



Универзитет у Нишу

ЕЛЕКТРОНСКИ ФАКУЛТЕТ

Форензика фајл система

Дигитална форензика

Професор **Братислав Предић**

Студент: **Јелена Стојковић 1607**

Садржај

Увод.....	3
Анализа фајл система	3
Структуре фајл система	4
Временски печати и значај за анализу	4
Категорије података у фајл систему.....	6
FAT фајл систем.....	8
Предности и ограничења FAT фајл система	8
Основне структуре FAT фајл система	9
Физичка организација FAT фајл система	11
NTFS fajl sistem	13
Master File Table (MFT)	14
Ext2 и Ext3 Фајл Системи	18
Организација фајл система	18
Суперблок.....	19
Inode структуре	19
Компатибилности и функционалности	20
UFS1 и UFS2 фајл системи	21
Организација података у UFS фајл систему.....	21
UFS суперблокови	22
UFS Cylinder Groups и дескриптор групе.....	22
Алат за анализу и визуализацију статистике датотека фајл система	23
Прикупљање података о фајловима.....	24
Чување података у CSV фајл.....	25
Учитавање података и њихова анализа	25
Визуализација података	25
Закључак.....	30
Референце	31

Увод

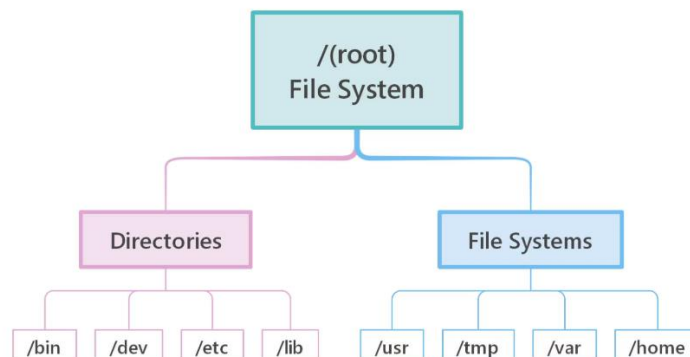
Форензика фајл система је кључна област дигиталне форензике која омогућава идентификацију, очување, анализу и презентацију дигиталних доказа пронађених на различитим врстама уређаја за складиштење података. У савременом свету, где су дигитални уређаји део свакодневног живота, форензичка анализа фајл система игра пресудну улогу у правним, пословним и истражним процесима. Фајл систем представља структуру која омогућава складиштење и приступ подацима на уређајима попут хард дискова, SSD-ова, USB дискова и меморијских картица. Анализа фајл система обухвата разумевање начина на који су подаци организовани и како се ти подаци могу искористити за реконструкцију догађаја.

Анализа фајл система

Форензичка анализа фајл система омогућава истражитељима да идентификују, очувају и анализирају дигиталне доказе са складишних уређаја, као што су хард дискови, SSD-ови и USB меморије. Ова анализа помаже у откривању неауторизованих активности, реконструкцији догађаја и прикупљању кључних доказа за правне и истражне поступке.

Шта је фајл систем?

Фајл систем је метода организације и управљања подацима на уређајима за складиштење. Омогућава оперативним системима да лоцирају, приступе и манипулишу подацима путем хијерархијске структуре директоријума и фајлова.



Слика 1: Пример структуре фајл система

Функције фајл система:

1. **Складиштење података:** Организација података у фајлове и директоријуме.
2. **Метаподаци:** Информације о датотекама, укључујући величину, тип, локацију и временске печате.
3. **Пристап подацима:** Омогућавање корисницима и апликацијама да приступе подацима ефикасно.

Структуре фајл система

Сваки фајл систем има специфичну структуру која дефинише начин на који се подаци организују и чувају. Ове структуре су кључне за форензичку анализу јер садрже метаподатке и информације о физичкој и логичкој алокацији фајлова.

Примери структура фајл система:

1. **FAT (File Allocation Table):** Једноставан фајл систем коришћен у ранијим верзијама Windows-а и на преносивим уређајима. Користи табелу алокације која прати кластере на диску и њихове везе са датотекама.
2. **NTFS (New Technology File System):** Напредан фајл систем са подршком за компресију, енкрипцију и напредне метаподатке. Базиран је на Master File Table (MFT), где сваки фајл или директоријум има свој запис.
3. **Ext (Extended File System):** Стандардни фајл систем за Linux, са верзијама Ext2, Ext3 и Ext4 које доносе различите нивое напредних функционалности. Складишти податке о фајловима у inode-има, са централизованом табелом која прати све inode-ове.

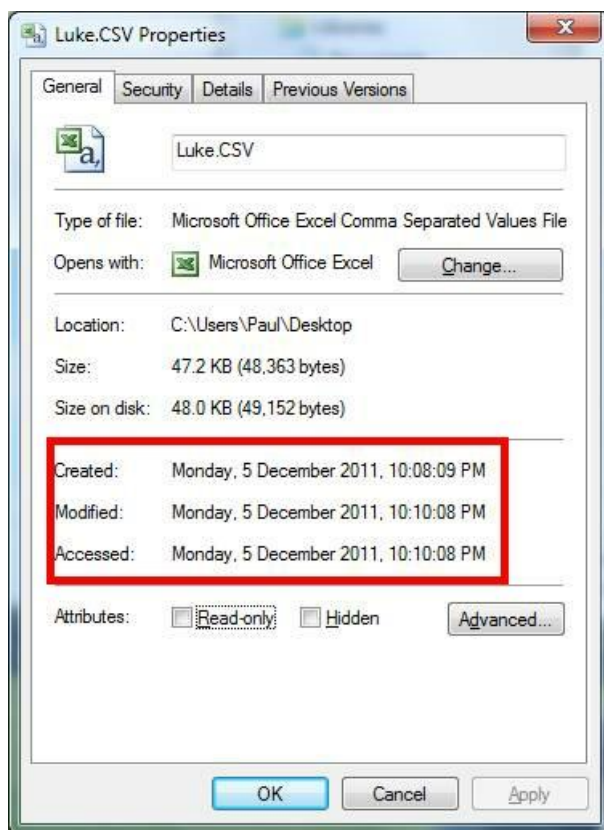
Временски печати и значај за анализу

Временски печати су кључни за форензичку анализу јер омогућавају истражитељима да реконструишу редослед догађаја. Ови печати укључују:

- **Време креирања фајла (Creation Time):** Када је фајл први пут креиран.
- **Време последње измене (Modification Time):** Када је садржај фајла последњи пут промењен.
- **Време последњег приступа (Access Time):** Када је фајл последњи пут отворен.

Значај временских печата:

- **Идентификација временског оквира активности.**
- **Праћење аномалија** (нпр. фајлови са печатима у будућности).
- **Корелација са логовима система и мреже** за реконструкцију догађаја.



Слика 2: Приказ MAC (Modification, Access, Creation) временског печата

Анализа фајл система

Анализа фајл система представља суштински корак у дигиталној форензици, који укључује испитивање, реконструкцију и тумачење структура података на медијуму складиштења. Овај процес обухвата идентификацију релевантних фајл система, екстракцију метаподатака, анализу садржаја и реконструкцију података. Циљ ових активности је да се обезбеди јасна слика о томе како су подаци организовани, складиштени и евентуално модификовани.

Основне фазе анализе фајл система

1. Идентификација фајл система

Први корак у анализи подразумева утврђивање типа фајл система који се користи на одређеном медијуму. Ово укључује испитивање структуре волумена и партиција. На пример, Windows системи најчешће користе NTFS или FAT, док Linux користи

Ext2/Ext3 или Vtrfs. Прецизно идентификовање фајл система је кључно за избор одговарајућих алата и техника анализе.

2. Екстракција метаподатака

Метаподаци садрже информације о фајловима и директоријумима, као што су датуми креирања, измене и приступа, као и атрибути повезани са дозволама. У NTFS-у, ови подаци су смештени у Master File Table (MFT), док ExtX користи inode структуре. Екстракција метаподатака омогућава реконструкцију временског контекста и анализу активности корисника.

3. Реконструкција и анализа садржаја фајлова

Ова фаза укључује испитивање садржаја фајлова, опоравак обрисаних података и анализу потенцијално скривених информација. Подаци могу бити смештени у континуираним или фрагментираним блоковима, што захтева пажљиво мапирање и реконструкцију.

4. Интерпретација података

Након екстракције, подаци се интерпретирају у контексту случаја. Ово укључује листање фајлова у директоријумима, идентификацију скривених података, откривање обрисаних фајлова и анализу сектора који нису део активних фајлова.

