Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Voľne šíriteľné nástroje na obnovu zmazaných súborov

Princípy informačnej bezpečnosti

Marek Čederle

xcederlem@stuba.sk

18. apríla 2024

Obsah

1 Špecifikácia projektu **2**

1.1 Progress report č.1 . . . 2

1.2 Progress report č.2 . . . 3

1.3 Ciele projektu . . . 3

2 Súborové systémy **3**

2.1 FAT - File Allocation Table . . . 3

2.1.1 FAT32 . . . 3

2.1.2 Štruktúra FAT a FAT32 . . . 4

2.1.3 exFAT - Extensible File Allocation Table . . . 5

2.1.4 Štruktúra exFAT . . . 5

2.1.5 Výhody a nevýhody FAT32 a exFAT . . . 7

2.2 NTFS - New Technology File System . . . 7

2.2.1 Štruktúra NTFS . . . 7

2.2.2 Bezpečnosť NTFS . . . 8

2.2.3 Výhody a nevýhody NTFS . . . 9

2.3 ext - Extended File System . . . 9

2.3.1 Štruktúra ext4 . . . 9

3 Nástroje na obnovu údajov **11**

3.1 Testdisk . . . 11

4 Experimentovanie s nástrojom testdisk **11**

4.1 Zmazanie a obnova súborov . . . 11

4.2 Zmazanie a obnova partície . . . 11

5 Výsledky experimentov **11**

6 Správne zmazanie dát a formátovanie disku **11**

7 Záver **12**

1 Špecifikácia projektu

V mojom projekte sa budem venovať analýze súborových systémov pre operačné systémy Windows a GNU+Linux. Bude sa jednať o súborové systémy typu NTFS a ext ale spomeniem aj dodnes veľmi používané FAT32 a exFAT ktoré sa používajú na prenosných médiách. Každý súborový systém by som chcel opísať s tým, že uvediem jeho výhody a nevýhody prípadné porovnanie s ďalšími spomenutými súborovými systémami.

Budem sa zaoberať aj tým, ako správne naformátovať disk (prepísať ho náhodnými dátami alebo samými nulami) aby pri jeho predaji sa z bezpečnostných dôvodov nedalo zistiť čo sa na ňom pred tým nachádzalo. Je to z dôvodu že pri mazaní dát z disku sa vlastne tieto dáta reálne nemažú. Dáta na disku zostanú, len sa z tabuľky záznamov zahodí záznam kde sa súbor nachádza a potom keď sa zapisuje na disk tak operačný systém vie, že môže na toto miesto zapisovať.

Taktiež sa budem zaoberať analýzou nástroja na obnovu zmazaných súborov s názvom testdisk. Vysvetlím, prečo som si vybral práve tento nástroj. S týmto nástrojom budem následne experimentovať. Experimenty budú spočívať v tom, že si naformátujem disk a vytvorím na ňom nejaké partície podľa typu daného súborového systému. Následne naň uložím rôzne typy súborov. Budú sa tam nachádzať fotky, textové súbory, archívy, atď. Potom vymažem nejaké z týchto súborov, ale na disk ďalej nič nezapíšem, aby sa nezačali prepisovať dané miesta na disku inými súbormi. Následne vyskúšam nástroj na obnovu zmazaných súborov (testdisk) či zvládne tieto súbory obnoviť. Tento experiment zopakujem s tým, že po zmazaní ďalších súborov zapíšem na disk zase nové súbory a vyskúšam použiť nástroj na obnovu či dokáže aj po takejto akcii obnoviť súbory. Ďalší experiment bude spočívať v zmazaní celej partície a jej následnej obnove týmto nástrojom. V neposlednom rade ukážem, že po správnom formátovaní disku sa nebudú dať dáta obnoviť. Na záver budem prezentovať výsledky experimentov.

1.1 Progress report č.1

V prvom progress reporte vypracujem teoretickú časť, ktorú som na začiatku uviedol. To znamená popísanie rôznych typov súborových systémov a nástrojov na obnovu súborov. V neposlednom rade uvediem ako z bezpečnostného hľadiska správne “zmazať” súbory na disku respektíve ako ho naformátovať tak, aby sa z neho minulé dáta nedali prečítať.

