가장 먼저 수집되어야 하는 데이터 유형을 결정해야 합니다.

분석가는 수집된 데이터로 수행할 작업과 잠재적인 파급 효과에 대한 계획을 고려해야 합니다. 경우에 따라 데이터 조사 및 분석을 위해 법 집행 기관이나 다른 외부 기관에 넘길 수 있습니다. 이로 인해 수집된 하드웨어를 장시간 사용할 수 없게 될 수 있습니다. 법적 절차를 위해 원본 미디어의 보안을 유지해야 하는 경우 수년간 사용할 수 없게 될 수 있습니다. 또 다른 우려는 조사와 관련 없는 민감한 정보(예: 의료 기록, 금융 정보)가 실수로 원하는 데이터와 함께 캡처될 수 있다는 것입니다.

### 3.1.3 사고 대응 고려사항

사고 대응 중에 포렌식을 수행할 때 중요한 고려사항은 사건이 언제, 어떻게, 언제, 포함되는지입니다. 외부 영향으로부터 해당 시스템을 격리하는 것은 시스템과 데이터에 대한 추가 손상을 방지하거나 증거를 보존하기 위해 필요할 수 있습니다. 대부분의 경우 분석가는 사고 대응팀과 협력하여 봉쇄 결정(예: 네트워크 케이블 연결 끊기, 전원 연결 해제, 물리적 보안 조치 늘리기, 호스트 정상 종료)을 수행해야 합니다. 이 결정은 사고 방지에 관한 기준 정책과 절차에 기반해

야 할 뿐만 아니라, 그 팀의 사고에 의한 위험 평가에도 기반해야 한다. 그래서 선정된 억제 전략이나 충분한 전술의 조합이 가능할 때마다, 잠재적 증거의 무결성을 유지하면서 위험을 충분히 완화할 수 있도록 합니다.

또한, 조직은 다양한 봉쇄 전략이 조직을 효과적으로 운영하는 능력에 미칠 수 있는 영향을 미리 고려해야 합니다. 예를 들어, 디스크 이미지 및 기타 데이터를 얻기 위해 중요한 시스템을 몇 시간 동안 오프라인 상태로 만들면 조직에서 필요한 작업을 수행하는 능력에 부정적인 영향을 미칠 수 있습니다. 상당한 가동 중지 시간은 조직에 막대한 금전적 손실을 초래할 수 있습니다. 그러므로 조직의 운영에 지장을 최소화하기 위해 주의를 기울여야 합니다.

사고를 억제하기 위해 취해지는 한 가지 조치는 증거물이 변경되지 않도록 컴퓨터 주변을 보호하고, 수집 프로세스 도중에 권한이 부여된 직원의 접근을 제한하는 것입니다. 또한, 컴퓨터에 대한 접근 권한이 있는 모든 사용자의 목록은 문서화되어야 합니다. 특정 사용자가 특정 데이터가 있는 위치에 대한 암호나 정보를 제공할 수 있기 때문입니다. 컴퓨터가 네트워크에 연결되어 있는 경우 컴퓨터에 연결된 네트워크 케이블을 분리하면, 원격 사용자가 컴퓨터의 데이터를 수정할 수 없습니다. 컴퓨터가 무선 네트워크 연결을 사용하는 경우, 외부 네트워크 어댑터의 연결이 컴퓨터에서 끊어지거나, 내부 네트워크 어댑터가 사용되지 않도록 설정되어서 네트워크 연결이 끊어 질 수 있습니다. 두 옵션을 모두 사용할 수 없는 경우 컴퓨터가 사용하는 무선 네트워크 액세스 포인트의 전원을 끄면 동일한 결과가 나타납니다. 그러나 이렇게 하면 조사 범위를 벗어난 사용자가 일상 업무를 수행하지 못할 수 있습니다. 또한, 컴퓨터 범위 내에 둘 이상의 액세스 지점이 있을 수 있습니다. 일부 무선 네트워크 어댑터는 주 액세스 지점을 사용할 수 없을 때 자동으로 다른 액세스 지점에 연결을 시도하므로 이 방법으로 조치를 하면 여러 액세스 지점의 연결이 끊길 수 있습니다.

## 3.2 검사

데이터가 수집 된 후, 다음 단계는 수집된 데이터에서 관련 정보를 평가하고 추출하는 데이터 검사입니다. 이 단계는 데이터 압축, 암호화 및 접근 제어 메커니즘과 같이 데이터 및 코드를 모호하게 만드는 OS 또는 애플리케이션 기능을 우회하거나 완화하는 과정을 포함할 수도 있습니다. 획득한 하드 드라이브에는 수십만 개의 데이터 파일이 포함될 수 있습니다. 파일 압축 및 접근 제어를 통해 숨겨진 정보를 포함하여 관심 있는 정보가 들어있는 데이터 파일을 식별하는 것은 어려운 작업이 될 수 있습니다. 또한, 관심 있는 데이터 파일에는 필터링을 해야 하는 불필요한 정보가 포함될 수 있습니다. 예를 들어, 어제의 방화벽 로그는 수백만 개의 레코드를 보유할 수 있지만, 레코드 중 5개만 관련된 이벤트와 연관될 수 있습니다.

다행스럽게도, 다양한 도구와 기술을 사용하여 데이터의 양을 줄일 수 있습니다. 텍스트 및 패턴 검색은 특정 주제 또는 사람을 언급한 문서를 찾거나 특정 전자 메일 주소에 대한 메일 로그 항목을 식별하는 것과 같은 관련 데이터를 식별하는 데 사용할 수 있습니다. 또 다른 유용한 기술

은 텍스트, 그래픽, 음악 또는 압축 파일 아카이브와 같은 각 데이터 파일의 내용 유형을 결정할 수 있는 도구를 사용하는 것입니다. 데이터 파일 유형에 대한 지식을 사용하면 추후 연구가 필요한 파일을 식별하고 검사에 관련이 없는 파일을 제외할 수 있습니다. 또한, 알려진 파일에 대한 정보가 들어있는 데이터베이스가 있으며, 이 파일을 사용하여 추가 고려 대상에서 파일을 포함하거나 제외할 수도 있습니다. 검사 도구 및 기법에 대한 특정 정보는 4.3절, 5.3절, 6.4절 및 7.4절에 나와 있습니다.

### 3.3 분석

관련 정보가 추출되면 분석가는 데이터를 연구하고 분석하여 결론을 도출해야 합니다. 포렌식의 기초는 이용 가능한 데이터를 기반으로 적절한 결론을 도출하거나 아직 결론을 도출할 수 없다는 결론을 내리는 체계적인 접근법을 사용하고 있습니다. 분석 절차에서는 사람, 장소, 항목 및 이벤트를 식별하고 이러한 요소가 어떻게 관련되어 있는지를 결정하여 결론에 도달할 수 있어야 합니다. 종종 이러한 노력에는 여러 소스 간의 데이터 상관 관계가 포함됩니다. 예를 들어, 네트워크 침입 탐지 시스템(IDS) 로그는 이벤트를 호스트에 연관 지을 수 있으며, 호스트 감사 로그는 이벤트를 특정 사용자 계정에 연관 지을 수 있고, 호스트 IDS 로그는 사용자가 수행한 작업을 나타낼 수 있습니다. 중앙집중식 로깅 및 보안 이벤트 관리 소프트웨어와 같은 도구는 데이터를 자동으로 수집하고 상호 연관시켜, 상기 절차를 용이하게 합니다. 시스템 특성을 알려진 기준선과 비교하면 시스템에 대한 다양한 유형의 변경 사항을 식별 할 수 있습니다. 8절에서는 이 분석 프로세스를 보다 자세히 설명합니다.

3.1.2절에서 설명한 바와 같이, 법적 또는 내부 징계 조치를 위해 증거가 필요할 수 있는 경우, 분석가는 발견한 사항과 취해진 모든 조치를 신중하게 기록해야 합니다.

### 3.4 보고

최종 단계는 보고이며, 분석 단계에서 나온 정보를 준비하고 표시하는 프로세스입니다. 다음을 포함하여 많은 요인이 보고에 영향을 줍니다:

- **대체 설명.** 사건에 관한 정보가 불완전하다면, 어떤 일이 일어 났는지에 대한 명확한 설명에 도달하지 못할 수도 있습니다. 사건에 2개 이상의 그럴듯한 설명이 있는 경우, 보고 과정에서 적절한 고려가 있어야 합니다. 분석가는 제안된 각각의 가능한 설명을 증명하거나 반증하려고 시도하는 체계적인 접근법을 사용해야 합니다.
- **청자 고려.** 데이터 또는 정보를 보게 될 잠재 고객을 파악하는 것이 중요합니다. 법 집행을 필요로 하는 사건에는 수집된 모든 정보에 대한 매우 상세한 보고서가 필요하며 또한 획득한 모든 증거 데이터의 사본이 필요할 수 있습니다. 시스템 관리자는 네트워크 트래픽 및 관련 통계를 매우 자세히 보고 싶어할 수 있습니다. 고위 경영진은 공격이 어떻게 발생했는지 단순화된 시각적 표현과,

비슷한 사건을 방지하기 위해 수행해야 할 작업과 같은 상황을 간단히 요약하여 보고 싶을 수도 있습니다.

- **사용 가능한 정보.** 보고 절차에는 새로운 정보 소스를 수집하기 위해 분석가에게 허락된 데이터로부터 얻은 사용 가능한 정보를 식별하는 것을 포함합니다. 예를 들어, 사고 또는 범죄에 대한 추가 정보로 이어질 수 있는 데이터를 바탕으로 연락처 목록을 작성할 수 있습니다. 또한, 미래의 공격에 사용될 수 있는 시스템의 백도어, 계획중인 범죄, 특정 시간에 확산되기 시작하는 웹 또는 악용될 수 있는 취약점과 같은 공격 이벤트를 방지할 수 있는 정보가 수집 될 수 있습니다.

보고 절차의 일부로 분석가는 정책 상의 단점이나 절차상의 오류와 같이 해결해야 할 수도 있는 문제를 식별해야 합니다. 많은 포렌식 및 사고 대응팀이 주요 이벤트가 끝날 때마다, 공식적인 검토를 실시합니다. 이러한 검토에는 지침 및 절차의 개선 가능성에 대한 진지한 고려가 포함되는 경향이 있으며, 일반적으로 최소한 검토할 때마다, 사소한 변경 사항이 승인되고 이행됩니다. 예를 들어, 하나의 공통적인 문제는 발생할 수 있는 각기 다른 유형의 사고와 관련하여 현재 인적 자원 목록을 이대로 유지 관리는 것이, 만약 사고가 발생한다면 그러한 인적 자원들에게 컨택하는데 많은 리소스가 필요한 경우입니다. 다른 일반적인 문제는 조사 중에 수집된 기가 바이트 또는 테라 바이트의 데이터와 향후 감사를 위해 도움이 될 수 있는 추가 데이터를 기록하기 위해 보안 제어(예: 감사, 로깅, 침입 탐지)를 변경하는 방법입니다. 공식적인 검토는 이러한 프로세스를 개선 할 수 있는 방법을 식별하는 데 도움이 될 수 있습니다. 지침과 절차가 변경되면 모든 팀 구성원에게 변경 사실을 통보하고 따라야 할 적절한 절차를 자주 상기시켜야 합니다. 팀은 일반적으로 변경 사항을 추적하고 각 프로세스 및 절차 문서의 최신 버전을 확인하기 위한 공식 메커니즘을 가지고 있습니다. 또한, 많은 팀들이 벽이나 문, 기타 눈에 잘 띠는 곳에 포스터나 문서를 올려 팀에게 주요 단계를 알려주기 때문에 상황을 어떻게 처리해야 하는지 모든 사람에게 끊임없이 상기시켜줍니다.

분석가들은 확인된 문제를 해결하는 것 외에도, 기술을 유지하고 성장시키기 위한 다른 조치를 취해야 합니다. 인증 또는 인증 유지의 문제로 일부 포렌식 심사관은 컴퓨터 저장 매체, 데이터 형식 및 기타 관련 문제에 대한 최신 기술을 다루는 도구 및 기술을 정기적으로 새로 고쳐야 합니다. 필요 여부에 상관없이 교과 과정, 실무 경험 및 학업 정보를 통해 기술을 주기적으로 새로 고침하면 포렌식 조치를 수행하는 사람들이 빠르게 변화하는 기술 및 직무에 보조를 맞출 수 있습니다. 일부 조직에서는 포렌식팀의 모든 구성원에게 매년 숙련도 시험을 통과할 것을 요구합니다. 정책, 지침 및 절차를 정기적으로 검토하면 조직의 기술 추세 및 법률 변경 사항을 최신 상태로 유지하는데 도움이 됩니다.

### 3.5 권고 사항

이번 절에서 포렌식 절차에 대해 제시하는 주요 권장 사항은 다음과 같습니다:

- **조직은 일관된 프로세스를 사용하여 포렌식을 수행해야 합니다.** 이 가이드는 수집, 검사, 분석 및 보고 단계를 포함하는 4단계 포렌식 프로세스를 제공합니다. 각 단계의 정확한 세부 사항은 포렌식의 필요성에 따라 다를 수 있습니다.
- **분석가는 사용 가능한 데이터 소스의 범위를 알고 있어야 합니다.** 분석가는 물리적 영역을 조사하고 가능한 데이터 소스를 인식할 수 있어야 합니다. 분석가들은 조직 내의 다른 곳과 조직 외부에 있는 가능한 데이터 소스를 생각해야 합니다. 분석가는 기본 소스에서 데이터를 수집하는 것이 가능하지 않은 경우 대체 데이터 소스를 사용할 준비가 되어있어야 합니다.
- **조직은 유용한 데이터를 수집하는데 능동적이어야 합니다.** 운영 체제에 대한 감사 설정, 중앙 집중식 로깅 구현, 정기적인 시스템 백업 수행 및 보안 모니터링 제어를 사용하는 것은 향후 포렌식 활동을 위한 데이터 소스를 생성할 수 있습니다.
- **분석가는 표준 프로세스를 사용하여 데이터 수집을 수행해야 합니다.** 이 프로세스에서 권장하는 단계는 데이터 원본 식별, 데이터 수집 계획 수립, 데이터 수집 및 데이터 무결성 확인입니다. 계획은 데이터 소스의 우선 순위를 정해야 하며, 데이터의 가치나, 데이터의 휘발성 및 필요한 노력의 양과 같은 것을 기반으로 데이터를 수집하는 순서를 정해야 합니다. 데이터 수집이 시작되기 전에 미래의 법적 또는 내부 징계 절차에서 증거 사용을 뒷받침하는 방식으로 증거를 수집하고 보존할 필요성에 대해 분석가 또는 관리자의 결정이 내려져야 합니다. 그러한 상황에서는, 잘못된 취급이나 증거의 변조를 피하기 위해 명확하게 정의된 관리 연속성(Chain of Custody)을 따라야합니다. 기본적으로는 증거를 보존할 필요가 있는지 여부가 불명확하면 보존해야 합니다.
- **분석가는 데이터를 연구하는 체계적인 접근법을 사용해야 합니다.** 포렌식의 기초는 분석가가 사용 가능한 데이터를 기반으로 적절한 결론을 도출하거나, 아직 결론을 내릴 수 없다는 결론을 내릴 수 있도록 이용 가능한 데이터를 체계적으로 분석하는 것입니다. 법적 또는 내부 징계 조치를 위해 증거가 필요할 수 있는 경우에, 분석가는 결과 및 취해진 모든 조치를 신중하게 기록해야 합니다.
- **분석가는 프로세스와 관행을 검토해야 합니다.** 현재 혹은 최근 포렌식 활동에 대한 검토는 정책 결점, 절차상의 오류 및 구제 조치가 필요한 기타 문제를 파악하는 데 도움을 줄뿐만 아니라 조직이 기술 동향 및 법률 변경 사항을 최신 상태로 유지할 수 있도록 도와줍니다.

## 4. 데이터 파일들의 데이터를 사용

데이터 파일은(파일이라고도 불리는) 단일 개체 안에 논리적으로 그룹화된 정보의 모음이며, 파일명과 같은 고유의 이름으로 참조됩니다. 파일은 문서, 이미지, 비디오, 어플리케이션을 포함한 많은 데이터 타입을 가질 수 있습니다. 성공적인 컴퓨터 매체 포렌식 절차는 매체에 존재하는 파일을 수집하고 검사하고, 분석하는 능력에 의존합니다. 이 절은 대부분의 일반적인 매체 유형과 파일시스템—파일 네이밍, 저장, 체계화, 접근에 대한 방법을 제공하는 시스템—에 대한 개관을 제공합니다. 그 후, 파일은 어떻게 수집되어야 하는지, 파일의 무결성이 어떻게 보존되어야 하는지에 대해서 논의합니다. 또한, 삭제된 파일들로부터 데이터 복구와 같은 파일 복구와 관련된 다양한 기술적 이슈에 대해서도 논의합니다. 이 절의 마지막에서는 파일 검사와 분석을 설명하고, 분석을 지원할 수 있는 도구와 기술에 대한 안내를 제공합니다.

### 4.1 파일 기본 사항

파일 수집 및 검사를 시도하기 전에, 분석가는 파일과 파일시스템에 대한 합리적이고 포괄적인 이해를 가져야 합니다. 첫째로, 분석가는 파일을 포함한 다양한 매체에 대해 인지해야 합니다. 4.1.1절에서는 개인 컴퓨터와 다른 유형의 디지털 기기에서 사용되는 매체의 몇몇 예제를 제공합니다. 그리고 4.1.2절에서는 파일시스템이 어떻게 파일들을 체계화하며, 각각의 일반적인 파일시스템들에 대한 개관을 설명합니다. 4.1.3절에서는 삭제된 파일들이 어떻게 파일시스템 안에 여전히 존재할 수 있는지에 대해서 논의합니다.

#### 4.1.1 파일 저장 매체

컴퓨터와 다른 디지털 장비의 광범위한 사용은 파일을 저장하기 위해 사용되는 서로 다른 매체들의 숫자의 현저한 증가를 초래했습니다. 하드 드라이브와 플로피 디스크와 같은 전통적인 매체 타입들에 더하여, 파일은 종종 PDA, 휴대폰과 같은 소비자 장치와 디지털 카메라에 의해 유명해진 플래쉬 메모리 카드와 같은 최신의 매체 타입들에 저장됩니다. [표 4-1]은 디지털 기기와 컴퓨터에서 일반적으로 사용되는 매체 유형들을 열거합니다. 해당 리스트는 가용한 모든 매체 유형을 포함하지는 않습니다. 오히려 분석가가 이해해야 할 다양한 매체 유형들에 대해 보여주기 위한 의도입니다.

Media Type	Reader	Typical Capacity <sup>16</sup>	Comments
<b>Primarily Used in Personal Computers</b>			
Floppy disk	Floppy disk drive	1.44 megabytes (MB)	3.5-inch disks; decreasing in popularity
CD-ROM	CD-ROM drive	650 MB–800 MB	Includes write-once (CD-R) and rewritable (CD-RW) disks; most commonly used media
DVD-ROM	DVD-ROM drive	1.67 gigabytes (GB)–15.9 GB	Includes write-once (DVD±R) and rewritable (DVD±RW) single and dual layer disks
Hard drive	N/A	20 GB–400 GB	Higher capacity drives used in many file servers
Zip disk	Zip drive	100 MB–750 MB	Larger than a floppy disk
Jaz disk	Jaz drive	1 GB–2 GB	Similar to Zip disks; no longer manufactured
Backup tape	Compatible tape drive	80 MB–320 GB	Many resemble audio cassette tapes; fairly susceptible to corruption from environmental conditions
Magneto optical (MO) disk	Compatible MO drive	600 MB–9.1 GB	5.25-inch disks; less susceptible to environmental conditions than backup tapes
Advanced Technology Attachment (ATA) flash card	PCMCIA slot	8 MB–2 GB	PCMCIA flash memory card; measures 85.6 x 54 x 5 mm
<b>Used by Many Types of Digital Devices</b>			
Flash/Jump drive	USB interface	16 MB–2 GB	Also known as thumb drives because of their size
CompactFlash card	PCMCIA adapter or memory card reader	16 MB–6 GB	Type I cards measure 43 x 36 x 3.3 mm; Type II cards measure 43 x 36 x 5 mm
Microdrive	PCMCIA adapter or memory card reader	340 MB–4 GB	Same interface and form factor as CompactFlash Type II cards
MultiMediaCard (MMC)	PCMCIA adapter or memory card reader	16 MB–512 MB	Measures 24 x 32 x 1.4 mm
Secure Digital (SD) Card	PCMCIA adapter or memory card reader	32 MB–1 GB	Compliant with Secure Digital Music Initiative (SDMI) requirements; provides built-in data encryption of file contents; similar in form factor to MMCs
Memory Stick	PCMCIA adapter or memory card reader	16 MB–2 GB	Includes Memory Stick (50 x 21.5 x 2.8 mm), Memory Stick Duo (31 x 20 x 1.6 mm), Memory Stick PRO, Memory Stick PRO Duo; some are compliant with SDMI requirements and provide built-in encryption of file contents
SmartMedia Card	PCMCIA adapter or memory card reader	8 MB–128 MB	Measures 37 x 45 x 0.76 mm
xD-Picture Card	PCMCIA adapter or xD-Picture card reader	16 MB–512 MB	Currently used only in Fujifilm and Olympus digital cameras; measures 20 x 25 x 1.7 mm

[표 4-1 : 일반적으로 사용되는 매체 유형]

#### 4.1.2 파일시스템

매체가 파일을 저장하기 전에, 매체는 보통 논리적 볼륨이 분할 및 포맷되어 있어야 합니다. 여기서 분할이란, 물리적으로 구성 단위를 분리시킨 부분 속에 매체를 논리적으로 나누는 행위입니다. 논리적 볼륨은 파티션이거나 하나의 파일시스템으로 포맷된, 독립 개체로써 행동하는 파티션

들의 모임일 수 있습니다. 플로피 디스크와 같은 몇몇 매체 유형들은, 최대 하나의 파티션(결과적으로 하나의 논리적 볼륨)을 가질 수 있습니다. 논리적 볼륨의 포맷은 선택된 파일시스템에 의해서 결정됩니다.

파일시스템은 논리적 볼륨에서 파일이 작명되는, 저장되는, 체계화되는, 그리고 접근되는 방법을 정의합니다. 많은 서로 다른 파일시스템들이 존재하며, 그 각각은 독특한 기능과 데이터 구조를 제공합니다. 그러나, 파일시스템들은 몇몇 공통적인 특징들을 공유합니다. 첫째로, 그것들은 데이터를 체계화하고 저장하기 위해 디렉토리와 파일이라는 개념을 사용합니다. 디렉토리는 파일들을 함께 그룹화하기 위해 사용되는 체계화된 구조입니다. 추가적으로 파일과 디렉토리는 서브 디렉토리라고 불리는 다른 디렉토리에 포함될 수도 있습니다. 둘째로, 파일시스템은 매체에서 파일의 위치를 가리키기 위한 몇몇 데이터 구조를 사용합니다. 또한, 그것들은 매체 안의 하나 혹은 그 이상의 파일 할당 단위에 작성된 각각의 데이터 파일들을 저장합니다. 그것들은 몇몇 파일시스템(예: 파일 할당 테이블[FAT], NT 파일시스템[NTFS], 다른 파일시스템[유닉스, 리눅스 등]에서는 블록)에 의해서 클러스터로써 참조됩니다. 파일 할당 단위는 간단히 말해서, 매체에 접근하는 가장 작은 단위의 섹터들의 그룹입니다.

다음은 일반적으로 사용되는 파일시스템들입니다.

- **FAT12.**<sup>17</sup> FAT12 is used only on floppy disks and FAT volumes smaller than 16 MB. FAT12 uses a 12-bit file allocation table entry to address an entry in the filesystem.
- **FAT16.** MS-DOS, Windows 95/98/NT/2000/XP, Windows Server 2003, and some UNIX OSs support FAT16 natively. FAT16 is also commonly used for multimedia devices such as digital cameras and audio players. FAT16 uses a 16-bit file allocation table entry to address an entry in the filesystem. FAT16 volumes are limited to a maximum size of 2 GB in MS-DOS and Windows 95/98. Windows NT and newer OSs increase the maximum volume size for FAT16 to 4 GB.
- **FAT32.**<sup>18</sup> Windows 95 Original Equipment Manufacturer (OEM) Service Release 2 (OSR2), Windows 98/2000/XP, and Windows Server 2003 support FAT32 natively, as do some multimedia devices. FAT32 uses a 32-bit file allocation table entry to address an entry in the filesystem. The maximum FAT32 volume size is 2 terabytes (TB).
- **NTFS.** Windows NT/2000/XP and Windows Server 2003 support NTFS natively. NTFS is a *recoverable filesystem*, which means that it can automatically restore the consistency of the filesystem when errors occur. In addition, NTFS supports data compression and encryption, and allows user and group-level access permissions to be defined for data files and directories.<sup>19</sup> The maximum NTFS volume size is 2 TB.
- **High-Performance File System (HPFS).** HPFS is supported natively by OS/2 and can be read by Windows NT 3.1, 3.5, and 3.51. HPFS builds on the directory organization of FAT by providing automatic sorting of directories. In addition, HPFS reduces the amount of lost disk space by utilizing smaller units of allocation. The maximum HPFS volume size is 64 GB.

- **Second Extended Filesystem (ext2fs).**<sup>20</sup> ext2fs is supported natively by Linux. It supports standard UNIX file types and filesystem checks to ensure filesystem consistency. The maximum ext2fs volume size is 4 TB.
- **Third Extended Filesystem (ext3fs).** ext3fs is supported natively by Linux. It is based on the ext2fs filesystem and provides journaling capabilities that allow consistency checks of the filesystem to be performed quickly on large amounts of data. The maximum ext3fs volume size is 4 TB.
- **ReiserFS.**<sup>21</sup> ReiserFS is supported by Linux and is the default filesystem for several common versions of Linux. It offers journaling capabilities and is significantly faster than the ext2fs and ext3fs filesystems. The maximum volume size is 16 TB.
- **Hierarchical File System (HFS).**<sup>22</sup> HFS is supported natively by Mac OS. HFS is mainly used in older versions of Mac OS but is still supported in newer versions. The maximum HFS volume size under Mac OS 6 and 7 is 2 GB. The maximum HFS volume size in Mac OS 7.5 is 4 GB. Mac OS 7.5.2 and newer Mac OSs increase the maximum HFS volume size to 2 TB.
- **HFS Plus.**<sup>23</sup> HFS Plus is supported natively by Mac OS 8.1 and later and is a journaling filesystem under Mac OS X. It is the successor to HFS and provides numerous enhancements, such as long filename support and Unicode filename support for international filenames. The maximum HFS Plus volume size is 2 TB.
- **UNIX File System (UFS).**<sup>24</sup> UFS is supported natively by several types of UNIX OSs, including Solaris, FreeBSD, OpenBSD, and Mac OS X. However, most OSs have added proprietary features, so the details of UFS differ among implementations.
- **Compact Disk File System (CDFS).** As the name indicates, the CDFS filesystem is used for CDs.
- **International Organization for Standardization (ISO) 9660 and Joliet.** The ISO 9660 filesystem is commonly used on CD-ROMs. Another popular CD-ROM filesystem, Joliet, is a variant of ISO 9660. ISO 9660 supports filename lengths of up to 32 characters, whereas Joliet supports up to 64 characters. Joliet also supports Unicode characters within filenames.
- **Universal Disk Format (UDF).** UDF is the filesystem used for DVDs and is also used for some CDs.

#### 4.1.3 미디어 상의 기타 데이터

4.1.2절에서 설명한 바와 같이, 파일시스템은 매체에 파일을 저장하기 위해 설계되었습니다. 그러나, 파일시스템은 삭제된 파일의 데이터나, 현존하는 파일의 이전 버전을 가지고 있을 수 있습니다. 이 데이터는 중요한 정보를 제공할 수 있습니다.(4.2절에서는 이러한 데이터 유형을 수집하기 위한 기술을 논의) 다음 항목들은 이러한 데이터가 어떻게 다양한 매체 안에 여전히 존재할 수 있는지에 대해서 설명합니다.

- **삭제된 파일:** 파일이 삭제되어도 일반적으로 매체로부터는 삭제되지 않습니다. 대신에, 파일의 위치를 가리키던 디렉토리 데이터 구조 안의 정보가 삭제로 표시됩니다. 이것은 파일은 여전히 매체 안에 저장되어 있지만, 더 이상 OS에 의해서 열거되지 않는다는 것을 의미합니다. 운영체제는 이를 자유 공간으로 고려하며, 언제든지 삭제된 전체 파일의 모든 부분에 덮어쓸 수 있습니다.

- **슬랙 공간:** 이전에 언급했던 것처럼, 파일시스템은 파일을 저장하기 위해서 파일 할당 단위를 사용합니다. 파일이 파일 할당 단위 크기보다 작은 공간을 요구해도, 전체의 파일 할당 단위는 여전히 해당 파일을 위해 예약됩니다. 예를 들면, 만약 파일 할당 단위 크기가 32KB이고 파일이 오직 7KB 라도, 전체 32KB는 여전히 파일을 위해 할당되지만, 오직 7KB만 사용되고, 결과적으로 미사용 공간 25KB가 남습니다. 이러한 미사용 공간은 파일 슬랙 공간이라고 불리며, 삭제된 파일의 일부분과 같은 잔여 데이터가 남아있을 수 있습니다.
- **자유 공간:** 자유 공간은 어떠한 파티션으로도 할당되지 않은 매체 상의 영역입니다. 데이터를 숨길 수 있는 또 다른 방법은 NTFS 볼륨 내의 ADS(Alternate Data Stream)를 사용하는 것입니다. NTFS는 오랫동안 파일과 디렉터리에 대한 다중 데이터 스트림을 지원했습니다. NTFS 볼륨의 각 파일은 파일의 기본 데이터를 저장하는데 사용되는 이름이 지정되지 않은 스트림과, 그림 썸네일이나, 파일 속성과 같은 데이터를 저장하는 하나 이상으로 명명된 보조 스트림(예: file.txt : Stream1, file.txt : Stream2)으로 구성된다. 예를 들어, 사용자가 Windows 탐색기에서 파일을 마우스 오른쪽 버튼으로 클릭하고, 파일의 속성을보고 요약 탭에 표시된 정보를 수정하면 OS는 명명된 스트림이 있는 파일의 경우 요약 정보를 저장합니다.

파일 내의 모든 데이터 스트림은 파일의 속성(예: 타임 스탬프, 보안 속성)을 공유합니다. 명명된 스트림은 파일의 저장소 할당량에 영향을 미치지만, Explorer와 같은 표준 Windows 파일 유ти리티는 파일의 이름이 지정되지 않은 스트림의 크기만 탐색하기 때문에 사용자로부터 숨겨집니다. 결과적으로 사용자는 표준 Windows 파일 유ти리티를 사용하여 파일에 ADS가 포함되어 있는지 여부를 쉽게 판단할 수 없습니다. 이를 통해, 숨겨진 데이터를 NTFS 파일 시스템에 포함시킬 수 있습니다. ADS를 사용한 파일을 NTFS가 아닌 파일 시스템으로 옮기는 것은 파일에서 ADS를 효과적으로 제거하므로 분석자가 그것의 존재를 인식하지 못하면 ADS가 손실될 수 있습니다. 소프트웨어 및 프로세스를 사용하여 ADS를 식별할 수 있습니다.

## 4.2 파일 수집

데이터 수집 중에 분석가는 관련 파일이나 파일 시스템(일반적으로 마스터 복사본과 작업 복사본)의 여러 복사본을 만들어야 합니다. 그러면, 분석자는 원본 파일이나 마스터 복사본에 영향을 주지 않고 작업 복사본을 사용할 수 있습니다. 4.2.1절에서는 미디어에서 파일 및 잔여 파일 데이터를 복사하기 위한 기본 기술 및 도구에 대해 설명합니다. 4.2.2절에서는 파일의 무결성을 유지하는 중요성에 대해 설명하고, 파일 무결성을 보존 및 확인하는데 도움이 되는 하드웨어 및 소프트웨어에 대한 지침을 제공합니다. 파일을 마지막으로 수정하거나 액세스 한 경우와 같이 파일 수집 뿐만 아니라, 파일의 타임 스탬프 수집도 중요합니다. 4.2.3절은 타임 스탬프를 설명하고 타임 스탬프를 보존하는 방법을 설명합니다. 숨겨진 파일을 찾거나 RAID(Redundant Array of Inexpensive Disks) 구현에서 파일을 복사하는 것과 같은 파일 수집과 관련된 다른 기술적 문제는 4.2.4절에서 설명합니다.

#### 4.2.1 매체에서 파일 복사

두 가지 기술을 사용하여 매체 파일을 복사할 수 있습니다.

1. **논리 백업:** 논리 백업은 논리 볼륨의 디렉토리와 파일을 복사합니다. 여유 공간에 저장된 삭제 파일 또는 잔여 데이터와 같이 미디어에 있을 수 있는 다른 데이터는 캡처하지 않습니다.
2. **비트 스트림 이미징:** 디스크 이미징이라고도 하는 비트 스트림 이미징은 자유 공간 및 슬랙 공간을 포함하여 원본 미디어의 bit-for-bit 복사본을 생성합니다. 비트 스트림 이미지는 더 많은 저장 공간을 필요로 하며 논리 백업보다 수행하는 데 오래 걸립니다.

기소 또는 징계 조치를 위해 증거가 필요한 경우, 분석가는 원본 미디어의 비트 스트림 이미지를 얻고 원본 미디어에 레이블을 붙여 증거로 안전하게 저장해야 합니다. 이후의 모든 분석은 복사된 미디어를 사용하여 수행해야 원본 미디어가 수정되지 않고, 필요한 경우 원본 미디어의 복사본을 항상 다시 만들수 있습니다. 이미지 사본을 작성하기 위해 취해진 모든 단계는 문서화되어야 합니다. 이렇게하면 모든 분석자가 동일한 절차를 사용하여 원본 미디어의 정확한 복제본을 제작할 수 있습니다. 또한, 수집 과정에서 증거가 잘못 처리되지 않았음을 입증하기 위해 적절한 문서화가 사용될 수 있습니다. 이미지를 기록하기 위해 취해진 조치 외에도 분석가는 하드 드라이브 모델 및 일련 번호, 매체 저장 용량, 사용된 이미징 소프트웨어 또는 하드웨어에 대한 정보(예: 이름, 버전 번호, 라이센스 정보)를 기록해야 합니다. 이러한 모든 조치는 관리 연속성을 지원합니다.

