Tytuł szkolenia: Odzyskiwanie danych w systemach plików w środowiskach Unix i Linux

Kod szkolenia: odzyskiwanie-danych-Unix-Linux

Wprowadzenie

Przeróżne wersje systemu operacyjnego Unix przez ćwierć wieku dominowały w większych środowiskach sieci akademickich i komercyjnych. Poprzez wprowadzone w nim koncepcje, rozwiązania i standardy, Unix wywarł ogromny wpływ na rozwój informatyki. Najsilniej jego dziedzictwo jest widoczne w rodzinie systemów linuxowych. Linux pojawił się jako odpowiedź ruchu wolnego oprogramowania na komercjalizację Unixa. Ponieważ kod Linuxa jest otwarty, sam projekt rozwoju oprogramowania nie jest scentralizowany i wkład w jego rozwój może wnieść w zasadzie każdy, kto czuje się na siłach.

Podobnie jak na poziomie systemu operacyjnego, tak i na poziomie systemu plików, środowisko linuxowe obficie czerpie z dorobku unixowych systemów UFS1 oraz UFS2. Jest to widoczne w rozbudowanym sposobie adresowania danych, a także w tradycyjnym zachowaniu zgodności wstecz z reliktami historycznymi sięgającymi czasów adresacji CHS odwołującej się bezpośrednio do fizycznych sektorów i ścieżek na dysku. I tak samo jak w przypadku licznych dystrybucji systemu operacyjnego, powstały liczne niezależne systemy plików i ich mutacje, które jednak charakteryzują się daleko posuniętą kompatybilnością oraz wiernością unixowym koncepcjom. W trakcie szkolenia nie będziemy w stanie omówić wszystkich systemów plików występujących w środowisku linuxowym. Wiele z tych systemów jest rzadko spotykanych i niszowych. Posiadają one bardzo podobną organizację i opierają się na tych samych założeniach. Dlatego dobre zrozumienie jednego z nich pozwoli na samodzielną analizę innych z wykorzystaniem zazwyczaj udostępnionej przez autorów w Internecie dokumentacji.

Na szkoleniu skupimy się na najpopularniejszym współczesnym linuxowym systemie plików – Ext4, który jest podstawowym systemem plików dla wiodących dystrybucji Linuxa, w tym dla Androida, począwszy od Androida 2.3. Podczas kursu poznasz organizację partycji z jej rozbudowanym adresowaniem, zrozumiesz wpływ organizacji metadanych na sposób alokacji plików, zobaczysz liczne bitmapy opisujące określone fragmenty partycji, a także dowiesz się w jaki sposób dawne sposoby adresowania danych wpływają na współczesne rozwiązania. Ze względu na dużą opcjonalność rozwiązań nawet w ramach jednego systemu plików, w czasie nauki duży nacisk kładziemy na samodzielną analizę struktur logicznych.

Adresaci szkolenia

Szkolenie adresowane jest do osób zamierzających profesjonalnie zajmować się odzyskiwaniem danych lub informatyką śledczą, techników serwisów komputerowych oraz innych osób zainteresowanych strukturami logicznymi systemów plików środowiska linuxowego. Wymagana ogólna wiedza o przechowywaniu danych, znajomość jednostek i pojęć używanych w informatyce, obsługa edytora heksadecymalnego, umiejętność wykonywania podstawowych obliczeń w systemie szesnastkowym. Z uwagi na złożoność struktur logicznych systemu plików Ext, wskazane także wcześniejsze doświadczenie w pracy z innymi systemami plików.

Zalecane wcześniejsze ukończenie szkoleń:

- Nośniki danych – podstawy działania i diagnostyki,
- Obsługa profesjonalnego oprogramowania do odzyskiwania danych na przykładzie DMDE,
- Zastosowanie matematyki w informatyce,

a także:

- Odzyskiwanie danych w systemach plików FAT
  lub
- Odzyskiwanie danych w systemie plików NTFS.

Cel szkolenia

Celem szkolenia jest zapoznanie uczestników z organizacją partycji i sposobem adresowania danych w systemach plików w środowisku unixowym i linuxowym, rozwinięcie umiejętności analitycznych w pracy ze strukturami logicznymi oraz przygotowanie ich do praktycznego rozwiązywania problemów związanych z utratą danych w tym środowisku.

Po szkoleniu uczestnik będzie:

- znał schemat organizacji partycji dla systemów plików występujących w środowisku linuxowym,
- znał struktury logiczne odpowiedzialne za adresowanie danych,
- rozumiał zależności pomiędzy tymi strukturami i potrafił je wykorzystać w procesie odzyskiwania danych,
- potrafił identyfikować i poprawiać błędy w strukturach logicznych.

Czas i forma szkolenia

- 14 godzin (2 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

1. Podstawowe pojęcia oraz architektura systemów plików w środowisku Unix i Linux
• Omówienie ogólnych założeń architektury systemów plików UFS, Ext i pokrewnych
• Pojęcie superbloku
• Pojęcie grup, bloków i fragmentów
• Elastyczne grupy bloków
• Deskryptor grup
• Pojęcie węzłów indeksowych – inode
• Struktura katalogów
2. Omówienie struktury superbloku na przykładzie systemu plików Ext4
• Omówienie parametrów superbloku i wewnętrznej organizacji partycji
• Zależność rozmiaru bloku i grupy
• Kopie superbloku i ich położenie. Rozrzedzony superblok
3. Omówienie tablicy deskryptora grup
• Tablica deskryptora grup
• Opis struktury grupy
• Bitmapy bloków i węzłów indeksowych
4. Omówienie tablicy węzłów indeksowych inode
• Struktura węzła indeksowego inode
• Sposoby adresowania plików. Bezpośrednie i pośrednie adresowanie bloków
• Atrybuty plików
5. Omówienie struktury katalogu
• Struktura rekordu katalogu
• Poruszanie się w strukturze logicznej z wykorzystaniem informacji z katalogów i węzłów indeksowych
6. Odnajdywanie plików z wykorzystaniem elementów struktur logicznych
• Ćwiczenia praktyczne
7. Analiza struktur uszkodzonej partycji Ext4
• Ćwiczenia praktyczne
8. Odnajdywanie pozostałości poprzednich metadanych i ich wykorzystanie w odzyskiwaniu danych
• Ćwiczenia praktyczne
9. Podsumowanie kształcenia
• Powtórzenie najważniejszych informacji o systemach plików z rodziny UFS i Ext
• Powtórzenie najtrudniejszych elementów ćwiczeń
• Panel dyskusyjny