Категорије података у фајл систему

У фајл систему подаци су организовани у пет основних категорија:

1. Фајл систем

представља скуп основних информација које описују начин организације и рада фајл система. Иако сви фајл системи имају неке заједничке карактеристике, сваки фајл систем је посебан због своје величине и начина на који је подешен за оптималне перформансе. Ови подаци служе као водич или "мапа" која нам говори где се налазе одређене структуре података (као што су табеле или блокови података) и како је тачно организован простор за чување података.

Ово је корисно јер нам ови подаци помажу да разумемо како је фајл систем изграђен и како се његови делови могу користити у анализи или реконструкцији

2. Садржај датотека

Ово обухвата стварне податке који се налазе у датотекама. Организација ових података може бити у кластерима или блоковима, зависно од фајл система.

3. Метаподаци

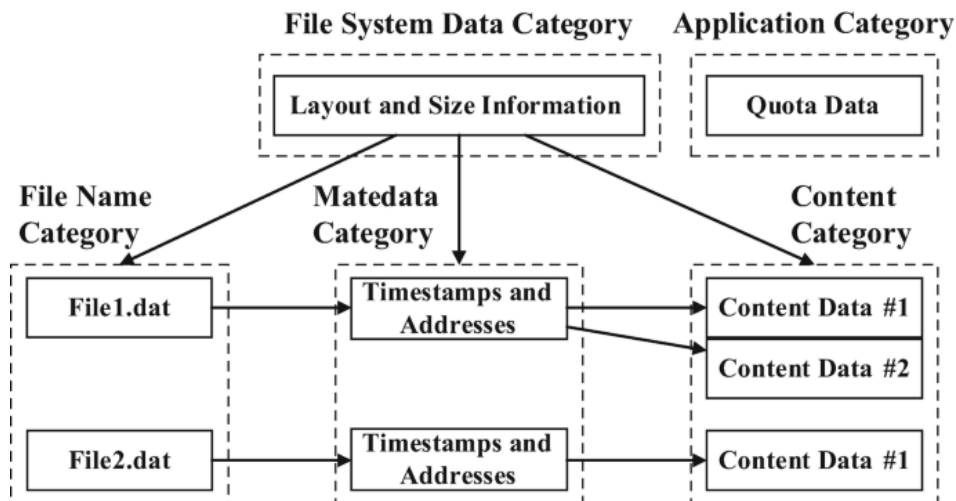
Подаци који описују фајлове, као што су локација, величина, време последњег читања или уписа, и дозволе (контола приступа). Метаподаци су кључни за форензичке анализе јер откривају када и како су фајлови коришћени.

4. Назив фајла

Ова категорија садржи информације које омогућавају да сваки фајл има јединствено име. У већини фајл система, ови подаци се чувају у директоријумима као спискови имена фајлова повезаних са њиховим метаподацима. Слично као што мрежни уређаји користе имена хостова за лакшу идентификацију и повезивање, корисницима је омогућено да приступају фајловима преко њихових имена, док систем користи метаподатке за њихову прецизну локацију и управљање.

5. Апликације

Категорија апликација обухвата податке који пружају додатне функционалности, али нису неопходни за основне операције читања или писања фајлова. Иако често нису део основне спецификације фајл система, њихова интеграција у фајл систем може бити ефикаснија него њихово складиштење у посебним фајловима. Примери укључују статистику коришћења и логове фајл система, који су корисни током форензичких анализа, али су подложни лакшем фалсификовању у поређењу са критичним подацима.



Слика 3: Категорије података

Важност референтног модела

Поседовање основног референтног модела је неопходно за разумевање и упоређивање различитих фајл система. На пример, поређење FAT и Ext3 фајл система открива значајне разлике у начину складиштења и организације података. Овај модел омогућава форензичарима да прецизније идентификују и анализирају податке од интереса.

Примена алата за анализу

Анализа фајл система захтева употребу специјализованих алата, као што су:

- **Sleuth Kit:** Овај алат омогућава детаљну анализу фајл система и екстракцију метаподатака.
- **Autopsy:** Кориснички интерфејс за Sleuth Kit који олакшава анализу и генерисање извештаја.
- **EnCase:** Комерцијални алат који нуди напредне опције за анализу и управљање доказима

Изазови у анализи

Анализа фајл система није без изазова. Скривени и обрисани подаци могу бити тешко доступни, а сложеност модерних фајл система, попут NTFS-а и ExtX-а, захтева дубоко техничко знање. Такође, манипулација подацима током анализе може довести до губитка доказа, што истиче важност примене правилних процедура.

FAT фајл систем

Фајл систем FAT (File Allocation Table) представља један од најједноставнијих и најраспрострањенијих фајл система који је коришћен у раним верзијама Microsoft DOS и Windows 9x оперативних система. Иако су модернији Windows оперативни системи прешли на NTFS, FAT остаје значајан због своје компатибилности са великим бројем уређаја и система. Он је подржан на свим Windows платформама, већини Unix оперативних система и бројним преносивим уређајима, као што су флеш меморије и меморијске картице.

Предности и ограничења FAT фајл система

FAT фајл систем је познат по својој једноставности и могућности интеграције са различитим платформама. Овај систем се одликује лакоћом имплементације и широко је прихваћен у различитим окружењима. Међутим, он поседује значајна ограничења, као што су:

- Ограничење величине фајлова и партиција.
- Слаба подршка за безбедносне механизме.
- Недостатак напредних функционалности присутних у модерним фајл системима, као што је NTFS.

Ипак, због своје једноставности и компатибилности, FAT се и даље користи у ситуацијама где су ресурси ограничени или је потребна брза и једноставна интеграција.

Основне структуре FAT фајл система

Главне компоненте FAT фајл система укључују **FAT табелу** и **директоријумску структуру**. FAT табела прати статус алокације кластера у систему и служи као индекс за повезивање блокова који чине садржај фајлова. Директоријумска структура чува информације о имену фајла, величини, почетној адреси и другим метаподацима.

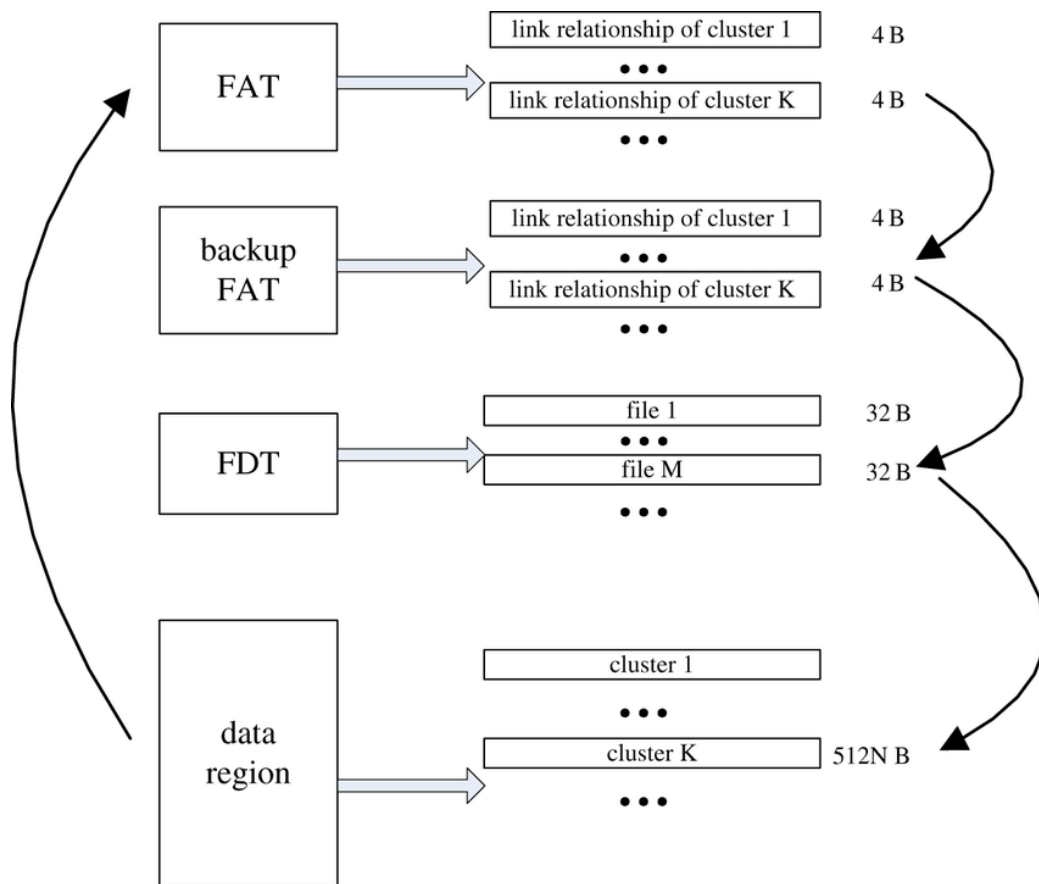
Основна концепција FAT фајл система је додела структуре података за сваки фајл и директоријум, која се назива **ставка директоријумске структуре**. Она укључује следеће податке:

- Име фајла (нпр. "document.txt"),
- Величину фајла (нпр. 10 KB),
- Почетну адресу где је садржај фајла смештен у меморији, и
- Друге метаподатке (датум креирања, дозволе приступа, итд.)