비트 스트림 이미지가 실행되면, 디스크 대 디스크 또는 디스크 대 파일 복사가 수행될 수 있습니다. 이름에서 알 수 있듯이, 디스크 대 디스크 복사본은 미디어의 내용을 다른 미디어에 직접 복사합니다. 디스크 대 파일 복사본은 미디어의 내용을 단일 논리 데이터 파일에 복사합니다. 디스크간 복사는 복사된 미디어를 컴퓨터에 직접 연결하고 그 내용을 쉽게 볼 수 있기 때문에 유용합니다. 그러나 디스크 대 디스크 복사에는 원본 미디어와 유사한 두 번째 미디어가 필요합니다. 디스크 대 파일 복사본을 사용하면 데이터 파일 이미지를 쉽게 이동하고 백업할 수 있습니다. 그러나 이미지 파일의 논리 내용을 보려면 분석자가 이미지를 미디어로 복원하거나 비트 스트림 이미지의 논리 내용을 표시할 수 있는 응용 프로그램에서 열거나 읽어야 합니다. 이것의 세부 사항은 운영체제와 포렌식 도구에 의존적입니다. 4.3절에서는 이 프로세스에 대해 자세히 설명합니다.

수 많은 하드웨어 및 소프트웨어 도구가 비트 스트림 이미징 및 논리 백업을 수행할 수 있습니다. 하드웨어 도구는 일반적으로 이식 가능하고 bit-by-bit 이미지를 제공하며, 이미지를 저장할 드라이브나 컴퓨터에 직접 연결되며 해시 기능이 내장되어 있습니다. 하드웨어 도구는 다음과 같은 일반적인 유형의 컨트롤러를 사용하는 드라이브에서 데이터를 수집할 수 있습니다. IDE(Integrated Drive Electronics) 및 SCSI(Small Computer System Interface) 소프트웨어 솔루션은

일반적으로 이미지 디스켓이 부착된 워크 스테이션에서 실행되는 시동 디스켓, CD 또는 설치된 프로그램으로 구성됩니다. 몇몇 소프트웨어 솔루션은 파일이나 파티션의 논리적 복사본을 생성하며, 매체의 비트 대 비트 이미지 복사에 반해 자유, 비활당 드라이브 공간에 대해서는 무시한다.

주요 기능 외에도 일부 디스크 이미징 도구는 자동화 된 감사 추적 및 연계 보관성과 같은 포렌식 기록 보관을 수행할 수 있습니다. 이러한 도구를 사용하면 검사 프로세스의 일관성과 결과의 정확성 및 재현성을 지원할 수 있습니다. 점점 더 많은 수의 디스크 이미징 도구를 사용할 수 있게 되고 있습니다. NIST의 Computer Forensics Tool Testing (CFTT) 프로젝트는 이러한 확산과, 이를 테스트하기 위한 표준이 부족함에 따라 도구 결과를 검증하기 위한 엄격한 테스트 절차를 개발했습니다. 현재 CFTT 테스트를 거친 디스크 이미징 도구는 몇 개 뿐입니다.

일반적으로 비트 스트림 이미징을 수행하는 도구는 라이브 시스템(현재 사용중인 시스템)에서 전체 물리적 장치의 비트 단위 사본을 얻는데 사용해서는 안되는데, 이는 이러한 시스템의 파일과 메모리가 지속적으로 변하기 때문에 유효성을 검증할 수 없기 때문입니다. 그러나 라이브 시스템의 논리 영역을 비트 단위로 복사하고 검증할 수는 있습니다. 논리 백업을 수행할 때 라이브 시스템에서 파일을 복사하지 않는 것이 좋습니다. 백업 중에 파일이 변경 될 수 있으며, 프로세스에 의해 열려 있는 파일은 복사하기가 쉽지 않을 수 있습니다. 따라서, 분석가는 파일을 가져와야 하는지, 복사가 얼마나 정확하고 완전해야하며, 라이브 시스템이 얼마나 중요한지에 따라 실제 시스템에서 파일을 복사할 수 있는지 여부를 결정해야 합니다. 예를 들어, 단일 사용자의 홈 디렉토리에서 파일을 수집하기 위해 수백 명의 사람들이 사용하는 중요한 서버를 제거할 필요는 없습니다. 실제 시스템의 논리 백업의 경우 분석가는 표준 시스템 백업 소프트웨어를 사용할 수 있습니다. 그러나 백업을 수행하면 시스템 성능에 영향을 미치고 백업이 로컬 또는 원격으로 수행되는지 여부에 따라 상당한 네트워크 대역폭이 소모될 수 있습니다.

조직은 포렌식 목적으로 수행할 수 있는 비트 스트림 이미지 및 논리 백업(라이브 시스템 포함)을 포함하는 상황을 나타내는 정책, 지침 및 절차를 갖추어야 합니다. 일반적으로 정책을 수립하는 것이 가장 효과적입니다.—지침, 절차(예: 낮음, 보통 또는 높음 영향) 및 관심있는 사건의 성격에 근거한 절차;— 일부 조직에서는 특히 중요한 시스템에 대한 정책 진술, 지침 및 절차를 별도로 작성하기도 합니다. 정책, 지침 또는 절차는 백업 및 이미지에 관한 결정을 내릴 수 있는 권한을 가진 개인 또는 그룹을 식별해야 합니다. 이 사람들은 위험을 감수하고 건전한 결정을 내릴 수 있어야 합니다. 정책, 지침 또는 절차는 각 유형의 시스템에 대해 백업 또는 이미징을 수행할 권리가 있는 개인 또는 그룹을 식별해야 합니다. 일부 시스템에 대한 접근은 시스템의 조작 또는 데이터의 민감도로 인해 제한될 수 있습니다.

#### 4.2.2 데이터 파일 무결성

백업 및 이미징 중에 원본 미디어의 무결성을 유지해야 합니다. 백업 또는 이미징 프로세스가 원본 미디어의 데이터를 변경하지 않도록 분석가는 미디어를 백업 또는 이미징하는 동안 쓰기 차

단기를 사용할 수 있습니다. 쓰기 차단기는 컴퓨터가 연결된 컴퓨터 저장 매체에 쓰지 못하게하는 하드웨어 또는 소프트웨어 기반 도구입니다. 하드웨어 쓰기 차단기는 실제로 컴퓨터와 처리중인 저장 매체에 연결되어 어떠한 쓰기도 예방하는 처리를 합니다. 소프트웨어 쓰기 차단기는 분석가의 포렌식 시스템에 설치되며, 현재 MS-DOS 및 Windows 시스템에서만 사용할 수 있습니다.(일부 OS [예: Mac OS X, Linux]는 탑재되지 않은 보조 장치로 부팅하도록 설정할 수 있기 때문에 소프트웨어 쓰기 차단기가 필요하지 않을 수 있지만, 하드웨어 쓰기 차단 장치를 부착하면 무결성이 유지됩니다.) MS -DOS 기반 소프트웨어 쓰기 차단기는 인터럽트 13 및 확장 인터럽트 13 디스크 쓰기를 트래핑하여 작동합니다. Windows 기반 소프트웨어 쓰기 차단기는 필터를 사용하여 장치로 전송된 인터럽트를 정렬하여 저장 매체에 쓰기를 방지합니다.

일반적으로 하드웨어 쓰기 차단기를 사용할 때, 매체를 읽는데 사용된 매체 또는 장치는 쓰기 차단기에 직접 연결되어야 하며, 쓰기 차단기는 백업 또는 이미징을 수행하는데 사용되는 컴퓨터 또는 장치에 연결되어야 합니다. 소프트웨어 쓰기 차단기를 사용하는 경우, 미디어를 읽는데 사용된 미디어나 장치가 컴퓨터에 연결되기 전에 소프트웨어를 컴퓨터에 로드해야 합니다. 쓰기 차단기는 특정 장치에 대해 쓰기 차단 기능을 켜거나 끌 수 있습니다. 쓰기 차단이 사용될 때, 연결된 모든 장치에 대해 켜기로 전환하는 것이 중요합니다. 쓰기 차단기는 새로운 장치를 지원하는지 정기적으로 검사해야 합니다. 예를 들어, 새 장치는 예약되거나 이전에 사용되지 않은 함수나 자리 표시자를 사용하여 궁극적으로 장치에 쓰고 내용을 변경할 수 있는 고유 기능으로 구현되었을 수 있습니다.

백업 또는 이미징이 수행된 후에는 복사된 데이터가 원본 데이터의 정확한 복제본인지 확인하는 것이 중요합니다. 복사된 데이터의 메시지 요약을 계산하여 데이터 무결성을 확인하고 보장할 수 있습니다. 메시지 요약은 데이터를 고유하게 식별하고 데이터의 단일 비트를 변경하면 완전히 다른 메시지 다이제스트가 생성되도록 하는 해시 함수입니다. 데이터의 메시지 요약을 계산하기 위한 알고리즘이 많이 있지만 가장 일반적으로 사용되는 두 가지 알고리즘은 MD5 및 보안 해시 알고리즘 1 (SHA-1)입니다. 이러한 알고리즘은 임의의 길이의 입력 데이터를 가져 와서 출력 128 비트 메시지 다이제스트를 생성합니다. SHA-1은 FIPS(Federal Information Processing Standard) 승인 알고리즘이고, MD5는 아니기 때문에 연방 기관은 MD5 대신 SHA-1을 사용하여 메시지 다이제스트를 사용해야합니다.

비트 스트림 이미지가 수행될 때, 이미징이 수행되기 전에 원본 미디어의 메시지 다이제스트가 계산되고 기록되어야 합니다. 이미징 후에는 복사된 미디어의 메시지 요약을 계산하고 원본 메시지 요약과 비교하여 데이터 무결성이 유지되었는지 확인해야 합니다. 원본 미디어의 메시지 다이제스트를 다시 계산하여, 이미징 프로세스가 원래 미디어를 변경하지 않았는지 확인하고 모든 결과를 문서화해야 합니다. 이 프로세스는 논리적 백업에 사용해야 하지만, 각각의 파일들에 메시지 다이제스트를 계산하고 비교해야 하는 것은 아닙니다. 비트 스트림 이미지와 논리 백업의 경우 데이터 무결성을 보장하기 위해 생성된 메시지 요약은 읽기 전용 또는 일회용 쓰기 미디어에 저장하거나 인쇄한 다음 적절한 위치에서 보호해야 합니다.

#### 4.2.3 파일 수정, 액세스 및 생성 시간

파일이 생성, 사용 또는 수정된 시기를 아는 것은 중요하며, 대부분의 OS는 파일과 관련된 특정 타임 스탬프를 추적합니다. 가장 일반적으로 사용되는 타임 스탬프는 다음과 같이 수정, 액세스 및 생성(MAC) 시간입니다.

1. **수정 시간:** 파일을 쓰거나 다른 프로그램에서 변경 한 경우를 포함하여 파일이 어떤 방식으로든 마지막으로 변경된 시간입니다.
2. **액세스 시간:** 파일에 대한 액세스가 마지막으로 있었던 시간입니다.(예: 보기, 열기, 출력하기)
3. **생성 시간:** 일반적으로 파일을 만든 시간과 날짜입니다. 그러나 파일을 시스템에 복사하면 작성 시간은 파일이 새 시스템으로 복사된 시간이 됩니다. 수정 시간은 그대로 유지됩니다.

다른 유형의 파일 시스템은 다른 유형의 시간을 저장할 수 있습니다. 예를 들어, Windows 시스템은 최종 수정 시간, 마지막 액세스 시간 및 파일 작성 시간을 유지합니다. UNIX 시스템은 최종 수정, 마지막 inode 변경 및 마지막 액세스 시간을 유지합니다. 그러나 일부 UNIX 시스템(BSD 및 SunOS 버전 포함)은 실행 파일이 실행될 때, 실행 파일의 마지막 액세스 시간을 업데이트하지 않습니다. 일부 UNIX 시스템은 파일 메타 데이터가 가장 최근에 변경된 시간을 기록합니다. 메타 데이터는 데이터에 대한 데이터입니다. 파일 시스템에서 메타 데이터는 파일 내용에 대한 정보를 제공하는 데이터입니다.

분석가가 이벤트의 정확한 타임 라인을 설정해야 하는 경우 파일 시간을 보존해야 합니다. 따라서, 분석가는 데이터 파일을 수집하는 모든 방법이 파일 시간을 보존할 수 있는 것은 아니라는 점을 알아야 합니다. 비트 대 비트 사본이 생성되기 때문에 비트 스트림 이미지는 파일 시간을 보존할 수 있습니다. 일부 도구를 사용하여 논리적 백업을 수행하면, 데이터 파일을 복사할 때 파일 생성 시간이 변경될 수 있습니다. 이러한 이유로 파일 시간이 필수적일 때는 비트 스트림 이미징을 사용하여 데이터를 수집해야합니다.

분석가들은 파일 시간이 항상 정확하지 않을 수도 있음을 알고 있어야 합니다. 이러한 부정확성에 대한 이유는 다음과 같습니다.

- 컴퓨터 시간이 정확한 시간을 가지지 못했을 수 있습니다. 예를 들어, 시계가 신뢰할 수 있는 시간 원본과 정기적으로 동기화되지 않았을 수 있습니다.
- 시간은 초 또는 분을 생략하는 등 세부적인 수준으로 기록되지 않을 수 있습니다.
- 공격자가 기록된 파일 시간을 변경했을 수 있습니다.

#### 4.2.4 기술적 문제

데이터 파일을 수집할 때 몇 가지 기술적인 문제가 발생할 수 있습니다. 4.2.1절에서 언급했듯이, 주요 문제는 삭제된 파일 및 미디어의 자유 및 슬랙 공간에 있는 파일의 잔재입니다. 개인들은 이러한 데이터의 수집을 방해하는 다양한 기술을 사용할 수 있습니다. 예를 들어, 임의의 값 또는 일정한 값(예: 모두 0)으로 미디어(또는 특정 파일과 같은 미디어의 일부)를 덮어 쓰는 와이핑을 수행하는 많은 유ти리티가 있습니다. 그러한 유ти리티의 대부분은 효과적으로 수집을 방해할 수 있습니다. 개인은 또한 하드 드라이브의 자기 제거(degaussing) 또는 물리적으로 미디어를 손상시키거나 파괴하는 등의 데이터 수집을 방지하기 위해 물리적 수단을 사용할 수 있습니다. 물리적 및 소프트웨어 기반 기술은 소프트웨어를 사용하여 모든 데이터를 복구하는 것을 매우 어렵거나 불가능하게 만듭니다. 이러한 경우의 복구 시도는 첨단 시설, 하드웨어 및 기법을 갖춘 고도의 전문화된 포렌식 전문가의 사용을 필요로 하지만 그러한 수단을 사용하는데 소요되는 비용과 노력은 일반적으로는 사용하기 불가능한 수준에 있습니다. 어떤 경우에는 데이터가 간단하게 복구할 수 없을 수도 있습니다.

또 다른 일반적인 문제는 숨겨진 데이터의 수집입니다. 대부분의 OS는 사용자가 특정 파일, 디렉토리 또는 파티션을 숨김으로 태그할 수 있게 합니다. 이는 기본적으로 디렉토리 목록에 표시되지 않음을 의미합니다. 일부 응용 프로그램과 OS는 구성 파일을 숨기므로, 사용자가 실수로 수정하거나 삭제할 가능성을 줄입니다. 또한, 일부 OS에서는 삭제된 디렉토리가 숨김으로 표시될 수 있습니다. 숨겨진 데이터에는 풍부한 정보가 포함될 수 있습니다. 예를 들어, 숨겨진 파티션에는 별도의 OS와 많은 데이터 파일이 포함될 수 있습니다. 사용자는 파티션 테이블을 변경하여 디스크 관리를 방해하고 응용 프로그램이 데이터 영역에 있음을 알 수 없도록 숨겨진 파티션을 만들 수 있습니다. 숨겨진 데이터는 NTFS 볼륨의 ADS, 파일의 슬랙 공간 및 매체의 슬랙 공간, 드라이브의 영역인 일부 하드 드라이브의 벤더사에 의해 사용되도록 의도된 HPA(Host Protected Area)에서도 찾을 수 있습니다. 많은 수집 도구는 데이터를 숨기고 관련 데이터를 복구하는 이러한 방법 중 일부 또는 전부를 인식할 수 있습니다.

발생할 수 있는 또 다른 문제는, 스트라이핑(예 : RAID-0, RAID-5)을 사용하는 RAID 어레이에서 데이터를 수집하는 것입니다. 이 구성에서 스트라이프 볼륨은 별도의 디스크 드라이브에 있는 동일한 크기의 파티션으로 구성됩니다. 데이터가 볼륨에 기록되면 디스크 성능을 향상시키기 위해 파티션 전체에 데이터가 고르게 분산됩니다. 스트라이프 볼륨의 모든 파티션이 내용 검사를 위해 있어야 하기 때문에 문제가 발생할 수 있지만, 이 경우 파티션은 별도의 물리적 디스크 드라이브에 상주합니다. 스트라이프 볼륨을 검사하려면 RAID 어레이의 각 디스크 드라이브를 이미징해야 하고 RAID 구성을 검사 시스템에서 다시 만들어야 합니다. 검사 시스템은 RAID를 인식하고 사용할 수 있는 포렌식 부트 디스크를 사용하여 쓰기 방지로 부팅해야 합니다. 일부 이미징 도구는 스트라이프된 볼륨을 확보하고 자유 공간 및 슬랙 공간과 같이 볼륨의 사용하지 않는 데이터 영역을 보존할 수 있습니다.

## 4.3 데이터 파일 검사

논리적 백업 또는 비트 스트림 이미징이 수행된 후, 데이터 검사 전에 백업 또는 이미지를 다른 미디어로 복원해야 할 수 있습니다. 이는 분석을 수행하는 데 사용되는 포렌식 도구에 따라 다릅니다. 일부 도구는 이미지 파일에서 직접 데이터를 분석 할 수 있지만, 다른 도구는 백업 또는 이미지를 먼저 매체로 복원해야 합니다. 이미지 파일 또는 복원된 이미지가 검사에 사용되는지 여부에 관계없이, 검사되는 데이터가 수정되지 않은 것을 보증하기 위해 오직 읽기 전용으로 접근되어야 한다. 4.2.2절에서 언급했듯이, 이 과정에서 쓰기 차단기를 사용하여 복원된 이미지에 쓰기가 발생하지 않도록 할 수 있습니다. 필요한 경우 백업을 복원한 후, 분석자는 수집된 데이터를 검사하기 시작하고 삭제된 파일, 자유 및 슬랙 공간에 있는 파일 잔여물 및 숨겨진 파일을 포함하여 모든 파일을 찾아 관련 파일 및 데이터에 대한 평가를 수행합니다. 그런 다음 분석가는 파일의 일부 또는 전체에서 데이터를 추출해야 할 수 있습니다. 암호화 및 암호 보호와 같은 방법으로 복잡해 질 수도 있습니다. 이 절에서는 파일 및 데이터 검사 과정과 검사를 신속하게 처리할 수 있는 기술에 대해 설명합니다.

### 4.3.1 파일 찾기

검사의 첫 번째 단계는 파일을 찾는 것입니다. 디스크 이미지는 수십 개의 파일과 파일 조각을 포함할 수 있는 많은 자유 공간과 슬랙 공간을 캡처할 수 있습니다. 사용되지 않는 공간에서 수동으로 데이터를 추출하는 것은 기본 파일 시스템 형식에 대한 지식이 필요하기 때문에, 시간이 많이 소요되는 어려운 프로세스가 될 수 있습니다. 다행스럽게도 사용하지 않은 공간에서 데이터를 추출하고 이를 데이터 파일에 저장하는 프로세스를 자동화하고 휴지통에서 삭제된 파일 및 파일을 복구할 수 있는 여러 가지 도구를 사용할 수 있습니다. 분석가는 16진수 편집기 또는 특수 슬랙 복구 도구를 사용하여 슬랙 공간의 내용을 표시할 수도 있습니다.

### 4.3.2 데이터 추출

나머지 검사 과정에는 일부 또는 모든 파일에서 데이터를 추출하는 과정이 포함됩니다. 분석가는 파일의 내용을 이해하기 위해 파일에 포함된 데이터의 유형을 알아야 합니다. 파일 확장자의 의도 된 목적은 파일 내용의 성격을 나타내는 것입니다. 예를 들어, jpg 확장자는 그래픽 파일을 나타내며 mp3 확장명은 음악 파일을 나타냅니다. 그러나 사용자는 텍스트 파일인 mysong.mp3의 이름을 지정하거나 파일 확장명을 생략하는 등 모든 유형의 파일에 파일 확장명을 할당할 수 있습니다. 또한, 일부 파일 확장명은 숨겨져 있거나 다른 OS에서 지원되지 않을 수 있습니다. 따라서 분석가는 파일 확장명이 정확하다고 가정해서는 안됩니다.

분석가는 파일 헤더를 보고 많은 파일에 저장된 데이터 유형을 보다 정확하게 식별 할 수 있습니다. 파일 헤더에는 파일에 대한 식별 정보와 파일 내용에 대한 정보를 제공하는 메타 데이터가

들어 있습니다. [그림 4-1]에 표시된 것처럼 파일 헤더에는 특정 파일에 포함된 데이터 유형을 식별하는 파일 시그니처가 포함되어 있습니다. [그림 4-1]의 예는 파일 헤더가 FF D8이며 JPEG 파일임을 나타냅니다. 파일 헤더는 실제 파일 데이터와 별도의 파일에 위치 할 수 있습니다. 파일의 데이터 유형을 식별하는 또 다른 효과적인 기술은 파일의 총 문자 수에 대한 ASCII 값 분포를 보여주는 간단한 히스토그램입니다. 예를 들어, 'space', 'a' 및 'e' 행의 스파이크는 일반적으로 텍스트 파일을 나타내지만 막대 그래프의 일관성은 압축 된 파일을 나타냅니다. 다른 패턴은 암호화되거나 스테가노 그래피를 통해 수정된 파일을 나타냅니다.

Offset	0	1	2	3	4	5	6	7	8	9	À	B	C	D	E	F
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01
00000010	00	01	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27
00000050	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09
00000060	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32

[그림 4-1 : 파일 헤더 정보]

암호화는 종종 분석가에게 어려움을 줍니다. 사용자는 개별 파일, 폴더, 볼륨 또는 파티션을 암호화하여 해독키나 패스워드 없이는 다른 사람이 내용에 접근하지 못하게 할 수 있습니다. 암호화는 OS 또는 타사 프로그램에서 수행할 수 있습니다. 암호화된 파일을 식별하는 것은 상대적으로 쉽지만 일반적으로 암호화된 파일을 해독하는 것은 쉽지 않습니다. 분석가는 파일 헤더를 검사하거나 시스템에 설치된 암호화 프로그램을 식별하거나 암호화 키(다른 미디어에 저장되는 경우가 있음)를 찾아 암호화 방법을 식별할 수 있습니다. 일단 암호화 방법이 알려지면 분석가는 파일 암호 해독의 가능성을 보다 잘 판단할 수 있습니다. 대부분의 경우 암호화 방법이 너무 강하고 암호 해독을 수행하는데 사용되는 인증(예: 암호)을 사용할 수 없으므로 파일을 해독할 수 없습니다.

분석가가 암호화된 데이터의 존재를 쉽게 감지할 수는 있지만, 스테가노그래피를 감지하는 것은 더 어렵습니다. 스테가노그래피는 stego라고도 하며 다른 데이터 내에 데이터를 포함시키는 것입니다. 디지털 워터마크와 이미지 내에 단어 및 정보를 숨기는 것이 스테가노그래피의 예입니다. 분석가가 데이터를 찾는 데 사용할 수 있는 몇 가지 기술은 동일한 이미지의 여러 버전을 찾고, 그레이 스케일 이미지가 있는지 확인하고, 메타 데이터 및 레지스트리를 검색하고, 히스토그램을 사용하고, 해시 세트를 사용하여 알려진 스테가노 소프트웨어를 검색하는 것입니다. 일단 스테깅된 데이터가 존재한다면, 분석가들은 어떤 소프트웨어가 데이터를 생성했는지 결정한 다음 stego 키를 찾거나 무차별 대입 및 암호 공격을 사용하여 암호를 결정함으로써 내장된 데이터를 추출할 수 있습니다. 그런 노력은 종종 분석가가 검토중인 미디어에 알려진 스테가노 소프트웨어의 존재

를 발견하지 못하면, 특히 시간 낭비일 수 있습니다. 또한, 일부 소프트웨어 프로그램은 파일을 분석하고 파일이 스테가노그래피로 변경되었을 가능성을 추정합니다.

분석가들은 패스워드로 보호되는 비스테가노 파일에 액세스해야 할 수도 있습니다. 암호는 종종 보호하는 파일과 동일한 시스템에 저장되지만 암호화되거나 암호화된 형식으로 저장됩니다. OS 암호 뿐만 아니라 개별 파일에 설정된 암호를 해독할 수 있는 다양한 유ти리티를 사용할 수 있습니다. 대부분의 크래킹 유ти리티는 가능한 모든 암호를 시도하는 무차별 대입 시도를 수행할 뿐만 아니라, 암호를 추측할 수 있습니다. 암호화된 암호에 대한 무차별 대입 공격에 필요한 시간은 사용되는 암호화 유형과 암호 자체의 정교함에 따라 크게 다를 수 있습니다. 또 다른 방법은 암호를 우회하는 것입니다. 예를 들어, 분석가는 시스템을 부팅하고 화면 보호기 암호를 비활성화하거나 시스템의 메인보드 BIOS 점퍼를 가져 와서 BIOS(Basic Input / Output System) 암호를 무시하거나 제조사의 백도어 패스워드 사용 등이 있습니다. 물론 암호를 무시하면, 시스템이 재부팅될 수 있으므로 바람직하지 않을 수 있습니다. 또 다른 가능성은 적절한 관리 및 법적 승인을 받아 네트워크 또는 호스트 기반 컨트롤(예: 패킷 스니퍼, 키 입력 로거)을 통해 비밀번호를 캡처하려고 시도하는 것입니다. 하드 드라이브에 부팅 암호가 설정되어있는 경우 해당 암호(예: 공급 업체의 기본 암호)를 추측하거나 특수한 하드웨어 및 소프트웨어로 암호를 우회할 수 있습니다.

#### 4.3.3 포렌식 툴킷 사용

분석가는 데이터 수집 및 분석을 수행할 수 있는 다양한 도구에 액세스할 수 있어야합니다. 많은 포렌식 제품을 사용해서 분석가는 파일 및 응용 프로그램을 분석하고 파일을 수집하고 디스크 이미지를 읽고 파일에서 데이터를 추출하는 등 다양한 프로세스를 수행할 수 있습니다. 대부분의 분석 제품은 또한 보고서를 생성하고 분석 중에 발생한 모든 오류를 기록하는 기능을 제공합니다. 이러한 제품은 분석 수행시 매우 중요하지만, 데이터에 대한 특정 질문에 대답하기 위해 어떤 프로세스를 실행해야 하는지를 이해하는 것이 중요합니다. 분석가는 신속한 응답을 제공하거나 수집된 데이터에 대한 간단한 질문에 답해야 할 수도 있습니다. 이러한 경우 완전한 포렌식 평가가 필요하지 않거나, 실행 가능하지 않을 수도 있습니다. 포렌식 툴킷에는 다양한 방법으로 데이터 검사 및 분석을 수행할 수 있는 응용 프로그램이 있어야하며, 플로피 디스크, CD 또는 포렌식 워크 스테이션에서 신속하고 효율적으로 실행할 수 있어야 합니다. 다음 프로세스는 분석가가 다양한 도구로 수행할 수 있어야 하는 프로세스입니다.

- 파일 뷰어 사용:** 원본 응용 프로그램 대신 뷰어를 사용하여 특정 파일 형식의 내용을 표시하는 것은 데이터를 검색하거나 미리 보는 중요한 기술이며, 분석자가 각 파일 형식을 볼 수 있는 네이티브 응용 프로그램을 필요로 하지 않기 때문에 보다 효율적입니다. 일반적인 유형의 파일을 볼 수 있는 다양한 도구가 있으며, 그래픽 전용 보기 전용 도구도 있습니다. 사용 가능한 파일 뷰어가 특정 파일 형식을 지원하지 않으면, 원본 소스 응용 프로그램을 사용해야 합니다. 이것이 가능하지 않다면,

파일 형식을 연구하고 수동으로 파일에서 데이터를 추출해야 할 수도 있습니다.

2. **파일 압축 해제:** 압축 파일에는 유용한 정보뿐만 아니라 다른 압축 파일이 포함될 수 있습니다. 따라서 분석가가 압축 파일을 찾아 추출하는 것이 중요합니다. 압축 파일의 내용이 검색 및 기타 작업에 포함되도록 포렌식 프로세스 초기에 파일 압축을 풀어야 합니다. 그러나 분석가는 압축 파일에 일반적으로 수십 또는 수백번 반복 압축된 압축 폭탄과 같은 악의적인 콘텐츠가 포함될 수 있다는 점을 명심해야 합니다. 압축 폭탄으로 인해 검사 도구가 실패하거나 상당한 자원을 소비할 수 있습니다. 악성 코드 및 기타 악의적인 페이로드도 포함될 수 있습니다. 파일을 압축 해제하기 전에 압축 폭탄을 감지하는 확실한 방법은 없지만, 그 영향을 최소화할 수 있는 방법이 있습니다. 예를 들어, 검사 시스템은 최신 바이러스 백신 소프트웨어를 사용해야하며, 해당 시스템에만 영향을 미치도록 독립 실행형이어야합니다. 또한, 필요한 경우 시스템을 복원할 수 있도록 검사 시스템의 이미지를 작성해야합니다.
3. **그래픽으로 디렉토리 구조 표시:** 이렇게 하면, 분석가는 설치된 소프트웨어의 유형 및 데이터를 만든 사용자의 기술적 적성과 같은 미디어 내용에 대한 일반 정보를 수집하는 것이 더 쉽고 빠릅니다. 대부분의 제품은 Windows, Linux 및 UNIX 디렉토리 구조를 표시할 수 있지만, 다른 제품은 Macintosh 디렉토리 구조에만 해당됩니다.
4. **알려진 파일 확인:** 관심있는 파일을 찾는 이점은 분명하지만, 잘 알려진 OS 및 응용 프로그램 파일과 같은 중요하지 않은 파일을 고려하지 않는 것이 좋습니다. 분석가들은 알려진 양성 및 악의적인 파일을 식별하기 위한 기초로 NIST의 NSRL(National Software Reference Library) 프로젝트에서 작성한 유효성이 검사된 해시 세트 또는 유효성을 검증받은 개인 작성 해시 세트를 사용해야 합니다. 해시 세트는 일반적으로 SHA-1 및 MD5 알고리즘을 사용하여 알려진 각 파일에 대한 메시지 요약 값을 설정합니다.
5. **문자열 검색 및 패턴 일치 수행:** 문자열 검색은 많은 양의 데이터를 열람하여 키워드 또는 문자열을 찾습니다. 부울, 퍼지 논리, 동의어와 개념, 형태소 분석 및 기타 검색 방법을 사용할 수 있는 다양한 검색 도구를 사용할 수 있습니다. 일반적인 검색의 예로는 단일 파일에서 여러 단어 검색 및 특정 단어의 맞춤법이 잘못된 버전 검색을 들 수 있습니다. 일반적인 상황에 대한 간결한 검색 용어 세트를 개발하면 분석자가 검토할 정보량을 줄일 수 있습니다. 문자열 검색을 수행 할 때, 고려해야 할 몇 가지 고려 사항 또는 가능한 어려움은 다음과 같습니다:
  - 일부 독점적인 파일 형식은 추가 도구 없이 문자열을 검색할 수 없습니다. 또한 압축, 암호화 및 암호로 보호된 파일은 문자열 검색 전에 추가 사전 처리가 필요합니다.
  - 외부 또는 유니 코드 문자를 포함하는 다중 문자 데이터 세트를 사용하면 문자열 검색에 문제가 발생할 수 있습니다. 일부 검색 도구는 언어 변환 기능을 제공하여 이를 극복하려고 시도합니다.
  - 또 다른 가능한 문제는 검색 도구 또는 알고리즘의 고유 한계입니다. 예를 들어, 문자열의 일부가 한 클러스터에 있고 문자열의 나머지가 인접하지 않은 클러스터에 있는 경우 검색 문자열에 대해 일치 항목을 찾지 못할 수 있습니다. 마찬가지로 일부 검색 도구는 검색 문자열의 일부가 하나의 클러스터에 있고 나머지 문자열이 첫 번째 클러스터를 포함하는 동일한 파일의 일부가 아닌 다른 클러스터에 있을 경우 거짓 일치를 보고 할 수 있습니다.

6. 파일 메타 데이터 액세스: 파일 메타 데이터는 주어진 파일에 대한 세부 정보를 제공합니다. 예를 들어, 그래픽 파일에 메타 데이터를 수집하면 그래픽의 생성 날짜, 저작권 정보 및 설명과 제작자의 ID가 제공될 수 있습니다. 디지털 카메라에서 생성된 그래픽의 메타 데이터에는 사용된 디지털 카메라의 제조업체와 모델이 포함될 수 있습니다 이미지, F- 스톱, 플래시 및 조리개 설정이 포함됩니다. 워드 프로세싱 파일의 경우 메타 데이터는 작성자, 소프트웨어를 라이센스한 조직, 편집자가 언제 그리고 누구에 의해 마지막으로 수행되었는지, 사용자 정의 주석을 지정할 수 있습니다. 특수 유ти리티는 파일에서 메타 데이터를 추출할 수 있습니다.