1.2 Progress report č.2

V tomto progress reporte sa budem zameriavať na praktickú/experimentálnu časť. To znamená, že sa pokúsim vykonať všetky vyššie spomenuté experimenty. Na záver budem pracovať na celkovej úprave finálneho dokumentu.

1.3 Ciele projektu

Cieľom tohto projektu je získať informácie z oblasti súborových systémov a vykonať rôzne experimenty s nástrojmi na obnovu údajov. Keďže sa jedná o predmet Princípy informačnej bezpečnosti, tak cieľom je poukázať na dopady neformátovania respektíve neefektívneho "ničenia" súborov na bezpečnosť.

2 Súborové systémy

Súborový systém je metóda a dátová štruktúra, ktorú operačný systém používa na riadenie spôsobu ukladania a načítavania dát. Bez súborového systému by dáta umiestnené na pamäťovom médiu boli jedným veľkým zväzkom dát bez možnosti určiť, kde končí jeden súbor a začína ďalší, alebo kde sa nachádza, keď je potrebné ho načítať. Rozdelením dát na časti a pomenovaním každej časti sa dáta ľahko izolujú a identifikujú. Každá skupina dát sa nazýva súbor.

2.1 FAT - File Allocation Table

FAT je súborový systém vyvinutý pre osobné počítače. Pôvodne vyvinutý v roku 1977 na použitie na disketách, neskôr bol prispôsobený na použitie na pevných diskoch a iných zariadeniach. Často je z dôvodov kompatibility podporovaný súčasnými operačnými systémami pre osobné počítače a mnohými mobilnými zariadeniami a "embed" systémami. FAT ako taký je už v dnešnej dobe nepoužívaný, ale jeho odnože (FAT32, exFAT) sa doteraz používajú napríklad v prenosných médiách ako USB kľúče, SD karty a podobne.