Садржај фајла и директоријума се физички чува у јединицама меморије које се називају **кластери**. Ако један фајл заузима више од једног кластера, његови додатни кластери се прате помоћу **FAT (File Allocation Table)** структуре.

FAT структура:

- Служи за повезивање кластера (сваки кластер указује на следећи, док се крај фајла обележава посебним кодом).
- Омогућава идентификацију слободних и заузетих кластера.



Слика 4: Дијаграм структуре FAT система фајлова

FAT (File Allocation Table)

- Ово је главна табела која бележи односе између кластера (јединица меморије на диску).
- Сваком кластеру је додељен запис који чува информације о томе где се налази следећи кластер повезаног фајла. Ако је кластер последњи, то је означено посебним кодом (нпр. EOF - End Of File).

2. Backup FAT

- Резервна копија FAT табеле, која се користи у случају оштећења главне табеле.
- Ово осигурава опоравак података, јер резервна копија дуплира све информације из примарне FAT табеле.

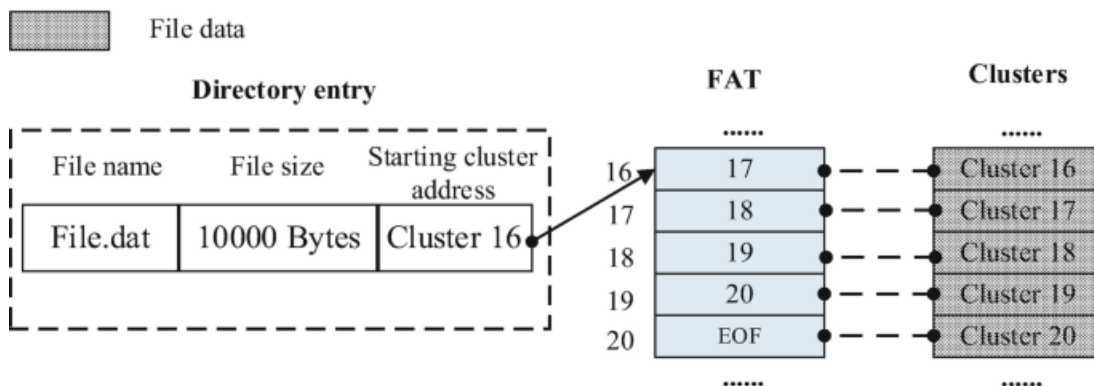
3. FDT (File Directory Table)

- Табела директоријума садржи листу фајлова са метаподацима (име фајла, величина, датум измене и сл.).

- Сваки запис у овој табели садржи информације о томе у ком кластеру почиње одређени фајл.

4. Data Region

- Овај део садржи стварне податке који припадају фајловима.
- Подаци су подељени у кластере, а њихова повезаност се управља преко FAT табеле.



FAT фајл систем долази у три главне верзије:

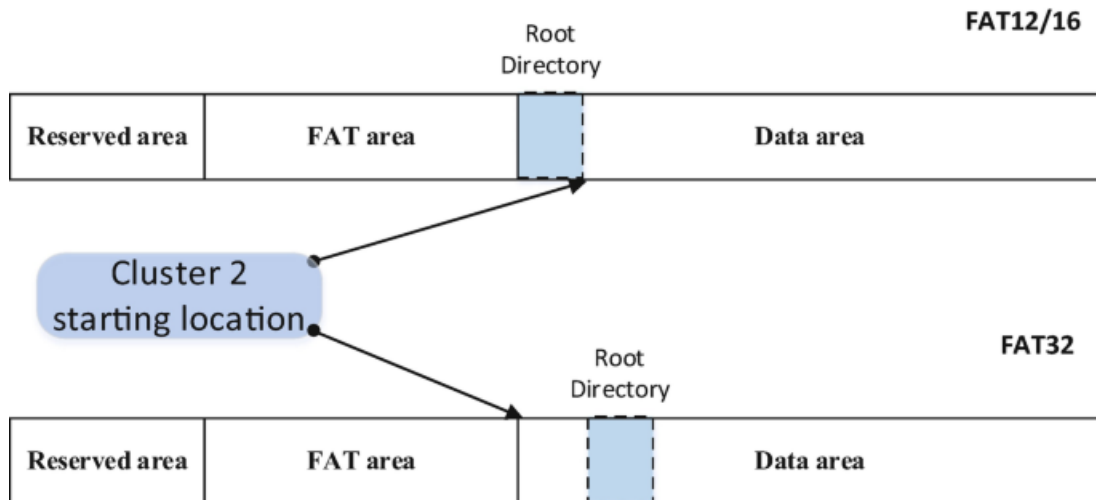
1. **FAT12** – намењен мањим уређајима са ограниченим простором.
2. **FAT16** – омогућава рад са већим партицијама, али је ограничен на величину партиција до 2 GB.
3. **FAT32** – најнапреднија верзија са подршком за веће величине фајлова и партиција, до 4 GB и 8 TB респективно.

Физичка организација FAT фајл система

FAT фајл систем је подељен на три дела:

1. **Резервисано подручје** – Садржи boot сектор и додатне структуре података специфичне за FAT систем.
 - **Boot сектор:** Ово је први сектор на диску, који садржи информације које се користе за покретање фајл система. Ту је и код за bootовање система, као и подаци који се односе на сам фајл систем, као што су величина кластера, величина FAT-а и други параметри.
 - **Табела за конфигурацију:** Садржи основне информације као што су број FAT табела, величина кластера, број сектора, итд.

2. **FAT подручје** – Обухвата основне и резервне FAT структуре које прате доделу кластера.
3. **Подручје података** – Чува стварни садржај фајлова и директоријума. Подручје података садржи **кластере** који су физичке јединице складиштења. Ако фајл има више од једног кластера, подаци се чувају у вези са другима, а FAT табела прати редослед кластера.



Распоред података у FAT12 и FAT16 верзијама резервише место за root директоријум на почетку подручја података, док FAT32 омогућава root директоријуму да се налази било где унутар овог простора. Овај дизајн FAT32 пружа већу флексибилност и отпорност на грешке у алокацији.

Резервисано подручје у FAT фајл систему почиње у сектору 0 и величина му је наведена у boot сектору. У FAT12/16, резервисано подручје обично заузима само један сектор, док FAT32 резервише више сектора. FAT подручје, које садржи једну или више FAT структура, почиње у сектору након резервисаног подручја. Величина FAT подручја се израчунава множењем броја FAT структура са величином сваке FAT, а ова два параметра су наведена у boot сектору.

Подручје података, које садржи кластере за чување садржаја фајлова и директоријума, почиње у сектору након FAT подручја. Његова величина се израчунава одузимањем почетне адресе сектора подручја података од укупног броја сектора у фајл систему, који је такође наведен у boot сектору. У овом подручју, подаци су организовани у кластере, а број сектора по кластеру се наводи у boot сектору.

Распоред подручја података се разликује између FAT12/16 и FAT32. У FAT12/16, почетак подручја података је резервисан за root директоријум, док у FAT32 root директоријум може бити смештен било где у подручју података, иако је обично на почетку. Ова динамична локација root директоријума у FAT32 омогућава већу флексибилност, укључујући

могућност прилагођавања лошим секторима на почетку подручја података и расту директоријума по потреби. У FAT12/16, root директоријум има фиксну величину, која је такође наведена у boot сектору. Почетна адреса за FAT32 root директоријум је такође наведена у boot сектору, а величина директоријума се одређује коришћењем FAT структуре.

Обрада података у FAT фајл систему

Када се фајлу, као што је `file.txt`, приступа у FAT фајл систему, систем користи директоријумску структуру да пронађе почетну локацију фајла. Преко FAT табеле идентификују се следећи блокови који чине фајл, што омогућава реконструкцију његовог садржаја. Овај процес се одвија кроз систем ланчане листе, где сваки кластер садржи показивач на наредни.