#### 4.4 분석

검사가 완료되면 다음 단계는 추출된 데이터의 분석을 수행하는 것입니다. 4.3.3절에서 언급했듯이, 다양한 유형의 데이터 분석에 도움이 되는 많은 도구가 있습니다. 이러한 도구를 사용하거나 데이터의 수동 검토를 수행할 때 분석가는 시스템 시간 및 파일 시간 사용의 가치를 인식해야 합니다. 사건이 언제 발생했는지, 파일을 만들거나 수정했는지, 전자 메일을 보냈는지 알면 포렌식 분석에 중요할 수 있습니다. 예를 들어, 이러한 정보는 활동의 타임라인을 재구성하는데 사용될 수 있습니다. 비록 이것이 간단한 업무처럼 보일지라도 시스템 사이에서 시간 설정은 의도한 혹은 의도하지 않은 불일치로 인해 매우 복잡합니다. 데이터가 분석될 컴퓨터의 시간, 날짜 및 시간 대 설정을 알고 있으면 분석가를 크게 지원할 수 있습니다. 5절에서 이에 대해 자세히 설명합니다.

조직에서 정확한 타임스탬프를 사용하여 시스템을 유지 관리하는 것은 일반적으로 분석가에게 도움이 됩니다. NTP(Network Time Protocol)는 NIST 또는 다른 조직에서 실행하는 원자 시계로 컴퓨터의 시간을 동기화합니다. 동기화를 통해 각 시스템이 합리적으로 정확한 시간 측정을 유지할 수 있습니다.

여러 도구를 사용하여 검사 및 분석을 완료하는 경우 분석가는 각 도구가 파일 수정, 액세스 및 작성(MAC) 시간을 추출, 수정 및 표시하는 방법을 이해해야 합니다. 예를 들어, 일부 도구는 파일 시스템이 OS에 의해 쓰기 권한으로 마운트된 경우 파일 또는 디렉토리의 마지막 액세스 시간을 수정합니다. 쓰기 차단기는 이러한 도구가 MAC 시간을 수정하는 것을 방지하는 데 사용할 수 있습니다. 그러나 쓰기 차단기는 이러한 시간이 미디어에서 수정되는 것을 방지 할 수 있지만, OS가 메모리의 변경 내용을 캐싱하지 못하게 할 수는 없습니다.(즉, 변경 내용을 임의 액세스 메모리 [RAM]에 저장하는 것) 그런 다음 OS는 실제 시간이 아니라 캐시된 MAC 시간을 보고할 수 있으므로, 부정확한 결과가 반환될 수 있습니다. 분석가는 쿼리를 수행하는데 사용되는 도구에 따라 데이터 파일 및 디렉토리의 마지막 액세스 시간이 쿼리 간에 변경될 수 있음을 알아야 합니다. 이러한 문제로 인해 분석가는 MAC 보기 방법을 선택하고 해당 방법의 세부 사항을 기록해야 합니다.

분석가는 이벤트 데이터를 기반으로 포렌식 타임라인을 생성할 수 있는 특수 도구를 사용할 수 있습니다. 이러한 도구는 일반적으로 분석가에게 일련의 이벤트를 보고, 분석할 수 있는 그래픽

인터페이스를 제공합니다. 이러한 도구의 공통적인 특징은 분석가가 관련 이벤트를 메타 이벤트로 그룹화 할 수 있도록 하는 것입니다. 이를 통해, 분석가는 이벤트에 대한 "큰 그림" 뷰를 얻을 수 있습니다.

대부분의 경우, 포렌식 분석에는 파일의 데이터뿐만 아니라 OS 상태, 네트워크 트래픽 또는 응용 프로그램과 같은 다른 출처의 데이터도 포함됩니다. 8절에서는 분석을 통해 파일의 데이터와 다른 소스의 데이터를 어떻게 상관시킬 수 있는지에 대한 예제를 제공합니다.

## 4.5 권고 사항

이 절에서 데이터 파일의 데이터 사용에 대한 주요 권장 사항은 다음과 같습니다.

- 분석가는 원본 파일이 아닌 파일의 복사본을 검사해야 합니다. 수집 단계에서 분석가는 원하는 파일이나 파일 시스템(일반적으로 마스터 복사본과 작업 복사본)을 여러 복사본으로 만들어야합니다. 그런 다음 분석가는 원본 파일이나 마스터 복사본에 영향을 주지 않고, 파일의 작업 복사본을 사용하여 작업할 수 있습니다. 기소 또는 징계 조치에 필요한 증거가 있거나 파일 보관 기간이 중요한 경우 비트 스트림 이미지를 수행해야합니다.
- 분석가는 파일 무결성을 보존하고 검증해야 합니다. 백업 및 이미징 중에 쓰기 차단 기능을 사용하면 컴퓨터가 해당 저장 미디어에 쓰는 것을 방지할 수 있습니다. 복사된 데이터의 무결성은 파일의 메시지 요약을 계산하고 비교하여 확인해야 합니다. 백업 및 이미지는 가능할 때마다, 읽기 전용으로 액세스해야 합니다. 쓰기 차단기를 사용하여 백업 또는 이미지 파일 또는 복원된 백업에 대한 쓰기를 방지할 수도 있습니다.
- 분석가는 파일 내용 유형을 식별하기 위해 파일 확장명이 아닌 파일 헤더에 의존해야합니다. 사용자는 파일 확장명을 파일에 할당할 수 있으므로 분석가는 파일 확장명이 정확하다고 가정해서는 안됩니다. 분석가는 파일 헤더를 보고 많은 파일에 저장된 데이터 유형을 식별할 수 있습니다. 파일 헤더를 변경하여 실제 파일 형식을 숨길 수는 있지만, 파일 확장명을 변경하는 것보다 훨씬 덜 일반적입니다.
- 분석가는 데이터 조사 및 분석을 위한 포렌식 툴킷을 보유해야 합니다. 툴킷에는 데이터의 신속한 검토는 물론 심층 분석을 수행할 수 있는 다양한 도구가 포함되어야 합니다. 이 툴킷은 이동식 미디어(예: 플로피 디스크, CD) 또는 포렌식 워크 스테이션에서 응용 프로그램을 빼르고 효율적으로 실행할 수 있어야합니다.

## 5. 운영 체제의 데이터 사용

운영 체제(OS)는 컴퓨터에서 실행되며 다른 프로그램을 실행할 수 있는 소프트웨어 플랫폼을 제공하는 프로그램입니다. 또한, OS는 사용자의 입력 명령을 처리하고 디스플레이에 출력을 보내며 저장 장치와 상호 작용하여 데이터를 저장 및 검색하고 프린터 및 모뎀과 같은 주변 장치를 제어합니다. 워크 스테이션이나 서버의 일반적인 OS에는 Windows, Linux, UNIX 및 Mac OS의 다양한 버전이 있습니다. 라우터와 같은 일부 네트워크 장치에는 자체 OS(예: Cisco Internetwork Operating System[IOS])가 있습니다. PDA는 종종 PalmOS 및 Windows CE를 포함한 특수한 OS를 실행합니다. 휴대폰, 디지털 카메라, 오디오 플레이어와 같은 많은 임베디드 시스템에서도 OS를 사용합니다. 이 절에서는 과학 수사와 관련이 있을 수 있는 운영 체제의 구성 요소에 대해 설명하고, 일반적인 워크 스테이션 및 서버 OS의 데이터 수집, 검사 및 분석 지침을 제공합니다.

### 5.1 OS 기초

OS 데이터는 비휘발성 및 휘발성 상태로 존재합니다. 비 휘발성 데이터는 하드 드라이브에 저장된 파일 시스템과 같이 컴퓨터의 전원이 꺼진 후에도 유지되는 데이터를 나타냅니다. 휘발성 데이터란 현재 시스템에 연결된 네트워크 연결과 같이 컴퓨터의 전원이 꺼진 후에 손실되는 라이브 시스템의 데이터를 말합니다. 많은 유형의 비휘발성 및 휘발성 데이터가 포렌식의 관점에서 중요할 수 있습니다. 이 절에서는 이러한 유형의 OS 데이터에 대해 설명합니다.

#### 5.1.1 비휘발성 데이터

OS 내의 비휘발성 데이터의 주된 소스는 파일시스템입니다. 파일시스템은 보통 OS 내에서 가장 크고 가장 풍부한 데이터 소스이기도 하며, 일반적인 포렌식 이벤트 중에 복구되는 대부분의 정보를 포함합니다. 파일시스템은 하나 이상의 미디어에 OS를 위한 저장 공간을 제공합니다. 파일시스템은 일반적으로 다양한 유형의 파일을 포함하며, 각 파일은 여러 상황에서 분석가에게 가치가 있을 수 있습니다. 또한, 4.1.2절에서 언급했듯이 중요한 잔여 데이터도 사용하지 않는 파일 시스템 공간에서 복구할 수 있습니다. OS 파일 시스템에서 흔히 볼 수 있는 몇 가지 유형의 데이터는 다음과 같습니다.

- **설정 파일:** OS는 OS 및 응용 프로그램 설정을 저장하기 위해 구성 파일을 사용할 수 있습니다. 예를 들어, 설정 파일은 시스템 부팅 후 자동으로 시작될 서비스를 나열하고 로그 파일과 임시 파일의 위치를 지정할 수 있습니다. 또한, 사용자는 하드웨어 관련 설정(예: 화면 해상도, 프린터 설정) 및 파일 연결과 같은 사용자별 정보 및 기본 설정을 포함하는 개별 OS 및 응용 프로그램 설정 파일을 가질 수 있습니다. 특히, 중요한 설정 파일은 다음과 같습니다:

1. **사용자 및 그룹:** OS는 사용자 계정과 그룹에 대한 기록을 유지합니다. 계정 정보에는 그룹 회원, 계정명 및 설명, 계정 권한, 계정 상태(예: 활성, 비활성) 및 계정 홈 디렉토리 경로가 포함될 수 있습니다.
  2. **암호 파일:** OS는 데이터 파일에 암호 해시를 저장할 수 있습니다. 다양한 암호 해독 유ти리티를 사용하여 암호 해시를 특정 OS에 해당하는 일반 텍스트로 변환할 수 있습니다.
  3. **예약된 작업:** OS는 특정 시간에 자동으로 수행되어야 하는 스케줄된 작업의 리스트를 유지합니다.(예를 들어, 매주 바이러스 스캔을 수행) 여기에서 수집할 수 있는 정보에는 작업 이름, 작업을 수행하는 데 사용된 프로그램, 명령 줄 스위치 및 인수, 작업을 수행할 요일과 시간이 포함됩니다.
- **로그:** OS 로그 파일에는 다양한 OS 이벤트에 대한 정보가 포함되어 있으며, 응용 프로그램별 이벤트 정보를 보유할 수도 있습니다. 운영 체제에 따라 로그는 텍스트 파일, 독점 형식의 이진 파일 또는 데이터베이스에 저장될 수 있습니다. 일부 OS는 두 개 이상의 개별 파일에 로그 항목을 작성합니다. OS 로그에서 일반적으로 발견되는 정보 유형은 다음과 같습니다.
1. **시스템 이벤트:** 시스템 이벤트는 시스템을 종료하거나 서비스를 시작하는 것과 같은 OS 구성 요소에 의해 수행되는 운영 작업입니다. 일반적으로 실패 이벤트와 가장 중요한 성공 이벤트가 기록되지만, 많은 OS가 시스템 관리자가 어떤 유형의 이벤트를 기록할지 지정할 수 있습니다. 각 이벤트에 기록된 세부 사항도 매우 다양합니다. 각 이벤트는 일반적으로 타임스탬프가 적용됩니다. 다른 지원 정보에는 이벤트 코드, 상태 코드 및 사용자 이름이 포함될 수 있습니다.
  2. **감사 기록:** 감사 레코드에는 성공 및 실패한 인증 시도 및 보안 정책 변경과 같은 보안 이벤트 정보가 포함됩니다. OS는 일반적으로 시스템 관리자가 어떤 유형의 이벤트를 감사해야 하는지 지정할 수 있습니다. 또한, 관리자는 특정 동작을 수행하려는 성공, 실패 또는 모든 시도를 기록하도록 일부 OS를 구성할 수 있습니다.
  3. **응용 프로그램 이벤트:** 응용 프로그램 이벤트는 응용 프로그램 시작 및 종료, 응용 프로그램 오류 및 주요 응용 프로그램 구성 변경과 같이 응용 프로그램에서 수행하는 중요한 작업 동작입니다. 7절에는 응용 프로그램 이벤트 로깅에 대한 자세한 정보가 들어 있습니다.
  4. **명령 기록:** 일부 OS에는 각 사용자가 수행한 OS 명령의 내역을 포함하는 별도의 로그 파일(일반적으로 각 사용자마다)이 있습니다.
  5. **최근 액세스한 파일:** OS는 가장 최근에 액세스한 파일의 목록을 작성하여 가장 최근의 파일 액세스 또는 기타 사용을 기록할 수 있습니다.
- **응용 프로그램 파일:** 응용 프로그램은 실행 파일, 스크립트, 설명서, 구성 파일, 로그 파일, 기록 파일, 그래픽, 사운드 및 아이콘을 비롯한 다양한 유형의 파일로 구성될 수 있습니다. 7절에서는 응용 프로그램 파일에 대해 자세히 설명합니다.

- **데이터 파일:** 데이터 파일은 응용 프로그램에 대한 정보를 저장합니다. 일반적인 데이터 파일의 예로는 텍스트 파일, 워드 프로세싱 문서, 스프레드 시트, 데이터베이스, 오디오 파일 및 그래픽 파일이 있습니다. 또한, 데이터가 인쇄될 때 대부분의 OS는 인쇄용 버전의 데이터를 포함하는 하나 이상의 임시 인쇄 파일을 작성합니다. 4절과 7절에서는 응용 프로그램 데이터 파일에 대해 자세히 설명합니다.
- **스왑 파일:** 대부분의 OS는 스왑 파일을 RAM과 함께 사용하여, 응용 프로그램에서 자주 사용하는 데이터를 임시로 저장합니다. 스왑 파일은 본질적으로 프로그램을 위한 가용 가능한 메모리양의 확장입니다. 그리고 그것은 램으로부터 스왑인-아웃되기 위해 페이지 혹은 세그먼트를 사용합니다. 스왑 파일에는 사용자 이름, 암호 해시 및 연락처 정보와 같은 광범위한 OS 및 응용 프로그램 정보가 포함될 수 있습니다. 5.1.2절에서는 메모리의 내용을 보다 자세히 설명합니다.
- **덤프 파일:** 일부 OS는 오류 상황에서 자동으로 메모리의 내용을 저장하여 후속 문제 해결을 지원합니다. 저장된 메모리 내용을 보유하는 파일을 덤프 파일이라고합니다.
- **최대 절전 모드 파일(Hibernation file):** 최대 절전 모드 파일은 시스템을 종료하기 전에 메모리를 기록하고 파일을 열어 시스템의 현재 상태(일반적으로 랩톱)를 보존하기 위해 작성됩니다. 다음에 시스템을 켜면 시스템의 상태가 복원됩니다.
- **임시 파일:** OS, 응용 프로그램 또는 응용 프로그램 업데이트 및 업그레이드 설치 중에 임시 파일이 종종 만들어집니다. 이러한 파일은 일반적으로 설치 프로세스가 끝날 때 삭제되지만 항상 발생하는 것은 아닙니다. 또한, 많은 응용 프로그램이 실행될 때 임시 파일이 만들어집니다. 다시 말하지만, 이러한 파일은 대개 응용 프로그램이 종료될 때 삭제되지만 항상 발생하는 것은 아닙니다. 임시 파일에는 시스템의 다른 파일, 응용 프로그램 데이터 또는 기타 정보의 사본이 들어있을 수 있습니다.

파일 시스템이 비휘발성 데이터의 주요 소스이지만, 다른 흥미로운 대상은 BIOS입니다. BIOS에는 연결된 장치(예: CDROM 드라이브, 하드 드라이브), 연결 유형 및 인터럽트 요청 라인(IRQ) 할당(예: 직렬, USB, 네트워크 카드), 마더 보드 구성 요소(예: 프로세서 유형 및 속도, 캐시 크기, 메모리 정보), 시스템 보안 설정 및 바로가기 키 등이 있습니다. BIOS는 또한 RAID 드라이버와 통신하고 드라이버가 제공하는 정보를 표시합니다. 예를 들어, BIOS는 하드웨어 RAID를 단일 드라이브로, 소프트웨어 RAID를 다중 드라이브로 간주합니다. BIOS는 일반적으로 사용자가 암호를 설정하도록 허용하여 BIOS 설정에 대한 액세스를 제한하고 암호가 제공되지 않으면 시스템이 부팅되지 않도록 합니다.

록 할 수 있습니다. BIOS에는 시스템 날짜와 시간도 저장됩니다.

### 5.1.2 휘발성 데이터

OS는 시스템의 RAM 내에서 실행됩니다. OS가 작동하는 동안 RAM 내용이 계속 변경됩니다. 주어진 시간에 RAM에는 많은 유형의 데이터와 정보가 포함될 수 있습니다. 예를 들어, RAM에는 자주 데이터 파일, 암호 해시 및 최근 명령과 같이 자주 액세스하는 데이터와 최근에 액세스한 데이터가 들어 있습니다. 또한 파일 시스템과 마찬가지로 RAM에도 다음과 같이 빈 공간과 여유 공간에 잔여 데이터가 포함될 수 있습니다.

- **슬랙 공간:** 메모리 슬랙 공간은 파일 슬랙 공간보다 훨씬 덜 결정론적입니다. 예를 들어, OS는 일반적으로 페이지 또는 블록이라고하는 단위로 메모리를 관리하고 이를 요청하는 응용 프로그램에 할당합니다. 때로는 응용 프로그램이 전체 장치를 요청하지 않을 수도 있지만, 어쨌든 하나만 지정됩니다. 따라서 잔여 데이터는 응용 프로그램에 할당할 수 있는 메모리 단위에 상주할 수 있지만 응용 프로그램에서 처리할 수는 없습니다. 성능과 효율성 면에서 일부 OS는 할당하는 장치의 크기가 다양하기 때문에 메모리 여유 공간은 더 작아지는 경향이 있습니다.
- **자유 공간:** 메모리 페이지는 파일 클러스터처럼 할당되고 할당이 해제됩니다. 할당되지 않은 메모리 페이지는 흔히 가비지 컬렉션이라고하는 가용 페이지의 공통 풀로 수집됩니다. 할당되지 않은 파일 클러스터와 유사한 이러한 재사용 가능한 메모리 페이지에 잔여 데이터가 상주하는 경우는 드뭅니다.

OS 내에 존재할 수 있는 다른 중요한 유형의 휘발성 데이터는 다음과 같습니다:

- **네트워크 구성:** 네트워크 인터페이스 카드(NIC) 드라이버 및 구성 설정과 같은 네트워킹의 많은 요소가 일반적으로 파일 시스템에 저장되지만, 네트워킹은 사실상 동적입니다. 예를 들어, 많은 호스트에 다른 호스트가 IP 주소를 동적으로 할당합니다. 즉, IP 주소는 저장된 구성의 일부가 아닙니다. 또한 많은 호스트에는 유선, 무선, 가상 사설망(VPN) 및 모뎀과 같은 여러 네트워크 인터페이스가 정의되어 있습니다. 현재 네트워크 구성은 현재 사용중인 인터페이스를 나타냅니다. 또한, 사용자는 수동으로 IP 주소를 변경하는 등 네트워크 인터페이스 구성을 기본 값에서 변경할 수 있습니다. 따라서 분석가는 가능하면 저장된 구성이 아닌 현재 네트워크 구성을 사용해야합니다.
- **네트워크 연결:** OS는 시스템과 다른 시스템 간의 연결을 용이하게합니다. 대부분의 OS는 현재 들어오고 나가는 네트워크 연결 목록을 제공할 수 있으며, 일부 OS는 최근 연결도 나열할 수 있습니다. 들어오는 연결의 경우 OS는 일반적으로 파일 공유 및 프린터와 같이 사용중인 리소스를 나타냅니다.

냅니다. 대부분의 OS는 시스템이 연결을 청취하는 포트 및 IP 주소 목록을 제공할 수도 있습니다. 6절에서는 네트워크 연결의 중요성을 심층적으로 검토합니다.

- **프로세스 실행:** 프로세스는 현재 컴퓨터에서 실행중인 프로그램입니다. 프로세스에는 운영 체제에서 제공하는 서비스와 관리자 및 사용자가 실행하는 응용 프로그램이 포함됩니다. 대부분의 OS는 현재 실행중인 프로세스의 목록을 볼 수 있는 방법을 제공합니다. 이 목록은 웹 서버와 같은 시스템에서 활성화된 서비스와 개별 사용자가 실행중인 프로그램(예: 암호화 유틸리티, 워드 프로세서, 전자 메일 클라이언트)을 확인하기 위해 조사될 수 있습니다. 프로세스 목록은 7절에서 설명한대로, 어떤 명령 옵션을 사용했는지 나타낼 수도 있습니다. 실행중인 프로세스를 식별하는 것은 실행중이어야 하지만 실행 중지되었거나 제거된 프로그램(예: 바이러스 백신 소프트웨어 및 방화벽)을 식별하는데 유용합니다.
- **열린 파일:** OS는 일반적으로 각 파일을 오픈한 사용자나 프로세스를 포함하는 열린 파일 목록을 유지 관리할 수 있습니다.
- **로그인 세션:** OS는 일반적으로 현재 로그인한 사용자(각 세션의 시작 시간과 지속 시간), 성공한 로그온과 실패한 로그온, 권한 있는 사용 등의 정보를 유지합니다. 그러나 로그인 세션 정보는 컴퓨터가 로그온 시도를 감사하도록 설정된 경우에만 사용할 수 있습니다. 로그온 기록은 사용자의 컴퓨터 사용 습관을 판별하고, 주어진 이벤트가 발생할 때 사용자 계정이 활성 상태인지 여부를 확인하는데 도움이됩니다.
- **운영 체제 시간:** OS는 현재 시간을 유지하고 일광 절약 시간 및 시간대 정보를 저장합니다. 이 정보는 이벤트의 타임라인을 작성하거나, 다른 시스템간에 이벤트를 상관시킬 때 유용할 수 있습니다. 분석가는 타임존 같은 OS 관련 설정 때문에, OS에 특정된 시간과 BIOS가 제공한 시간이 다를 수 있음을 알고 있어야합니다.

## 5.2 OS 데이터 수집

5.1절에서 설명했듯이 OS 데이터는 비휘발성 및 휘발성 상태로 존재합니다. 파일시스템 데이터와 같은 비휘발성 OS 데이터는 논리적 백업 및 비트 스트림 이미징 수행을 통해 4절에서 설명한 방법을 사용하여 수집할 수 있습니다. 컴퓨터의 전원이 꺼지기 전에 휘발성 OS 데이터를 수집해야 합니다. 5.2.1절 및 5.2.2절은 각각 휘발성 및 비휘발성 OS 데이터를 수집하기 위한 권장 사항을 제공합니다. 5.2.3절은 데이터 수집을 방해할 수 있는 기술적 문제에 대해 논의합니다.

### 5.2.1 휘발성 OS 데이터 수집

이벤트와 관련된 휘발성 OS 데이터는 이벤트가 발생한 후 다시 부팅되거나 종료되지 않은 라이브 시스템에서만 수집할 수 있습니다. 시스템에서 수행되는 모든 작업은 사람이 시작했던 OS 자체에서 시작하든 거의 확실하게 휘발성 OS 데이터를 어떤 방식으로든 변경합니다. 따라서 분석가는 휘발성 OS 데이터를 보존할지 여부를 가능한 빨리 결정해야 합니다. 분석가는 최상의 결정을 즉시 내릴 수 있도록 이 결정을 내리는 기준을 미리 문서화해야 합니다. 시스템의 전원을 끄거나 네트워크에서 연결을 끊으면 잠재적으로 중요한 정보를 수집할 기회가 없어지기 때문에 이 결정의 중요성은 충분히 강조되어야 합니다. 예를 들어, 사용자가 최근에 데이터를 보호하기 위해 암호화 도구를 실행한 경우, 컴퓨터의 RAM에 암호 해시가 포함되므로 암호를 확인할 수도 있습니다.

반면에 실행중인 컴퓨터에서 휘발성 OS 데이터를 수집하는 것은 고유한 위험이 있습니다. 예를 들어, 컴퓨터의 파일이 변경되고 기타 휘발성 OS 데이터가 변경될 수 있는 가능성이 항상 존재합니다. 또한, 악의적인 사용자가 잘못된 정보를 반환하거나 파일을 삭제하거나 기타 악의적인 행위를 수행하도록 설계된 루트킷을 설치했을 수 있습니다. 휘발성 데이터를 수집할지 여부를 결정할 때, 이러한 수집과 관련된 위험은 중요한 정보를 복구할 수 있는지의 잠재력에 비중을 두어야 합니다. 3.2절에서 언급했듯이, 증거가 필요할 수 있는 경우, 분석가는 시스템을 만지기 전에 화면에 보이는 것을 완벽하게 문서화해야 합니다. 라이브 시스템이 절전 모드이거나 암호 보호 기능이 있는 경우 분석가는 시스템을 절전 모드에서 깨우거나 암호 보호를 우회하여 시스템의 상태를 변경할지 여부를 결정해야, 분석가는 휘발성 데이터 수집을 시도할 수 있습니다. 휘발성 데이터를 수집하는데 필요한 노력이 도움이 되지 않는다면, 분석가는 5.2.2절에 설명된 대로 종료를 수행하기로 결정할 수 있습니다.

5.2.1.1절은 휘발성 OS 데이터를 수집하기 위한 준비에서 포렌식 도구를 컴파일하는 방법을 설명합니다. 다음 5.2.1.2절에서는 몇 가지 유형의 데이터에 대해 설명하고 각 유형의 데이터를 수집하는 데 효과적인 도구 또는 특정 OS 도구의 범주에 대해 설명합니다. 마지막으로 5.2.1.3절에서는 특정 상황에서 가장 가치가 있는 휘발성 OS 데이터 유형을 식별한 다음, 중요성 및 상대적 변동성에 따라 데이터 수집의 우선 순위를 결정할 필요성을 설명합니다.

#### 5.2.1.1 포렌식 도구 준비

휘발성 OS 데이터를 수집할 때 도구가 실행되어야 하는 플로피 디스크, CD-ROM 또는 USB 플래시 드라이브에 포렌식 도구를 배치해야 합니다. 이렇게하면 분석가는 시스템에 최소한의 방해로 OS 데이터를 수집할 수 있습니다. 또한, 사용자가 시스템 명령을 하드디스크를 포맷하거나 잘못된 정보를 반환하는 악성 프로그램으로 대체했을 수 있으므로 포렌식 도구만 사용해야합니다. 그러나 포렌식 도구를 사용한다고해서 검색된 데이터가 정확하다는 보장은 없습니다. 시스템이

완전히 손상된 경우 커널 수준에서 시스템의 기능을 변경하는 루트킷 및 기타 악성 유ти리티가 설치되었을 수 있습니다. 이로 인해 허위 데이터가 사용자 수준 도구로 반환될 수 있습니다.

포렌식 도구 모음을 만들 때 정적으로 링크된 이진 파일을 사용해야 합니다. 이러한 실행 파일에는 참조하는 모든 함수와 라이브러리 함수가 들어 있으므로 별도의 DLL(동적 연결 라이브러리)과 다른 지원 파일은 필요하지 않습니다. 따라서, 도구 미디어에 적절한 버전의 DLL을 배치할 필요가 없으므로 도구의 신뢰성이 향상됩니다. 분석가는 휘발성 데이터를 수집하기 전에 각 도구가 시스템에 어떤 영향을 미치는지 또는 변경 하는지를 알아야합니다. 각 도구의 메시지ダイアログは는 파일 무결성을 확인하기 위해 안전하게 계산되고 저장되어야 합니다. 각 포렌식 도구에 대한 라이센스 및 버전 정보도 문서화해야 합니다. 또한, 각 포렌식 도구를 실행하는 데 사용된 정확한 명령(예: 명령줄 인수 및 스위치)을 문서화해야 합니다. 어떤 명령이 실행되었는지, 언제, 어떤 결과로 캡처될지를 알기 위해 실행할 수 있는 스크립트를 도구 매체에 배치하는 것이 좋습니다.

도구가 들어있는 매체는 변경 사항으로부터 보호되어야 합니다. 플로피 디스크는 도구를 변경하지 않도록 쓰기 보호되어야 합니다. 재기록 가능 CD의 내용은 사용자 컴퓨터의 CD 굽기 유ти리티로 변경될 수 있기 때문에 CD-ROM은 재기록 가능 CD가 아닌 일회용 CD(즉, CDR)이어야 합니다. 1회 기록 CD에 도구를 구운 후에는 추가 데이터를 기록할 수 없도록 디스크를 마무리해야 합니다.

도구가 들어있는 미디어는 쓰기 금지되어 있어야 하므로 도구로 생성된 결과를 도구 미디어에 배치할 수 없습니다. 분석가들은 종종 도구 출력물을 플로피 디스크로 보내지만 컴퓨팅 장치에서 플로피 디스크 드라이브의 유행은 줄어들고 있습니다. 결과적으로 출력을 수집하는 대안적인 방법이 개발되었습니다. Windows 또는 Linux 기반 환경이 포함된 특별히 준비된 CD 및 USB 플래시 드라이브를 사용하여 시스템 상태를 변경하지 않고 출력을 수집합니다. 일반적으로는 출력을 다른 USB 플래시 드라이브나 외장 하드 드라이브 또는 기타 쓰기 가능한 미디어로 보내거나 원격 시스템으로 보낼 수 있습니다.

### 5.2.1.2 휘발성 OS 데이터 유형

다음 목록은 몇 가지 유형의 휘발성 OS 데이터를 보여주고 각 유형의 데이터를 수집하는 포렌식 도구를 사용하는 방법을 설명합니다.

- **메모리 컨텐츠:** RAM의 내용을 데이터 파일로 복사하고 후속 데이터 분석을 지원할 수 있는 몇 가지 유ти리티가 있습니다. 대부분의 시스템에서는 RAM 복사를 시도하는 유ти리티를 실행할 때 RAM의 변경을 피할 수 없습니다. 대신 목표는 가능한 RAM 변경을 최소화하여 복사를 수행하여 RAM의 중단을 최소화하는 것입니다.
- **네트워크 설정:** 대부분의 OS에는 UNIX 시스템의 ifconfig 및 Windows 시스템의 ipconfig와 같은 현재 네트워크 구성을 표시하는 유ти리티가 포함되어 있습니다. 네트워크 구성 유ти리티를 통해

제공될 수 있는 정보는 호스트 이름, 물리적 및 논리적 네트워크 인터페이스 및 각 인터페이스(예: IP 주소, MAC—Media Access Control— 주소, 현재 상태) 구성 정보를 포함합니다.

- **네트워크 연결:** OS는 일반적으로 현재 네트워크 연결 목록을 표시하는 방법을 제공합니다. Windows 및 UNIX 기반 시스템에는 일반적으로 소스 및 대상 IP 주소와 포트별로 네트워크 연결을 나열하는 netstat 프로그램과 각 인터페이스에서 열려있는 포트 목록이 들어 있습니다. 타사 유ти리티는 각각의 응용 프로그램 포트 할당을 표시할 수 있습니다. 대부분의 OS는 원격으로 마운트된 파일 시스템 목록을 표시할 수 있으며, 네트워크 연결 목록보다 자세한 정보를 제공합니다. 6.2.7절은 네트워크 연결 정보 수집에 대한 추가 정보를 제공합니다.
- **실행중인 프로세스:** 모든 UNIX 기반 시스템은 현재 실행중인 프로세스를 표시하는 ps 명령을 제공합니다. Windows는 그래픽 사용자 인터페이스(GUI) 기반 프로세스 목록 유ти리티인 작업 관리자를 제공하지만 일반적으로 텍스트 기반 목록을 갖는 것이 좋습니다. 타사 유ти리티는 Windows 시스템에서 실행중인 프로세스의 텍스트 목록을 생성하는데 사용할 수 있습니다.
- **열린 파일:** 모든 UNIX 기반 시스템은 열린 파일 목록을 표시하기 위한 lsof 명령을 제공합니다. 타사 유ти리티도 Windows 시스템용 열린 파일의 텍스트 목록을 생성하는데 사용할 수 있습니다.
- **로그인 세션:** 일부 OS에는 UNIX 시스템의 w 명령과 같이 현재 로그온한 사용자를 나열하는 명령이 내장되어 있습니다. 이 명령은 각 사용자의 소스 주소와 사용자가 시스템에 로그온한 시간을 나열합니다. Windows 시스템의 현재 연결된 사용자를 나열할 수 있는 타사 유ти리티를 사용할 수 있습니다.
- **운영 체제 시간:** 현재 시스템 시간, 표준 시간대 정보 및 일광 절약 시간 설정을 검색하는데 사용할 수 있는 여러 가지 유ти리티가 있습니다. UNIX 시스템에서는 date 명령을 사용하여 정보를 검색할 수 있습니다. Windows 시스템에서는 date, time 및 nlsinfo 명령을 사용하여 이 정보를 검색할 수 있습니다.

앞의 목록에 있는 도구 외에도, 다음과 같이 포렌식 도구 키트에 일부 범용 도구를 포함하는 것이 유용합니다.

- **OS 명령 프롬프트:** 이 유ти리티는 Windows 시스템의 cmd와 같이 도구 키트의 다른 도구를 실행할 수 있는 OS 명령 프롬프트를 제공합니다.
- **SHA-1 체크섬:** 데이터 파일의 SHA-1 메시지 디아제스트를 계산할 수 있는 유ти리티는 파일 검증에 유용합니다. 또한, 파일 검증을 돋기 위해 대상 OS와 관련된 시스템 데이터 파일에 대한 SHA-1 메시지 요약 목록을 툴킷에 포함하는 것이 유용할 수 있습니다. 이 목적을 위해 다양한 OS에서 유ти리티를 사용할 수 있습니다.
- **디렉토리 목록:** 파일 시스템을 탐색하고 그 내용을 보기 위해서는 디렉토리 내용을 나열하는 유ти리티가 포함되어야 합니다. 실질적으로 모든 OS에는 이러한 유ти리티가 포함됩니다. 예를 들어, UNIX 시스템에서는 ls 명령이 사용되고 Windows 시스템에서는 dir 명령

이 사용됩니다.