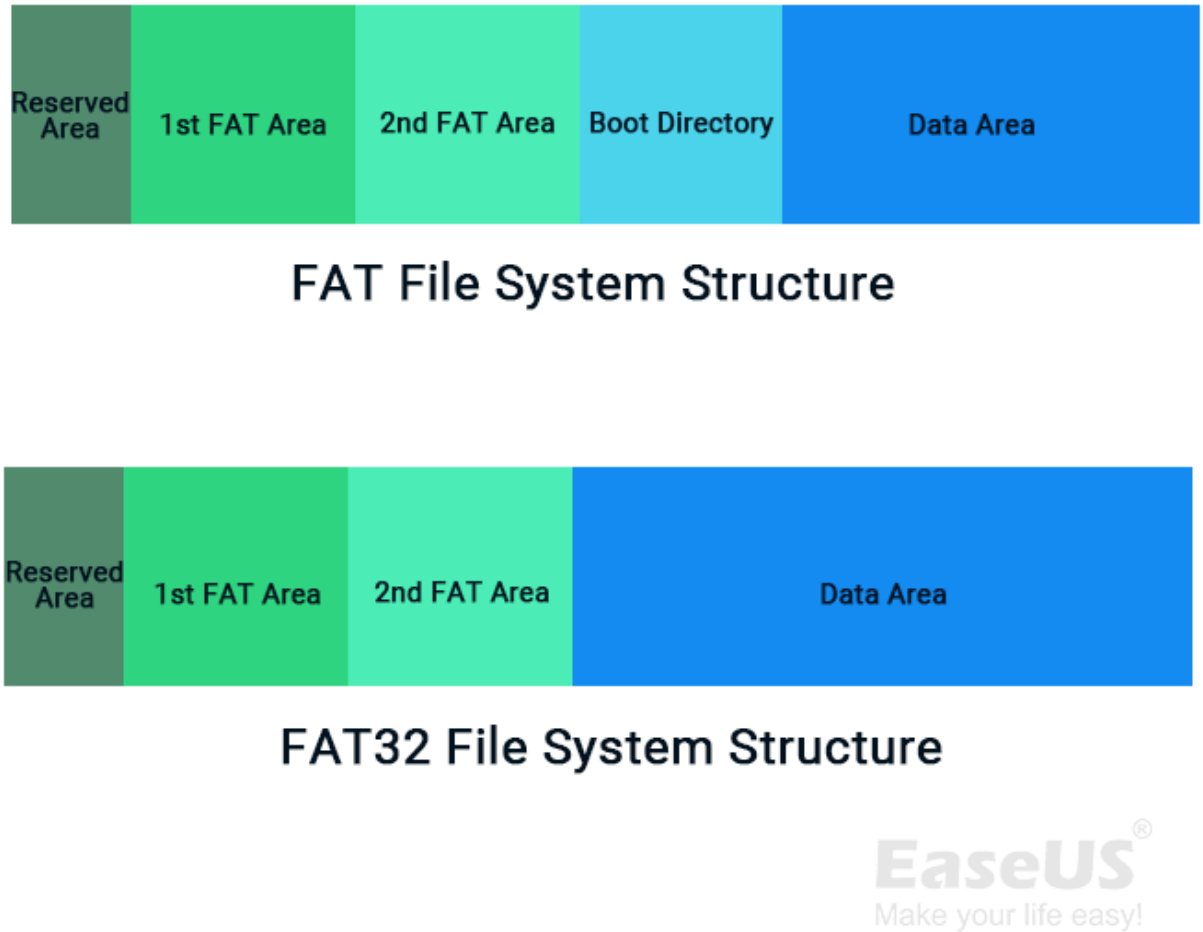
2.1.1 FAT32

Najpokročilejšia verzia súborového systému FAT je FAT32. S FAT32 sa Microsoft snažil prekonať obmedzenia FAT16 a prispôsobiť sa väčším možným partíciám. Existuje už od Windowsu 95 a naďalej zostáva populárny, pretože je vysoko kompatibilný s väčšinou operačných systé-

mov (GNU+Linux, MAC) a prenosných zariadení. FAT32 podporuje súbory menšie ako 4 GB a partície s maximálnou veľkosťou 2 TB.

2.1.2 Štruktúra FAT a FAT32

Novo naformátovaný disk s FAT vyzerá nasledovne:



Obr. 1: Štruktúra súborového systému FAT a FAT32
Zdroj: https://www.easeus.com/diskmanager/file-system.html

- Reserved Area
  - Obsahuje boot sector, BPB (BIOS Parameter Block) a celkovo informácie potrebné pre bootovanie a súborový systém.
- 1st FAT Area
  - FAT tabuľka obsahujúca informácie o súboroch a ich umiestnení na disku.
- 2nd FAT Area
  - Obsahuje kópiu FAT tabuľky.
- Boot Directory

  - Niekedy sa nazýva aj Root Directory. Používa sa iba v derivátoch FAT12 a FAT16. Obsahuje informácie o súboroch, ktoré sa nachádzajú priamo v koreňovom adresári.

- Data Area
  - Obsahuje samotné dáta súborov.

2.1.3 exFAT - Extensible File Allocation Table

exFAT je súborový systém predstavený spoločnosťou Microsoft v roku 2006 a optimalizovaný pre flash pamäte, ako sú USB flash disky a SD karty. exFAT bol proprietárny do 28. augusta 2019, kedy Microsoft zverejnil jeho špecifikáciu. Microsoft však stále vlastní patenty na niekoľko častí svojho dizajnu.

exFAT možno použiť tam, kde NTFS nie je vhodným riešením (kvôli vysokej réžii[1]), ale kde je potrebná podpora súborov väčších ako 4 GB.

exFAT bol prijatý SD Association ako predvolený súborový systém pre karty SDXC väčšie ako 32 GB.

Windows 8 a novšie verzie natívne podporujú bootovanie z exFAT.

2.1.4 Štruktúra exFAT

Novo naformátovaný disk s exFAT vyzerá nasledovne:

[1] angl. overhead

Obr. 2: Štruktúra súborového systému exFAT
Zdroj: https://www.easeus.com/diskmanager/file-system.html

- Main Boot Region
  - Informácie potrebné pre bootovanie.
- Backup Boot Region
  - Záloha Main Boot Region.
- FAT Alignment
  - FAT offset a veľkosť.
- 1st FAT
  - FAT tabuľka obsahujúca informácie o súboroch a ich umiestnení na disku.
- 2nd FAT
  - Záloha FAT tabuľky.
- Cluster Heap Alignment
  - Cluster heap offset a veľkosť.
- Cluster Heap
  - Obsahuje samotné dáta súborov.