Скривање података у FAT фајл систему

FAT системи садрже одређене области које могу бити неискоришћене и представљати потенцијално место за скривање података:

- Простор између краја boot сектора и ознаке о крају сектора.
- Резервисане области у FAT32 структури, укључујући FSINFO.
- Простор између краја фајл система и краја волумена.

Скривени подаци се могу детектовати анализом неусаглашености између величине фајл система и физичког волумена.

Примена FAT фајл система у форензичкој анализи

У форензичким истрагама, FAT систем је релевантан због своје распрострањености у преносивим уређајима. Анализа FAT система обухвата идентификацију локација фајлова, реконструкцију обрисаних фајлова и испитивање неискоришћених сектора. Овај процес захтева пажљиво планирање како би се очувао интегритет података и идентификовали потенцијални докази.

NTFS fajl sistem

NTFS (New Technology File System) је један од најнапреднијих фајл система, дизајниран за високе перформансе, стабилност и сигурност. Захваљујући својој флексибилној структури

и богатству метаподатака, NTFS омогућава детаљну форензичку анализу, што га чини кључним у истраживањима на Windows платформама.

NTFS је дизајниран са циљем да обезбеди поузданост, безбедност и подршку за велике уређаје за складиштење података. Једна од кључних карактеристика NTFS-а је да је сваки бајт података у фајл систему, било да се ради о садржају датотека или метаподацима, увек повезан са одређеним фајлом. Овај принцип омогућава бољу организацију и контролу над подацима, као и бржи приступ, јер сваки податак има своју прецизну локацију и може се лако идентификовати. Поред тога, употребом универзалних структура података (познатих као "wrapper-и"), NTFS омогућава прилагођавање новим захтевима фајл система без измене основне архитектуре. Ова флексибилност и скалабилност чине NTFS ефикасним и практичним за рад са великим количинама података и различитим типовима уређаја за складиштење.

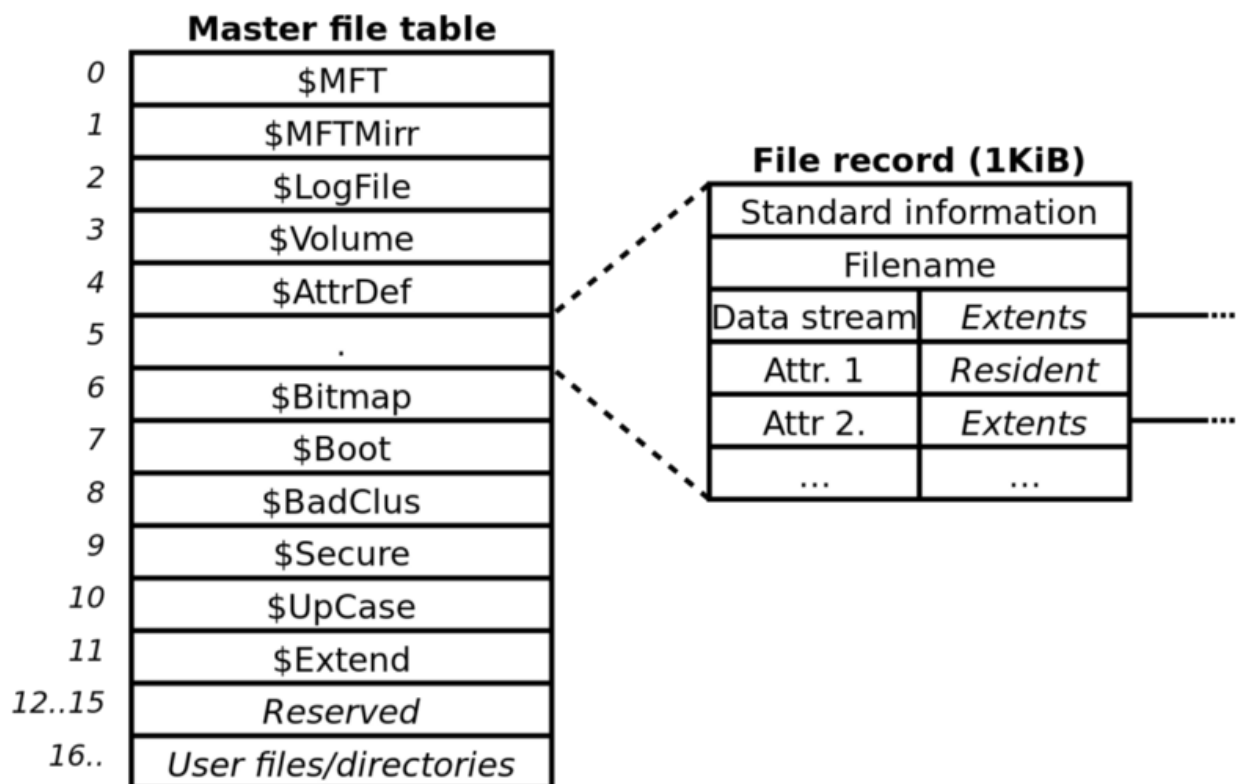
Сви важни подаци, укључујући административне информације, чувају се као фајлови. За разлику од других фајл система који имају фиксна места за административне податке, NTFS дозвољава да се ови подаци налазе било где на волумену, као и обични фајлови. Оваква организација чини цео волумен областима података где сваки сектор може бити додељен неком фајлу. Једини изузетак је почетак волумена, који увек садржи boot сектор и код за подизање система. Овај дизајн обезбеђује већу флексибилност, ефикасно коришћење простора и могућност лакшег прилагођавања различитим потребама.

Master File Table (MFT)

MFT је централна компонента NTFS фајл система, где се чувају записи о свим датотекама и директоријумима. Свака датотека има барем један запис у MFT-у, а веће датотеке могу користити додатне записе за складиштење података.

Структура MFT-а: Као и FAT, NTFS користи кластере, који су групе узастопних сектора.

- **Записи у MFT-у:** Сваки запис има фиксну величину (1 KB) али само првих 42 бајта имају дефинисану сврху. Преостали бајтови чувају атрибуте. Један атрибут се користи за чување имена фајла, док се други користи за чување садржаја фајла.
- **Атрибути:** Кључне информације о датотеци, као што су име, величина, временски печати, права приступа и садржај.



MFT структура

Метаподаци

У NTFS фајл систему, метаподаци су фајлови који чувају административне податке о фајл систему. Првих 16 уноса у Master File Table (MFT) су резервисани за метаподатке, као што су \$MFT (описује сам MFT), \$LogFile (садржи дневнике активности) и други.

Ови фајлови су скривени како би се избегле случајне измене и брисања. Корисници са одговарајућим привилегијама могу им приступити за одржавање или дијагностику.

Стандардни метаподаци фајлови у NTFS-у су:

- **\$MFT** – садржи све уносе о фајловима и директоријумима на волумену.
- **\$MFTMirr** – копија првих 4 уноса из \$MFT-а ради редунданције.
- **\$LogFile** – чува записе о трансакцијама у фајл систему за опоравак.
- **\$Volume** – садржи информације о волумену.
- **\$AttrDef** – дефинише атрибуте који могу бити додељени фајловима.
- **.** – root директоријум са уносима за све фајлове.
- **\$Bitmap** – прати који су кластери алоцирани или слободни.
- **\$Boot** – садржи boot сектор за покретање система.
- **\$BadClus** – бележи оштећене кластере.
- **\$Secure** – чува информације о безбедносним дескрипторима.

- **\$Upcase** – садржи табелу за конверзију слова.
- **\$Extend** – додатни фајлови метаподатака који проширују функционалност NTFS-a

Атрибути

NTFS атрибути чувају различите информације о фајловима унутар MFT табеле, која је основа за структуру фајл система. Сваки атрибут има заглавље и садржај: заглавље је стандардно за све атрибуте – идентификује тип атрибута, његову величину и име, и има flag-ове које идентификују да ли је вредност компресована или енкриптована, док је садржај специфичан за тип атрибута. Атрибут такође има идентификациони број који му је додељен и који је јединствен за ту MFT ставку. Ако ставка има више атрибута истог типа, овај идентификатор може бити коришћен за разликовање између њих.. Атрибути се могу класификовати као резидентни (чувају се директно у MFT запису) – користи се за мање атрибуте или нерезидентни (чувају се у спољним кластерима). Нерезидентни атрибути се чувају у низовима кластера, који су узастопни кластери, и тај низ је одређен на основу почетне адресе кластера и дужине низа.

Заглавље атрибута одређује да ли је атрибут резидентан или нерезидентан. Ако је атрибут резидентан, садржај ће одмах следити заглавље. Ако је атрибут нерезидентан, заглавље ће дати адресе кластера где се садржај налази.