- **문자열 검색:** 텍스트 문자열 검색을 수행하는 유ти리티는 관심있는 데이터 파일을 식별하는데 유용할 수 있습니다. UNIX 시스템은 텍스트 문자열 검색을 수행하는 grep 명령을 제공하고 타사 grep 유ти리티는 Windows 시스템에서도 사용할 수 있습니다.
- **텍스트 에디터:** 간단한 텍스트 편집기는 텍스트 파일을 보거나 메모를 작성하는데 유용할 수 있습니다. Windows 시스템에서는 메모장, UNIX 시스템에서는 vi와 같은 많은 텍스트 편집기를 사용할 수 있습니다.

#### 5.2.1.3 데이터 수집의 우선 순위 지정

툴킷으로 수집해야 하는 휘발성 데이터의 유형은 특정 필요성에 따라 다릅니다. 예를 들어, 네트워크 침입이 의심되는 경우 네트워크 구성 정보, 네트워크 연결, 로그인 세션 및 실행 프로세스를 수집하여 누군가가 시스템에 액세스한 방법을 결정하는 것이 유용할 수 있습니다. 조사가 신분 도용에 관련되면 RAM의 내용, 실행중인 프로세스 목록, 열린 파일 목록, 네트워크 구성 정보 및 네트워크 연결이 사회 보장 및 신용 카드 번호, 데이터를 얻거나 암호화하는데 사용되는 프로그램, 암호 해시 및 기타 방법을 사용하여 네트워크를 통해 정보를 얻습니다. 의심스러운 경우, 수집할 수 있는 모든 기회가 있기 때문에 가능한 많은 변동 데이터를 수집하는 것이 좋습니다. 나중에 어떤 수집된 휘발성 데이터를 검사해야 하는지도 결정할 수 있습니다. 툴킷 CD의 자동화된 스크립트는 휘발성 데이터 수집의 일관성을 위해 사용될 수 있습니다. 스크립트에는 수집된 정보를 썬 드라이브 및 네트워크 드라이브 위치와 같은 로컬 저장 미디어로 전송하는 방법이 포함될 수 있습니다.

휘발성 데이터는 시간이 지남에 따라 변경되는 경향이 있으므로 휘발성 데이터가 수집되는 순서와 적시성이 중요합니다. 대부분의 경우 분석가는 네트워크 연결 및 로그인 세션에 대한 정보를 먼저 수집해야 합니다. 네트워크 연결 시간이 초과되거나, 연결이 끊어질 수 있으며 시스템에 연결된 사용자 목록이 달라질 수 있기 때문입니다. 네트워크 구성 정보와 같이 변경 가능성이 적은 휘발성 데이터는 나중에 수집해야합니다. 휘발성 데이터를 처음부터 끝까지 수집할 때, 권장 순서는 다음과 같습니다.

1. 네트워크 연결
2. 로그인 세션
3. 메모리 내용
4. 실행 프로세스
5. 열린 파일
6. 네트워크 구성

## 7. 운영 체제 시간

### 5.2.2 비 휘발성 OS 데이터 수집

휘발성 OS 데이터를 얻은 후에 분석가는 종종 비휘발성 OS 데이터를 수집해야합니다. 이를 위해, 분석가는 먼저 시스템을 종료해야 하는지 여부를 결정해야 합니다. 시스템을 종료하면 비트 스트림 이미징 및 많은 논리 백업을 수행할 수 있지만, 보존되는 OS 데이터를 변경할 수도 있습니다. 대부분의 시스템은 두 가지 방법으로 종료할 수 있습니다.

- **올바른 OS 종료 수행:** 거의 모든 OS가 종료 옵션을 제공합니다. 그러면 OS를 종료하기 전에 열려 있는 파일 닫기, 임시 파일 삭제 및 스왑 파일 지우기와 같은 정리 작업을 수행합니다. 정상적인 종료는 악성 물질의 제거를 유발할 수도 있습니다. 예를 들어, 메모리 상주 루트킷이 사라질 수 있으며 트로이 목마와 같은 악성 활동의 증거를 제거할 수도 있습니다. OS는 일반적으로 관리자 또는 현재 시스템 사용자(현재 사용자에게 충분한 권한이 있는 사용자)의 계정에서 종료됩니다.
- **시스템에서 전원 제거:** 컴퓨터 뒤에서 전원 코드를 분리하고 랩톱 또는 기타 휴대용 장치의 배터리를 분리하면 스왑 파일, 임시 데이터 파일 및 정상 종료 중에 변경되거나 삭제될 수 있는 기타 정보가 보존될 수 있습니다. 불행하게도 갑작스런 종료는 열린 파일과 같은 곳에서 OS로 총돌 데이터를 유발시킬 수도 있습니다. 또한, PDA 및 휴대폰과 같은 일부 소비자 장치의 경우 배터리 전원을 제거하면 데이터가 손실될 수 있습니다.

일부 도구는 문제 없이 실행중인 시스템에서 수집 작업을 수행할 수 있지만, 다른 도구는 종료된 시스템에서 실행하는 것이 가장 좋습니다. 후자의 경우 분석가는 각 OS의 특성을 인식하고 OS의 일반적인 동작 및 보존해야 할 데이터 유형에 따라 종료 방법을 선택해야 합니다. 예를 들어, DOS 및 Windows 95/98 시스템 갑자기 전원이 꺼지면 일반적으로 데이터가 손상되지 않으므로 전원을 제거하면 데이터가 보존됩니다. 다른 운영 체제는 전원이 손실될 경우 열려 있는 파일이나 당시 액세스한 파일과 같은 데이터를 손상시킬 수 있습니다. 이러한 경우 일반적으로 스왑 파일이나 임시 데이터 파일이 중요하지 않거나, 정상 종료로 인해 트리거 될 수 있는 루트킷, 트로이 목마 또는 기타 악의적인 프로그램이 시스템에 포함되어 있지 않으면, 정상적으로 종료하는 것이 가장 좋습니다. 시스템 종료(필요한 경우)를 수행한 후에 분석가는 4절에서 설명한 방법을 사용하여 시스템의 저장 매체에서 파일 시스템 데이터를 수집해야 합니다.

컴퓨터의 전원을 끈 후에, 컴퓨터에 연결된 모든 구성 요소, 저장 장치, 미디어 및 주변 장치가 증거로 필요할 경우 인벤토리를 작성하고 레이블을 지정해야 합니다. 가능한 경우 인벤토리에는 모델 번호, 일련 번호 및 품목 설명이 포함되어야 합니다. 또한, 각 항목이 컴퓨터 외부 또는 내부(예: 케이블 연결, 점퍼 설정)에 연결되는 방법에 대한 정보를 문서화하고 촬영해야 합니다. 그

러면 분석가는 사용자의 컴퓨터 설정을 다시 재생성하는데 도움을 받을 수 있습니다. 증거가 합법적으로 압류될 수 있다고 가정하면, 각 품목은 정전기 방지 팔찌를 사용하여 처리해야 합니다. 정전기 방전 팔찌는 물품을 손상시키거나 적절히 밀봉해(즉, 테이프로 밀봉한 상자) 정전기 방전을 방지하여, 운송을 안전하게 합니다. 취급자는 민감한 물품을 취급할 때, 정전기 방지용 팔찌를 착용하고 정전기 방지백 및 기타 특수 포장재로 물품을 보호해야 합니다.

파일 시스템 데이터가 수집되면 도구를 사용하여 파일 시스템에서 특정 유형의 데이터를 얻을 수 있습니다. 데이터, 응용 프로그램 및 설정 파일과 같은 일반 파일을 획득하는 것은 비교적 간단하며, 4절에서 보다 자세하게 설명합니다. 다음 목록은 몇 가지 다른 유형의 비휘발성 OS 데이터를 설명하고 도구가 각각을 파일시스템에서 얻는데 유용할 수 있는 방법을 설명합니다.

- **사용자 및 그룹:** 운영 체제는 시스템에 액세스할 수 있는 사용자 및 그룹 목록을 유지 관리합니다. UNIX 시스템에서 사용자 및 그룹은 각각 /etc/passwd 및 /etc/groups에 나열됩니다. 또한, groups 및 users 명령을 사용하여 시스템에 로그온한 사용자와 해당 그룹이 속한 그룹을 식별할 수 있습니다. Windows 시스템에서는 net user 및 net group 명령을 사용하여 시스템의 사용자 및 그룹을 열거할 수 있습니다.
- **암호:** 대부분의 OS는 디스크상의 사용자 암호에 대한 암호 해시를 유지합니다. Windows 시스템에서 타사 유틸리티를 사용하여 SAM(Security Account Manager) 데이터베이스에서 암호 해시를 덤프할 수 있습니다. UNIX 시스템에서 암호 해시는 일반적으로 /etc/passwd 또는 /etc/shadow 파일에 있습니다. 4.3.2절에서 설명했듯이 암호 해독 프로그램을 사용하여 해시에서 암호를 추출할 수도 있습니다.
- **네트워크 공유:** 시스템을 통해 로컬 리소스를 네트워크에서 공유할 수 있습니다. Windows 시스템에서 SrvCheck 유틸리티를 사용하여 네트워크 공유를 나열할 수 있습니다. 타사 유틸리티는 다른 OS에 대해 유사한 정보를 제공할 수 있습니다.
- **로그:** 텍스트 파일에 저장되지 않은 로그는 로그 추출 유틸리티를 사용해야 할 수도 있습니다. 예를 들어, 특수 유틸리티는 Windows 시스템에서 이진 형식 로그에 저장된 최근 성공 및 실패 로그 온 시도에 대한 정보를 검색할 수 있습니다. 유닉스 시스템의 대부분의 로그 항목은 syslog 또는 /var/log 디렉토리의 텍스트 파일에 저장되므로 로그에서 정보를 얻으려면 특별한 유틸리티가 필요하지 않습니다. .log로 끝나는 파일 이름을 검색하면 대부분의 로그 파일을 식별할 수 있습니다.

때때로 분석가는 시스템 날짜 및 시간 또는 프로세서 유형 및 속도와 같은 BIOS에서 데이터를 수집해야 할 수 있습니다. BIOS에는 주로 시스템 하드웨어 구성과 관련된 정보가 포함되어 있기 때문에, BIOS 데이터 수집은 시스템 관리자가 운영 문제를 해결할 때 필요할 수 있습니다. 일반적으로 BIOS 데이터가 필요한 분석가는 먼저 필요한 휘발성 데이터 및 파일 시스템을 수집한 다음 시스템을 재부팅하고 적절한 기능 키(일반적으로 부팅 초기 화면에서 지정)를 눌러 BIOS 설정을 표시합니다. BIOS 암호가 설정되어 있으면, 분석가가 BIOS 설정에 쉽게 액세스하지 못할 수 있으

며 기본 암호를 추측하거나 암호 보호를 우회해야 할 수 있습니다. 적절한 제조업체 백도어 암호 찾기, 암호 크래커 사용, 마더 보드의 적절한 점퍼 이동 또는 CMOS(Complementary Metal Oxide Semiconductor) 배터리 제거(가능한 경우) 등 다양한 방법을 사용하여 BIOS 암호를 무시할 수 있습니다. 시스템이 다양하므로 분석가는 마더 보드 설명서에 설명된 대로 분석중인 시스템의 특정 특성을 먼저 조사하여 시스템을 불필요하게 손상시키지 않아야 합니다.

### 5.2.3 데이터 수집과 관련된 기술적 문제

기술 문제로 인해 OS 데이터를 수집하지 못할 수도 있습니다. 4절에서는 몇 가지 파일 시스템 관련 문제에 대해 설명합니다. 이 절에서는 추가 수집 문제에 중점을 두고 문제를 완화하기 위해 수행할 수 있는 작업에 대한 지침을 제공합니다. 이 절의 목적은 모든 가능한 문제에 대한 철저한 토론을 제공하는 것이 아니라 일반적인 문제에 대한 기본 정보를 제공하는 것입니다.

- **OS 액세스:** 분석가가 OS에 쉽게 액세스할 수 없기 때문에 휘발성 데이터 수집이 어려울 수 있습니다. 예를 들어, 사용자가 암호로 보호된 화면 보호기를 실행하거나 시스템을 잠글 수 있습니다. 이러한 경우 분석가는 이 보호를 우회하거나 휘발성 OS 데이터에 액세스하는 다른 방법을 찾아야 합니다. 암호로 보호 된 화면 보호기가 활성화되어 있으면 시스템을 다시 시작하면 분석가가 화면 보호기를 우회할 수 있지만, 또한 모든 휘발성 OS 데이터가 손실될 수 있습니다. 호스트가 지문 판독기 또는 다른 애드온 인증 서비스와 같은 생체 인식 기반 인증을 사용하는 경우 휘발성 OS 데이터에 액세스할 때, 비슷한 문제가 발생할 수 있습니다. 몇 가지 다른 OS를 위한 서드파티 유ти리티가 있으며, 그것들은 시스템을 재부팅시키지 않고 화면보호기 패스워드를 우회할 수 있습니다. 이러한 유ти리티는 일반적으로 CD 드라이브의 자동 실행 기능에 의존합니다. 이 유ти리티는 백그라운드에서 자동으로 실행된 다음 암호화된 패스워드를 찾아 암호 해독을 시도합니다.
- **로그 수정:** 사용자는 로그 기능을 비활성화하거나, 로그 설정을 수정하여 로그에서 사용할 수 있는 스토리지가 거의 없도록 하거나 로그에 많은 가짜 이벤트를 작성하여 로그의 유용성을 줄이려고 할 수 있습니다. 로깅 변경의 영향을 줄이는 한 가지 방법은 중앙 집중식 서버에 로그 항목을 보관하도록 시스템을 구성하는 것입니다.
- **플래시 메모리가 장착된 하드 드라이브:** 때때로 분석가가 플래시 메모리를 포함하는 하드 드라이브를 발견할 수도 있습니다. 이 플래시 메모리에는 드라이브가 컴퓨터에서 분리된 경우에도 드라이브에 액세스하는데 필요한 암호가 포함될 수 있습니다. 일반적으로 분석가는 드라이브에 액세스하기 위해 암호를 찾거나 추측하거나 해독해야 합니다.
- **키 재매핑:** 일부 컴퓨터에서는 초기 키와 다른 기능을 수행하기 위해 개별 키 또는 키 조합을 다시 매핑 할 수 있습니다. 예를 들어, Ctrl키, Alt키 및 Del키를 매핑하여, 예상되는 동작 대신 컴퓨터의 하드 드라이브를 지우고 시스템을 재부팅할 수 있습니다. 컴퓨터의 키보드를 사용하는 분석가는 예상치 못한 동작을 수행하는 키 입력을 입력할 수 있습니다. 키 재매핑 문제를 방지하는 가장

좋은 방법은 키보드를 사용하지 않고, 컴퓨터에서 데이터를 수집하는 것입니다. 예를 들어, 분석가는 크로스 오버 네트워크 케이블을 사용하여 포렌식 워크스테이션을 원하는 컴퓨터에 연결하고 포렌식 워크스테이션의 스크립트를 실행할 수 있습니다.

### 5.3 OS 데이터의 조사와 분석

다양한 도구와 기법을 사용하여 시험 과정을 지원할 수 있습니다. 수집된 데이터 파일을 검사하기 위해 4.3절에서 설명된 많은 도구와 기법을 수집된 OS 데이터와 함께 사용할 수도 있습니다. 또한 7절에서 설명한 것처럼 파일 무결성 검사기 및 호스트 IDS와 같은 보안 응용 프로그램은 OS에 대한 악성 활동을 식별하는 데 매우 유용할 수 있습니다. 예를 들어, 파일 무결성 검사 프로그램을 사용하여 OS 파일의 메시지 요약을 계산하고 알려진 메시지 요약의 데이터베이스와 비교하여 파일이 손상되었는지 여부를 확인할 수 있습니다. 침입 탐지 소프트웨어가 컴퓨터에 설치되어 있으면, OS에 대해 수행된 작업을 나타내는 로그가 포함될 수 있습니다.

분석가가 직면하는 또 다른 문제는 스왑 파일과 RAM 덤프(비구조적 데이터가 포함된 큰 바이너리 데이터 파일)를 검사하는 것입니다. 16진수 편집기는 이러한 파일을 열고 내용을 검사하는데 사용할 수 있습니다. 그러나 대용량 파일의 경우 16진수 편집기를 사용하여 가능한 데이터를 수동으로 찾으려면 시간이 많이 걸릴 수 있습니다. 필터링 도구는 전화 번호, 사람 이름, 전자 메일 주소, 웹 주소 및 기타 유형의 중요한 정보를 나타내는 텍스트 패턴과 숫자 값을 식별하여 스왑 및 RAM 덤프 파일을 검사하는 프로세스를 자동화합니다.

분석가는 프로세스의 목적 및 제조업체와 같이 시스템에서 실행중인 특정 프로그램에 대한 추가 정보를 수집하길 원합니다. 현재, 시스템에서 실행중인 프로세스 목록을 얻은 후에 분석가는 프로세스 이름을 조회하여 추가 정보를 얻을 수 있습니다. 그러나 사용자는 트로이 목마 프로그램을 calculator.exe으로 이름 짓는 등 프로그램의 이름을 변경하여 기능을 숨길 수 있습니다. 따라서 프로세스 이름 조회는 메시지 디제스트를 계산하고 비교하여 프로세스 파일의 ID를 확인한 후에만 수행해야 합니다. Windows 시스템의 DLL과 같은 라이브러리 파일에서도 유사한 라이브러리가 수행되어 어떤 라이브러리가 로드되고 그들의 일반적인 목적이 무엇인지 판별할 수 있습니다.

5.2절에서 설명한 것처럼 분석가는 여러 파일 시스템을 포함하여 다양한 유형의 OS 데이터를 수집할 수 있습니다. 관련 정보를 찾기 위해 각 유형의 데이터를 조사하려고 하면 시간이 많이 걸릴 수 있습니다. 분석가들은 일반적으로 초기에 검토할 몇 가지 데이터 소스를 확인한 다음 해당 리뷰를 기반으로 다른 중요한 정보 소스를 찾는 것이 유용하다는 것을 알고 있습니다. 또한, 분석에는 네트워크 트래픽이나 응용 프로그램과 같은 다른 유형의 원본에서 가져온 데이터가 포함될 수 있습니다. 8절에서는 분석을 통해 OS 및 기타 소스의 데이터를 어떻게 상관시킬 수 있는지에 대한 예제를 제공합니다.

## 5.4 권고 사항

OS에서 데이터를 사용하기 위해 이 섹션에서 제시하는 주요 권장 사항은 다음과 같습니다.

- **분석가는 휘발성 OS 데이터를 보존하기 위해 적절히 행동해야 합니다.** 휘발성 OS 데이터를 보존해야 하는지 여부를 결정하기 위한 기준은 분석가가 최대한 신속하게 정보에 입각한 의사 결정을 내릴 수 있도록 미리 문서화해야 합니다. 휘발성 OS 데이터를 수집하는데 필요한 노력이 필요한지 여부를 확인하려면, 이러한 수집과 관련된 위험을 중요한 정보를 복구할 수 있는 잠재력과 비교 검토해야 합니다.
- **분석가는 휘발성 OS 데이터를 수집하기 위해 포렌식 툴킷을 사용해야 합니다.** 포렌식 툴킷을 사용하면 정확한 OS 데이터를 수집하면서 시스템 장애를 최소화하고 변경으로부터 보호할 수 있습니다. 분석가는 데이터 수집 중에 각 도구가 시스템에 영향을 주거나 변경하는 방법을 알아야 합니다.
- **분석가는 각 시스템에 대해 적절한 시스템 종료 방법을 선택해야 합니다.** 특정 OS를 종료하는 각 방법으로 인해 다른 유형의 데이터가 보존되거나 손상될 수 있습니다. 분석가는 각 OS의 일반적인 종료 동작을 알고 있어야 합니다.

## 6. 네트워크 트래픽 데이터 사용

분석가는 네트워크 트래픽의 데이터를 사용하여 네트워크 기반 공격 및 부적절한 네트워크 사용을 재구성 및 분석하고 다양한 유형의 운영 문제를 해결할 수 있습니다. 전자 메일 메시지나 오디오와 같이 네트워크를 통해 전달되는 통신 내용도 조사할 수 있습니다. 네트워크 트래픽이라는 용어는 호스트간에 유선 또는 무선 네트워크를 통해 전달되는 컴퓨터 네트워크 통신을 의미합니다. 이 절에서는 침입 탐지 소프트웨어, 방화벽과 같은 주요 네트워크 트래픽 데이터 출처에 대한 설명을 포함하여 네트워크 트래픽에 대해 소개합니다. 또한, 이러한 출처에서 데이터를 수집하는 기술에 대해 논의하고 그러한 데이터 수집의 잠재적인 법적 및 기술적 문제를 지적합니다. 이 절의 나머지 부분에서는 네트워크 트래픽의 데이터를 조사하고 분석하기 위한 기술과 도구에 중점을 둡니다. 이 절에서는 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP)에 대한 개요로 시작합니다. TCP/IP에 대한 기본 지식은 이 섹션에 제시된 데이터, 도구 및 방법을 이해하는데 필요합니다.

### 6.1 TCP/IP 기본 사항

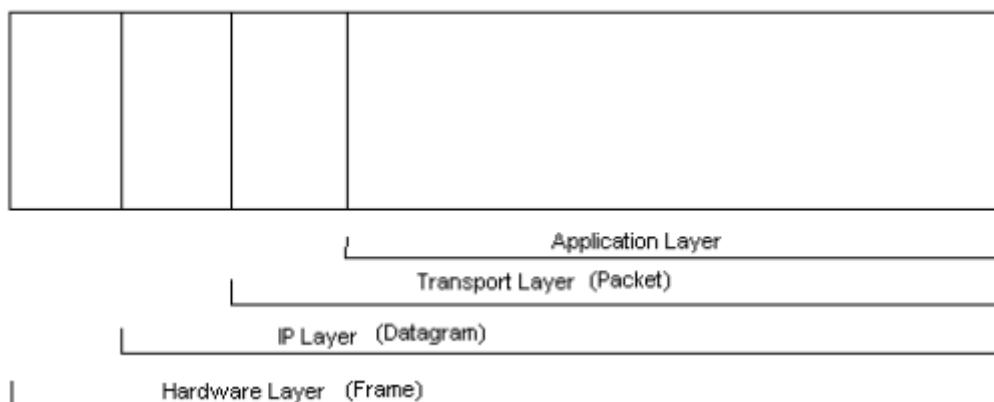
TCP / IP는 전세계에 널리 사용되어 네트워크 통신을 제공합니다. TCP/IP 통신은 함께 작동하는

4개의 계층으로 구성됩니다. 사용자가 네트워크를 통해 데이터를 전송하려는 경우 데이터는 최상위 계층에서 중간 계층을 거쳐 최하위 계층으로 전달되며 각 계층에는 추가 정보가 추가됩니다. 최하위 계층은 축적된 데이터를 물리적 네트워크를 통해 전송합니다. 데이터는 레이어를 통해 대상으로 전달됩니다. 본질적으로, 레이어에 의해 생성된 데이터는 그 아래 레이어에 의해 더 큰 컨테이너에 캡슐화됩니다. 네 개의 TCP/IP 계층이 [그림 6-1]에 나와 있습니다.

<b>Application Layer.</b> This layer sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).
<b>Transport Layer.</b> This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally ensure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.
<b>Internet Protocol Layer (also known as Network Layer).</b> This layer routes packets across networks. IP is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).
<b>Hardware Layer (also known as Data Link Layer).</b> This layer handles communications on the physical network components. The best known data link layer protocol is Ethernet.

[그림 6-1 : TCP/IP 계층]

4개의 TCP/IP 계층이 함께 작동하여 호스트 간에 데이터를 전송합니다. [그림 6-2]에서 볼 수 있듯이 각 레이어는 이전 레이어를 캡슐화합니다. 6.1.1절부터 6.1.4절까지는 이러한 계층을 보다 자세하게 설명하고 네트워크 포렌식과 가장 관련이 있는 특징을 설명합니다. 6.1.5절은 레이어가 서로 어떻게 관련되는지 설명합니다.



[그림 6-2 : TCP/IP 캡슐화]

### 6.1.1 응용 계층

응용 프로그램 계층을 사용하면 응용 프로그램이 응용 프로그램 서버와 클라이언트간에 데이터를 전송할 수 있습니다. 응용 프로그램 계층 프로토콜의 예로는 웹 서버와 웹 브라우저간에 데이터를 전송하는 HTTP(Hypertext Transfer Protocol)가 있습니다. 다른 일반적인 응용 프로그램 계층 프로토콜로는 DNS(Domain Name System), FTP(File Transfer Protocol), SMTP(Simple Mail Transfer Protocol) 및 SNMP(Simple Network Management Protocol)가 있습니다. 공통적으로 사용되는 수백 가지의 고유 응용 프로그램 계층 프로토콜이 있으며 그 중 많은 것이 일반적이지 않습니다. 사용중인 프로토콜과 관계 없이 응용 프로그램 데이터가 생성된 다음 추가 처리를 위해 전송 계층으로 전달됩니다. 7절에서는 응용 프로그램 관련 데이터 수집, 검사 및 분석에 중점을 둡니다.

### 6.1.2 전송 계층

전송 계층은 데이터를 패키징하여 호스트간에 전송되도록 합니다. 전송 계층에 응용 프로그램 데이터가 캡슐화되면, 그 결과의 논리 단위를 패킷이라고 합니다.(패킷은 응용 프로그램 데이터없이 생성될 수도 있음) (예 : 연결이 처음 협상 될 때) 각 패킷은 사용중인 전송 프로토콜의 특성을 지정하는 다양한 필드로 구성된 헤더를 포함합니다. 선택적으로, 패킷은 애플리케이션 데이터를 보유하는 페이로드(payload)를 또한 포함할 수 있습니다.

네트워크를 통해 통신하는 대부분의 응용 프로그램은 전송 계층을 사용하여 안정적인 데이터 전달을 보장합니다. 일반적으로 이 작업은 두 호스트간에 연결을 설정하는 TCP 전송 계층 프로토콜을 사용하여 수행한 다음 해당 연결을 통해 안정적인 데이터 전송을 보장하기 위해 최선을 다합니다. 각 TCP 패킷에는 원본 포트와 대상 포트가 포함됩니다. 포트중 하나는 한 시스템의 서버 응용 프로그램과 연관됩니다. 다른 포트는 다른 시스템의 해당 클라이언트 응용 프로그램과 연관됩니다. 클라이언트 시스템은 일반적으로 응용 프로그램 사용을 위해 사용 가능한 포트 번호를 선택하는 반면, 서버 시스템은 일반적으로 각 응용 프로그램 전용의 정적 포트 번호를 사용합니다. 많은 서버 포트가 일반적으로 특정 응용 프로그램에서 사용되지만(HTTP: 80, FTP: 21), 많은 서버 응용 프로그램은 모든 포트 번호에서 실행할 수 있으므로 네트워크 트래픽에서 서버 포트 번호만을 기준으로 특정 응용 프로그램의 데이터가 있다고 가정하는 것은 현명하지 않습니다.

일부 애플리케이션 데이터의 손실이 우려되지 않으면(예: 오디오, 비디오 스트리밍), 일반적으로 UDP(User Datagram Protocol)가 사용됩니다. UDP는 비연결이기 때문에 UDP는 TCP보다 오버 헤드 및 대기 시간이 적습니다. 한 호스트는 사전 협상 없이 다른 호스트에 데이터를 보냅니다. UDP는 DNS와 같은 신뢰할 수 있는 데이터 전송 및 DHCP(Dynamic Host Configuration Protocol) 및 SNMP와 같은 로컬 영역 네트워크에서만 사용하려는 응용 프로그램에서 수행되는 응용 프로그램에도 사용됩니다. TCP의 경우와 마찬가지로 각 UDP 패킷에는 원본 포트와 대상 포트가 있습니다.

UDP 포트와 TCP 포트는 매우 유사하지만 서로 구별되며 상호 교환할 수 없습니다. 일부 응용 프로그램(예: DNS)은 TCP 및 UDP 포트를 모두 사용할 수 있습니다. 이러한 응용 프로그램은 일반적으로 TCP 포트와 UDP 포트에 동일한 번호를 사용하지만 필수는 아닙니다.

### 6.1.3 IP 계층

IP 계층은 전송 계층에서 수신하는 데이터의 주소 지정 및 라우팅 처리를 담당하기 때문에 네트워크 계층이라고도 부를 수 있습니다. IP 헤더에는 사용중인 IP 버전을 나타내는 IP 버전이라는 필드가 있습니다. 일반적으로 이것은 IPv4의 경우 4로 설정됩니다. 그러나 IPv6의 사용이 증가하고 있으므로 이 필드는 대신 6으로 설정할 수 있습니다. 기타 중요한 IP 헤더 필드는 다음과 같습니다:

- **출발지 및 목적지 IP 주소:** IP 주소의 예는 10.3.1.70(IPv4)이고, 1000:0:0:2F:8A:400:0427:9BD1입니다.(IPv6)
- **IP 프로토콜 번호:** IP 페이로드에 포함된 전송 계층 프로토콜을 나타냅니다. 일반적으로 사용되는 IP 번호는 1(인터넷 제어 메시지 프로토콜[ICMP]), 6(TCP), 17(UDP) 및 50(ESP)입니다.

또한, IP 계층은 데이터의 주소 지정 및 라우팅과 관련된 오류 및 상태 정보를 제공해야합니다. ICMP로 이것을 합니다. ICMP는 오류 및 상태 메시지가 전달되도록 하는 연결 없는 프로토콜입니다. 응용 프로그램 데이터가 아닌 제한된 정보를 전송하도록 설계되었으므로 ICMP에는 포트가 없습니다. 대신에 각 ICMP 메시지의 목적을 나타내는 메시지 유형이 있습니다. 일부 메시지 유형에는 메시지 코드가 있으며, 이 메시지 코드는 부속 유형으로 간주될 수 있습니다. 예를 들어, ICMP 메시지 유형 Destination Unreachable에는 도달할 수 없는 것을 나타내는 몇 가지 가능한 메시지 코드가 있습니다.(예: 네트워크, 호스트, 프로토콜) 대부분의 ICMP 메시지는 응답을 이끌어 내기 위한 것이 아닙니다.

IP 주소는 종종 간접 계층을 통해 사용됩니다. 사람들이 웹 서버나 전자 메일 서버와 같은 네트워크의 리소스에 액세스해야 하는 경우 일반적으로 서버의 IP 주소가 아닌 www.nist.gov와 같은 서버의 이름을 입력합니다. 이름(도메인 이름이라고도 함)은 DNS 계층 프로토콜에 의해 IP로 매핑됩니다. IP 주소 대신 도메인 이름을 입력하는 가장 큰 이유는 일반적으로 사람들이 기억하기가 더 쉽기 때문입니다. 또한, 도메인 이름이 동일하게 유지되는 경우 호스트의 IP 주소는 시간이 지남에 따라 변경될 수 있습니다. 호스트의 IP 주소에 매핑되는 도메인 이름으로 호스트를 참조함으로써 사용자는 현재 호스트가 사용중인 IP 주소와 상관없이 호스트에 연결할 수 있습니다.

#### 6.1.4 하드웨어 계층

이름에서 알 수 있듯이 하드웨어 계층에는 케이블, 라우터, 스위치 및 NIC를 비롯한 네트워크의 물리적 구성 요소가 포함됩니다. 하드웨어 계층에는 다양한 하드웨어 계층 프로토콜도 포함됩니다. 이더넷은 이러한 프로토콜 중에서 가장 널리 사용됩니다. 이더넷은 특정 NIC에 영구적으로 할당되는 고유한 6 바이트 값(예: 00-02-B4-DA-92-2C)인 MAC 주소의 개념에 의존합니다. 각 프레임에는 두 개의 MAC 주소가 있고, 이는 프레임을 방금 라우팅 한 NIC의 MAC 주소와 프레임이 전송되는 다음 NIC의 MAC 주소를 나타냅니다. 프레임이 원본 소스 호스트와 최종 대상 호스트 사이의 경로에 있는 네트워킹 장비(예: 라우터 및 방화벽)를 통과할 때, MAC 주소는 로컬 소스 및 대상을 참조하도록 업데이트됩니다. 여러 개의 개별 하드웨어 계층 전송이 단일 IP 계층 전송 내에서 함께 링크될 수 있습니다.

MAC 주소 외에 각 프레임에는 프레임의 헤더에 들어있는 프로토콜(일반적으로 IP 또는 ARP(Address Resolution Protocol))을 나타내는 EtherType 값이 포함됩니다. 여러 IP 주소가 많은 MAC 주소에 매핑될 수 있기 때문에 MAC 주소가 반드시 IP 주소를 고유하게 식별하지는 않습니다.

#### 6.1.5 네트워크 포렌식에서 계층의 중요성

TCP/IP 프로토콜 제품군의 4개 계층에는 각각 중요한 정보가 들어 있습니다. 하드웨어 계층은 물리적 구성 요소에 대한 정보를 제공하고 다른 계층은 논리적 측면을 설명합니다. 분석가는 네트워크 내의 이벤트의 경우 IP 주소(IP 계층의 논리적 식별자)를 특정 NIC의 MAC 주소(물리적 계층의 물리적 식별자)에 매핑하여 관심있는 호스트를 식별할 수 있습니다. IP 프로토콜 번호(IP 계층 필드)와 포트 번호(전송 계층 필드)의 조합은 가장 많이 사용되거나 대상이 될 가능성이 높은 애플리케이션을 분석가에게 알게해줄 수 있습니다. 이는 응용 프로그램 계층 데이터를 검사하여 확인할 수 있습니다.