2.1.5 Výhody a nevýhody FAT32 a exFAT

2.2 NTFS - New Technology File System

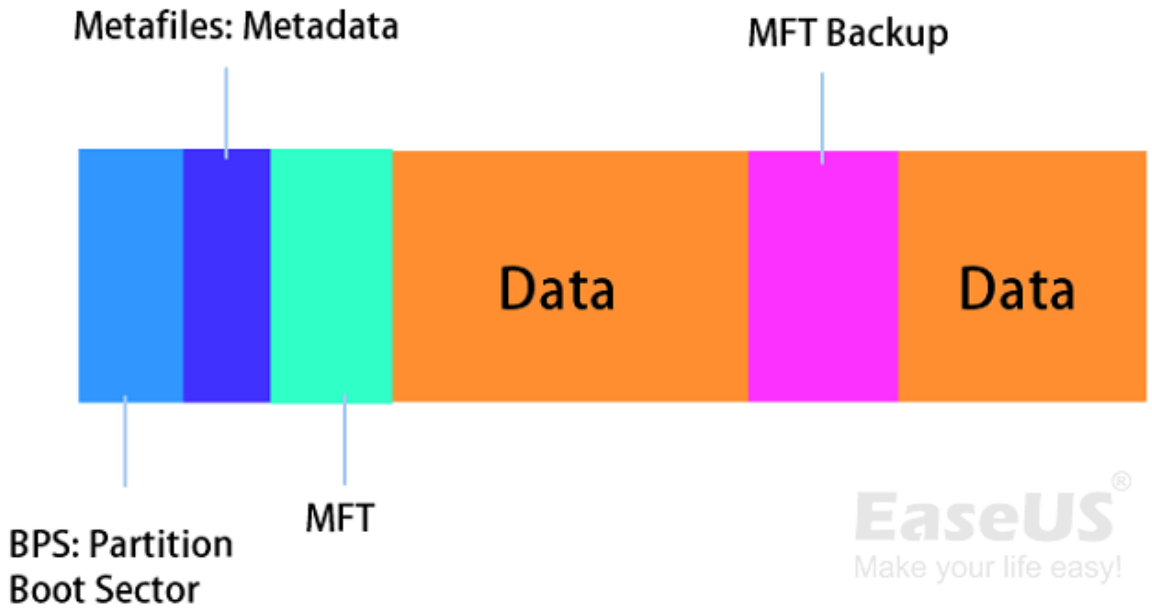
NTFS je proprietárny súborový systém vytvorený spoločnosťou Microsoft. Bol uvedený s vtedy novým operačným systémom Windows NT[2] v roku 1993. Vtedy nahradil dovtedy veľmi používaný súborový systém FAT. NTFS je predovšetkým určený pre pevné disky HDD[3] a neskôr aj pre SSD[4]. Je však možné ho použiť aj na prenosové média typu USB kľúč a podobne.

Súborový systém NTFS prináša kombináciu vyššej rýchlosti, väčšej spoľahlivosti a kompatibility oproti súborovému systému FAT, ktorý bol jeho predchodcom v ére operačného systému MS DOS.

Ide o žurnálový súborový system, čo znamená, že všetky zmeny na disku sú zaznamenané v tzv. žurnáli. V prípade výpadku napájania alebo zlyhania systému je možné rýchlo obnoviť dáta na disku.

2.2.1 Štruktúra NTFS

Novo naformátovaný disk s NTFS vyzerá nasledovne:



Obr. 3: Štruktúra súborového systému NTFS
Zdroj: https://www.easeus.com/diskmanager/file-system.html

- Partition Boot Sector

[2] New Technology
[3] Hard Disk Drive
[4] Solid State Drive

  - Obsahuje informácie potrebné pre bootovanie. Primárne sa jedná o BootStrap čo je vlastne malý program, ktorý ma za úlohu načítať operačný systém do pamäte.

- Metadata
  - Pomáhajú definovať a organizovať súborový systém, zálohovať kritické údaje súborového systému.
- Master File Table (MFT)
  - Obsahuje záznamy o všetkých súboroch a adresároch na disku. Je to v podstate ekvivalent FAT tabuľky.
- Data
  - Obsahuje samotné dáta súborov.
- MFT Backup
  - Obsahuje zálohu MFT tabuľky.