NTFS користи логичке и виртуелне адресе кластера за мапирање ових атрибута.

Типови атрибута укључују, на пример, атрибут за име фајла, датуме, и садржај фајла. Атрибути су идентификовани бројем и именом које почиње знаком "\$". Стандардни атрибути могу се редеофинисати у \$AttrDef фајлу.

MFT запис

	Signature	Link Count	Flags															
00h:	46	49	4C	45	30	00	03	00	64	6F	11	01	00	00	00	00	00	00
10h:	01	00	01	00	38	00	01	00	A0	01	00	00	00	00	04	00	00	00
20h:	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00	00	00
30h:	50	00	00	00	00	00	00	00	10	00	00	00	00	60	00	00	00	00
40h:	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	00	00
50h:	26	B8	8D	B1	12	55	C4	01	26	B8	8D	B1	12	55	C4	01		
60h:	26	B8	8D	B1	12	55	C4	01	26	B8	8D	B1	12	55	C4	01		
70h:	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
80h:	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00
90h:	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	00	00

Прво поље у сваком MFT запису је потпис, које код стандардних записа има вредност ASCII низ карактера "FILE." Ако се пронађе грешка у запису, може имати вредност "BAAD."

Постоји и поље за flag-ове које идентификује да ли се ставка табеле користи и да ли се та ставка односи на директоријум. Статус алокације MFT ставке такође се може одредити из \$BITMAP атрибута у \$MFT фајлу.

Ако атрибути фајла не могу да стану у једану ставку табеле, могу се користити више ставки. Када се то деси, прва ставка се зове *base file record*, или *base MFT entry* (основна MFT ставка), а свака од наредних ставки садржи адресу основне ставки у једном од својих фиксних поља.

NTFS користи индексне структуре података у многим ситуацијама. Индекс у NTFS-у је колекција атрибута који су поређани у сортираном редоследу. Најчешћа употреба индекса је у директоријумима, јер директоријуми садрже \$FILE_NAME атрибуте.

NTFS користи B-стабла, која су слична бинарним стаблима, али могу имати више од два детета по чвору.

Скривени и неалоковани подаци

Скривени подаци у NTFS-у NTFS омогућава скривање података кроз:

1. **Alternate Data Streams (ADS):** Додатни токови података повезани са фајлом, који се не приказују стандардним методама прегледа.
 - **Пример:** Фајл file.txt може имати додатни ток података file.txt:hidden_data.
2. **Slack Space:** Простори унутар кластера који нису заузети садржајем фајла, али могу садржати остатке претходних података.

Анализа неалокованих података Неалоковани простори на диску често садрже остатке обрисаних фајлова. За анализу ових података користе се технике попут:

- Тражења потписних вредности фајлова (нпр. HEX кодова).
- Анализе фрагментисаних кластера за реконструкцију обрисаних фајлова.

Ext2 и Ext3 Фајл Системи

Фајл системи Ext2 и Ext3, често обједињени под термином ExtX, представљају стандардне системе за складиштење података код многих Linux дистрибуција. Оба система имају корене у UNIX фајл систему (UFS), али су оптимизовани за једноставност и ефикасност, уз уклањање непотребних компоненти.

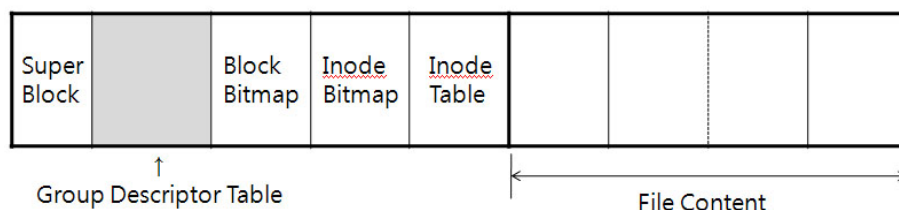
Основне карактеристике

Journaling је техника која се користи у фајл системима, попут Ext3 и новијих, за повећање **поузданости** и **брзине опоравка** података након неочекиваних прекида рада, као што су падови система или неочекивано гашење.

Ext2 је стандардни фајл систем који је дизајниран за брзину и једноставност. Он не подржава journaling, што га чини бржим у одређеним условима, али мање отпорним на грешке – користи се кад је брзина битнија од отпорности на решке.

Ext3, као његова надоградња, додаје journaling, што омогућава бржи опоравак података након системских грешака или наглог гашења. Journaling бележи промене пре него што се оне примене на главни фајл систем, чиме се смањује ризик од оштећења.

Организација фајл система



ExtX фајл систем је подељен у **блок групе**, а свака група садржи следеће структуре података:

1. **Суперблок** – Чува основне информације о фајл систему, као што су величина, број блокова, број inodo-ова и резервне копије за случај оштећења.
2. **Дескриптори група** – Пружају детаље о распореду блокова и inodo-ова унутар групе.

3. **Табела inode-ова** – Садржи метаподатке за сваки фајл и директоријум.
4. **Битмапе** – Управљају алокацијом блокова и inode-ова.
5. **Блокови података** – Чувају стварне податке фајлова.

Свака блок група је дизајнирана тако да минимизира померање главе хард диска приликом приступа подацима, чиме се повећава брзина рада.

Суперблок

Суперблок је кључна структура која се налази на почетку фајл система. Он садржи следеће информације:

- Величина блока и inode-ова.
- Укупна и слободна количина блокова и inode-ова.
- Резервне копије за случај оштећења примарног суперблока.
- Информације о последњем монтирању и модификацији.

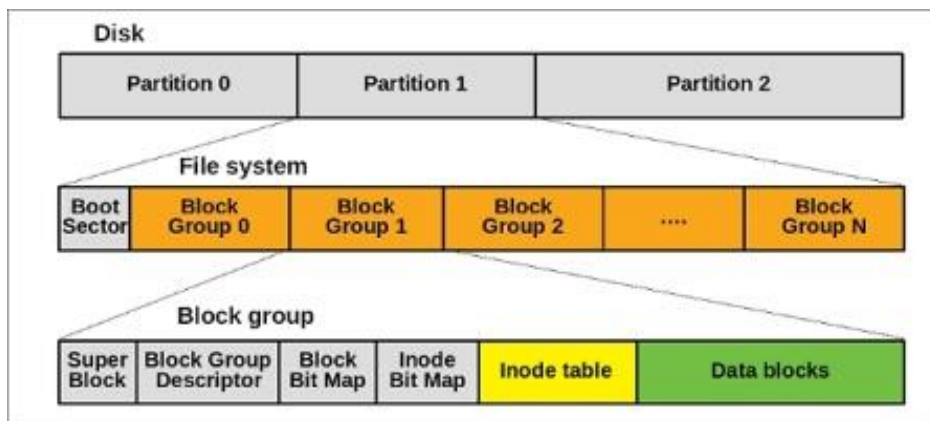
Суперблок игра виталну улогу у структури ExtX система, а резервне копије суперблока су стратешки распоређене широм фајл система ради заштите података.

Inode структуре

Inode представља основну јединицу за чување метаподатака о фајлу или директоријуму. Сваки inode садржи:

- Величину фајла.
- Датуме креирања, измене и приступа.
- Локацију блокова који чувају садржај фајла.
- Дозволе приступа и власника.

Inode је фиксне величине (обично 128 бајтова) и налази се у табели inode-ова унутар сваке блок групе.



Основна разлика између Ext2 и Ext3 система лежи у подршци за journaling. Док је **Ext2** погодан за апликације где је брзина приоритет, **Ext3** је дизајниран за побољшану отпорност на грешке и брже опорављање након кварова. Ext3 journaling омогућава следеће:

1. **Ordered Mode** – Бележи метаподатке и обезбеђује да се садржај фајла чува пре промена у метаподацима.
2. **Writeback Mode** – Бележи само метаподатке, али без гаранције редоследа.
3. **Data Mode** – Бележи и податке и метаподатке.

Компатибилности и функционалности

Функционалности ExtX система су подељене у три категорије на основу начина на који оперативни систем реагује на непознате функције унутар фајл система:

1. **Компатибилне функционалности:**
Оперативни систем може да ради са фајл системом чак и ако не подржава одређене функције из ове категорије. Оне му омогућавају нормалан рад без прекида. Примери укључују методе алокације, постојање журнала фајл система и коришћење проширених атрибута.
2. **Некомпатибилне функционалности:**
Ако оперативни систем наиђе на функцију из ове категорије коју не подржава, фајл систем неће бити прихваћен за употребу. На пример, компресија је једна од таквих функција.
3. **Функционалности компатибилне само за читање:**
У случају да оперативни систем не подржава функцију из ове групе, фајл систем ће бити постављен у режим само за читање. Примери укључују подршку за велике фајлове и употребу В-стабала за сортирање директоријума, уместо несортиране листе.