네트워크 포렌식 분석은 모든 계층에 의존합니다. 분석가가 데이터를 검사하기 시작할 때, 일반적으로 관심있는 IP 주소, 프로토콜 및 포트 정보와 같은 제한된 정보가 있습니다. 그럼에도 불구하고, 이 정보는 일반적인 정보 출처 검색을 지원하기에 충분한 정보입니다. 대부분의 경우 응용 프로그램 계층에는 실제 활동이 포함되어 있습니다. 대부분의 공격은 응용 프로그램(서비스 포함)의 취약점에 대한 것이며, 대부분 오용은 응용 프로그램의 오용을 포함합니다. 분석가는 활동에 참여한 호스트를 식별할 수 있도록 IP 주소가 필요합니다. 호스트는 활동을 분석하는데 사용할 수 있는 추가 데이터를 포함할 수도 있습니다. 관심있는 일부 이벤트는 관련 애플리케이션 레벨 데이터(예: 모든 네트워크 대역폭을 소모하도록 설계된 분산 서비스 거부 공격)가 없을 수도 있지만, 대부분의 경우는 존재합니다. 네트워크 포렌식은 애플리케이션 계층 활동 분석에 중요한 지원을

제공합니다.

## 6.2 네트워크 트래픽 데이터 출처

조직은 일반적으로 네트워크 포렌식에 유용할 수 있는 네트워크 트래픽과 관련된 여러 유형의 정보 출처를 보유합니다. 이러한 출처는 4개의 모든 TCP/IP 계층에서 중요한 데이터를 수집합니다. 다음 하위 절에서는 방화벽 및 라우터, 패킷 스니퍼 및 프로토콜 분석기, IDS, 원격 액세스, 보안 이벤트 관리 소프트웨어 및 네트워크 포렌식 분석 도구와 같은 몇 가지 다른 유형의 데이터 출처와 같은 네트워크 트래픽 데이터 원본의 주요 범주를 강조해서 설명합니다. 소단원은 설명된 각 출처의 목적과 일반적으로 수집되고, 잠재적으로 수집될 수 있는 데이터의 유형을 설명합니다.

### 6.2.1 방화벽 및 라우터

방화벽 및 라우터와 같은 네트워크 기반 장치 및 개인 방화벽과 같은 호스트 기반 장치는 네트워크 트래픽을 검사하고 규칙 집합을 기반으로 네트워크 트래픽을 허용하거나 거부합니다. 방화벽과 라우터는 일반적으로 대부분의 또는 모든 거부된 연결 시도 및 비연결 패킷에 대한 기본 정보를 기록하도록 구성됩니다. 일반적으로 기록된 정보에는 패킷이 처리된 날짜와 시간, 원본 및 대상 IP 주소, 전송 계층 프로토콜(예: TCP, UDP, ICMP) 및 기본 프로토콜 정보(예: TCP 또는 UDP)가 기록됩니다. ICMP 유형의 패킷은 일반적으로 페이로드 데이터가 기록되지 않습니다.

네트워크 주소 변환(NAT)을 수행하는 네트워크 기반 방화벽 및 라우터에는 네트워크 트래픽과 관련하여 중요한 데이터가 추가될 수 있습니다. NAT는 한 네트워크의 주소를 다른 네트워크의 주소에 매핑하는 프로세스입니다. 이는 내부 네트워크의 개인 주소를 인터넷에 연결된 네트워크의 하나 이상의 공용 주소에 매핑하기 위해 가장 자주 수행됩니다. NAT는 각 내부 주소에 대해 외부 주소에 다른 소스 포트 번호를 할당하여 단일 외부 주소에 매핑되는 여러 내부 주소를 구분합니다. NAT 장치는 일반적으로 각 NAT 주소 및 포트 매핑을 기록합니다.

일부 방화벽은 프록시 역할도합니다. 프록시는 클라이언트로부터 요청을 수신한 다음 클라이언트를 대신하여 요청을 원하는 대상으로 보냅니다. 프록시를 사용하면 클라이언트와 프록시 서버 사이의 연결과 프록시 서버와 실제 대상 사이의 연결이 실제로 성공적으로 연결될 때마다, 두 개의 개별 연결이 생성됩니다. 프록시 서버는 각 연결에 대한 기본 정보를 기록할 수 있습니다. 많은 프록시는 응용 프로그램마다 다르며 일부는 실제로 HTTP와 같은 응용 프로그램 프로토콜의 분석 및 유효성 검사를 수행합니다. 프록시는 유효하지 않은 것으로 보이는 클라이언트 요청을 거부하고 이러한 요청과 관련된 정보를 기록할 수 있습니다.

NAT 및 프록시 서비스를 제공하는 것 외에도 방화벽 및 라우터는 침입 탐지 및 VPN과 같은 기타 기능을 수행할 수 있습니다. 침입 탐지 및 VPN 기능은 각각 6.2.3절과 6.2.4절에서 보다 자

세히 설명합니다.

### 6.2.2 패킷 스니퍼 및 프로토콜 분석기

패킷 스니퍼는 유선 또는 무선 네트워크의 네트워크 트래픽을 모니터링하고 패킷을 캡처하도록 설계되었습니다. 일반적으로 NIC는 특별히 의도된 들어오는 패킷만 수락합니다. 그러나 NIC가 무차별 모드로 세팅되었을 때, 의도한 목적지와 관계 없이 그것이 보고 있는 모든 들어오는 패킷을 수용합니다. 패킷 스니퍼는 일반적으로 NIC를 무차별 모드로 설정하여 작동합니다. 사용자는 모든 패킷 또는 특정 특성(예: 특정 TCP 포트, 특정 소스 또는 대상 IP 주소)을 가진 패킷 만 캡처하도록 스니퍼를 구성합니다. 패킷 스니퍼는 일반적으로 문제 해결이나 조사 목적으로 특정 유형의 트래픽을 캡처하는데 사용됩니다. 예를 들어, IDS 경고가 두 호스트 사이의 비정상적인 네트워크 활동을 나타내는 경우 패킷 스니퍼는 호스트간에 이동하는 모든 패킷을 기록하여 분석가에게 추가 정보를 제공할 수 있습니다.

대부분의 패킷 스니퍼는 프로토콜 분석기이기도 합니다. 즉, 개별 패킷의 스트림을 재구성하고 수백 또는 수천 개의 다른 프로토콜을 사용하는 통신을 디코딩할 수 있습니다. 프로토콜 분석기는 일반적으로 실제 네트워크 트래픽뿐만 아니라 기록 된 패킷도 처리할 수 있습니다. 프로토콜 분석기는 원시 패킷 데이터를 이해하기 쉬운 형식으로 표시하는데 매우 중요합니다. 프로토콜 분석기는 6.4절과 7절에서 더 자세하게 논의됩니다.

### 6.2.3 침입 탐지 시스템

네트워크 IDS는 패킷 스니핑을 수행하고 네트워크 트래픽을 분석하여 의심스러운 활동을 식별하고 관련 정보를 기록합니다. 호스트 IDS는 네트워크 트래픽을 포함할 수 있는 시스템 내에서 발생하는 특정 시스템 및 이벤트의 특성을 모니터링합니다. 네트워크 IDS 센서는 특정 네트워크 세그먼트에서 모든 네트워크 트래픽을 모니터할 수 있고, 호스트 IDS 소프트웨어는 설치된 호스트에 대해서만 네트워크 트래픽을 모니터링합니다. 의심스러운 각 이벤트에 대해 IDS 소프트웨어는 일반적으로 방화벽과 라우터가 기록하는 것과 동일한 기본 이벤트 특성을 기록합니다. 예를 들면, 날짜 및 시간, 소스 및 대상 IP 주소, 프로토콜, 기본 프로토콜 특성, 응용 프로그램 별 정보, 사용자 이름, 파일 이름, 명령, 상태 코드가 포함됩니다. 또한, IDS 소프트웨어는 활동의 가능한 의도를 나타내는 정보를 기록합니다. 예에는 공격 유형(예: 버퍼 오버 플로우), 대상 취약성, 공격의 명백한 성공 또는 실패, 공격에 대한 추가 정보의 포인터가 포함됩니다.

일부 IDS는 의심스러운 활동과 관련된 패킷을 캡처하도록 구성할 수 있습니다. IDS를 트리거한 패킷만 기록하여 의심스러운 활동에 레이블을 지정하는 것부터 세션의 나머지 부분을 기록하는 것까지 다양합니다. 일부 IDS는 의심되는 항목이 발견될 경우 동일한 세션의 이전 활동을 보존할 수 있도록 짧은 기간 동안 모든 세션을 저장할 수 있습니다.

패킷은 주로 침입 탐지 분석가가 IDS 경보의 유효성을 검사하고 의심스러운 활동을 조사할 때 검토할 수 있도록 캡처됩니다. 일부 IDS에는 침입 방지 기능이 있습니다. 즉, 진행중인 공격을 적극적으로 차단하려고 시도합니다. IDS 로그에 침입 방지 기능을 사용해야 합니다.

#### 6.2.4 원격 액세스

원격 액세스 서버는 네트워크간 연결을 용이하게하는 VPN 게이트웨이 및 모뎀 서버와 같은 장치입니다. 여기에는 종종 외부 시스템이 원격 액세스 서버를 통해 내부 시스템에 연결되지만 외부 또는 내부 시스템에 연결되는 내부 시스템이 포함될 수도 있습니다. 원격 액세스 서버는 일반적으로 각 연결의 원본을 기록하며 각 세션에 대해 인증된 사용자 계정을 나타낼 수도 있습니다. 원격 액세스 서버가 원격 사용자에게 IP 주소를 할당하면 이 또한 기록될 수 있습니다. 일부 원격 액세스 서버는 패킷 필터링 기능도 제공합니다. 이 기능은 일반적으로 6.2.1절에 설명된대로 방화벽 및 라우터에서 제공하는 것과 유사한 로깅을 수행합니다. 원격 액세스 서버는 일반적으로 네트워크 수준에서 작동하므로 다양한 응용 프로그램을 사용할 수 있습니다. 서버는 응용 프로그램 기능에 대한 이해가 없기 때문에 대개 응용 프로그램 별 데이터를 기록하지 않습니다.

원격 액세스 서버 외에도 조직에서는 일반적으로 특정 호스트의 OS에 대한 원격 액세스를 제공하도록 특별히 고안된 여러 응용 프로그램을 사용합니다. 예를 들면, SSH(Secure Shell), 텔넷, 터미널 서버 및 원격 제어 소프트웨어가 있습니다. 이러한 응용 프로그램은 일반적으로 소스 IP 주소 및 사용자 계정을 포함하여 각 연결에 대한 기본 정보를 기록하도록 구성할 수 있습니다. 또한 조직은 일반적으로 클라이언트/서버 응용 프로그램과 같이 원격으로 액세스되는 많은 응용 프로그램을 사용합니다. 이러한 응용 프로그램 중 일부는 연결에 대한 기본 정보도 기록합니다.

대부분의 원격 액세스 관련 로깅은 원격 액세스 서버 또는 응용 프로그램 서버에서 발생하지만 클라이언트는 연결과 관련된 정보도 기록합니다.

#### 6.2.5 보안 이벤트 관리 소프트웨어

보안 이벤트 관리(SEM) 소프트웨어는 다양 네트워크 트래픽 관련 보안 이벤트 데이터 소스(예: IDS 로그, 방화벽 로그)에서 보안 이벤트 정보를 가져 와서 이벤트를 상관시킬 수 있습니다. 일반적으로 로그 보안 채널을 통해 다양한 데이터 소스에서 로그를 표준 형식으로 정규화한 다음 IP 주소, 타임 스탬프 및 기타 특성을 일치시켜 관련 이벤트를 식별합니다. SEM 제품은 일반적으로 이벤트 데이터를 생성하지 않습니다. 대신 가져온 이벤트 데이터를 기반으로 메타 이벤트를 생성합니다. 많은 SEM 제품은 공격 및 바이러스 감염과 같은 악성 활동을 식별할 수 있을뿐만 아니라 시스템 및 네트워크의 오용과 부적절한 사용을 탐지할 수 있습니다. SEM 소프트웨어는 단일 인터페이스를 통해 많은 네트워크 트래픽 정보 소스에 액세스할 수 있도록 도와줍니다.

SEM 제품은 OS 로그, 바이러스 백신 소프트웨어 경고 및 물리적 보안 장치 로그와 같은 거의 모든 보안 이벤트 데이터 원본을 처리할 수 있으므로, SEM 제품에는 이벤트와 관련된 다양한 정보가 포함될 수 있습니다. 그러나 일부 데이터 필드만 가져 오는 것이 일반적입니다. 예를 들어, IDS가 패킷을 기록하면 대역폭 및 저장 용량 제한으로 인해 패킷이 SEM으로 전송되지 않을 수 있습니다. 또한 대부분의 데이터 소스는 다양한 형식으로 정보를 기록하기 때문에 SEM 제품은 일반적으로 데이터를 표준화하여 각 데이터 필드를 표준 형식으로 변환하고 레이블을 지정합니다. 이것은 분석에 유익하지만(6.4 절 참조), 정규화 프로세스에서는 때때로 데이터에 오류가 발생하거나 일부 데이터가 손실됩니다. 다행히도 SEM 제품은 일반적으로 원본 데이터 소스를 변경하지 않으므로 분석가는 원본 로그의 사본을 보관하고 필요할 경우 데이터의 정확성을 확인하는데 사용합니다.

#### 6.2.6 네트워크 포렌식 분석 도구

네트워크 포렌식 분석 도구(NFAT)는 일반적으로 패킷 스니퍼, 프로토콜 분석기 및 SEM 소프트웨어와 동일한 기능을 단일 제품에 제공합니다. SEM 소프트웨어는 기존 데이터 소스(일반적으로 여러 네트워크 트래픽 관련 소스 포함) 간의 이벤트를 연관시키는 데 주력하지만 NFAT 소프트웨어는 주로 네트워크 트래픽을 수집, 검사 및 분석하는 데 중점을 둡니다. NFAT 소프트웨어는 또한 다음과 같은 네트워크 포렌식을 더욱 촉진시키는 추가 기능을 제공합니다.

- 도구 내에서 개별 세션(예: 두 명의 사용자 간 인스턴트 메시징[IM])에서 특정 기간 동안 모든 세션 까지 네트워크 트래픽을 재생하여 이벤트를 재구성합니다. 일반적으로 재생 속도는 필요에 따라 조정할 수 있습니다.
- 트래픽 흐름과 호스트 간의 관계를 시각화합니다. 일부 도구는 IP 주소, 도메인 이름 또는 기타 데이터를 실제 위치에 연결하고 활동의 자리적인 지도를 생성할 수도 있습니다.
- 전형적인 활동의 프로파일을 작성하고 중요한 편차를 확인합니다.
- 키워드에 대한 애플리케이션 콘텐츠 검색(예: '기밀', '독점')

#### 6.2.7 다른 출처들

대부분의 조직은 다음과 같은 포렌식에 사용할 수 있는 네트워크 트래픽 정보의 다른 출처를 가지고 있습니다.

- **동적 호스트 구성 프로토콜 서버:** DHCP 서비스는 필요한 경우 네트워크의 호스트에 IP 주소를 할

당합니다. 일부 호스트에는 정적 IP 주소가 있을 수 있습니다. 즉, 항상 동일한 IP 주소 할당 받습니다. 그러나 대부분의 호스트는 일반적으로 동적 할당을 받습니다. 즉, 호스트는 IP 주소 할당을 정기적으로 갱신해야하며 동일한 주소가 할당된다는 보장이 없음을 의미합니다. DHCP 서버에는 MAC 주소, 해당 MAC 주소에 할당된 IP 주소 및 할당이 발생한 시간을 포함하는 할당 로그가 포함될 수 있습니다.

- **네트워크 모니터링 소프트웨어:** 네트워크 모니터링 소프트웨어는 네트워크 트래픽을 관찰하고 그에 대한 통계를 수집하도록 설계되었습니다. 예를 들어, 다양한 프로토콜에 의해 일반적으로 소비되는 대역폭의 양과 같이 특정 네트워크 세그먼트에 대한 혹은 트래픽 흐름에 대한 상위 수준의 정보를 기록할 수 있습니다. 네트워크 모니터링 소프트웨어는 페이로드 크기, 소스 및 대상 IP 주소 및 각 패킷의 포트와 같은 네트워크 활동에 대한 보다 자세한 정보도 수집할 수 있습니다. 일부 관리 스위치 및 기타 네트워크 장치는 대역폭 사용과 관련된 통계 수집과 같은 기본적인 네트워크 모니터링 기능을 제공합니다.
- **인터넷 서비스 공급자 기록:** ISP는 네트워크 트래픽 관련 데이터를 정상적인 작업의 일부로 수집하거나 트래픽 양이 엄청나고 명백한 공격과 같은 비정상적인 활동을 조사 할 수 있습니다. 일반적인 ISP 기록은 수일 또는 수시간 동안만 보관될 수 있습니다. 6.3.1절은 ISP 및 다른 제 3자로부터 네트워크 트래픽 데이터를 수집하는 것과 관련된 법적 고려 사항을 논의합니다.
- **클라이언트/서버 응용 프로그램:** 네트워크를 통해 사용되는 일부 클라이언트/서버 응용 프로그램은 클라이언트의 IP 주소 및 포트와 같은 연결 관련 데이터를 포함할 수 있는 성공 및 실패한 사용 시도에 대한 정보를 기록할 수 있습니다. 기록된 데이터 필드(있는 경우)는 응용 프로그램마다 매우 다양합니다.
- **호스트의 네트워크 구성 및 연결:** 5.1.2절 및 5.2.1절은 호스트가 수신 대기중인 TCP 및 UDP 포트를 포함하여 개별 호스트에서 수집할 수 있는 네트워크 정보 유형을 설명합니다.

### 6.3 네트워크 트래픽 데이터 수집

6.2절에서 설명했듯이 조직은 일반적으로 정상 작동 중에 여러 장소에 기록된 네트워크 트래픽 데이터를 보유합니다. 또한 조직에서는 사고를 조사하거나 문제를 해결할 때 필요에 따라 추가 데이터를 수집하기 위해 동일한 데이터 기록 메커니즘을 사용합니다. 예를 들어, 네트워크 관리자 또는 사건 처리자는 패킷 스니퍼를 배포하여 호스트가 보낸 비정상적인 패킷을 검사할 수 있습니다.

네트워크 트래픽 데이터는 대개 로그에 기록되거나 패킷 캡처 파일에 저장됩니다. 대부분의 경우 데이터 수집은 로그 및 패킷 캡처 파일을 수집하는 것처럼 간단합니다. 4절에서는 증거 목적으로 적절한 방식으로 파일을 수집하는 방법을 설명합니다. 데이터가 파일에 저장되지 않은 경우(예: 트래픽 흐름 지도가 그래픽으로 표시되고 콘솔 화면에만 표시됨) 화면 캡쳐 또는 사진이 필요할 수 있습니다. 네트워크 트래픽 데이터 수집은 일반적으로 간단하지만 데이터 수집을 더욱 복잡하게 만들 수 있는 몇 가지 중요한 법률적 및 기술적 문제가 있습니다.

### 6.3.1 법적 고려 사항

네트워크 트래픽을 수집하면 법적 문제가 발생할 수 있습니다. 이 쟁점들 중에는 비밀번호나 이메일 내용과 같은 개인 정보 보호 또는 보안 관련 정보의 포착(고의적 또는 우발적인)이 있습니다. 이로 인해 수집된 데이터를 분석하거나 기록 시스템을 관리하는 직원(예: IDS 센서)에게 정보가 노출될 수 있습니다. 조직은 부주의한 민감한 정보의 처리에 관한 정책을 마련해야 합니다. 전자 메일 및 텍스트 문서와 같은 데이터 캡처와 관련된 또 다른 문제는 이러한 정보를 장기간 보관하면 조직의 데이터 보존 정책을 위반할 수 있다는 것입니다. 또한, 네트워크 감시와 관련된 정책을 수립하고 시스템을 모니터링하여 활동을 모니터링할 수 있는 경고 배너를 제공하는 것도 중요합니다.

대부분의 네트워크 트래픽 데이터 수집은 일반 작업의 일부로 발생하지만, 문제 해결 또는 사고 처리의 일부로 발생할 수도 있습니다. 후자의 경우 일관된 프로세스를 따르고 수행된 모든 작업을 문서화하는 것이 중요합니다. 예를 들어, 특정 사용자가 보내고 받은 모든 패킷 기록은 공식 요청 및 승인 프로세스가 성공적으로 완료된 후에 시작해야 합니다. 조직은 승인 없이 수행할 수 있고 수행할 수 없는 모니터링의 유형을 명확하게 설명하고 요청 및 승인 프로세스를 자세히 설명하는 절차를 설명하거나 참조하는 정책을 가지고 있어야 합니다.

### 6.3.2 기술적 문제

몇 가지 기술적인 문제로 인해 네트워크 트래픽에 대한 데이터 수집이 어려워 질 수 있습니다. 이 섹션에서는 몇 가지 주요 쟁점과 각각을 완화하기 위해 수행할 수 있는 작업에 대한 지침을 제공합니다.

- **데이터 저장소:** 네트워크 활동이 많은 경우, 특히 불리한 경우 공격과 같은 이벤트는 짧은 시간에 많은 이벤트를 기록할 수 있습니다. 저장 공간이 충분하지 않은 경우에는 최근 활동에 대한 정보를 덮어 쓰거나 잃어버릴 수 있습니다. 조직은 전형적인 로그 사용량 및 피크 사용량을 예측하고, 몇 시간 또는 몇 일간의 데이터가 있어야 하는지 결정하고 유지해야 합니다. 시스템 및 애플리케이션에 해당 스토리지를 충족시킬 수 있는 충분한 저장공간이 있는지 확인합니다.
- **암호화 된 트래픽:** IP 보안(IPSec), SSH 및 SSL(Secure Sockets Layer)과 같은 프로토콜을 사용하여 네트워크 트래픽을 암호화하면, 암호화된 네트워크 트래픽을 모니터링하는 장치는 원본 및 대상과 같은 트래픽의 가장 기본적인 특성만 볼 수 있습니다 IP 주소. VPN 또는 기타 터널링 기술이 사용되는 경우 IP 주소는 터널 자체에 대한 것이지 실제 활동의 소스 및 목적지가 아닐 수 있습니다. 해독된 트래픽에 대한 데이터를 수집하려면 해독된 활동을 볼 수 있는 곳에 데이터 소스를 배치해야 합니다. 예를 들어, IDS 센서를 VPN 게이트웨이 바로 뒤에 배치하면 해독된 통신에서 비정상적인 활동을 식별하는데 효과적일 수 있습니다. 통신이 내부 호스트(예: SSL 암호화 웹 세션)로 끝까지 암호화되면 네트워크 트래픽을 모니터링하는 장치는 해독된 패킷을 볼 수 없습니다. 기업은 트

래픽 암호화 기술의 적절한 사용을 지정하는 정책을 수립하여 IDS 센서와 같은 보안 제어가 암호화되지 않아도 되는 트래픽의 내용을 모니터링할 수 있도록 해야 합니다.

- **예상치 못한 포트에서 실행되는 서비스:** IDS 및 프로토콜 분석기와 같은 응용 프로그램은 포트 번호를 사용하여 특정 연결에 사용되는 서비스를 식별하는 경우가 많습니다. 불행히도, 6.1.2절에서 설명한 것처럼 대부분의 서비스는 모든 포트 번호에서 실행할 수 있습니다. 예기치 않은 포트 번호에서 실행되는 서비스와 관련된 트래픽이 제대로 캡처, 모니터링 또는 분석되지 않을 수 있으므로(예: 비정형 포트에서 웹 서비스를 제공하는) 권한이 부여되지 않은 서비스 사용이 감지되지 않을 수 있습니다. 예기치 않은 포트 번호를 사용하는 또 다른 동기는 포트 번호를 기반으로 필터링하는 주변 장치를 통해 트래픽을 연결 해제하는 것입니다. 예기치 않은 포트 사용을 식별하는 방법은 다음과 같이 여러 가지가 있습니다.
  - 알 수 없는 서버 포트와 관련된 연결에 대해 경고하도록 IDS 센서 구성
  - 예기치 않은 프로토콜(예: 표준 HTTP 포트를 사용하는 FTP 트래픽)을 사용하는 연결에 대해 경고하기 위해 프로토콜 분석을 수행하는 응용 프로그램 프록시 또는 IDS 센서 구성
  - 트래픽 흐름 모니터링 수행 및 새롭고 비정상적인 트래픽 흐름 식별
  - 특정 스트림을 다른 것으로 분석하도록 프로토콜 분석기 구성.
- **대체 액세스 포인트:** 공격자는 종종 조직의 인터넷 게이트웨이와 같은 주요 액세스 포인트를 모니터링하는 보안 컨트롤에 의한 탐지를 피하기 위해 대체 액세스 포인트에서 네트워크에 들어갑니다. 대체 액세스 포인트의 전형적인 예는 사용자 워크 스테이션의 모뎀입니다. 공격자가 워크 스테이션에 전화 접속하여 액세스할 수 있으면, 해당 워크 스테이션에서 다른 호스트에 대해 공격을 시작할 수 있습니다. 이 경우 활동이 방화벽, IDS 모니터링 네트워크 세그먼트 및 기타 공통 데이터 수집 지점을 통과하지 않기 때문에 네트워크 활동과 관련된 정보가 거의 또는 전혀 기록되지 않을 수 있습니다. 기업은 일반적으로 모뎀 및 무선 액세스 포인트와 같은 대체 액세스 포인트를 제한하고 방화벽, IDS 센서 및 기타 제어를 통해 각 액세스 포인트를 모니터링하고 제한함으로써 이러한 잠재적 문제를 해결합니다.
- **모니터링 실패:** 필연적으로 시스템 및 애플리케이션은 다양한 이유로(예: 시스템 유지 보수, 소프트웨어 오류, 공격) 장애 또는 정지를 경험하게 됩니다. IDS 센서와 같은 전용 모니터링 시스템의 경우 이중화 장비(예: 동일한 활동을 모니터링하는 두 개의 센서)를 사용하면 실패 모니터링의 영향을 줄일 수 있습니다. 또 다른 전략은 로그 연결을 위한 네트워크 기반 및 호스트 기반 방화벽과 같은 여러 레벨의 모니터링을 수행하는 것입니다.

#### 6.4 네트워크 트래픽 데이터 조사 및 분석

관심 있는 이벤트가 확인되면 분석가는 발생한 일과 조직의 시스템 및 네트워크가 어떻게 영향을 받았는지 확인하기 위해 네트워크 트래픽 데이터를 평가, 추출 및 분석합니다. 이 프로세스는 단일 데이터 소스의 몇 가지 로그 항목을 검토하고 이벤트가 오경보인지 또는 수십 개의 소스(대부분 관련 데이터가 없을 수도 있음)를 순차적으로 검사 및 분석하는 것과 같은 복잡한 작업으로

수동으로 수행하거나 여러 소스 간의 데이터 상관 관계를 분석한 다음 전체 데이터를 분석하여 이벤트의 예상 의도 및 중요성을 결정합니다. 그러나 몇 가지 로그 항목의 유효성을 검사하는 상대적으로 간단한 경우조차도 놀랍게 복잡하고 시간 소모적 일 수 있습니다.

현재 도구(예: SEM 소프트웨어, NFAT 소프트웨어)가 네트워크 트래픽 데이터를 수집하고 표시하는데 유용할 수 있지만, 이러한 도구는 분석 기능이 제한되어 있으며 잘 훈련되고 경험이 풍부한 분석가만 효과적으로 사용할 수 있습니다. 분석가는 도구를 이해하는 것 외에도 네트워킹 원리, 공통 네트워크 및 응용 프로그램 프로토콜, 네트워크 및 응용 프로그램 보안 제품, 네트워크 기반 위협 및 공격 방법에 대해 합리적으로 포괄적인 지식을 갖추고 있어야 합니다. 분석가는 네트워크 구조와 중요한 자산(예: 방화벽, 공개적으로 액세스 가능한 서버)의 IP 주소와 같은 기관의 환경에 대한 배경지식은 물론, 조직에서 사용하는 어플리케이션과 운영 체제에 대한 정보 제공을 받는 것도 매우 중요하다.

분석가가 기업 전반의 시스템 및 네트워크에서의 일반적인 사용 패턴과 같은 조직의 정상적인 컴퓨팅 기준을 이해하면 업무를 보다 쉽고 빠르게 수행할 수 있습니다. 분석가는 침입 탐지 시그니처 문서와 같은 지원 자료에 대한 액세스뿐만 아니라 네트워크 트래픽 데이터 소스 각각에 대한 확고한 이해를 가져야 합니다. 분석가는 관련 데이터를 신속하게 찾을 수 있도록 각 데이터 소스의 특성과 상대 가치를 이해해야 합니다.

분석 프로세스의 복잡성과 네트워크 트래픽 데이터를 효과적으로 분석하는데 필요한 네트워킹 및 정보 보안에 대한 광범위한 지식을 고려할 때, 복잡한 상황에서 데이터를 분석하고 결론을 도출하는데 필요한 기술에 대한 자세한 설명은 이 문서에서 다루지 않습니다. 대신 이 섹션에서는 검사 및 분석 프로세스의 기본 단계에 중점을 두고 분석가가 고려해야 할 중요한 기술적 문제를 강조합니다.

#### 6.4.1 관심있는 이벤트 식별

심사 과정의 첫 번째 단계는 관심 있는 사건을 확인하는 것입니다. 일반적으로 식별은 다음 두 가지 방법 중 하나를 통해 수행됩니다.

- 조직 내의 누군가(예: 헬프 데스크 담당자, 시스템 관리자, 보안 관리자)는 자동화된 경고 또는 사용자 불만과 같은 보안 또는 운영 관련 문제가 있음을 알립니다. 분석가는 해당 활동을 조사해야 합니다.
- 분석가의 정기적인 업무의 일부인 보안 이벤트 데이터(예: IDS 모니터링, 네트워크 모니터링, 방화벽 로그 검토)를 검토하는 동안 분석가는 관심 이벤트를 식별하고 추가로 조사해야 한다고 결정합니다.

관심 있는 사건이 확인되면 분석가는 조사의 근간을 위한 이벤트에 관한 기본 정보를 알아야 할 필요가 있습니다. 대부분의 경우 이벤트는 IDS 센서나 방화벽과 같은 네트워크 트래픽 데이터

소스를 통해 감지되므로 분석가가 더 많은 정보를 얻기 위해 해당 데이터 소스를 가리킬 수 있습니다. 그러나 사용자 불만과 같은 경우에는 어떤 데이터 소스(있는 경우)에 관련 정보가 포함되어 있는지 또는 어떤 호스트 또는 네트워크가 관련되어 있는지 분명하지 않을 수 있습니다. 따라서 분석가는 보다 일반적인 정보에 의존해야 할 수 있습니다. 예를 들어, 4층의 여러 시스템이 스스로 재부팅된 보고 등이 있습니다. 이벤트 정보가 구체적이면(예: 영향을 받는 시스템의 IP 주소) 데이터 검사가 더 쉽지만, 일반적인 정보조차도 분석가에게 관련 데이터 소스를 찾는 시작점을 제공합니다.

#### 6.4.2 데이터 출처 검사

6.2절에서 설명한 것처럼 조직에는 네트워크 트래픽 관련 데이터의 출처가 많이 있을 수 있습니다. 관심 있는 단일 이벤트는 이러한 데이터 소스 중 많은 곳에 기록될 수 있지만 개별 소스를 개별적으로 점검하는 것은 비효율적이거나 비실용적입니다. 초기 이벤트 데이터 검사의 경우 분석가는 일반적으로 모든 IDS 센서의 경고를 표시하는 IDS 콘솔 또는 다른 많은 데이터 소스를 통합하고 데이터를 구성하는 SEM 또는 NFAT 소프트웨어와 같은 몇 가지 기본 데이터 소스를 사용합니다. 이 방법은 효율적인 솔루션일 뿐만 아니라 대부분의 경우 관심 있는 이벤트는 이러한 기본 데이터 소스 중 하나에서 경고로 식별됩니다.

분석된 각 데이터 소스에 대해 분석가는 충실도를 고려해야 합니다. 일반적으로 분석가는 다른 원본에서 정규화된(수정된) 데이터를 받는 데이터보다 원본 데이터에 대한 신뢰도가 높아야 합니다. 또한, 분석가는 IDS 및 SEM 경고와 같은 해석을 기반으로 하는 데이터의 유효성을 검사해야 합니다. 악의적인 활동을 식별하는 도구는 완전히 정확하지 않습니다. 악의적인 활동을 악의적이지 않은 것으로 잘못 보고하는 오탐과 거짓 악의(악의적인 활동을 안좋지 않은 것으로 잘못 분류함) 보고를 생성하는 예가 있습니다. NFAT 및 IDS와 같은 도구는 연결 내의 모든 패킷을 처리하지 않으면 부정확한 경고를 생성할 수 있습니다. 유효성 검사(예: 원시 패킷, 다른 출처에서 수집한 정보 지원), 경고 유효성에 대한 사용 가능한 정보 검토(예: 알려진 가용성에 대한 공급 업체 의견) 및 문제가 된 도구에 대한 과거 경험을 기반으로 분석해야 합니다. 대부분의 경우 숙련된 분석가는 지원 데이터를 신속하게 검토하여 경고가 거짓 긍정이며, 더 조사할 필요가 없다고 판단할 수 있습니다.

분석가는 호스트 기반 방화벽 로그 및 패킷 캡처와 같은 보조 네트워크 트래픽 데이터 원본과 호스트 OS 감사 로그 및 바이러스 백신 소프트웨어 로그와 같은 네트워크 트래픽이 아닌 데이터 원본을 검사해야 할 수도 있습니다. 이렇게 하는 가장 일반적인 이유는 다음과 같습니다:

- **1차 출처에 자료 없음:** 경우에 따라 일반적인 주 네트워크 트래픽 데이터 원본에 활동 기록이 없을 수 있습니다. 예를 들어, 내부 네트워크 세그먼트의 두 호스트간에 네트워크 보안 장치로 모니터링되거나, 제어되지 않는 공격이 발생할 수 있습니다. 이러한 경우 분석가는 다른 가능한 데이터 소스를 식별하고 증거를 조사해야 합니다.