2.2.2 Bezpečnosť NTFS

Súborový systém NTFS umožňuje nastaviť povolenia na prístup k niektorým lokálnym súborom a priečinkom. Inými slovami, dôverný súbor môžete nastaviť tak, aby bol pre niektorých iných používateľov nedostupný.

2.2.3 Výhody a nevýhody NTFS

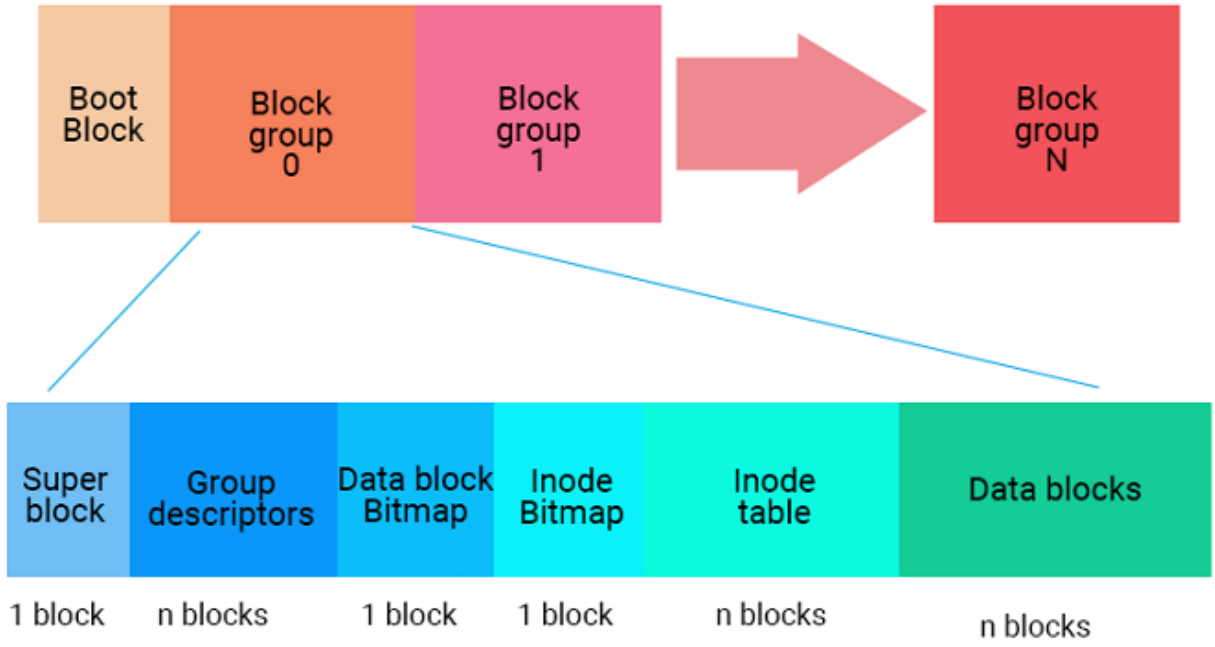
Výhody	Nevýhody
Podporuje veľmi veľké súbory a nemá takmer žiadne reálne obmedzenie veľkosti oddielu.	Má uzatvorený zdrojový kód.
Poskytuje vylepšené zabezpečenie údajov pomocou funkcií riadenia úrovne prístupu a natívneho šifrovania.	Mac OS dokáže čítať jednotky naformátované v systéme NTFS, ale na systém NTFS je možné zapisovať iba prostredníctvom softvéru tretej strany.
Podporuje automatickú kompresiu súborov, čo umožňuje rýchlejší prenos súborov a väčší úložný priestor na disku.	Prenosné zariadenia, ako sú smartfóny so systémom Android a digitálne fotoaparáty, ho nepodporujú.
Umožňuje diskové kvóty, ktoré firmám poskytujú väčšiu kontrolu nad úložným priestorom.	Kompatibilita so systémami založenými na GNU+Linux síce existuje ale iba kvôli vôli softvérových inžinierov urobiť ovladače vďaka reverznému inžinierstvu.
Umožňuje používateľom sledovať pridané, upravené alebo odstránené súbory na disku.	
Zameriava na konzistenciu súborového systému, takže v prípade výpadku napájania alebo zlyhania systému môžete rýchlo obnoviť svoje údaje.	

