Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE

Ons Kompjoeterblad

Jaargang 34 - Nummer 3 - mei 2019

Nieuwtjes

* Hoe werkt encryptie?
* Rapide E - Aston Martin's eerste elektrische auto
* Miljoen besmette Asus-laptops
* Gmail krijgt een nieuw R-muis menu
* Microsoft Surface Laptop 2
* Audacity geluidsbewerkingssoftware

Met steun van ROESELARE IS 'R VOOR JOU

VRIJE TIJDSPAS

Midden West-Vlaamse Hobby
Computer Club Roeselare
Skaldenstraat 27
8800 Roeselare

info@hccr.be
http://www.hccr.be

☸ HCCR NIEUWS

* Onze kalender voor - 2019

4 mei 2019	Nieuwigheden in iOS12 door Lisa
18 mei 2019	Arduino door Peter *+ Algemene Vergadering*

Uitnodiging Algemene Vergadering

Roeselare, 22 april 2019

vzw Midden West-Vlaamse Hobby Computer Club Roeselare

Bij deze nodigen wij graag,
alle leden uit op de Jaarlijkse Algemene Vergadering
van de vzw Midden West-Vlaamse Hobby Computer Club Roeselare,
op zaterdag 18 mei 2019 om 16 uur in het clublokaal, Nijverheidsstraat te Roeselare *(ingang via parking OLV-Markt)*

AGENDA

1 Openingswoord door de Heer Voorzitter

2 Overzicht van de activiteiten van het afgelopen werkjaar 2018 - 2019

3 Overzicht van de financiële toestand. Inkomsten en uitgaven v/h boekjaar 2018

4 Ontlasting aan de beheerders voor de handelingen van het afgelopen werk en boekjaar

5 Begroting boekjaar 2020

6 Goedkeuring door de Algemene Vergadering van de begroting voor het boekjaar 2019

7 Rondvraag

8 Slotwoord door de Heer Voorzitter

Deze Algemene Vergadering is een openboek omtrent de werking van de club.

Het is dan ook belangrijk op deze vergadering aanwezig te zijn.

De voorzitter

Kevin Florin

De secretaris

Rik Durnez

❁ NIEUWTJES

* Hoe werkt encryptie?

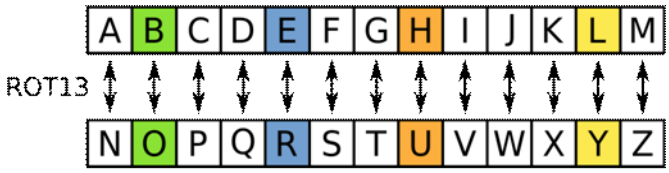
Door je bestanden te encrypteren, voorkom je dat dieven gevoelige data kunnen lezen. Hoe werkt de technologie en hoe kan je deze toepassen?

Om te voorkomen dat iemand die meeluistert op je netwerk al je berichten kan lezen, maken de meeste websites gebruik van encryptie. Je kan deze pagina's herkennen doordat hun url met https start. De meeste browsers tonen bovendien aan dat een website versleuteld is met behulp van een slotje. Zie je dat slotje niet, dan weet je dat je verbinding met de server van de website niet versleuteld is. Alle info die je naar de server verstuurd, kan op zo'n momenten in principe worden gelezen door een hacker.

- ***Cilinder***

Dat encryptie erg belangrijk is om veilig het internet op te gaan, wil niet zeggen dat de technologie tezamen met het internet werd uitgevonden. Integendeel zelfs; de oude Grieken versleutelden hun berichten al op uiteenlopende manieren. Zo gebruikten de Spartanen een cilinder om hun boodschappen onleesbaar te maken. Een generaal die een bericht wilde sturen met behulp van een boodschapper rolde een perkament rond een cilinder en schreef langs de lange kant van het voorwerp zijn tekst. Weer afgerold was de tekst op het perkament volledig onleesbaar. Enkel door de rol perkament te rollen rond een voorwerp met eenzelfde diameter kon je het bericht lezen.