- **1차 출처에 데이터가 불충분하거나 유효하지 않음:** 분석가는 기본 데이터 소스에 충분한 정보가 없거나 분석가가 데이터의 유효성을 검사해야 하는 경우, 보조 데이터 소스를 검토해야 할 수 있습니다. 분석가는 하나 이상의 기본 데이터 소스를 검토한 후, 기본 데이터 소스의 관련 데이터를 기반으로 적절한 보조 데이터 소스를 쿼리해야 합니다. 예를 들어, IDS 레코드 출처가 IP 주소 10.3.0.1인 IP 주소에서 10.20.30.40으로의 공격을 나타내면 하나 또는 두 개의 IP 주소를 사용하여 다른 데이터 원본을 쿼리하면 해당 활동과 관련된 추가 데이터가 노출될 수 있습니다. 분석가는 타임 스탬프, 프로토콜, 포트 번호 및 기타 일반 데이터 필드를 사용하여 필요에 따라 검색 범위를 좁힙니다.
- **다른 곳에 있는 최고의 데이터 출처:** 때로는 공격받은 시스템의 호스트 기반 방화벽 및 IDS 로그와 같은 특정 호스트에 네트워크 트래픽 데이터에 최상의 출처가 있습니다. 이러한 데이터 소스는 매우 유용할 수 있지만 성공적인 공격 중에 데이터가 변경되거나 파괴될 수 있습니다.

추가 데이터가 필요하지만 위치를 찾을 수 없고 의심스러운 활동이 여전히 발생하는 경우 분석가는 더 많은 데이터 수집 작업을 수행해야 할 수 있습니다. 예를 들어, 분석가는 네트워크의 적절한 지점에서 패킷 캡처를 수행하여 더 많은 정보를 수집할 수 있습니다. 더 많은 정보를 수집하는 다른 방법으로는 방화벽이나 라우터를 구성하여 특정 활동에 대한 자세한 정보를 기록하고, 활동에 대한 패킷을 캡처하도록 IDS 시그니처를 설정하고, 특정 활동이 발생할 때 경고하는 사용자 지정 IDS 시그니처를 작성하는 방법이 있습니다. 데이터를 수집할 수 있는 도구에 대한 추가 지침은 6.2절을 참조하십시오. 활동이 진행 중이거나 간헐적인 경우 추가 데이터 수집이 도움이 될 수 있습니다. 활동이 끝나면 추가 데이터를 수집할 기회가 없습니다.

#### 6.4.2.1 데이터 소스 값

6.2 절에서 설명한 것처럼 조직에는 일반적으로 네트워크 트래픽 데이터의 다양한 소스가 있습니다. 이러한 출처에서 수집한 정보가 다양하기 때문에, 그 출처는 일반적인 혹은 특수한 상황에서 모두 분석가에게 다른 가치를 가지게 한다. 다음 항목은 네트워크 포렌식에서 가장 일반적인 데이터 소스의 일반적인 값을 설명합니다:

- **IDS 소프트웨어:** IDS 데이터는 종종 의심스러운 활동을 조사하기 위한 출발점입니다. IDS는 일반적으로 모든 TCP/IP 계층에서 악의적인 네트워크 트래픽을 식별하려고 할뿐만 아니라, 이벤트를 확인하고 다른 데이터 소스와 상호 연관시키는데 유용한 많은 데이터 필드(및 때로는 원시 패킷)를 기록합니다. 그럼에도 불구하고, 이전에 언급했듯이 IDS 소프트웨어는 오탐지를 유발하므로 IDS 경고를 검증해야 합니다. 이를 수행할 수 있는 범위는 경고와 관련된 기록된 데이터의 양에 의존하고 경고를 유발시키는 시그니처 특성이나 이상 탐지 방법에 관한 분석가가 사용할 수 있는(유용한) 정보입니다.
- **SEM 소프트웨어:** 이론적으로 SEM은 여러 데이터 소스 간의 이벤트를 자동으로 상관시킨 다음, 관련 정보를 추출하여 사용자에게 제시할 수 있기 때문에 포렌식에 매우 유용할 수 있습니다. 그러나 SEM 소프트웨어는 다른 여러 소스에서 데이터를 가져 와서 작동하기 때문에 SEM의 가치는 데이터 소스가 공급되

는 방식, 각 데이터 소스의 안정성, 소프트웨어가 데이터를 표준화하고 이벤트를 상관시키는 정도에 따라 다릅니다.

- **NFAT 소프트웨어:** NFAT 소프트웨어는 네트워크 트래픽 분석을 돋기 위해 특별히 설계되었으므로 관심 있는 이벤트를 모니터링한 경우 유용합니다. NFAT 소프트웨어는 일반적으로 트래픽 재구성 및 시각화와 같은 분석을 지원하는 기능을 제공합니다. 6.2.6절은 이것들에 대해 보다 자세히 설명합니다.

- **방화벽, 라우터, 프록시 서버 및 원격 액세스 서버:** 이러한 소스의 데이터는 그 자체만으로는 별로 가치가 없습니다. 시간 경과에 따른 데이터 분석은 차단된 연결 시도의 증가와 같은 전반적인 추세를 나타낼 수 있습니다. 그러나 이러한 소스는 일반적으로 각 이벤트에 대한 정보를 거의 기록하지 않기 때문에 데이터를 통해 이벤트의 특성을 거의 파악할 수 없습니다. 또한, 매일 많은 이벤트가 기록될 수 있으므로 엄청난 양의 데이터가 있을 수 있습니다. 데이터의 주요 값은 다른 소스에 의해 기록된 이벤트를 상관시키는 것입니다. 예를 들어, 호스트가 손상되어 네트워크 IDS 센서가 공격을 탐지한 경우 공격자의 IP 주소와 관련된 이벤트를 방화벽 로그에 쿼리하면 공격이 네트워크에 들어온 위치를 확인할 수 있으며 공격자가 공격한 다른 호스트를 나타낼 수 있습니다. 또한 공격자 또는 희생자의 명백한 IP 주소가 실제로 수 백 또는 수천 개의 호스트에 의해 사용 되었기 때문에 이러한 장치에 의해 수행되는 주소 매핑(예: NAT)은 네트워크 포렌식에서 중요합니다. 다행히도 분석가는 대개 로그를 검토하여 사용중인 내부 주소를 확인합니다.

- **DHCP 서버:** DHCP 서버는 일반적으로 타임 스탬프와 함께 각 IP 주소 할당 및 관련 MAC 주소를 기록하도록 구성할 수 있습니다. 이 정보는 분석가가 특정 IP 주소를 사용하여 어떤 호스트가 활동을 수행했는지 식별하는데 도움이 될 수 있습니다. 그러나 분석가들은 조직의 내부 네트워크에 있는 공격자가 MAC 주소나 IP 주소를 위조할 가능성을 염두에 두어야 합니다. 이는 스퓌핑으로 알려져 있습니다.

- **패킷 스니퍼:** 모든 네트워크 트래픽 데이터 소스 중에서 패킷 스니퍼는 네트워크 활동에 대한 대부분의 정보를 수집할 수 있습니다. 그러나 스니퍼는 수백만 또는 수십억 개의 패킷과 같이 양이 많은 데이터를 캡처할 수 있지만, 일반적으로 어떤 패킷에 악의적인 활동이 포함되어 있는지 알 수 없습니다. 대부분의 경우 패킷 스니퍼는 다른 장치나 소프트웨어가 악의적인 것으로 식별한 이벤트에 대해 더 많은 데이터를 제공하는 데 가장 적합합니다. 일부 조직에서는 일정 시간 동안 대부분 또는 모든 패킷을 기록하므로 사고가 발생하면 원시 네트워크 데이터를 검사 및 분석 할 수 있습니다. 패킷 스니퍼 데이터는 분석가 기반의 데이터를 해석하는 프로토콜 분석기로 가장 잘 검토됩니다.

- **네트워크 모니터링:** 네트워크 모니터링 소프트웨어는 DDoS 공격으로 인해 발생하는 것과 같은, 일반적인 트래픽 흐름과의 큰 차이를 확인하는데 유용합니다. DDoS 공격으로 인해 수백 또는 수천 개의 시스템이 특정 호스트나 네트워크에 대해 동시 공격을 시작합니다. 네트워크 모니터링 소프트웨어는 명백한 대상에 대한 정보를 제공할 뿐만 아니라 네트워크 대역폭 및 가용성에 대한 이러한 공격의 영향을 문서화 할 수 있습니다. 트래픽 흐름 데이터는 다른 출처에서 확인된 의심스러운 활동을 조사하는데도 유용합니다. 예를 들어, 특정 통신 패턴이 작일 또는 전주에 발생했는지 여부를 나타낼 수 있습니다.

- **ISP 기록:** ISP의 정보는 주로 공격이 스퓌핑된 IP 주소를 사용하는 경우, 소스를 추적하는데 특히 유용합니다. 6.4.4절에서는 이 주제에 대해 자세히 설명합니다.

#### 6.4.2.2 검사 및 분석 도구

수십 가지 데이터 소스 유형을 사용하여 네트워크 포렌식을 여러 가지 목적으로 수행할 수 있기 때문에 분석가는 특정 상황에 적합한 여러 가지 도구를 정기적으로 사용할 수 있습니다. 분석가는 네트워크 트래픽 데이터를 검사하고 분석할 수 있는 방법을 알고 있어야 하며, 모든 상황에 동일한 도구를 적용하는 대신 각 사례에 가장 적합한 도구를 선택해야 합니다. 분석가는 또한 도구의 단점에 유의해야 합니다. 예를 들어, 특정 프로토콜 분석기는 특정 프로토콜을 변환하거나 예기치 않은 프로토콜 데이터(예: 불법 데이터 필드 값)를 처리할 수 없을 수도 있습니다. 동일한 결함이 없는 대체 도구를 사용하는 것이 도움이 될 수 있습니다.

도구는 종종 데이터를 필터링하는데 유용합니다. 예를 들어, 분석가는 검색 범위를 좁힐 수 있는 구체적인 정보 없이 데이터를 검색해야 할 수 있습니다. 이는 분석가가 보안 이벤트 데이터 로그 및 경고를 주기적으로 또는 지속적으로 검토할 책임이 있는 경우에 가장 많이 발생합니다. 로그 항목 및 경고의 볼륨이 낮으면 데이터를 검토하는 것이 상대적으로 쉽습니다. 그러나 경우에 따라 수천 개의 이벤트가 하루에 나열될 수 있습니다. 수동 데이터 검토가 불가능하거나, 실용적이지 않은 경우 분석가는 이벤트를 필터링하고 분석가에게 가장 관련이 있는 이벤트만 제공하는 자동화된 솔루션을 사용해야 합니다. 하나의 효과적인 검토 기법은 로그를 데이터베이스로 가져 와서 쿼리를 실행하여 악성일 가능성이 높은 활동 유형을 제거하고, 나머지를 검토하거나 악성일 가능성이 가장 높은 활동 유형에 집중하는 것입니다. 예를 들어, 초기의 의심이 HTTP 활동을 통해 서버가 손상된 것이라면, 고려 사항에서 HTTP 활동을 제외한 모든 것을 제거하여 로그 필터링을 시작할 수 있습니다. 특정 데이터 소스에 대해 매우 잘 알고 있는 분석가는 일반적으로 비교적 빠르게 블라인드 검색을 수행할 수 있지만, 익숙하지 않은 데이터 소스의 경우 특정 유형을 제거하기 위한 기초가 거의 없거나 또는 전혀 없을 수도 있기 때문에 블라인드 검색에 매우 오랜 시간이 걸릴 수 있습니다.

또 다른 분석 옵션은 시각화 도구를 사용하는 것입니다. 이러한 도구는 보안 이벤트 데이터를 그래픽 형식으로 표시합니다. 이는 네트워크 트래픽 흐름을 시각적으로 표현하는데 가장 자주 사용되며 운영 문제를 해결하고 오용을 식별하는데 매우 유용합니다. 예를 들어, 공격자는 정보를 비밀리에 전달하기 위해 의도하지 않은 방식으로 프로토콜을 사용하여 은밀한 채널을 사용할 수 있습니다(예: 네트워크 프로토콜 헤더 또는 애플리케이션 페이로드의 특정 값 설정) 은밀한 채널의 사용은 일반적으로 감지하기가 어렵지만, 유용한 네트워크 트래픽 흐름의 편차를 식별하는 유용한 방법이 있습니다.

6.2.6절에서 설명한대로 시각화 도구는 종종 NFAT 소프트웨어에 포함됩니다. 일부 시각화 도구는 타임 스탬프 및 순차적 데이터 필드를 사용하여 트래픽 재구성을 수행할 수 있습니다. 도구는 이벤트 시퀀스를 결정하고 패킷이 조직의 네트워크를 통과하는 방식을 그래픽으로 표시할 수 있습니다. 일부 시각화 도구는 다른 유형의 보안 이벤트 데이터를 표시하는데 사용될 수도 있습니다. 예를 들어, 분석가는 침입 탐지 기록을 시각화 도구로 가져올 수 있으며, 소스 또는 대상 IP

주소 또는 포트와 같은 여러 가지 특성에 따라 데이터를 표시합니다. 그런 다음 분석가는 알려진 양호한 활동의 표시를 억제하여 알려지지 않은 이벤트만 표시할 수 있습니다.

시각화 도구는 특정 유형의 데이터를 분석하는데 매우 효과적일 수 있지만 일반적으로 분석가는 이러한 도구로 가파른 학습 곡선을 경험합니다. 도구로 데이터를 가져 와서 표시하는 것은 일반적으로 비교적 직관적이지만 도구를 효율적으로 사용하여 대용량 데이터 집합을 관심 있는 몇 가지 이벤트로 줄이는 방법을 배우는 것은 상당한 노력이 필요합니다. 트래픽 재구성은 프로토콜 분석기로 수행할 수도 있습니다. 이러한 도구는 일반적으로 시각화 기능이 없지만 개별 패킷을 데이터 스트림으로 변환하고 활동에 순차적인 문맥을 제공할 수 있습니다.

#### 6.4.3 결론 짓기

네트워크 포렌식의 가장 어려운 측면 중 하나는 일반적으로 사용 가능한 데이터가 포괄적이지 않다는 것입니다. 많은 경우 대부분의 경우 일부 네트워크 트래픽 데이터가 기록되지 않아 결과가 손실될 수 있습니다. 일반적으로 분석가는 분석 프로세스를 사용할 수 있는 데이터와 누락된 데이터(기술적 지식과 전문 지식을 기반으로)에 대한 가정을 기반으로 결론을 내는 체계적인 접근 방식으로 생각해야 합니다. 분석가는 이벤트와 관련하여 사용 가능한 모든 데이터를 찾고 조사해야 하지만, 경우에 따라서는, 특히 중복 데이터 소스가 많은 경우에는 실용적이지 않습니다. 분석가는 결국 이벤트를 재구성하고 그 중요성을 이해하며 그 영향을 결정할 수 있을 만큼 충분한 데이터를 찾아서 검증하고 분석해야 합니다. 많은 경우, 네트워크 트래픽 관련 소스(예: 데이터 파일 또는 호스트 OS) 이외의 소스에서 추가 데이터를 사용할 수 있습니다. 8절에서는 분석을 통해 다른 데이터를 네트워크 트래픽의 데이터와 어떻게 연관 시켜서 발생된 결과를 보다 정확하고 포괄적으로 볼 수 있는지에 대한 예제를 제공합니다.

일반적으로 분석가는 활동의 가장 중요한 특성을 파악하고 그것이 야기한 또는 조직에 초래할 수 있는 부정적인 영향을 평가하는 데 초점을 맞추어야 합니다. 외부 공격자의 신원 확인과 같은 다른 작업은 대개 시간이 많이 걸리고 성취하기 어렵고 조직이 운영 문제나 보안 취약점을 수정하는데는 도움이 되지 않습니다. 공격자의 의도를 결정하는 것도 매우 어렵습니다. 예를 들어, 공격자, 악의적인 코드, 잘못 구성된 소프트웨어 또는 잘못된 키 입력 등으로 인해 비정상적인 연결 시도가 발생할 수 있습니다. 비록 의도를 이해하는 것이 중요 할지라도, 사건의 부정적인 영향이 주요 관심사가 되어야 합니다. 침입자의 신원을 수립하는 것은 조직에서 특히 범죄 활동이 발생했을 때 중요할 수 있지만, 다른 경우에는 다른 중요한 목표와 비교하여 시야에 넣을지를 결정해야 합니다. 특정 상황에 대한 지침이 필요할 때뿐만 아니라 그러한 결정을 내리는 것과 관련된 정책 및 절차를 개발할 때 법률 고문의 조언을 구하는 것이 특히 중요합니다.

조직은 실제 사건을 분석하는 것뿐만 아니라 허위 경보의 원인을 이해하는데도 관심을 가지고 있어야 합니다. 분석가들은 종종 IDS 오탐지의 근본 원인을 파악할 수 있는 좋은 위치에 있습니다. 분석가는 보안 이벤트 데이터 원본을 변경하여 검색 정확도를 향상시킬 것을 권장해야 합니

다.

#### 6.4.4 공격자 식별

대부분의 공격을 분석 할 때, 공격자를 식별하는 것은 즉각적인 문제가 아닙니다. 즉, 공격이 중지되고 시스템과 데이터를 복구하는 것이 주요 관심사입니다. 확장된 서비스 거부 공격과 같은 공격이 진행중인 경우 조직은 공격자가 사용하는 IP 주소를 식별하여 공격을 중지할 수 있습니다. 불행하게도, 이것은 종종 말처럼 단순하지 않습니다. 다음 항목은 공격을 수행하는데 사용된 것으로 보이는 IP 주소와 관련된 잠재적인 문제를 설명합니다.

- **스푸핑된 IP 주소:** 많은 공격은 스푸핑된 IP 주소를 사용합니다. 스푸핑은 연결을 설정하는 공격에 대해 성공적으로 수행하기가 훨씬 어렵기 때문에 연결이 필요 없는 경우에 가장 일반적으로 사용됩니다. 패킷이 스푸핑되면 일반적으로 공격자는 응답을 보지 않습니다. 이는 항상 사실은 아닙니다. 침입자는 모니터하는 서브넷에서 주소를 스푸핑할 수 있으므로 응답이 해당 시스템으로 이동하면 네트워크에서 스니핑할 수도 있습니다. 때때로 스푸핑은 공격자가 도구를 잘못 구성하고 실제로 내부 NAT 주소를 사용하는 것과 같이 인위적으로 발생합니다. 때로는 공격자가 특정 주소를 의도적으로 스푸핑하는 경우가 있습니다. 예를 들어, 스푸핑된 주소가 공격의 실제 의도된 대상일 수 있으며 활동을 보는 조직은 단순히 중개자일 수 있습니다.
- **많은 소스 IP 주소:** 일부 공격은 수백 또는 수천 개의 서로 다른 원본 IP 주소를 사용하는 것처럼 보입니다. 때로는 이 모양이 현실일 수 있습니다. 예를 들어, DDoS 공격은 일반적으로 제어된 공격을 수행하는 다수의 손상된 시스템에 의존합니다. 때로는 이 모양이 환상적일 수도 있습니다. 왜냐하면, 공격은 실제 소스 IP 주소를 사용할 필요가 없기 때문에 공격자는 혼란을 주기 위해 다양한 가짜 IP 주소를 생성하기도 합니다. 때때로 공격자는 하나의 실제 IP 주소와 많은 가짜 IP 주소를 사용합니다. 이 경우 동일한 IP 주소를 사용하는 공격 전후에 발생하는 다른 네트워크 활동을 찾아 실제 IP 주소를 식별할 수도 있습니다. 침입자는 우연히 또는 의도적으로 조직과 상호작용할 수 있는 합법적인 IP 주소를 스푸핑할 수 있습니다.
- **IP 주소의 유효성:** IP 주소는 종종 동적으로 할당되기 때문에 현재 특정 IP 주소에 있는 시스템은 공격이 발생한 시스템과 다를 수 있습니다. 또한, 많은 IP 주소는 최종 사용자 시스템에 속하지 않고 NAT를 수행하는 방화벽과 같이 실제 원본 주소로 IP 주소를 대체하는 네트워크 인프라 구성 요소에 속하기도 합니다. 일부 공격자는 개인 정보를 보호하기 위해 공격자를 대신하여 활동을 수행하는 중간 서버인 익명 장치를 사용합니다.

의심스러운 호스트의 신원을 확인하는 몇 가지 방법은 다음과 같습니다:

- **IP 주소 소유자에게 문의:** ARIN(American Registry for Internet Numbers)과 같은 지역 인터넷 등록 기관(Regional Internet Registries)은 자신의 웹 사이트에서 WHOIS 쿼리 메커니즘을 제공하여 특정 IP 주소를 소유하고 있는 조직이나 사람을 식별합니다. 이 정보는 의심스러운 활동을 생성하는 세 가지 다른 IP 주소가 모두 동일한 소유자에게 등록되어 있음을 보는 것과 같은 일부 공격을 분석

하는데 도움이 될 수 있습니다. 그러나 대부분의 경우 분석가는 소유자에게 직접 연락해서는 안됩니다. 대신, 그들은 분석가의 경영 및 법률 고문에게 소유자에 대한 정보를 제공해야 하며 조직과 연락을 취하거나 필요한 경우 분석가의 승인을 얻을 수 있습니다. 주의 사항은 주로 외부 조직과 정보를 공유하는 것에 대한 우려와 관련이 있습니다. 또한, IP 주소의 소유자는 조직을 공격하는 사람이 될 수 있습니다.

- **IP 주소로 네트워크 트래픽을 송신:** 조직은 신원을 확인하기 위해 명백한 공격 IP 주소로 네트워크 트래픽을 보내면 안됩니다. 생성된 모든 응답은 공격 호스트의 신원을 결정적으로 확인할 수 없습니다. 또한, IP 주소가 공격자 시스템에 대한 것이면 공격자는 트래픽을 보고 트래픽을 보내는 호스트를 공격하거나 증거를 파괴하여 대응할 수 있습니다. IP 주소가 스퓌핑된 경우 원치 않는 네트워크 트래픽을 시스템에 보내는 것은 무단 사용 또는 공격으로 해석될 수 있습니다. 어떠한 경우에도 개인은 다른 사람들에게 권한 없이 접근하려고 시도하지 않아야 합니다.
- **ISP 지원 탐색:** 6.3.1절에서 언급했듯이 ISP는 일반적으로 의심스러운 네트워크 활동에 대한 정보를 조직에 제공하기 전에 법원 명령을 요구합니다. 따라서 ISP 지원은 일반적으로 가장 심각한 네트워크 기반 공격에 대한 유일한 옵션입니다. 이 지원은 특히 IP 주소 스퓌핑과 관련된 공격과 관련하여 유용합니다. ISP는 IP 주소가 스퓌핑되었는지 여부에 관계없이 진행중인 공격을 스스로 추적할 수 있습니다.
- **IP 주소의 히스토리를 연구:** 분석가는 이전과 동일한 IP 주소 또는 IP 주소 블록과 관련된 의심스러운 활동을 찾을 수 있습니다. 조직의 자체 네트워크 트래픽 데이터 아카이브 및 사건 추적 데이터베이스는 이전 활동을 표시할 수 있습니다. 가능한 외부 소스로는 IP 주소로 검색할 수 있는 인터넷 검색 엔진 및 온라인 사건 데이터베이스가 있습니다.
- **응용 프로그램 콘텐츠에서 단서 찾기:** 공격과 관련된 어플리케이션 데이터 패킷은 공격자의 신원에 대한 단서를 포함할 수 있습니다. IP 주소 외에도 중요한 정보에는 전자 메일 주소 또는 IRC(Internet Relay Chat) 닉네임이 포함될 수 있습니다.

대부분의 경우 조직에서는 공격에 사용된 IP 주소를 확실하게 식별할 필요가 없습니다.

## 6.5 권고 사항

이 섹션에서 네트워크 트래픽의 데이터 사용에 대한 주요 권장 사항은 다음과 같습니다:

- **조직은 개인 정보 및 민감한 정보에 관한 정책을 가지고 있어야 합니다.** 포렌식 도구 및 기술을 사용하면 실수로 포렌식 활동에 참여한 분석가 및 기타 사람들에게 민감한 정보를 공개할 수 있습니다. 또한 포렌식 도구가 실수로 캡처한 중요한 정보를 장기간 저장하면 데이터 보존 정책이 위반될 수 있습니다. 정책은 네트워크 모니터링뿐만 아니라 활동을 모니터링할 수 있는 시스템에 대한 경고 배너를 요구해야 합니다.
- **조직은 네트워크 활동 관련 로그를 위한 적절한 저장소를 제공해야 합니다.** 조직은 전형적인 로그 사용량을 예측하고 얼마나 많은 시간을 가치 있는 데이터를 조직의 정책에 따라 유지할지 시스템 및 애플리케이션에 충분한 저장 공간이 있는지 확인할지 결정해야 한다. 컴퓨터 보안 사고와 관련

된 로그는 다른 로그보다 훨씬 오랜 시간 동안 보관해야 합니다.

- **조직은 정보 수집을 향상시키기 위해 데이터 출처를 구성해야 합니다.** 시간이 지남에 따라 조직의 포렌식 분석 기능을 향상시키기 위해 운영 경험을 사용해야 합니다. 조직에서는 주기적으로 데이터 소스의 구성 설정을 검토하고 조정하여 관련 정보의 캡처를 최적화해야 합니다.
- **분석가는 합리적으로 포괄적인 기술적 지식을 가져야 합니다.** 현재 도구에는 분석 기능이 제한되어 있기 때문에 분석가는 네트워킹 원리, 일반적인 네트워크 및 응용 프로그램 프로토콜, 보안 제품, 네트워크 기반 위협 및 공격 방법에 대해 잘 훈련되고 경험이 풍부해야 합니다.
- **분석가는 각 데이터 소스의 충실도와 가치를 고려해야 합니다.** 분석가는 다른 출처의 정규화된 데이터를 받는 데이터 소스보다 원본 데이터 소스에 대한 신뢰도가 높아야 합니다. 분석가는 IDS 및 SEM 경고와 같이 데이터 해석을 기반으로 비정상적이거나 예상치 못한 데이터를 확인해야 합니다.
- **분석가들은 일반적으로 사건의 특성과 영향에 초점을 맞추어야 합니다.** 공격자의 신원 및 기타 유사한 작업을 결정하는 것은 일반적으로 시간이 많이 걸리고 성취하기 어렵고 조직이 운영 문제 또는 보안 취약점을 수정하는데 도움이 되지 않습니다. 침입자의 신원과 의도를 수립하는 것이 중요할 수 있습니다. 특히 범죄 수사가 발생하는 경우 중요하지만, 공격 대응 및 시스템 및 데이터 복구와 같은 다른 중요한 목표에 비해 중요해야 합니다.

## 7. 응용 프로그램의 데이터 사용

전자 메일, 웹 브라우저 및 워드 프로세서와 같은 응용 프로그램은 컴퓨터를 사용자에게 가치 있게 만드는 요소입니다. 응용 프로그램을 실행하기 위한 OS, 시스템간에 응용 프로그램 데이터를 전송하는 네트워크 및 응용 프로그램 데이터, 구성 설정 및 로그를 저장하기 위한 파일은 OS 와 네트워크 모두에서 응용 프로그램을 지원하는데 필요합니다. 포렌식적인 관점에서 볼 때, 응용 프로그램은 파일, OS 및 네트워크를 통합합니다. 이 절에서는 응용 프로그램 아키텍처(일반적으로 응용 프로그램을 구성하는 구성 요소)와 포렌식의 핵심인 응용 프로그램 유형에 대한 통찰력에 대해 설명합니다. 또한 응용 프로그램 데이터 수집, 검사 및 분석에 대한 지침을 제공합니다.

### 7.1 응용 프로그램 구성 요소

모든 응용 프로그램에는 실행 파일(및 공유 코드 라이브러리와 같은 관련 파일) 또는 스크립트의 형태로 코드가 포함되어 있습니다. 코드 외에도 많은 응용 프로그램에는 구성 설정, 인증, 로그, 데이터 및 지원 파일과 같은 구성 요소 중 하나 이상이 있습니다. 7.1.1절부터 7.1.5절까지는 이러한 구성 요소를 자세히 설명하고 7.1.6절에서는 주요 구성 요소의 의도된 배포와 관련된 응용 프로그램 아키텍처의 주요 유형에 대해 설명합니다.

#### 7.1.1 구성 설정

대부분의 응용 프로그램은 사용자나 관리자가 구성 설정을 변경하여 응용 프로그램의 특정 동작을 사용자 지정할 수 있게 합니다. 포렌식 관점에서 볼 때 많은 설정이 중요하지만(예: 배경색 지정) 데이터 파일과 로그가 저장되는 호스트 및 디렉토리 또는 기본 사용자 이름과 같은 다른 설정은 매우 중요할 수 있습니다. 구성 설정은 특정 응용 프로그램 세션 동안 동적으로 설정되거나 영구적일 수 있습니다. 많은 응용 프로그램에는 모든 사용자에게 적용되는 일부 설정이 있으며 일부 사용자별 설정도 지원됩니다. 구성 설정은 다음을 포함하여 여러 가지 방법으로 저장될 수 있습니다:

- **구성 파일:** 응용 프로그램은 설정을 텍스트 파일이나 전용 바이너리 형식의 파일에 저장할 수 있습니다. 일부 응용 프로그램은 구성 파일을 응용 프로그램과 동일한 호스트에 배치하지만, 다른 응용 프로그램에서는 구성 파일을 다른 호스트에 배치할 수 있습니다. 예를 들어, 응용 프로그램은 워크 스테이션에 설치될 수 있지만, 특정 사용자의 구성 파일은 파일 서버의 사용자 홈 디렉토리에 저장될 수 있습니다.
- **런타임 옵션:** 일부 응용 프로그램에서는 명령줄 옵션을 사용하여 런타임에 특정 구성 설정을 지정할 수 있습니다. 예를 들어, UNIX 전자 메일 클라이언트 mutt에는 열려는 사서함의 위치와 구성 파일의 위치를 지정하는 옵션이 있습니다. 활성 세션에 사용되는 옵션의 식별은 OS 및 응용 프로그램에 따라 다릅니다. 가능한 식별 방법에는 활성 OS 프로세스 목록 검토, OS 기록 파일 검사 및

응용 프로그램 로그 검토가 포함됩니다. 런타임 옵션은 아이콘, 시작 파일, 배치 파일 및 기타 방법으로 지정할 수도 있습니다.

- **소스 코드에 추가:** 소스 코드를 사용할 수 있게 만드는 일부 애플리케이션(예: 오픈 소스 애플리케이션, 스크립트)은 실제로 사용자 또는 관리자가 지정한 구성 설정을 소스 코드에 직접 배치합니다. 그런 다음 응용 프로그램을 컴파일하면(예: 사람이 읽을 수 있는 코드에서 기계로 읽을 수 있는 형식의 이진 파일로 변환 한 경우) 구성 설정이 실제로 실행 파일에 포함될 수 있으므로 설정보다 액세스가 훨씬 어려워 질 수 있습니다. 경우에 따라 실행 파일 내의 텍스트 문자열을 검색하여 설정을 찾을 수 있습니다.

### 7.1.2 인증

일부 응용 프로그램은 응용 프로그램을 실행하려고 시도하는 각 사용자의 신원을 확인합니다. 이 작업은 대개 응용 프로그램에 대한 무단 액세스를 방지하기 위해 수행된다. 일반적인 인증 방법은 다음과 같습니다:

- **외부 인증:** 응용 프로그램은 디렉토리 서버와 같은 외부 인증 서비스를 사용할 수 있습니다. 응용 프로그램에는 인증과 관련된 일부 레코드가 포함될 수 있지만, 외부 인증 서비스에는 보다 자세한 인증 정보가 포함될 수 있습니다.
- **독점 인증:** 응용 프로그램에는 OS가 아니라 응용 프로그램의 일부인 사용자 계정 및 암호와 같은 자체 인증 메커니즘이 있을 수 있습니다.
- **통과 인증:** 통과 인증은 OS 자격 증명(일반적으로 사용자 이름 및 암호)을 암호화되지 않은 상태로 OS에서 응용 프로그램으로 전달하는 것을 말합니다.
- **호스트/사용자 환경:** 제어된 환경(예: 조직 내의 관리되는 워크 스테이션 및 서버)에서 일부 응용 프로그램은 OS가 수행한 이전 인증에 의존할 수 있습니다. 예를 들어, 응용 프로그램을 사용하는 모든 호스트가 동일한 Windows 도메인에 속하고 각 사용자가 이미 도메인에서 인증된 경우 응용 프로그램은 각 워크 스테이션 환경에서 OS 인증 ID를 추출할 수 있습니다. 그런 다음 응용 프로그램은 액세스 권한이 있는 사용자를 추적하고, OS 인증 ID를 권한 부여된 사용자 목록과 비교하여 응용 프로그램에 대한 액세스를 제한할 수 있습니다. 이 기술은 사용자가 워크 스테이션 환경에서 사용자 ID를 변경할 수 없는 경우에만 효과적입니다.

인증 구현은 환경 및 응용 프로그램에 따라 매우 다양합니다. 이러한 구현의 세부 사항은 이 문서의 범위를 벗어납니다. 그러나 분석가는 사용자를 인증할 수 있는 방법이 다양하므로 사용자 인증 레코드의 출처가 응용 프로그램 및 응용 프로그램 구현간에 크게 다를 수 있음을 인식해야 합니다. 또한, 분석가는 특정 유형의 정보 또는 응용 프로그램 기능에 대한 액세스를 제한하기 위해 일부 응용 프로그램이 액세스 제어(일반적으로 OS에 의해 시행됨)를 사용함을 알아야 합니다. 이 지식은 특정 응용 프로그램 사용자가 수행할 수 있는 작업을 결정하는 데 도움이 될 수 있습니다.

니다. 또한, 일부 응용 프로그램은 중요한 작업을 수행하거나 제한된 데이터에 액세스하려는 시도 실패와 같은 액세스 제어와 관련된 정보를 기록합니다.