Tabuľka 1: Výhody a nevýhody súborového systému NTFS
Zdroj: https://superops.com/ntfs-vs-fat32

2.3 ext - Extended File System

2.3.1 Štruktúra ext4

Novo naformátovaný disk s ext4 vyzerá nasledovne:



Obr. 4: Štruktúra súborového systému ext4
Zdroj: https://www.easeus.com/diskmanager/file-system.html

- –
- –
- –
- –
- –

3 Nástroje na obnovu údajov

3.1 Testdisk

4 Experimentovanie s nástrojom testdisk

4.1 Zmazanie a obnova súborov

podarilo uplne v pohode pri fat32 a exfat, pri ntfs bol problem asi to ze to bezalo na linuxe ale podarilo sa to obnovit cez inodes ale bolo treba premenovat subor aj s koncovkou a nastavit ownership nad nim, z ext4 sa nepodarilo z nejakoho dovodu, pri SSD diskoch je treba mat vypnutu funkciu TRIM, ktora je zodpovedna za rovnomerne opotrebovávanie disku a preto neukladá dáta sekvenčne ako HDD aby bolo rýchlejšie ale ukladá náhodne na rôzne bunky.

4.2 Zmazanie a obnova partície

zvladol vsetky obnovit, dokonca aj ked bolo viacej particii na jednom disku a kazda mala iný filesystem.

5 Výsledky experimentov

sem napisat vysledky a nakoniec napisat toto: ak spravne naformatujeme disk tak ze ho pomocou nejakeho nastroja prepiseme cey viacej krat nahodnymi datami tak je mozne ho predat bez obavy ze sa z neho daju obnovit data ktore tam boli pred tym, je to preto lebo pri vymazavani sa v "mazu"v podstate iba zaznami o danych suboroch repsketive sa oznacia ze tam je teraz volne miesto a moze sa tam zapisovat

6 Správne zmazanie dát a formátovanie disku

Prikaz shred, funguje vsak iba na HDD lebo SSD pouzivaju TRIM (da sa asi vypnut ?) ktory vlastne robi wear and tear mechanizmus aby sa disk opotrebovaval rovnomerne a preto sa data ukladaju náhodne na rôzne bunky a nie sekvenčne ako na HDD aby to bolo rýchlejšie lebo pri ssd na tom nezalezi

7 Záver

ak sa nam stalo ze sme omylom vymazali particiu alebo subory ktore sme nechceli tak treba hned prestat zapisovat na disk a je velka sanca ze data vieme zachranit avsak ak zacneme robit zmeny na disku a nasledne nan zapisovat tak je v podstate jedno aky suborovy system pouzivame v kazdom pripade prepiseme data ktore tam boli

Literatúra

[1] Christophe GRENIER. Testdisk - cgsecurity, 2016 - 2023. URL https://www.cgsecurity.org/testdisk_doc/. [Online; accessed 28-February-2024].

[2] Ntfs documentation linux reverse engineered, . URL https://dubeyko.com/development/FileSystems/NTFS/ntfsdoc.pdf. [Online; accessed 28-February-2024].

[3] Ntfs documentation, . URL https://www.ntfs.com/. [Online; accessed 12-March-2024].

[4] Ntfs file system, . URL https://www.easeus.com/partition-manager-software/ntfs-file-system.html. [Online; accessed 13-March-2024].

[5] Fat documentation linux sranda. URL https://dubeyko.com/development/FileSystems/FAT/FAT%20Specs%201.03.pdf. [Online; accessed 28-February-2024].

[6] Linux Foundation asi kedze kernel.org. Ext documentation. URL https://www.kernel.org/doc/html/v4.19/filesystems/ext4/index.html. [Online; accessed 28-February-2024].

[7] Easeus. File systems. URL https://www.easeus.com/diskmanager/file-system.html. [Online; accessed 1š-March-2024].

[8] Wikipedia. File system. URL https://en.wikipedia.org/wiki/File_system. [Online; accessed 13-March-2024].

[9] URL https://superops.com/ntfs-vs-fat32. [Online; accessed 14-March-2024].

[10] URL https://en.wikipedia.org/wiki/ExFAT. [Online; accessed 14-March-2024].

[11] Gabriel Ramuglia. Using shred — The Linux Command for Secure File Deletion, 2024. URL https://ioflood.com/blog/shred-linux-command/. [Online; accessed 14-March-2024].