Een andere manier waarmee men in de oudheid berichten versleutelden, was door de letters van het alfabet enkele plaatsen op te schuiven. De 'a' kon zo bijvoorbeeld een 'n' zijn, waardoor Roeselare, nu Ebrfryner wordt. Bij complexere encryptiemethodes werden de letters van het alfabet in willekeurige volgorde in een matrix geplaatst. De letter die in de linkerbovenhoek van deze matrix staat, wordt aangeduid met het getal '11'. Om een bericht te ontcijferen dat via deze weg werd versleuteld, heb je de gebruikte matrix nodig. Door hard genoeg te zoeken, kan iedereen voorgaande encryptiemethodes kraken, waardoor ze niet langer in gebruik zijn.



- ***Symmetrische encryptie***

Je kan moderne encryptiemethodes in twee grote groepen indelen. Symmetrische versleuteling is de eenvoudigste en snelste methode, maar deze techniek is eveneens minder veilig. Asymmetrische encryptie is een stuk veiliger dan de andere beveiligingsmethode, maar vergt meer rekenkracht en tijd. Om deze redenen worden beide versleutelmethodes doorgaans door elkaar gebruikt.

Aangezien encryptie een nogal abstract begrip is, leg ik de technologie uit aan de hand van een voorbeeld. Stel dat Annie een geheim bericht wil versturen naar Bart via de post. Bij symmetrische encryptie beveiligt ze haar bericht door de doos te sluiten met behulp van een slot waarvan zowel Annie als Bart de sleutel hebben. Bart ontvangt de doos in zijn brievenbus en opent het pakket simpelweg met de sleutel die hij in zijn bezit heeft. Een antwoord op het bericht stuurt Bart op dezelfde manier op. Hij beveiligt de doos met hetzelfde slot en stuurt het pakket op naar Annie. Aangezien Annie eveneens een sleutel heeft, kan ze het bericht zonder problemen lezen.

- ***Nadelen***

Een groot nadeel aan symmetrische encryptie is dat zowel Annie als Bart een sleutel van het slot nodig hebben. Deze sleutel moet Annie op voorhand naar Bart opsturen, waardoor iemand de sleutel kan onderscheppen en kopiëren. Om veilig gebruik te kunnen maken van symmetrische encryptie is het cruciaal dat je een veilige manier vindt om je sleutel met anderen te delen.

Symmetrische encryptie wordt op twee manieren toegepast. De technologie kan berichten bit per bit versleutelen, of per blok. Deze laatste methode is sneller, maar minder veilig. Voorbeelden van symmetrische encryptie zijn Twofish, Serpent en AES.

- ***Asymmetrische encryptie***

Stel dat Annie en Bart geen veilige manier vinden om

NIEUWTJES

een sleutel naar elkaar op te sturen, dan kunnen ze gebruik maken van asymmetrische encryptie. Bij asymmetrische versleuteling maak je gebruik van een publieke en private sleutel. Of in ons voorbeeld: een publiek slot en een private sleutel. Bart stuurt een open slot op naar Annie, maar houdt de sleutel van het slot bij. Annie kan vervolgens haar bericht schrijven en dat in een doos stoppen die ze op slot doet met behulp van Barts slot. Bart krijgt het pakketje aan via de reguliere post en opent de doos met de sleutel die nooit zijn huis heeft verlaten. Indien Bart een versleuteld antwoord wil sturen op de brief van Annie, dan moet hij eerst een open slot van Annie ontvangen. Zonder dat hij zelf de bijhorende sleutel heeft, kan hij de doos op slot doen. Hierna kan Annie het slot zonder problemen openen.

Zoals eerder aangehaald werkt de technologie in de praktijk met twee sleutels. De ene sleutel is publiek en kan door iedereen gebruikt worden om een tekst te encrypteren. De enige die deze teksten kan lezen, is de eigenaar van de private sleutel. De publieke sleutel dient met andere woorden uitsluitend om teksten te encrypteren en kan door iedereen gebruikt worden. De private sleutel gebruik je om de versleutelde teksten te decrypteren en is slechts in het bezit van één persoon.