### 7.1.3 로그

일부 응용 프로그램(주로 간단한 응용 프로그램)은 로그에 정보를 기록하지 않지만 대부분의 응용 프로그램은 일부 유형의 로깅을 수행합니다. 응용 프로그램은 로그 항목을 OS 고유의 로그(예: UNIX 시스템의 syslog, Windows 시스템의 이벤트 로그), 텍스트 파일, 데이터베이스 또는 독점적인 파일 형식에 기록할 수 있습니다. 일부 응용 프로그램은 서로 다른 유형의 이벤트를 서로 다른 로그에 기록합니다. 일반적인 로그 항목 유형은 다음과 같습니다:

- **이벤트:** 이벤트 로그 항목에는 일반적으로 수행된 작업, 각 작업이 발생한 날짜와 시간 및 각 작업의 결과가 나열됩니다. 기록될 수 있는 조치의 예는 다른 시스템에 대한 연결 설정 및 관리자 레벨의 명령 발행입니다. 이벤트 로그 항목에는 각 작업을 수행하는데 사용된 사용자 이름과 반환된 상태 코드(간단한 성공/실패 상태보다 결과에 대한 자세한 정보를 제공)와 같은 지원 정보가 포함될 수도 있습니다.
- **감사:** 보안 로그 항목이라는 감사 로그 항목에는 로그온 시도 성공 및 실패, 보안 정책 변경, 파일 액세스 및 프로세스 실행과 같은 감사된 활동과 관련된 정보가 들어 있습니다. 응용 프로그램은 OS에 내장된 감사 기능을 사용하거나, 자체 감사 기능을 제공합니다.
- **오류:** 일부 응용 프로그램은 응용 프로그램 오류와 관련된 정보(일반적으로 타임 스탬프 포함)를 기록하는 오류 로그를 만듭니다. 오류 로그는 운영 문제와 공격 문제를 해결하는데 유용합니다. 오류 메시지는 관심 이벤트가 발생한 시기를 판별하고 이벤트의 일부 특성을 식별하는데 도움이 될 수 있습니다.
- **설치:** 응용 프로그램은 초기 설치 및 해당 응용 프로그램의 후속 업데이트와 관련된 정보를 기록하는 별도의 설치 로그 파일을 만들 수 있습니다. 설치 로그에 기록된 정보는 매우 다양하지만, 설치의 다양한 단계의 상태가 포함될 수 있습니다. 로그에는 설치 파일의 소스, 응용 프로그램 구성 요소가 있던 위치 및 응용 프로그램 구성과 관련된 옵션이 표시될 수도 있습니다.
- **디버깅:** 일부 응용 프로그램은 디버깅 모드에서 실행할 수 있습니다. 즉, 응용 프로그램의 작동과 관련하여 평상시보다 훨씬 많은 정보를 기록합니다. 디버깅 기록은 종종 매우 신빙성이 있으며 소프트웨어의 오류 코드와 다른 면을 해독할 수 있는 소프트웨어 제작자에게만 의미가 있을 수 있습니다. 응용 프로그램이 디버깅 기능을 제공하는 경우 일반적으로 관리자 또는 개발자가 특정 운영 문제를 해결해야 하는 경우에만 디버깅 기능이 활용 가능하게 됩니다.

### 7.1.4 데이터

거의 모든 응용 프로그램은 데이터 작성, 표시, 전송, 수신, 수정, 삭제, 보호 및 저장과 같은 하

나 이상의 방법으로 데이터를 처리하도록 특별히 설계되었습니다. 예를 들어, 전자 메일 클라이언트를 사용하면 전자 메일 메시지를 만들어 다른 사람에게 전자 메일 메시지를 보내고 보거나 삭제할 수 있습니다. 응용 프로그램 데이터는 종종 메모리에 일시적으로 있거나 영구적으로 파일에 있습니다. 애플리케이션 데이터를 포함하는 파일의 포맷은 일반적인 것(예컨대, 텍스트 파일, 비트 맵 그래픽) 또는 독점적인 것일 수 있습니다. 데이터는 고도로 구조화된 파일 및 데이터 모음인 데이터베이스에도 저장될 수 있습니다. 일부 응용 프로그램은 세션 중에 응용 프로그램 데이터를 포함할 수 있는 임시 파일을 만듭니다. 응용 프로그램이 정상적으로 종료되지 않으면 임시 파일이 미디어에 남아있을 수 있습니다. 대부분의 OS에는 임시 파일용으로 지정된 디렉토리가 있습니다. 그러나 일부 응용 프로그램에는 자체 임시 디렉토리가 있고 다른 응용 프로그램에는 데이터가 저장되는 동일한 디렉토리에 임시 파일이 있습니다. 애플리케이션은 데이터 파일 템플릿 및 샘플 데이터 파일(예: 데이터베이스, 문서)을 포함할 수도 있습니다.

### 7.1.5 지원하는 파일

응용 프로그램에는 문서 및 그래픽과 같은 지원 파일 유형이 하나 이상 포함되는 경우가 있습니다. 지원 파일은 정적인 경향이 있지만 그것이 포렌식에 가치가 없다는 것을 의미하지는 않습니다. 지원 파일 유형은 다음과 같습니다:

- **문서:** 여기에는 관리자 및 사용자 설명서, 도움말 파일 및 라이센스 정보가 포함될 수 있습니다. 문서는 분석자가 응용 프로그램의 기능, 응용 프로그램의 작동 방식 및 응용 프로그램의 구성 요소를 설명하는 등 다양한 방법으로 도움이 될 수 있습니다. 또한 문서에는 일반적으로 응용 프로그램 공급 업체의 연락처 정보가 들어 있습니다. 공급 업체는 질문에 답하고 응용 프로그램을 이해하는데 도움을 줄 수 있습니다.
- **링크:** 바로가기 파일이라고도 하는 링크는 실행 파일을 가리키는 포인터일 뿐입니다. 링크는 Windows 시스템에서 가장 자주 사용됩니다. 예를 들어, 시작 메뉴에 나열된 항목은 실제로 프로그램에 대한 링크입니다. 분석자는 링크의 속성을 검사하여 링크가 실행되는 프로그램, 프로그램의 위치 및 설정된 옵션(있는 경우)을 결정할 수 있습니다.
- **그래픽:** 이러한 파일에는 응용 프로그램에서 사용하는 독립형 그래픽과 아이콘 그래픽이 포함될 수 있습니다. 응용 프로그램 그래픽은 일반적으로 분석가에게는 거의 관심이 없지만 실행중인 실행 파일을 식별하기 위해 아이콘 그래픽이 중요할 수도 있습니다.

### 7.1.6 응용 프로그램 아키텍처

모든 응용 프로그램에는 구성 요소의 논리적 분리와 구성 요소간에 사용되는 통신 메커니즘을 나타내는 아키텍처가 있습니다. 대부분의 응용 프로그램은 다음과 같이 세 가지의 주요 응용 프로그램 아키텍처 범주 중 하나를 따르도록 설계되었습니다:

- **로컬:** 로컬 응용 프로그램은 주로 단일 시스템 내에 포함되도록 고안되었습니다. 코드, 구성 설정, 로그 및 지원 파일은 사용자 시스템에 있습니다. 로컬 응용 프로그램은 인증을 수행하지 않습니다. 애플리케이션 데이터는 사용자 시스템 또는 다른 시스템(예를 들어, 파일 서버)에 포함될 수 있으며, 보통 다수의 사용자에 의해 동시에 수정될 수 없습니다. 로컬 응용 프로그램의 예로는 텍스트 편집기, 그래픽 편집기 및 사무 생산성 제품군(예: 워드 프로세서, 스프레드 시트)이 있습니다.
- **클라이언트 서버:** 클라이언트/서버 응용 프로그램은 여러 시스템으로 분할되도록 설계되었습니다. 2 계층 클라이언트/서버 응용 프로그램은 각 사용자 워크 스테이션에 코드, 구성 설정 및 지원 파일을 저장하고 모든 사용자가 액세스하는 하나 이상의 중앙 서버에 데이터를 저장합니다. 로그는 대부분 워크 스테이션에만 저장됩니다. 3 계층 클라이언트/서버 응용 프로그램은 나머지 응용 프로그램과 사용자 인터페이스를 분리하며 데이터를 다른 구성 요소와 분리합니다. 클래식 3 계층 모델은 사용자 인터페이스 코드를 클라이언트 워크 스테이션(일부 지원 파일 포함), 응용 프로그램 서버의 나머지 응용 프로그램 코드 및 데이터베이스 서버의 데이터에 배치합니다. 많은 웹 기반 응용 프로그램은 웹 브라우저, 웹 서버, 응용 프로그램 서버 및 데이터베이스 서버 등 4 계층 모델을 사용합니다. 각 계층은 인접한 계층하고만 상호 작용하므로 3 계층 및 4 계층 모델에서 클라이언트는 데이터베이스 서버와 직접 상호 작용하지 않습니다. 일반적인 클라이언트/서버 응용 프로그램의 예로는 의료 기록 시스템, 전자 상거래 응용 프로그램 및 인벤토리 시스템이 있습니다.
- **피어 투 피어:** 피어-투-피어 응용 프로그램은 개별 클라이언트 호스트가 직접 통신하고 서로 데이터를 공유하도록 설계되었습니다. 일반적으로 클라이언트는 먼저 다른 클라이언트에 대한 정보를 제공하는 중앙 집중식 서버와 통신합니다. 이 정보는 중앙 집중식 서버를 통과할 필요가 없는 직접 연결을 설정하는데 사용됩니다. 피어-투-피어 응용 프로그램의 예로는 특정 파일 공유, 채팅 및 IM 프로그램이 있습니다. 그러나 클라이언트가 서로 직접 통신하는 대신 중앙 집중식 서버와 통신하기 때문에 이러한 유형의 일부 프로그램은 P2P(peer-to-peer)로 널리 알려져 있지만, 클라이언트/서버입니다.

대부분의 응용 프로그램은 아키텍처 측면에서 매우 융통성이 있습니다. 예를 들어, 많은 클라이언트/서버 응용 프로그램은 단일 시스템에 여러 계층을 설치할 수 있습니다. 특히 응용 프로그램 데모 또는 테스트 중에 모든 시스템이 하나의 시스템에 설치될 수 있습니다. 반면에 일부 로컬 응용 프로그램은 시스템간에 분할될 수 있으며, 일부 구성 요소는 로컬 시스템에 있고 일부는 원격 시스템에 있습니다. 응용 프로그램을 사용하면 여러 구성 요소를 설치해야 하는 위치와 데이터 및 구성 파일을 저장해야 하는 위치를 쉽게 지정할 수 있습니다. 많은 응용 프로그램의 경우 배포간에 다양성이 있을 수 있습니다.

여러 호스트간에 코드를 분할하도록 설계된 응용 프로그램은 일반적으로 호스트 간의 통신을 위해 응용 프로그램 프로토콜을 사용합니다. 전자 메일 및 웹과 같은 유비쿼터스 유형의 응용 프로그램은 잘 알려진 표준화된 응용 프로그램 프로토콜을 사용하여 여러 구성 요소 간의 상호 운용성을 용이하게 합니다. 예를 들어, 거의 모든 전자 메일 클라이언트 프로그램은 동일한 응용

프로그램 프로토콜 표준을 기반으로 하기 때문에 거의 모든 전자 메일 서버 프로그램과 호환됩니다. 그러나 표준을 기반으로 한 프로그램은 독점적인 기능을 추가하거나 표준을 어떤 식으로든 위반할 수 있습니다. 특히 표준이 철저히 상세되지 않은 경우 더욱 그렇습니다. 다른 응용 프로그램과의 상호 운용성이 문제가 되지 않거나, 바람직하지 않고 동일한 당사자가 모든 응용 프로그램 구성 요소를 만드는 경우 비표준 프로토콜이 자주 사용됩니다.

7.1 절에서 설명한 것처럼 응용 프로그램은 함께 작동하는 많은 다른 구성 요소를 가질 수 있습니다. 또한 응용 프로그램은 하나 이상의 다른 응용 프로그램에 종속되어 있을 수 있습니다. 예를 들어, 많은 전자 상거래 응용 프로그램 클라이언트가 웹 브라우저에서 실행됩니다. 또한 많은 응용 프로그램은 인쇄 및 DNS 조회(응용 프로그램 서버 및 기타 장치의 IP 주소 찾기)와 같은 OS 서비스에 의존합니다. 응용 프로그램은 계산기와 같은 간단한 유ти리티 프로그램에서부터 수천 개의 구성 요소를 포함하고 수백만 명의 사용자가 있는 대규모 전자 상거래 응용 프로그램에 이르기까지 복잡성이 매우 다양합니다.

## 7.2 응용 프로그램의 유형

응용 프로그램은 상상할 수 있는 거의 모든 목적을 위해 존재합니다. 포렌식 기술이 모든 응용 프로그램에 적용될 수 있지만 전자 메일, 웹 사용, 대화형 메시징, 파일 공유, 문서 사용, 보안 응용 프로그램 및 데이터 은폐 도구를 비롯한 특정 유형의 응용 프로그램이 포렌식 분석의 중심이 될 가능성이 큽니다. 거의 모든 컴퓨터에는 이 범주에서 최소한 몇 가지 응용 프로그램이 설치되어 있습니다. 다음 절에서는 이러한 유형의 응용 프로그램에 대해 자세히 설명합니다.

### 7.2.1 이메일

이메일은 사람들이 전자적으로 의사 소통하는데 가장 중요한 수단이 되었습니다. 각 전자 메일 메시지는 머리글과 본문으로 구성됩니다. 전자 메일의 본문에는 메모 또는 개인 서신과 같은 실제 메시지 내용이 들어 있습니다. 전자 메일의 헤더에는 전자 메일에 관한 다양한 정보가 포함됩니다. 기본적으로 대부분의 전자 메일 클라이언트 응용 프로그램은 각 메시지에 대해 몇 가지 헤더 필드만 표시합니다. 보낸 사람 및 받는 사람, 전자 메일 주소, 메시지를 보낸 날짜와 시간 및 메시지 제목을 표시합니다. 그러나 헤더에는 일반적으로 다음과 같은 몇 가지 다른 필드가 포함됩니다:

- 메시지 ID
- 메시지 작성에 사용된 전자 메일 클라이언트의 유형
- 보낸 사람에 의해 지정된 메시지의 중요성(예: 낮음, 보통, 높음)
- 라우팅 정보 - 메시지가 전송 중에 통과한 전자 메일 서버와 각 서버가 메시지를 수신한 시각

- 전자 메일 콘텐츠가 단순히 텍스트 본문으로 구성되는지 또는 첨부 파일, 포함 그래픽 등을 나타내는지의 메시지 내용 유형

전자 메일 클라이언트 응용 프로그램은 전자 메일을 수신, 저장, 읽기, 작성 및 전송하는데 사용됩니다. 대부분의 전자 메일 클라이언트는 전자 메일 주소, 이름 및 전화 번호와 같은 연락처 정보를 저장할 수 있는 주소록도 제공합니다. 암호화 프로그램은 전자 메일 클라이언트와 함께 전자 메일의 본문 및 첨부 파일을 암호화하는데 사용됩니다.

사용자가 전자 메일을 보내면 SMTP를 사용하여 전자 메일 클라이언트에서 서버로 전송됩니다. 전자 메일을 보낸 사람과 받는 사람이 다른 전자 메일 서버를 사용하는 경우 전자 메일은 받는 사람의 서버에 도달할 때까지 SMTP를 사용하여 추가 전자 메일 서버를 통해 라우팅됩니다. 일반적으로 받는 사람은 별도의 시스템에서 전자 메일 클라이언트를 사용하여 POP3(Post Office Protocol 3) 또는 IMAP(Internet Message Access Protocol)을 사용하여 전자 메일을 검색합니다. 몇몇 경우에, 이메일 클라이언트는 목적지 서버(예를 들어, 다중 사용자 UNIX 시스템) 상에 있을 수 있습니다. 대상 서버는 종종 부적절한 콘텐츠(예: 스팸, 바이러스)로 메시지를 차단하는 등 전자 메일을 검색 가능하게 만들기 전에 전자 메일을 검사합니다. 끝에서 끝까지, 단일 전자 메일 메시지에 관한 정보는 보낸 사람의 시스템, 메시지를 처리하는 각 전자 메일 서버, 받는 사람의 시스템, 바이러스 백신, 스팸 및 콘텐츠 필터링 서버 등 여러 위치에 기록될 수 있습니다.

## 7.2.2 웹 사용

웹 브라우저를 통해 사람들은 상상할 수 있는 거의 모든 유형의 데이터를 포함하는 웹 서버에 액세스합니다. 많은 응용 프로그램은 웹 브라우저를 통해 액세스할 수 있는 웹 기반 인터페이스도 제공합니다. 웹 브라우저는 많은 용도로 사용될 수 있기 때문에 가장 일반적으로 사용되는 응용 프로그램 중 하나입니다. 웹 통신의 기본 표준은 HTTP입니다. 그러나 HTTP에는 다양한 표준 및 독점 형식으로 다양한 유형의 데이터가 포함될 수 있습니다. HTTP는 기본적으로 웹 브라우저와 웹 서버간에 데이터를 전송하는 메커니즘입니다.

일반적으로 웹 사용과 관련된 가장 풍부한 정보 소스는 웹 브라우저를 실행하는 호스트입니다. 웹 브라우저에서 검색할 수 있는 정보로는 즐겨 찾는 웹 사이트 목록, 방문한 웹 사이트의 기록(캐시된 웹 데이터 파일 및 쿠키-생성 날짜 및 만료 날짜 포함-)이 있습니다. 웹 사용 정보의 또 다른 좋은 소스는 웹 서버입니다. 웹 서버는 대개 수신한 요청에 대한 로그를 보관합니다. 각 요청에 대해 웹 서버에서 자주 기록하는 데이터에는 타임 스탬프가 포함됩니다. IP 주소; 웹 브라우저 버전 및 요청을 작성한 호스트의 OS; 요청 유형(예: 데이터 읽기, 쓰기 데이터); 요구 된 자원; 및 상태 코드 등; 각 요청에 대한 응답에는 요청의 성공 또는 실패를 나타내는 세자리 숫자 상태 코드가 포함됩니다. 성공적인 요청의 경우 상태 코드는 수행된 작업을 설명합니다. 실패의 경우

상태 코드는 요청이 실패한 이유를 설명합니다.

웹 브라우저와 서버 외에도 몇 가지 다른 유형의 장치와 소프트웨어에는 관련 정보가 기록 될 수 있습니다. 예를 들어, 웹 프록시 서버와 응용 프로그램 프록시 방화벽은 웹 서버 로그와 비슷한 세부 수준의 HTTP 활동 로깅을 수행할 수 있습니다. 라우터, 프록시가 아닌 방화벽 및 기타 네트워크 장치는 원본 및 목적지 IP 주소, 포트, 네트워크 연결과 같은 HTTP의 기본적인 측면을 기록할 수 있습니다. 웹 콘텐츠 모니터링 및 필터링 서비스를 사용하는 조직은 서비스 로그에서 특히 거부된 웹 요청과 관련하여, 유용한 데이터를 찾을 수 있을 것입니다.

### 7.2.3 대화형 통신

대화형 통신 서비스는 발신자에서 수신자로 갈 때, 일반적으로 몇 분이 걸리는 전자 메일 메시지와 달리 실시간(또는 거의 실시간) 통신을 제공합니다. 대화형 통신에 일반적으로 사용되는 응용 프로그램 유형은 다음과 같습니다:

- **그룹 채팅:** 그룹 채팅 응용 프로그램은 많은 사용자가 한 번에 메시지를 공유할 수 있는 가상 회의 공간을 제공합니다. 그룹 채팅 응용 프로그램은 일반적으로 클라이언트/서버 아키텍처를 사용합니다. 가장 인기 있는 그룹 채팅 프로토콜인 IRC(Internet Relay Chat)는 비교적 간단한 텍스트 기반 통신을 사용하는 표준 프로토콜입니다. IRC는 또한 사용자가 파일을 보내고 받을 수 있는 메커니즘을 제공합니다.
- **인스턴트 메시징 응용 프로그램:** 인스턴트 메시징 응용 프로그램은 피어-투-피어(peer-to-peer) 방식으로 사용자가 텍스트 메시지와 파일을 서로 직접 또는 클라이언트/서버로 보내고 메시지와 파일을 중앙 집중식 서버를 통해 전달할 수 있습니다. IM 응용 프로그램 구성 설정에는 사용자 정보, 사용자가 통신한 사용자 목록, 파일 전송 정보 및 보관된 메시지 또는 채팅 세션이 포함될 수 있습니다. 몇 가지 주요 인터넷 기반 IM 서비스가 있으며, 각 서비스는 고유한 통신 프로토콜을 사용합니다. 여러 회사는 조직 내에서 실행되는 엔터프라이즈 IM 제품도 제공합니다. 이러한 제품은 조직의 전자 메일 서비스와 함께 어느 정도 통합되는 경우가 많으며, 인증된 전자 메일 사용자만 사용할 수 있습니다.
- **오디오 및 비디오:** 네트워크의 용량이 계속 증가함에 따라 컴퓨터 네트워크에서 실시간 비디오 및 오디오 통신을 수행하는 것이 일반적으로 발생합니다. VoIP(Voice over IP)와 같은 기술은 사람들이 인터넷과 같은 네트워크를 통해 전화 통화를 할 수 있게 해줍니다. 일부 오디오 구현은 컴퓨터 기반 서비스를 종단 간에서 제공하지만, 나머지는 중간 서버와 함께 컴퓨터 네트워크와 표준 전화 네트워크 간의 부분적인 컴퓨터 기반으로 제공합니다. 많은 오디오 기술은 주로 피어-투-피어 응용 프로그램입니다. 비디오 기술은 원격 회의를 개최하거나 두 사람 사이에 '화상 전화' 통신을 하는데 사용될 수 있습니다. 오디오 및 비디오 통신에 일반적으로 사용되는 프로토콜로는 H.323 및 SIP(Session Initiation Protocol)가 있습니다.

#### 7.2.4 파일 공유

사용자는 다양한 프로그램을 통해 파일을 공유할 수 있습니다. 이 섹션의 앞부분에서 설명한 것처럼 전자 메일, 그룹 채팅 프로그램 및 IM 소프트웨어는 모두 특정 파일을 보내고, 받을 수 있는 기능을 제공합니다. 그러나 이러한 프로그램은 일반적으로 받는 사람이 파일을 찾아보고, 전송 할 파일을 선택하는 것을 허용하지 않습니다. 이러한 기능 수준을 위해서는 완전한 파일 공유 프로그램과 프로토콜이 필요합니다. 파일 공유 프로그램은 다음과 같이 아키텍처 별로 그룹화할 수 있습니다:

- **클라이언트/서버:** 전통적인 파일 공유 서비스는 파일 저장소를 포함하는 중앙 파일 서버와 함께 클라이언트/서버 아키텍처를 사용합니다. 클라이언트는 연결을 시작하고, 필요한 경우 인증하고, 필요한 경우 사용 가능한 파일 목록을 검토한 다음 파일을 전송하여 사용할 수 있습니다. 일반적으로 사용되는 클라이언트/서버 파일 공유 서비스는 FTP, NFS(Network File Sharing), AFP(Apple Filing Protocol) 및 SMB(Server Message Block)입니다. 이것은 암호처럼 제공된 인증 자격 증명을 포함하여 전송중인 데이터의 기밀성을 보호하지 않는 표준화된 프로토콜입니다. Secure FTP(SFTP) 및 Secure Copy(scpt)와 같은 보안 대안은 네트워크 통신을 암호화합니다. 대부분의 OS에는 파일 공유 클라이언트(예: FTP, SMB)가 내장되어 있지만, 유사한 기능을 제공하는 다양한 타사 프로그램을 설치할 수도 있습니다.
- **피어-투-피어:** 대부분의 피어-투-피어 파일 공유 서비스는 주로 인터넷을 통해 음악, 그래픽 또는 소프트웨어를 교환하는데 사용됩니다. 단일 서버가 파일 저장소를 보유하는 클라이언트/서버 파일 공유와는 달리, 여러 호스트에 파일이 있는 피어-투-피어-파일 공유본이 배포됩니다. 피어-투-피어 파일 공유 서비스에서 서버는 일반적으로 클라이언트에게 다른 클라이언트의 위치에 대한 정보를 제공하지만, 중앙 서버는 파일 또는 파일 정보 전송에는 참여하지 않습니다. 피어-투-피어 파일 공유 서비스는 일반적으로 사용자 인증이 필요하지 않습니다. 모든 파일 찾아보기 및 전송은 클라이언트(피어) 간에 직접 이루어집니다. 사용자는 일반적으로 특정 서비스를 사용할 때, 여러 클라이언트 프로그램에서 선택할 수 있습니다. 대부분의 서비스가 각 사용자가 자신의 시스템에서 공유되는 파일을 제어할 수 있도록 하지만, 암호화된 피어-투-피어로 알려진 서비스는 각각의 사용자 하드 드라이브의 암호화된 부분에 저장된 다른 파일들을 저장함으로써 작동하여, 사용자가 자신의 시스템 영역에 저장된 내용을 제어하거나 지식을 주지 못하게 합니다.

#### 7.2.5 문서 사용

많은 사용자가 편지, 보고서 및 차트와 같은 문서 작업에 많은 시간을 할애합니다. 문서에는 모든 유형의 데이터가 포함될 수 있으므로, 분석가가 종종 관심을 갖습니다. 이러한 문서를 만들고, 보고 편집하는데 사용되는 소프트웨어 클래스를 Office 생산성 응용 프로그램이라고 합니다. 여기에는 워드 프로세서, 스프레드 시트, 프레젠테이션 및 개인 데이터베이스 소프트웨어가 포함됩니다. 문서에는 종종 문서를 작성하거나 가장 최근에 편집한 사람의 이름 또는 사용자 이름 또는 문서를 만드는데 사용된 소프트웨어의 라이센스 번호 또는 시스템의 MAC 주소와 같은 사용자

또는 시스템 정보가 포함되어 있습니다.

### 7.2.6 보안 응용 프로그램

호스트는 흔히 전자 메일 클라이언트 및 웹 브라우저와 같이 일반적으로 사용되는 응용 프로그램을 통해 발생하는 오용 및 남용으로부터 호스트를 보호하려는 하나 이상의 보안 응용 프로그램을 실행합니다. 일반적으로 사용되는 보안 응용 프로그램에는 바이러스 백신 소프트웨어, 스파이웨어 검색 및 제거 유ти리티, 콘텐츠 필터링(예: 스팸 방지 조치) 및 호스트 기반 침입 탐지 소프트웨어가 있습니다. 보안 응용 프로그램의 로그에는 의심스러운 활동에 대한 자세한 기록이 포함될 수 있으며, 보안 손상이 발생했는지 또는 예방되었는지 여부를 나타낼 수도 있습니다. 보안 응용 프로그램이 중앙에서 관리되고 제어되는 바이러스 백신 소프트웨어와 같은 엔터프라이즈 배포의 일부인 경우 개별 호스트 및 중앙 집중식 응용 프로그램에서 로그를 사용할 수 있습니다.

### 7.2.7 데이터 은폐 도구

어떤 사람들은 다른 사람들의 데이터를 은폐하는 도구를 사용합니다. 이는 승인되지 않은 당사자의 액세스에 대한 데이터의 기밀성 및 무결성을 보호하거나 부적절한 활동의 증거를 숨기는 등의 악의적인 목적을 위해 양호한 목적으로 수행될 수 있습니다. 데이터 은폐 도구의 예로 파일 암호화 유ти리티, 스테가노그래피 도구 및 시스템 정리 도구가 있습니다. 시스템 정리 도구는 웹 브라우저와 같은 특정 응용 프로그램뿐만 아니라, 임시 디렉토리와 같은 일반 위치의 데이터를 제거하는 특수 목적의 소프트웨어입니다. 대부분의 데이터 은폐 도구를 로그에서 캡처하지는 않습니다. 분석가는 시스템에서 이러한 도구를 식별하고 도구를 인식할 수 있도록, 이러한 도구의 기능을 알고 있어야 합니다.

## 7.3 응용 프로그램 데이터 수집

7.1절에서 설명한 것처럼 응용 프로그램 관련 데이터는 파일 시스템, 휘발성 OS 데이터 및 네트워크 트래픽 내에 위치할 수 있습니다. 4.2, 5.2절 및 6.3절에는 이러한 각 소스에서 데이터를 수집하는 특정 정보가 들어 있습니다. 이러한 소스에 포함될 수 있는 응용 프로그램 데이터 유형은 다음과 같습니다.

- **파일 시스템:** 파일 시스템은 실행 파일 및 스크립트, 구성 파일, 지원 파일(예: 문서), 로그 및 데이터 파일을 비롯하여 응용 프로그램과 관련된 많은 유형의 파일을 포함할 수 있습니다.
- **휘발성 OS 데이터:** 휘발성 OS 데이터에는 응용 프로그램에서 사용하는 네트워크 연결, 시스템에서 실행중인 응용 프로그램 프로세스 및 각 프로세스에 사용된 명령줄 인수, 응용 프로그램에서 열린 파일 및 기타 지원 정보가 포함될 수 있습니다.

- **네트워크 트래픽:** 가장 관련성이 높은 네트워크 트래픽 데이터는 원격 응용 프로그램에 대한 사용자 연결과 다른 시스템에 있는 응용 프로그램 구성 요소 간의 통신을 포함합니다. 다른 네트워크 트래픽 레코드는 응용 프로그램에서 원격 인쇄를 위한 네트워크 연결 및 응용 프로그램 구성 요소를 해결하기 위해 응용 프로그램 클라이언트나 다른 구성 요소에 의한 DNS 조회와 같은 지원 정보를 제공할 수도 있습니다.

분석가들은 수집해야 할 데이터를 결정할 때 큰 어려움에 처하는 경우가 많습니다. 대부분의 경우 분석가는 먼저 어떤 응용 프로그램이 중요한지 결정해야 합니다. 예를 들어, 하나의 시스템에 여러 웹 브라우저와 전자 메일 클라이언트를 설치하는 것이 일반적입니다. 분석자가 개인의 조직 전자 메일 서비스 사용과 관련된 데이터를 수집하도록 요청 받으면 개인이 해당 서비스에 액세스 할 수 있는 모든 방법을 염두에 두어야 합니다. 사용자 컴퓨터에는 세 가지 전자 메일 클라이언트와 조직에서 제공하는 웹 기반 전자 메일 클라이언트에 액세스하는데 사용할 수 있는 두 개의 웹 브라우저가 포함될 수 있습니다. 사용자 컴퓨터의 경우 분석가는 컴퓨터에서 모든 데이터를 수집한 다음 시험 과정에서 실제로 어떤 전자 메일에 사용된 클라이언트를 결정할 수 있습니다. 그러나 사용자의 컴퓨터 이외에도 많은 잠재적인 데이터 소스가 있으며, 이러한 소스는 사용된 클라이언트에 따라 다를 수 있습니다. 예를 들어, 웹 기반 클라이언트의 사용은 웹 브라우저, 웹 브라우저 캐시, 쿠키 및 개인 방화벽 로그는 물론 웹 서버, 방화벽, IDS 및 콘텐츠 모니터링 소프트웨어 로그에 기록되었을 수 있습니다. 어떤 상황에서는 필요한 데이터를 수집하는 과정에서 응용 프로그램의 모든 구성 요소를 확인하고(상황과 요구 사항의 세부 사항을 기반으로) 관심을 가질 가능성이 가장 높은 항목을 결정하고, 각 구성 요소의 위치를 찾아야 합니다. 8절에는 구성 요소 식별의 복잡성과 응용 프로그램의 데이터 수집 우선 순위에 대한 예가 나와 있습니다.

#### 7.4 응용 데이터 검사 및 분석

응용 프로그램 데이터를 검사하고 분석하는 것은 크게 각각 4.3절과 4.4절, 5.3절 및 6.4절에서 설명하는 도구와 기술을 사용하여 응용 프로그램 데이터의 특정 부분, 파일 시스템, 휘발성 OS 데이터 및 네트워크 트래픽을 확인하는 것으로 구성됩니다. 응용 프로그램이 사용자 정의 프로그램(예: 사용자가 작성한 프로그램)인 경우 검사 및 분석이 방해 받을 수 있습니다. 분석가는 그러한 응용 프로그램에 대해 알지 못할 것입니다. 검사에서 또 다른 문제는 데이터 암호화 및 암호화 같은 응용 프로그램 기반 보안 제어를 사용하는 것입니다. 많은 응용 프로그램이 이러한 보안 제어를 사용하여 권한이 부여된 사용자가 중요한 데이터에 무단으로 액세스하지 못하게 합니다.

경우에 따라 분석가는 여러 가지 애플리케이션 데이터 소스의 관련 애플리케이션 데이터를 수집합니다. 이것은 주로 수동 프로세스입니다. 응용 프로그램 관련 이벤트 및 이벤트 재구성에 대한 자세한 분석에는 일반적으로 모든 소스에서 제공하는 정보를 이해하는 숙련되고 지식이 풍부한 분석가가 필요합니다. 분석가는 개별 응용 프로그램 데이터 원본의 검사 및 분석 결과를 검토

하고 정보가 함께 어울리는 지 확인할 수 있습니다. 분석가에게 도움이 될 수 있는 도구로는 여러 데이터 소스간에 일부 응용 프로그램 관련 이벤트를 연관시킬 수 있는 보안 이벤트 관리 소프트웨어(6.2.5 절 참조) 및 로그 분석 소프트웨어(일부 유형의 호스트 기반 침입 탐지 소프트웨어 포함)가 있으며, 의심스러운 활동을 식별하기 위해 특정 유형의 로그에 대해 실행할 수 있습니다. 8절에서는 여러 유형의 출처에서 나온 데이터를 분석을 상호 연관시키는 것을 통해 발생된 결과를 보다 정확하고 포괄적으로 볼 수 있습니다.

## 7.5 권고 사항

애플리케이션에서 데이터를 사용하기 위해, 이 섹션에서 제시되는 주요 권장 사항은 다음과 같습니다:

- **분석가는 가능한 모든 응용 프로그램 데이터 소스를 고려해야 합니다.** 응용 프로그램 이벤트는 다양한 데이터 소스에서 기록될 수 있습니다. 또한, 응용 프로그램은 시스템에 설치된 다중 클라이언트 프로그램 및 웹 기반 클라이언트 인터페이스와 같은 여러 메커니즘을 통해 사용될 수 있습니다. 이러한 상황에서 분석가는 모든 응용 프로그램 구성 요소를 식별하고, 관심 대상이 될 가능성이 가장 높은 항목을 결정하며 관심 있는 각 구성 요소의 위치를 찾고 데이터를 수집해야 합니다.
- **분석가는 다양한 출처의 응용 프로그램 데이터를 수집해야 합니다.** 분석가는 개별 응용 프로그램 데이터 원본의 검사 및 분석 결과를 검토하고 정보가 맞는 방식을 결정하고, 응용 프로그램 관련 이벤트 및 이벤트 재구성에 대한 자세한 분석을 수행해야 합니다.