За форензичке анализе, Ext2 и Ext3 су посебно погодни због њихове структуре. Форензичари могу анализирати резервне копије суперблока, табеле дескриптора групе и inode-ове да би идентификовали:

- Избрисане фајлове и њихове остатке.
- Хронологију приступа и измена.
- Потенцијалне скривене податке у неискоришћеним блоковима.

UFS1 и UFS2 фајл системи

UFS (UNIX File System), познат и као FFS (Fast File System), представља један од кључних фајл система који се користи у многим UNIX и UNIX-подобним оперативним системима. UFS има две главне верзије: UFS1 и UFS2, које деле основне концепте, али се значајно разликују у неколико кључних аспеката који утичу на перформансе, функционалност и скалабилност.

- **UFS1** је први имплементирани фајл систем и уведен је у BSD UNIX почетком 1980-их. Пружио је значајно побољшање у односу на претходне UNIX фајл системе, захваљујући новим техникама расподеле података и метаподатака. UFS1 је био основни фајл систем у системима као што су OpenBSD и Solaris, а касније је био коришћен и у FreeBSD и NetBSD све док верзије FreeBSD 5.0 и NetBSD 2.0 нису увеле UFS2.
- **UFS2** је развијен да побољша могућности које је пружао UFS1. UFS2, који је уведен у FreeBSD 5.0, доноси неколико кључних унапређења, укључујући подршку за веће фајлове, бољу организацију метаподатака и проширене могућности за веће фајл системе. Поред тога, UFS2 омогућава ефикасније управљање великим бројем фајлова и бољу употребу простора на диску.

Разлике између UFS1 и UFS2:

- **Величина iNode-а:** UFS2 користи веће iNode структуре које укључују додатне временске жигове и поља која омогућавају напредне функционалности.
- **Подршка за веће фајлове:** UFS2 омогућава алокацију већих фајлова и подржава веће укупне величине фајл система у односу на UFS1.
- **Боља организација метаподатака:** UFS2 пружа побољшану организацију и управљање метаподацима, што доводи до бољих перформанси и веће скалабилности.

Иако су оба фајл система, UFS1 и UFS2, кључна у историји UNIX и UNIX-подобних оперативних система, разумевање ових верзија даје основу за проучавање савремених фајл система и њихових карактеристика.

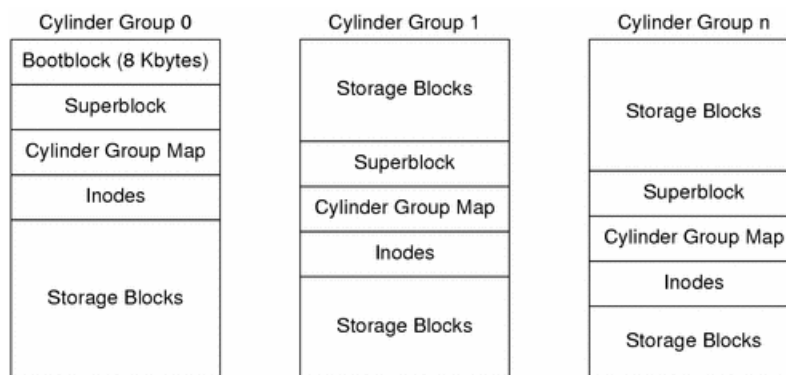
Организација података у UFS фајл систему

Фајл систем UFS је организован у секције познате као "cylinder groups" (групе цилиндра), а величина сваке од тих група зависи од геометрије хард диска. Свака cylinder group је организована тако да садржи одређене структуре података, укључујући bitmap-е за

праћење заузетих и слободних блокова, као и inode таблице. Свака од ових група садржи и резервну копију суперблока.

UFS суперблокови

Суперблок у UFS-у садржи основне информације о распореде фајл система. Он пружа информације о величини сваког фрагмента и броју фрагмената у сваком блоку, као и о томе како су груписане cylinder groups. Осим тога, суперблок може садржати ознаку волумена и време када је фајл систем последњи пут монтиран. У UFS фајл систему, суперблок се налази на почетку фајл система. На преносивим медијима може започети у првом сектору, док је у UFS1 обично лоциран 8 KB од почетка фајл система, а у UFS2 на 64 KB од почетка. Такође, може постојати и резервна копија суперблока која је лоцирана у свакој cylinder group.



UFS Cylinder Groups и дескриптор групе

UFS фајл систем је организован у cylinder groups, које су у ствари блокови на хард диску који садрже податке о метаподацима, укључујући дескрипторе који описују сваку групу. Дескриптор групе садрже информације као што су локација последње алоциране inode-a, бројеви слободних блокова и фрагмената, и време последњег уписа у групу. Свака cylinder group садржи bitmap-е које прате заузете inode-ове, блокове и фрагменте. Такође садржи табелу која омогућава ефикасно проналажење узастопних фрагмената и блокова одређених величина. Структура дескриптора групе у UFS-у је значајно већа од одговарајуће структуре у ExtX-у, јер садржи додатне информације о организацији фајл система и алокацији.

Значај Cylinder Groups Cylinder groups су биле оптимизоване како би се смањио утицај на перформансе приликом читања података са диска, јер су раније хард дискови имали исти број сектора по сваком цилиндру. Овај принцип није толико релевантан на савременим хард дисковима са различитим бројем сектора по цилиндру, због чега UFS2 више не користи ову стратегију.

Алат за анализу и визуализацију статистике датотека фајл система

Анализа података о датотекама и фајл системима важан је аспект за разумевање начина на који се ресурси користе, као и за оптимизацију и управљање фајловима.

У оквиру овог семинарског рада, имплементиран је алат који омогућава анализу и визуализацију података о коришћењу датотека на фајл систему у одређеном временском периоду. Главни циљ пројекта је да корисницима пружи боље разумевање начина на који се датотеке користе и приступају на фајл систему, што може бити од великог значаја у форензичким истраживањима, научним радовима или за потребе оптимизације система.

Овај алат је развијен у програмском језику Python и служи за прикупљање података о фајловима као и за анализу и визуализацију тих података на различите начине.

Алат је примењен на одређене екстензије.

Коришћене библиотеке:

- **os**

os је стандардна Python библиотека која омогућава рад са оперативним системом. Користи се за управљање фајловима и директоријумима, као и за добијање информација о фајловима као што су датум последњег приступа, величина фајла и други метаподаци. У овом програму, библиотека os је коришћена за приступ информацијама о фајловима и за пролазак кроз директоријуме.

- **datetime**

datetime је библиотека за рад са датумима и временом. Омогућава претварање временских ознака у читљивије формате и манипулацију са њима, као и рад са временским интервалима. У овом програму, datetime је коришћен за конверзију времена приступа фајловима и груписање података по месецима и годинама.

- **csv**

csv библиотека омогућава рад са подацима у CSV формату, што је један од најпопуларнијих формата за складиштење података у табеларном облику. Користи се за читање и писање података из и у CSV фајлове. У овом програму, csv је коришћен за запис података о приступу фајловима у CSV фајл, што омогућава каснију анализу и визуализацију.

- **pandas**

pandas је једна од најпопуларнијих библиотека за анализу података у Python-у. Пружа структуре као што су DataFrame и Series, које олакшавају манипулацију подацима, филтрирање, груписање и агрегацију. У овом програму, pandas је коришћен за обраду података о приступу фајловима и за анализу трендова као што су број приступа по месецима или по екстензијама.

- matplotlib

matplotlib је библиотека за визуализацију података која омогућава креирање широког спектра графика као што су бар графикони, линијски графикони, и хистограми. У овом програму, matplotlib је коришћен за креирање стандардних бар графика који визуализују број приступа фајловима по месецима.

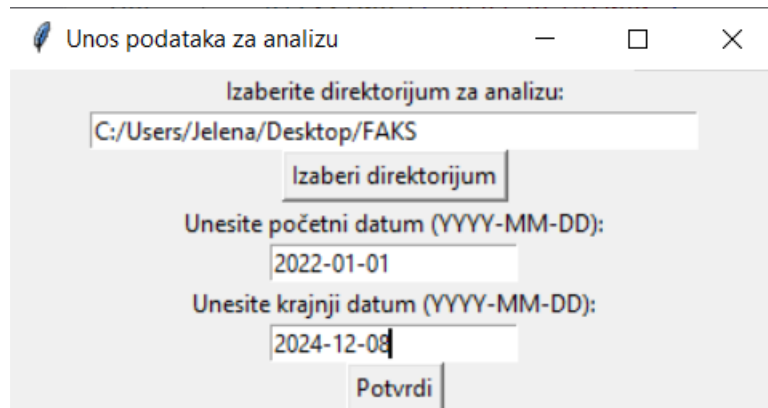
- plotly.express

plotly.express је библиотека за интерактивну визуализацију података. Омогућава креирање графика који омогућавају динамичку интеракцију са подацима, као што је увећавање, померање и додатне опције. У овом програму, plotly.express је коришћен за креирање интерактивних графика који се могу лако делити и користити у веб апликацијама.