- ***Onderscheppen***

Asymmetrische encryptie heeft als belangrijk voordeel dat je geen veilige manier moet vinden om sleutels uit te wisselen. De kans dat iemand je sleutel kaapt, is erg klein, waardoor onderschepte berichten normaliter onleesbaar zijn en blijven. Zelfs wanneer Bart zijn sleutel per ongeluk met iemand deelt, blijft de schade beperkt. De berichten die Annie naar Bart stuurt, zullen in dat geval onderschept en gelezen kunnen worden door een hacker. Alle andere informatie die Annie of Bart uitsturen blijft echter wel beveiligd. Voor deze communicatie maken ze immers gebruik van andere sleutels.

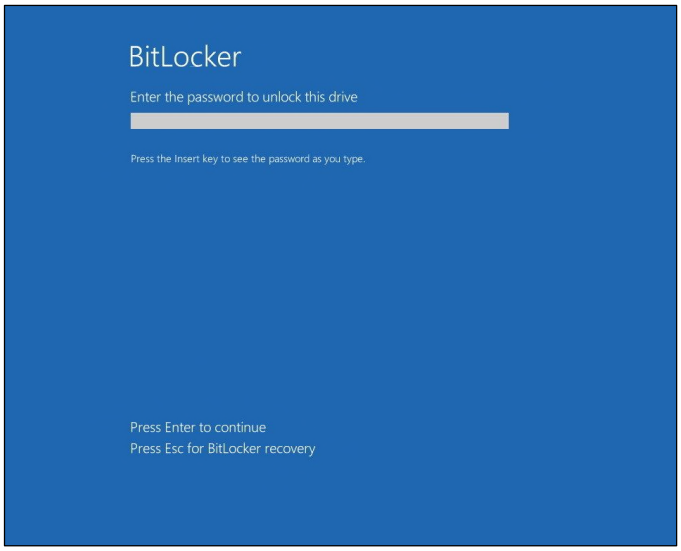
- ***Https***

Een populaire toepassing van asymmetrische encryptie is Secure Sockets Layer (*SSL*). Je internetbrowser en webservers gebruiken dat protocol om al het verkeer tussen hen te versleutelen. Wanneer je https voor een url ziet staan en er een slotje verschijnt in de adresbalk van je browser, dan weet je dat je internetverkeer met behulp van SSL is beveiligd.

SSL maakt gebruik van zowel symmetrische als asymmetrische encryptie. Je browser vraagt om een veilige pagina te openen, waarna de webserver zijn publieke sleutel en certificaat verstuurt. Je browser kijkt vervolgens na of dat certificaat werd uitgereikt door een vertrouwde partij, dat het certificaat nog steeds geldig is en dat het toebehoort tot de website waar je naar surfte. Klopt al deze informatie? Dan gebruikt je browser de publieke sleutel van de website om een symmetrische encryptiesleutel te versleutelen. De webserver gebruikt ten slotte zijn private sleutel om de symmetrische encryptiesleutel te kunnen gebruiken. Je browser en de webserver communiceren nu versleuteld met elkaar. Wanneer je naar een andere website gaat, wordt de sessie beëindigd en vernietigt je browser de symmetrische sleutel. Voor iedere sessie maakt de software een nieuwe sleutel aan, om de veiligheid van je dataverkeer te garanderen.