## 8. 여러 소스의 데이터 사용

4절부터 6절은 세 가지 데이터 소스 범주(데이터 파일, OS 및 네트워크 트래픽)의 데이터 수집, 조사 및 분석을 설명합니다. 이러한 범주의 데이터를 수집, 검사 및 분석하는 기술과 프로세스는 근본적으로 다릅니다. 7절에서는 세 가지 데이터 소스 범주를 결합하는 응용 프로그램 데이터의 수집, 검사 및 분석에 대해 설명합니다. 예를 들어, 많은 응용 프로그램은 데이터 파일을 사용하고 OS 구성과 네트워크 트래픽을 생성합니다. 컴퓨터 보안 사고와 같은 많은 상황은 여러 유형의 데이터 원본을 분석하고 여러 원본에서 이벤트를 상호 연관시킴으로써 가장 효과적으로 처리 할 수 있습니다.

이 섹션에서는 디지털 포렌식 중에 여러 데이터 소스를 사용하는 두 가지 예를 제시합니다. 각 예제는 시나리오를 설명하고 포렌식 분석에 대한 구체적인 필요성을 나타내며, 포렌식 프로세스가 수행되는 방법에 대한 설명을 제공합니다. 설명은 프로세스가 얼마나 복잡한지를 보여줍니다. 이 섹션에 제시된 예는 다음과 같습니다:

- 어떤 웜이 시스템에 감염되었는지 확인하고 웜의 특징 식별
- 협박 전자 메일이 포함된 사이버 이벤트의 순서 재구성

### 8.1 의심되는 네트워크 서비스 웜 감염

조직의 헬프 데스크는 느린 응답을 제공하는 특정 서버에 대해 불평하는 사용자로부터 짧은 시간에 여러 번 전화를 받습니다. 지원 센터는 문제점 티켓을 모니터링 그룹에 보냅니다. 그 그룹의 네트워크 IDS는 최근에 서버와 관련된 몇 가지 비정상적인 경고를 보고했으며, 경고를 검토한 분석가는 정확하다고 믿습니다. 경고의 데이터는 일부 의심스러운 활동이 서버로 보내졌음을 나타내며, 서버는 이제 다른 시스템으로 향하는 동일한 활동을 생성합니다. 침입 탐지 분석가의 초기 가설은 웜이 취약한 네트워크 서비스를 공격하여, 다른 시스템을 감염시키기 위해 감염되었을 수 있다는 것입니다. 모니터링 그룹은 서버에 발생할 수 있는 사고를 조사할 의무가 있는 사고 처리자에게 접촉합니다.

사건의 경우, 이 특정 사건 처리자의 역할은 시스템에 감염된 웜 유형을 판별하고, 웜의 특징을 식별하는 것입니다. 이 정보는 효과적으로 봉쇄, 박멸 및 복구 활동을 수행하고 조직 내의 다른 시스템이 감염되는 것을 방지하기 위한 사고 대응팀의 능력에 매우 중요합니다. 사건 처리자의 조사에서 사건이 웜이 아닌 다른 원인에 의해 발생한 것으로 밝혀지면, 처리자가 식별한 특성이 실제로 발생한 결과를 설명하는데 유용해야 합니다.

이 사건과 관련된 정보는 여러 곳에서 기록될 수 있습니다. 사고 처리자는 데이터 소스에 대한 핸들러의 이전 경험 및 사고와 관련하여, 사용 가능한 초기 정보를 기반으로 관련 정보를 가장 많이 가질 수 있는 데이터 소스를 먼저 확인해야 합니다. 예를 들어, 네트워크 IDS 센서가 의심스

러운 활동을 보았기 때문에 동일한 네트워크 세그먼트를 모니터링하는 다른 네트워크 기반 데이터 소스에도 관련 정보가 포함될 수 있습니다. 조직에서 다양한 이벤트 소스의 데이터를 가져오는 보안 이벤트 관리 또는 네트워크 포렌식 분석 도구 소프트웨어를 사용하는 경우 SEM 또는 NFAT 콘솔에서 몇 가지 쿼리를 실행하여 필요한 모든 정보를 수집할 수 있습니다. 중앙 집중식 데이터 소스를 사용할 수 없는 경우 처리자는 다음과 같이 잠재적인 개별 공격 출처를 확인해야 합니다:

- **네트워크 IDS:** 사건의 초기 보고서는 네트워크 IDS 센서에 의해 생성되었기 때문에 네트워크 IDS 데이터에 네트워크 활동의 기본 특성에 대한 정보가 포함되어있을 가능성이 큽니다. 최소한 데이터는 공격받은 서버와, 대상으로 지정된 네트워크 서비스를 나타내는 포트 번호를 표시해야 합니다. 서비스를 확인하는 것은 익스플로잇된 취약점을 발견하고 유사한 시스템에서 발생하는 것을 방지하기 위한 완화 전략을 개발하는데 매우 중요합니다. 분석의 관점에서 볼 때 대상 서비스와 포트 번호를 아는 것도 중요합니다. 왜냐하면 이 정보를 사용하여 다른 가능한 데이터 소스를 식별하고, 관련 정보를 쿼리할 수 있기 때문입니다. 일부 네트워크 IDS 배포판은 응용 프로그램 데이터(예: 웹 요청 및 응답, 전자 메일 헤더 및 파일 첨부 이름)와 같은 유용한 추가 정보를 기록할 수 있습니다. 응용 프로그램 데이터에는 특정 웜과 관련된 단어, 구 또는 다른 문자 시퀀스가 포함될 수 있습니다.
- **네트워크 기반 방화벽:** 방화벽은 일반적으로 의도된 대상 IP 주소 및 포트를 포함하여 차단된 연결 시도를 기록하도록 구성됩니다. 따라서 방화벽에는 차단된 웜 활동 기록이 있을 수 있습니다. 일부 웜은 여러 서비스나 서비스 포트를 악용하려고 시도합니다. 방화벽 기록은 웜이 실제로 4개 이상의 다른 포트 번호에 대한 연결을 설정하려고 시도했지만 방화벽이 3개의 포트를 사용하여 연결을 차단했음을 나타낼 수 있습니다. 이 정보는 웜을 식별하는데 유용할 수 있습니다. 허용된 연결을 기록하도록 방화벽을 구성하면 조직의 어떤 호스트가 웜 트래픽을 수신했는지 또는 감염되어 자체 웜 트래픽을 생성했는지를 로그에 표시할 수 있습니다. 이것은 네트워크 IDS 센서가 방화벽에 도달하는 모든 트래픽을 모니터링하지 않는 상황에 특히 유용합니다. 라우터, VPN 게이트웨이 및 원격 액세스 서버와 같이 웜 트래픽이 통과했을 수 있는 다른 경계 장치는 네트워크 기반 방화벽으로 기록된 것과 유사한 정보를 기록할 수 있습니다.
- **호스트 IDS 및 방화벽:** 감염된 시스템에서 실행되는 IDS 및 방화벽 제품은 네트워크 IDS 및 방화벽 제품보다 자세한 정보가 포함될 수 있습니다. 예를 들어, 호스트 IDS는 웜에 의해 수행된 호스트의 파일 또는 구성 설정에 대한 변경 사항을 식별할 수 있습니다. 이 정보는 웜이 호스트에 어떤 영향을 주었는지 파악하고, 시스템을 감염시킨 웜을 식별하여 봉쇄, 박멸 및 복구 활동을 계획하는데 도움이 됩니다. 그러나 많은 웜이 호스트 기반 보안 제어를 비활성화하고 로그 항목을 없애기 때문에 호스트 IDS 및 방화벽 소프트웨어의 데이터가 제한되거나 누락될 수 있습니다. 소프트웨어가 로그 사본을 중앙 집중식 로그 서버로 전달하도록 구성된 경우에는 해당 서버에 대한 쿼리가 일부 정보를 제공할 수 있습니다.
- **바이러스 백신 소프트웨어:** 위협이 서버에 도달하여 성공적으로 침입했기 때문에 네트워크 또는 호스트 기반 바이러스 백신 소프트웨어에 위협 요소에 대한 기록이 포함되어 있을 가능성은 거의 없습니다. 바이러스 백신 소프트웨어가 웜을 탐지한 경우에는 그것을 중지시켜야 합니다. 또한 사건 처리자는 포렌식 툴킷의 최신 버전 바이러스 백신 소프트웨어를 사용하여 서버에서 웜

을 검색할 수 있습니다.

- **응용 프로그램 로그:** 웜이 HTTP 또는 SMTP와 같은 공통 응용 프로그램 프로토콜을 사용하는 경우 웜이 응용 프로그램 서버 로그, 프록시 서버 및 응용 프로그램별 보안 제어와 같은 여러 위치에 기록될 수 있습니다. 보편적이지 않은 응용 프로그램 프로토콜은 응용 프로그램 서버로 그에만 정보가 있을 수 있습니다. 응용 프로그램 로그는 활동의 응용 프로그램별 특성에 대한 세부적인 내용을 기록하며, 일반적이지 않은 응용 프로그램의 공격 특성을 식별하는데 특히 유용합니다.

초기 정보 수집 노력의 목표는 웜의 확실한 식별을 위한 충분한 특성을 식별하는 것입니다. 특히 수십 가지의 변종이 있는 웜의 경우 어려울 수 있습니다. 이러한 변형은 종종 유사한 특성을 갖지만 시스템에 다른 영향을 미칩니다. 분석가는 바이러스 백신 공급 업체의 멀웨어 데이터베이스에 대한 쿼리를 수행하여 제품 이름, 서비스 이름 또는 포트 번호, 멀웨어 내의 텍스트 문자열 및 대상에서 수정된 파일 또는 설정과 같은 확인된 특성을 검색할 수 있습니다. 사실상 멀웨어의 모든 최근 위협(예: 지난 몇 시간 동안 릴리스 됨) 사례는 주요 멀웨어 데이터베이스에 포함될 가능성이 큽니다. 각 데이터베이스 항목에는 일반적으로 웜 전파 방식, 시스템에 미치는 영향(예: 변경 사항), 다른 시스템에서의 감염 예방과 관련된 조치를 포함하여 어떻게 제거할 수 있는지에 대한 광범위한 정보가 포함되어 있습니다.

멀웨어 데이터베이스 검색으로 웜이 식별되지 않으면 멀웨어 데이터베이스 항목에서 일반적으로 제공하는 정보를 검색하기 위해 사건 처리자가 추가 조사 및 분석을 수행해야 할 수 있습니다. 조직은 웜의 복사본을 분석 및 식별을 위해 조직의 바이러스 백신 공급 업체로 보낼 수 있지만 조직은 그 동안 자체 분석을 수행해야 합니다. 공급 업체의 응답 시간은 알 수 없으므로 분석을 수행해야 합니다. 분석가는 더 많은 정보를 수집하기 위해 다음과 같은 방법으로 감염을 검사 할 수 있습니다:

- **호스트의 현재 상태:** 분석가는 호스트를 조사하여 현재 상태의 여러 측면을 살펴볼 수 있습니다. 이 경우 비정상적인 연결(예: 많은 수의 예기치 않은 포트 번호 사용, 예기치 않은 호스트) 및 예상치 못한 수신 포트(예: 웜에 의해 생성된 백도어)를 식별하기 위해 네트워크 연결 목록을 검사하는 것이 가장 효과적일 수 있습니다. 유용한 다른 단계로는 실행중인 프로세스 목록에서 알 수 없는 프로세스를 식별하고 호스트 로그를 검사하여 감염과 관련될 수 있는 비정상적인 항목을 표시하는 단계가 있습니다.
- **호스트의 네트워크 활동:** 분석가는 패킷 스니퍼 및 프로토콜 분석기를 통해 감염된 서버에서 생성되는 웜 트래픽을 수집할 수 있습니다. 분석자가 주요 멀웨어 데이터베이스에서 멀웨어를 찾을 수 있도록 웜의 특성과 관련하여 충분한 추가 정보를 제공할 수 있습니다.

감염된 시스템이 조직 내부 및 외부의 다른 시스템을 공격 할 수 있으므로, 웜 사건은 가능한 한 신속하게 대응해야 합니다. 또한, 웜은 공격자가 감염된 시스템에 원격으로 액세스할 수 있는 백도어 및 기타 도구를 설치하는 경우가 많습니다. 이로 인해, 추가 손상이 발생할 수 있습니다.

따라서, 조직은 먼저 호스트의 데이터 수집을 수행하는 대신 감염된 시스템을 네트워크에서 즉시 분리할 수 있습니다. 이 단계를 통해 분석자가 웜을 식별하고 시스템에 미치는 영향을 판별하는 것이 훨씬 더 어려워질 수 있습니다. 예를 들어, 시스템이 네트워크에서 연결이 끊어진 경우 네트워크 활동과 호스트 상태의 특정 측면을 사용할 수 없습니다. 이러한 경우 분석자는 파일 시스템을 수집하고 악의적인 활동의 징후(예: 변경된 시스템 실행 파일)를 검사하여 정확하게 서버에 발생한 결과를 확인하는 등 서버에 대한 자세한 포렌식 분석을 수행해야 할 수 있습니다. 분석자는 또한 웜에 의해 추가되었을 수 있는 관리 수준의 사용자 계정 및 그룹을 찾는 것과 같이 서버 OS의 비 휘발성 특성을 검사할 수 있습니다. 궁극적으로, 분석자는 사고대응팀이 사고를 억제, 근절 및 복구할 수 있도록 충분히 자세히 웜의 행동을 식별할 수 있는 충분한 정보를 수집해야 합니다.

## 8.2 이메일 위협

사고 처리자는 내부 조사에 대한 도움 요청에 응답합니다. 직원이 조직의 전자 메일 시스템을 통해 다른 직원에게 협박 전자 메일을 보내는 혐의로 기소되었습니다. 사고 처리자는 조사관이 전자 메일의 기록을 포함할 수 있는 모든 데이터 소스를 찾도록 도울 것을 요청 받았습니다. 이 정보는 조사관이 전자 메일을 보낸 사람을 결정하는데 도움이 됩니다. 전자 메일은 쉽게 위조 될 수 있으므로 사용 가능한 모든 데이터 원본을 사용하여 전자 메일을 작성, 보내고 받는 순서를 재구성하는 것이 중요합니다. 또한, 사고 처리자는 포렌식 도구, 기술 및 절차를 사용하여 모든 작업을 수행하고 수행된 모든 작업을 문서화해야 합니다.

위협 전자 메일은 조사의 핵심이며 헤더에는 사고 처리자에게 가장 중요한 정보가 들어 있습니다. 전자 메일을 보낸 호스트의 도메인 이름과 IP 주소, 전자 메일을 보내는데 사용되는 전자 메일 클라이언트의 유형, 전자 메일의 메시지 ID 및 전자 메일이 전송된 날짜와 시간을 포함해야 합니다. 전자 메일 헤더에는 메시지가 통과한 각 전자 메일 서버(도메인 이름 및 IP 주소)와 각 서버가 전자 메일을 처리한 날짜 및 시간이 나열되어야 합니다. 전자 메일은 조직을 사용하여 보낸 것으로 추정되기 때문에 전자 메일 시스템에서 전자 메일 헤더는 조직 내의 시스템만 나열해야 합니다. 이 경우 사고 처리자는 목록의 각 시스템에서 상관 정보를 확인할 수 있습니다.

협박 전자 메일의 중요성 때문에 사고 처리자는 먼저 헤더를 포함하여 전자 메일 사본을 수집하는 데 집중해야 합니다. 받는 사람이 사용하는 전자 메일 클라이언트 유형 및 구성에 따라 전자 메일이 받는 사람 워크 스테이션에 다운로드되었거나 전자 메일 서버에 남아있을 수 있습니다. 전자 메일은 여전히 두 위치에 모두 저장되어 있을 수도 있습니다. 사고 처리자는 가능한 경우 전자 메일의 내용이 전송 중에 또는 수신자에 의해 변경되지 않았음을 확인하기 위해 가능한 여러 원본에서 전자 메일 복사본을 수집해야 합니다.

사고 처리자는 헤더를 검토한 후, 전자 메일 보내기에 대한 자세한 정보를 수집해야 합니다. 헤더는 보낸 사람이 사용하는 IP 주소와 전자 메일 클라이언트를 나열해야 합니다. 사고 처리자는

전자 메일을 보낸 시점에 해당 호스트의 IP 주소를 사용하고 있는지 확인해야 합니다. IP 주소에는 세 가지 가능성이 있습니다:

- **로컬 전자 메일 클라이언트:** 이 경우 사고 처리자는 DHCP 로그와 같은 네트워크 레코드를 사용하여 전자 메일을 보내는데 사용되는 데스크톱, 랩톱, PDA 또는 기타 장치를 식별할 수 있어야 합니다. 그런 다음 사고 처리자는 식별된 장치의 이미지를 만들고 이미지 복사본을 검사하여 멀웨어 및 전자 메일과 관련된 레코드를 찾습니다. 예를 들어, 전자 메일 클라이언트는 보내는 각 전자 메일의 복사본을 보관하도록 구성되어 있거나, 사용자의 전자 메일 메시지 초안을 저장하도록 되어 있을 수 있습니다. 메시지가 시스템에서 손상되지 않으면, 삭제된 파일과 임시 파일을 포함하여 장치의 메모리 및 파일 시스템에서 데이터를 수집하여 전자 메일 조각을 식별할 수 있습니다. 또한, 스팸 필터링 및 바이러스 백신 소프트웨어와 같은 장치의 보안 제어 기능은 보내는 전자 메일을 검사하고 이 전자 메일의 레코드를 기록했을 수 있습니다. 전자 메일 복사본을 전자 메일 서버에 저장하는 것도 가능하지만, 가능성은 없습니다. 사고 처리자는 로컬 호스트에서 전자 메일 레코드를 찾는 것 외에도 전자 메일을 보낼 때 사용한 사용자 계정을 확인하기 위해 호스트의 인증 레코드를 분석해야 합니다.
- **서버 기반 전자 메일 클라이언트:** 조직이 웹 기반 전자 메일 인터페이스와 같은 서버 기반 클라이언트를 제공하면 IP 주소가 해당 서버에 해당할 수 있습니다. 일반적으로 이러한 서버를 사용하려면 사용자가 자신을 인증해야 하므로, 인증된 레코드가 서버에 로그온한 혐의자와 사용자 시스템의 IP 주소를 나타낼 수 있습니다. 그런 다음 사고 처리자는 당시에 해당 시스템에 할당된 IP 주소를 확인하고 식별된 시스템에 대해 비트 스트림 이미징을 수행하여, 악성 코드 및 전자 메일에 대한 이미지 복사본을 검사할 수 있습니다. 예를 들어, 웹 브라우저의 임시 파일에는 전자 메일의 복사본이 들어있을 수 있습니다.
- **스푸핑 된 IP:** 주소가 조작된 경우(예: 조직의 네트워크 내에 유효한 주소가 아닌 경우) 사고 처리자는 다른 데이터 원본을 사용하여 실제로 전자 메일 메시지를 보낸 호스트를 식별해야 합니다.

조직의 전자 메일 서버는 또 다른 정보 소스입니다. 전자 메일 헤더에 나열된 각 서버 IP 주소에는 메시지 ID 값을 비롯하여 전자 메일의 일부 레코드가 포함되어 있어야 관련 레코드를 빠르게 식별할 수 있습니다. 앞에서 언급했듯이 목록의 최종 전자 메일 서버에는 전자 메일 복사본이 포함될 수 있습니다. 해당 서버의 백업에는 전자 메일 사본이 포함될 수 있지만, 몇 시간 이상 배달된 경우에만 백업됩니다. 바이러스 백신 소프트웨어 및 스팸 필터와 같이 전자 메일과 관련된 다른 서비스에는 전자 메일 활동의 기본 레코드가 포함될 수 있지만, 많은 세부 정보는 포함되지 않을 수 있습니다. 정보의 또 다른 가능한 출처는 인증 레코드입니다. 사용자가 전자 메일을 보내려면 인증을 요구하는 전자 메일 서버는 거의 없지만, 일반적으로 전자 메일을 사용자에게 배달하려면 인증이 필요합니다. 사용자는 단일 세션에서 전자 메일을 자주 보내고 받기 때문에 인증로그에는 특정 전자 메일을 보낸 사람을 결정하는데 도움이 되는 전자 메일 수신 레코드가 포함될 수 있습니다.

정보의 또 다른 가능한 소스는 전자 우편을 보내거나 수신하여 생성된 네트워크 트래픽의 레코드입니다. 네트워크 활동을 모니터링하는 패킷 스니퍼 또는 네트워크 포렌식 분석 도구는 송신 또는 수신 호스트의 실제 IP 주소, 전자 메일의 내용, 헤더 및 연관된 인증 활동을 포함하여 활동을 캡처 했을 수 있습니다.

궁극적으로 사고 처리자는 전자 메일을 보내고 받는 데 사용된 호스트와, 보낸 사람에서 받는 사람에게 전자 메일을 전송한 모든 중간 호스트를 식별해야 합니다. 사고 처리자는 각 관련 호스트로부터 전자 메일 및 지원 정보의 사본을 수집해야 하며, 레코드의 타임 스탬프를 사용하여 사이버 관점에서 일련의 이벤트를 재생성해야 합니다. 예를 들어, 가능한 순서는 다음과 같습니다:

오전 8시 37분에 특정 데스크톱 컴퓨터에 로그온한 사용자의 해당 컴퓨터에서, 오전 10시 2분에 위협적인 전자 메일이 기본 제공 전자 메일 클라이언트를 사용해서 전송되었습니다. 전자 메일은 조직의 전자 메일 서버 중 세 개를 통과하고, '서버 4'에 저장되어 의도한 수신자의 검색을 기다리고 있습니다. 수신자 사용자가 오전 11시 20분에 특정 랩톱 컴퓨터에 로그온하여 협박 전자 메일을 포함하여 전자 메일을 오전 11시 23분에 다운로드했습니다. 받는 사람 컴퓨터의 전자 메일 내용과 사용자 제공 헤더 필드(예: From, To, Subject)는 첫 번째 사용자의 데스크톱 컴퓨터에 있는 보낸 편지함 폴더에 저장된 사본과 동일합니다.

이 정보는 추가 조사를 위한 기초 자료로 사용될 수 있습니다. 사이버 활동을 기록하고는 있지만 전체 이야기를 말하지는 않습니다. 예를 들어, 어떤 사람이 특정 계정으로 해당 시간에 해당 데스크톱으로 이메일을 보냈다는 것을 확정할 수는 없다. 사건 처리자는 그것의 무결성을 확인하기 위한 질문으로써 데스크톱을 분석할 수 있다.(예: 보안 설정 비교, 조직의 기준 설정 제어, 시간 확인, 시스템 손상 및 기타 보안 침해 확인)

### 8.3 권고사항

여러 소스의 데이터를 사용하기 위해 이 섹션에서 제시하는 주요 권장 사항은 다음과 같습니다:

- **분석가는 여러 개의 개별 데이터 소스를 분석한 다음 이벤트를 상호 연관시킴으로써 가장 효과적으로 여러 상황을 처리할 수 있습니다.** 다양한 유형의 데이터 소스를 수집, 검사 및 분석하는 기술과 프로세스는 근본적으로 다릅니다. 응용 프로그램에는 데이터 파일, OS 및 네트워크 트래픽에서 캡처된 많은 데이터가 있습니다.
- **조직은 분석의 기술적 및 물류 복잡성을 인식하고 있어야 합니다.** 단일 이벤트로 여러 데이터 소스에서 레코드를 생성할 수 있으며 분석가가 실제로 검토할 수 있는 것보다 많은 정보를 생성할 수 있습니다. SEM과 같은 도구는 많은 데이터 소스의 정보를 한 곳에서 가져와 분석가를 도울 수 있습니다.

## **부록 A**

(상기 내용 재언급하는 내용)

## **부록 B**

포렌식 도구와 기법을 다양한 시나리오에서 사용하는 방법에 초점을 맞춘 사전 훈련은 기술을 구축하고 유지하며 지침, 절차 및 정책의 문제점을 식별하는 저렴하고 효과적인 방법을 제공합니다. 훈련 참가자는 간단한 시나리오를 검토한 다음 시나리오와 관련된 몇 가지 질문을 합니다. 참가자들은 각 질문에 대해 토론하고 상황에서 실제로 무엇을 할 것인지에 따라 답변을 작성합니다. 그런 다음 응답을 조직의 정책, 절차 및 지침과 비교하여 불일치 또는 결함을 식별합니다. 예를 들어, 한 질문에 대한 대답은 참여자가 특정 소프트웨어가 없고 조직 내의 특정 팀이 업무 시간 외 지원을 제공하지 않아 포렌식 조치가 지연될 수 있음을 나타낼 수 있습니다.

B.1절은 거의 모든 시나리오에 적용될 수 있는 일반적인 질문 목록을 포함합니다. B.2절에는 몇 가지 예제 시나리오가 포함되어 있으며, 그 중 일부 시나리오 뒤에 추가 시나리오별 질문이 나옵니다. 조직에서는 이러한 질문과 시나리오를 자신들의 상황에 맞게 적용하는 것이 좋습니다.

### **B.1 시나리오 질문**

1. 잠재적인 데이터 출처는 무엇입니까?
2. 도움이 되는 정보를 포함할 가능성이 가장 높은 잠재적인 데이터 출처와 그 이유는 무엇입니까?
3. 어떤 데이터 소스가 가장 먼저 검사될 것이며 그 이유는 무엇입니까?
4. 어떤 포렌식 도구와 기술이 가장 많이 사용될 것입니까? 어떤 다른 도구와 기법을 사용할 수 있습니까?
5. 조직 내의 어떤 그룹과 개인이 포렌식 활동에 참여할 것입니까?
6. 외부 당사자와 어떤 커뮤니케이션이 있을 수 있습니까?
7. 포렌식 관점에서, 시나리오가 다른 날이나 다른 시간에 발생했다면(정규 시간대 근무외 시간) 다르게 수행되는 것은 무엇입니까?
8. 포렌식 관점에서, 시나리오가 다른 물리적 위치(현장과 현장외)에서 발생했다면 다르게 수행됩니까?

### **B.2 시나리오들**

#### **시나리오 1 : 가능한 DDoS 공격**

토요일 오후, 외부 사용자는 조직의 공개 웹 사이트에 액세스하는데 문제가 발생하기 시작합니다. 그 다음 몇 시간 동안 문제는 조직의 공용 웹 사이트에 액세스하려는 거의 모든 시도가 실패할 때까지 악화됩니다. 한편, 조직의 네트워킹 담당자는 인터넷 경계 라우터에서 자동으로 생성된 경고에 응답했고, 비정상적으로 많은 양의 UDP(User Datagram Protocol) 패킷과 공용 DNS(Domain Name System) 서버를 보내고 받는 두 조직의 인터넷 대역폭이 많이 사용되고 있는

것을 확인했습니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. DDoS 공격이 다른 주에 있는 네트워크에서 오는 것처럼 보이는 경우, 포렌식 활동이 어떻게 변경될까요? 아니면 다른 나라에서이면?
2. DDoS 공격이 비즈니스 파트너의 네트워크에서 오는 것처럼 보이는 경우 포렌식 활동이 어떻게 변경됩니까?

## 시나리오 2 : 온라인 지불 문제

1주일 동안, 온라인 청구서 제출 및 지불을 위해 조직의 헬프 라인에 들어오는 전화 건수는 400% 증가합니다. 대부분의 발신자는 지불 정보를 여러 번 다시 제출해야 하는 불편을 호소하며 많은 사람들이 지불을 완료할 수 없습니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. 문제는 새로운 사용자에 대한 명확한 지침이 없는 등의 기술적이지 않은 것이 원인이 될 수 있습니다. 조사의 기술적 측면과 비 기술적 측면은 어떻게 조율되고 균형을 이루어야 합니까?
2. 개인정보보호 고려사항은 포렌식 도구 및 기법의 사용에 어떤 영향을 미칩니다?
3. 애플리케이션 개발자가 운영상의 문제로 인해 문제가 발생했다는 확신이 들면 포렌식 도구와 기법을 어떻게 사용합니까?

## 시나리오 3 : 알 수 없는 무선 액세스 지점

월요일 아침, 조직의 헬프 데스크는 무선 액세스에 문제가 있다고 말한 건물의 같은 층에 있는 5명의 사용자로부터 전화를 받습니다. 문제를 해결하는데 도움을 요청 받은 네트워크 관리자는 해당 사용자의 층에 무선 기능이 있는 랩톱을 가져옵니다. 무선 네트워크 구성을 보면서 새로운 무선 액세스 지점이 사용 가능한 것으로 표시된다는 것을 알았습니다. 액세스 포인트에서 전송하는 안전하지 않은 구성 설정을 기반으로 관리자는 해당 팀이 그것을 배치한 것으로 생각하지 않았습니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. 명백하게 액세스 포인트를 찾는데 사용할 수 있는 포렌식 도구 유형은 무엇입니까? 은밀하게?
2. 액세스 포인트가 합법적인 비즈니스 목적(예: 계약자의 사무실에서 임시 작업)으로 배포되었다고 판단되면 포렌식 활동이 어떻게 변경됩니까?
3. 알려지지 않은 개인이 액세스 포인트를 배치한 것으로 확인되었다면 포렌식 활동이 어떻게 바뀌겠습니까?

## **시나리오 4 : 재감염된 호스트**

지난 2주 동안 사용자는 동일한 바이러스를 랩톱 컴퓨터에서 두 번 제거해야 했고, 지금 그 사용자는 비슷한 증상을 다시 보고합니다. 이전의 감염을 처리한 기술 지원 직원은 컴퓨터의 바이러스 백신 소프트웨어가 활성화되어 최신 상태이며 바이러스가 컴퓨터를 다시 감염시키는 방식을 확인할 수 없음을 확인했습니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. 시각적으로 사용자의 사무실을 조사하여 다른 데이터 소스를 발견할 수 있습니까?
2. 사용자의 사무실 밖에서 가장 가능성 있는 데이터 소스는 무엇입니까?
3. 조직이 소유하지 않은 데이터 소스를 조사하려는 경우 분석가가 알고 있어야 하는 법적 고려 사항은 무엇입니까?

## **시나리오 5 : 잘못된 식별**

지난 24시간 동안 조직의 두 직원이 조직에서 발행한 신용 카드로 부당 구매를 신고했습니다. 조직은 질문된 거래에서 품목을 판매한 회사의 품목을 자주 구입합니다. 후속 평가에 따르면 조직 전체의 신용 카드 요금이 지난 3일 동안 30 % 증가했습니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. 포렌식 도구 및 기법을 사용하면 분석가가 발생한 상황(예: 조직의 개별 직원이 신분 도용의 피해자이며, 금융 자원이 손상된 경우)을 파악하는데 도움이 될 수 있습니까?
2. 직원을 조사 할 때 어떤 개인 정보 보호 문제를 고려해야 합니까? 금융 거래?

## **시나리오 6 : 원치 않는 화면 보호기**

조직의 헬프 데스크는 목적이 풍경을 묘사하는 화면 보호기가 컴퓨터에서 작업하는 동안 활성화된다는 불평을 하는 사용자로부터 몇 번의 전화를 받았습니다. 화면 보호기는 각 사용자가 화면 보호기의 잠금을 해제하고, 작업을 계속하기 위해 암호를 제출하도록 요구합니다. 동시에 조직의 네트워크 침입 탐지 시스템은 웹 서버와 관련된 몇 가지 비정상적인 경고를 보고합니다. 경고의 데이터는 일부 의심스러운 활동이 서버로 보내졌음을 나타내며, 서버는 이제 다른 시스템으로 향하는 유사한 활동을 생성합니다. 침입 탐지 분석가의 초기 가설은 웜이 웹 서버의 취약한 네트워크 서비스를 공격했을 수 있다는 것입니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. 이 시나리오의 시간에 민감한 특성을 감안할 때, 분석가가 자신의 행동에 우선 순위를 부여하는 방법은 무엇입니까?
2. 웜이 네트워크 통신을 방해한다면 포렌식 도구와 기술의 사용은 어떻게 바뀌겠습니까?
3. 감염된 데스크톱 시스템을 사용하여 조직에서 보호해야 하는 중요한 정보를 처리하는 경우, 포렌식 도

구와 기법을 어떻게 사용합니까?

### 시나리오 7 : 피싱 시도

지난 24시간 동안 여러 직원이 헬프 데스크에 연락하여 조직의 공식 신용 카드 제공업체로부터 전자 메일의 유효성에 대해 질문했습니다. 전자 메일은 금융 기관의 기록에 대한 보안 침해 가능성을 시사하고 수신자에게 기관의 웹 사이트 링크를 따라 가서 기존 암호 및 계정 정보를 제공하여 신원을 확인한 후 새 암호를 작성하도록 요청합니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. 이 시나리오의 시간에, 민감한 특성을 감안할 때 분석가가 자신의 행동에 우선 순위를 부여하는 방법은 무엇입니까?
2. 잠재적인 신원 도용 사례를 줄이기 위해 어떤 다른 조직에 연락해야 합니까?

### 시나리오 8 : 암호화된 파일

직원은 조직을 예기치 않게 떠나고 직원의 관리자는 이전 직원의 데스크톱 컴퓨터에 액세스하여 중요한 프로젝트 정보를 가져와 저장해야 합니다. 관리자는 프로젝트와 관련된 것으로 보이는 일부 파일 이름을 찾지만 관리자는 파일의 내용에 액세스 할 수 없습니다. 시스템 관리자는 시스템을 보고 이전 직원이 아마도 파일을 암호화했다고 결론을 내립니다. 이 시나리오에 대한 추가 질문은 다음과 같습니다:

1. 암호화된 데이터를 복구하려고 시도해야 하는지를 누가 결정해야 합니까? 어떻게 결정 될까요?
2. 유사한 미래 사건의 영향을 줄이기 위해 조직의 정책, 지침 및 절차를 어떻게 변경할 수 있습니까?

## **부록 C, D, E, F, G**

(용어에 대한 설명 및 URL 정보는 따로 번역하지 않음)