Прикупљање података о фајловима

Прва компонента овог алата подразумева рекурсивно прегледање директоријума и прикупљање података о фајловима који испуњавају специфичне услове, као што су дозволе за екстензије фајлова. Алгоритам користи библиотеку os за добијање основних мета-података о фајловима (попут величине, времена последњег приступа, екстензије). Сваки фајл се обрађује на следећи начин:

- **Пут до фајла:** Путања се добија преко функције os.path.join(), која комбинује директоријум са именом фајла.
- **Екстензије:** Систем проверава да ли је екстензија фајла на списку дозвољених.
- **Мета-подаци:** Величина фајла и време последњег приступа добијају се преко os.stat() функције.



Податке о сваком фајлу, као што су путања, величина, екстензија и време последњег приступа, чувају се у листи која се касније користи за анализу.

Чување података у CSV фајл

Након што се подаци прикупе, они се чувају у CSV формату помоћу Python библиотеке csv. Ово омогућава лакше даље обрађивање и анализу података, као и њихово архивирање за каснију употребу. Структура CSV фајла укључује следеће колоне:

- **Putanja:** Путања до фајла.
- **Velicina:** Величина фајла у бајтовима.
- **Ekstenzija:** Екстензија фајла (или "без_екстензије" ако није доступна).
- **Vreme_pristupa:** Време последњег приступа фајлу.

Учитавање података и њихова анализа

Након што су подаци сачувани у CSV, библиотека pandas се користи за њихово учитавање у DataFrame. Ово омогућава лаку манипулацију подацима и вршење различитих анализа. На пример:

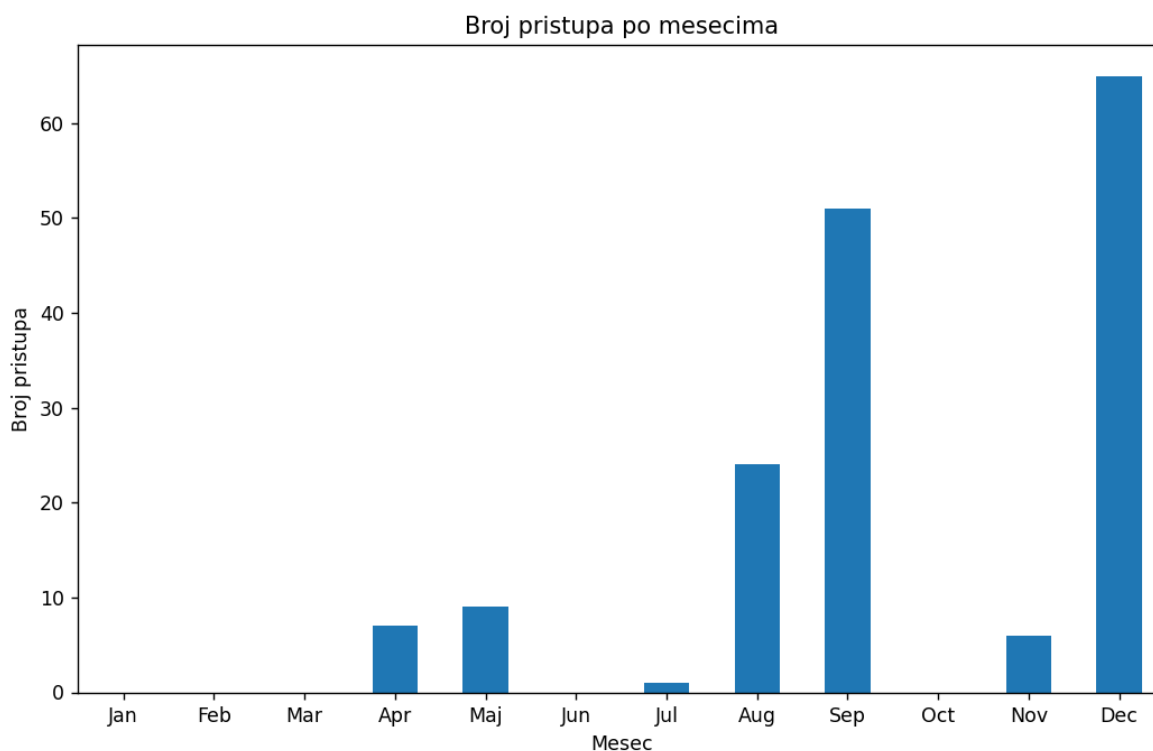
- **Конверзија датума:** Колона "vreme_pristupa" се конвертује у datetime формат ради лакше манипулације.
- **Издавање месеца:** На основу времена последњег приступа, извршава се додаток нове колоне која приказује месец у којем је фајл последњи пут био приступљен.

Визуализација података

Након што су подаци анализирани, следи корак визуализације. Визуелни прикази помоћу графикана омогућавају брзу анализу и откривање трендова у подацима. У овом примеру, користе се библиотеке као што су matplotlib и plotly за креирање различитих типова графикана:

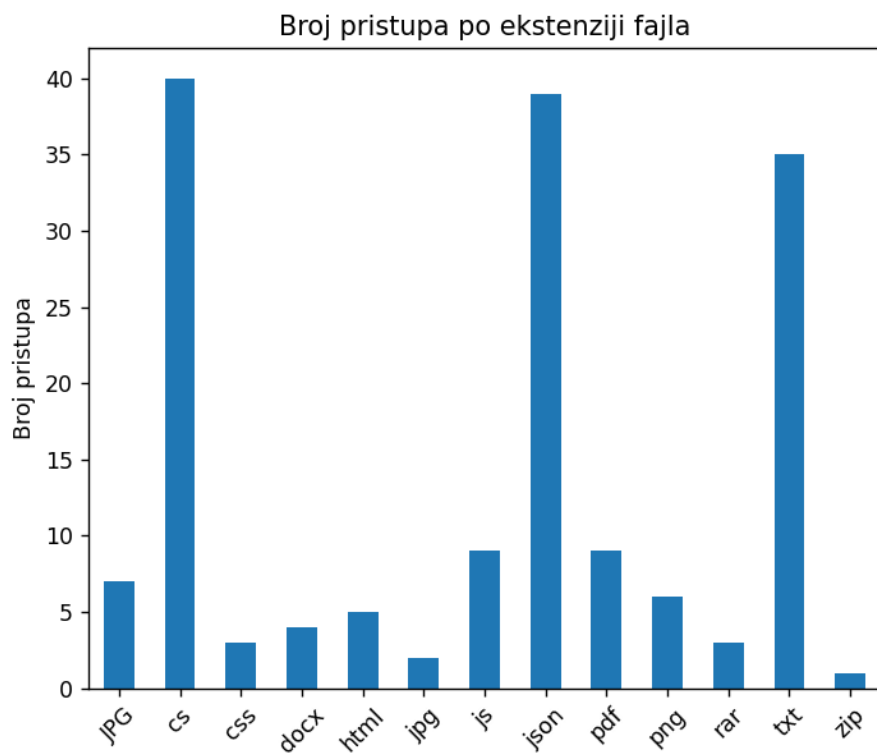
Број приступа по месецима

Број приступа фајловима се групише по месецима, а затим визуализује као бар графикон. Ово помаже у процени активност на фајловима током године.



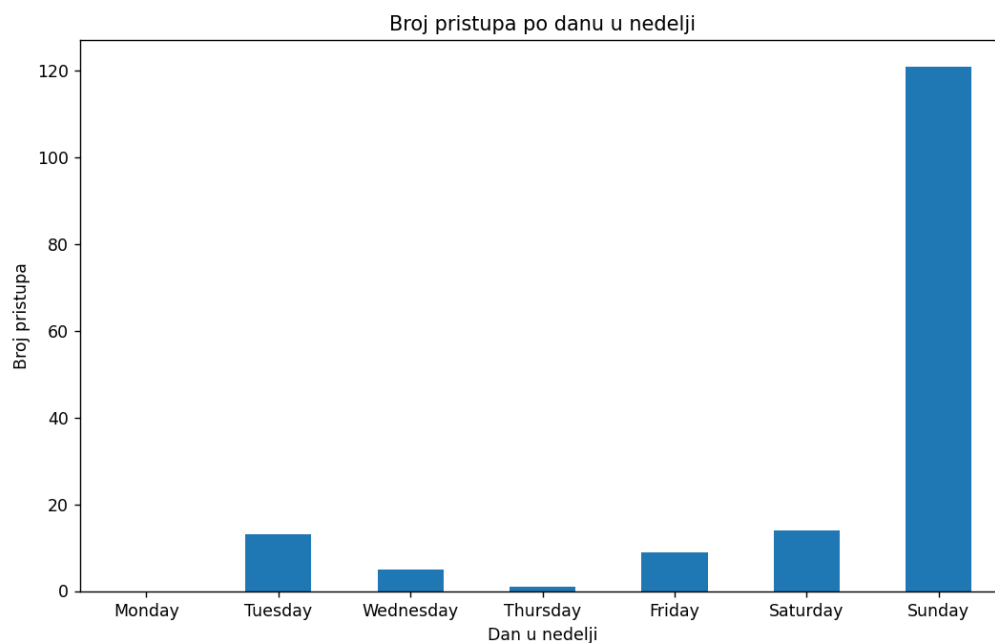
Број приступа по екстензији

Помоћу овог графикона може се видети који типови фајлова (нпр. .txt, .pdf, .jpg) се највише приступају, што може бити корисно за анализу учесталости одређених типова фајлова у систему.



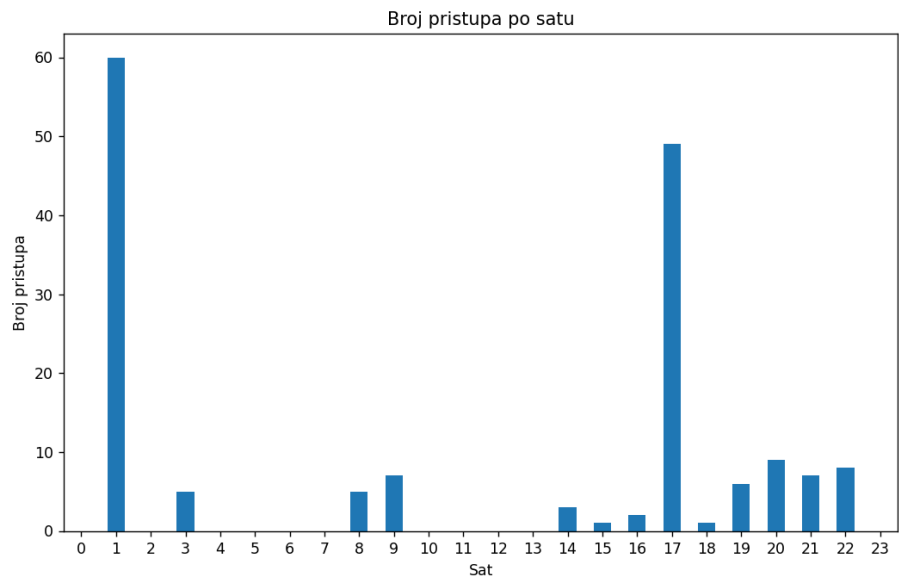
Broj pristupa po danu u nedelji

Груписањем по дану у недељи, могу се уочити трендови у активностима корисника, као што је повећана активност током радних дана.



Број приступа по сату

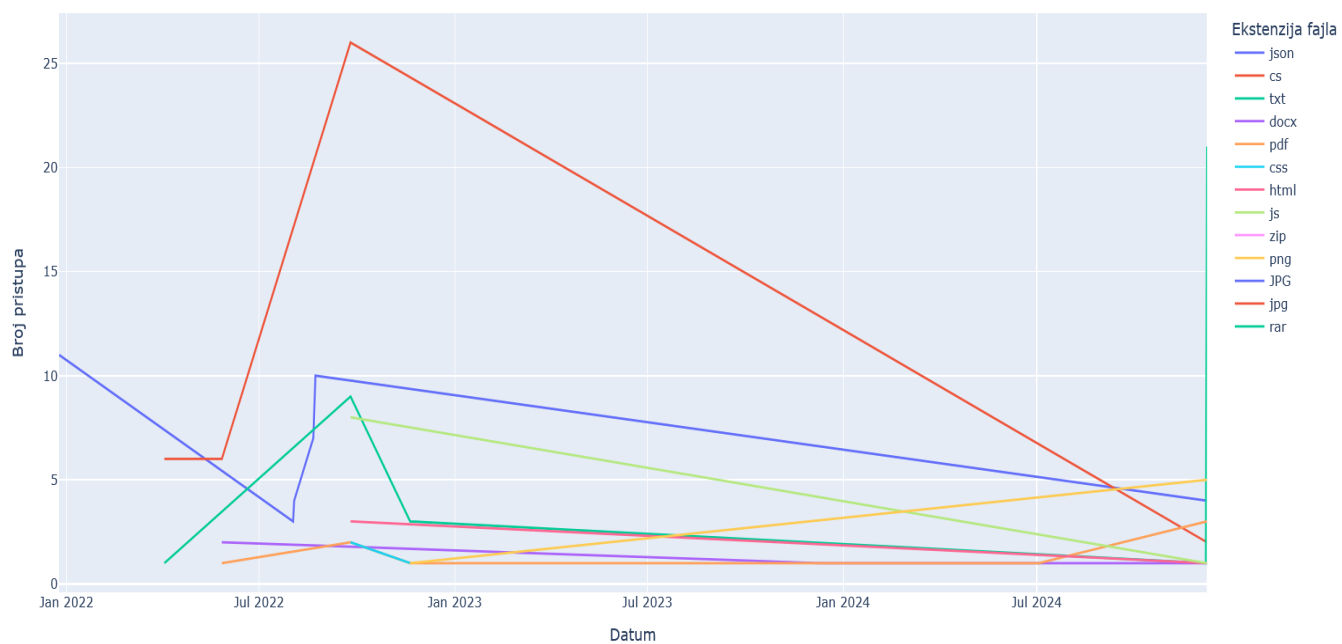
Овај графикон омогућава детектовање трендова активности на фајловима током дана, што је корисно за оптимизацију ресурса.



Број приступа по екстензијама у календару

Овај графикон показује како се број приступа разликује по типу фајлова, уз додатак различитих екстензија, чиме се добија детаљнији увид у коришћење различитих типова фајлова у временском оквиру.

Broj pristupa po ekstenzijama



Закључак

У овом семинарском раду истражили смо структуру и принципе рада неколико најзначајнијих фајл система, као што су NTFS, Ext2, Ext3, UFS1 и UFS2. Разумевање ових фајл система има кључну улогу у форензичким анализама, јер сваки од њих има јединствене структуре података, механизме за управљање фајловима и метаподацима, као и методе за заштиту и опоравак података.

Посебно је разматран NTFS, који је детаљно анализиран због своје комплексне структуре и напредних функција као што су journaling и подршка за велики број атрибута. Фајл системи Ext2 и Ext3 су такође обрађени због своје широко распрострањене употребе у Linux оперативним системима и начина на који управљају метаподацима путем inode структура и организације у блок групе. UFS1 и UFS2, који су широко коришћени у BSD системима, разматрани су због своје историјске и техничке важности, посебно због своје структуре цилиндричних група и начина чувања резервних копија података.

Циљ рада био је да се прикажу разлике у организацији и управљању подацима у овим фајл системима, као и њихов утицај на форензичке анализе. Препознавање и разумевање структура података као што су суперблокови, inode-ови и битмапе од пресудног је значаја за успешну анализу и опоравак података у форензичким истрагама.

Фајл системи имају кључну улогу у управљању подацима, и њихово дубинско разумевање је неопходно за ефикасну форензику и очување дигиталних доказа.

Референце

- [1] Carrier, B. (2005). *File System Forensic Analysis*. Addison Wesley Professional.
- [2] Santo, N. (2019). *NTFS File System and Cloud Computing Forensics: Part III. Advanced Techniques and Tools for Digital Forensics*. CSF: Forensics Cyber-Security, Fall 2019.
- [3] Garfinkel, S. (2012). *Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C 2012, San Diego, CA, USA, August 27-30, 2012, Proceedings*. Springer.
- [4] McKemmish, R. (1999). *What is Forensic Computer Science?* Australian Journal of Forensic Sciences, 31(3), 3-8.
- [5] Kessler, G. C. (2011). *File System Forensics: A Case Study on FAT, NTFS, and Ext3*. International Journal of Digital Evidence, 9(1), 1-19.