- ***Schijfversleuteling***

Encryptie is een onontbeerlijk onderdeel van je browser om van het internet een veilige plaats te maken. Je kan de technologie evenwel voor meer toepassingen gebruiken dan je internetverkeer te beveiligen. Zo biedt Microsoft een encryptietool voor Windows aan. Indien je Windows Vista, 7 Ultimate, 7 Enterprise, Windows 8.1 Pro, Windows 8.1 Enterprise, of Windows 10 Pro gebruikt, staat deze software standaard op je computer. Bitlocker maakt gebruik van AES om je data te versleutelen. Je hebt minstens twee partities en een Trusted Platform Module (*TPM*) nodig om van de tool gebruik te maken. Een TPM is een speciale chip die een authenticatiecheck van je hardware, software en firmware uitvoert. Indien de chip een ongeautoriseerde verandering detecteert, boot je pc in een speciale modus om mogelijke aanvallers te slim af te zijn.
Bitlocker beschermt je computer tegen ongeautoriseerde veranderingen van je systeem en kan je gebruiken om je drive te versleutelen. Zelfs wanneer hackers inbreken op je computer zullen ze niet in staat zijn je bestanden te lezen.



Bitlocker is een erg gebruiksvriendelijke tool die jammer genoeg niet beschikbaar is voor de basisversie van Windows. Gelukkig bestaan er alternatieven zoals VeraCrypt waarmee je aan de slag kan gaan. VeraCrypt

☸ NIEUWTJES

is een gratis applicatie die eveneens AES gebruikt om je schijf te versleutelen. Bovendien is de tool in staat om geëncrypteerde partities te verbergen.

- ***7-Zip***

Wil je niet je volledige harde schijf encrypteren? Dan kan je nog steeds afzonderlijke bestanden beveiligen door gebruik te maken van 7-Zip. Deze applicatie ken je hoogstwaarschijnlijk al, aangezien het een populaire tool is om bestanden en mappen te zippen en weer uit te pakken. Je kan 7-Zip echter eveneens gebruiken om bestanden te encrypteren.
Klik hiervoor met je rechtermuisknop op een document of map, ga naar 7-Zip en kies voor toevoegen aan archief.

Een venster opent zich, waarin je in de eerste plaats de compressieparameters van je bestand kan kiezen.
Onder het menu Codering vind je de mogelijkheden terug om je bestand te beschermen. Kies een wachtwoord om je document te versleutelen en verander de codeermethode naar AES-256. Wanneer je nu op OK klikt, worden je bestanden niet alleen ingepakt, maar eveneens geëncrypteerd.

- ***VPN***

Wie de standaard beveiliging van zijn browser niet vertrouwt, kan een Virtual Private Network (*VPN*) gebruiken. Deze software maakt een geëncrypteerd kanaal aan, waarover jij met andere internetgebruikers kan communiceren. De kracht van de technologie bevindt zich in de combinatie van tunneling en encryptie. Datapakketjes worden in andere pakketjes ingepakt, zodat niemand weet van waar een bericht komt en naar waar hij gaat. Hierdoor kan je doen alsof je je in een ander land bevindt, om bijvoorbeeld je Netflix-aanbod uitgebreider te maken. Een VPN-dienst versleutelt eveneens je datapakketjes om er zeker van te zijn dat niemand berichten kan onderscheppen en lezen. Door gebruik te maken van een VPN-dienst verzeker je je privacy, maar zorg je er jammer genoeg eveneens voor dat je internetverbinding trager wordt.

Bron: Techpulse.be

* Rapide E - Aston Martin's eerste elektrische auto

Het is niet de eerste keer dat we van de Rapide E horen, maar tijdens de Shanghai Auto Show werd het pareltje wel officieel voorgesteld aan het grote publiek.

De Rapide E is het vervolg op de 9 jaar oude Rapide Sedan. Achteraan vinden we een elektromotor die 601 pk en 950 Nm levert. Dit maakt van de Rapide E niet meteen de snelste elektrische wagen, hij schakelt van 0 naar 100 km/u in een 4-tal seconden en kan een topsnelheid bereiken van 250 km/u.

Onder de motorkap vinden we vervolgens een 65 kWh-accu. Volgens de WLTP-norm kan de wagen hiermee een bereik van 320 kilometer aan. Na een uur laden zou je terug 298 kilometer verder kunnen dankzij 50 Kw en 400V. Snelladen aan 100 kW en 800V is eveneens mogelijk. Een uurtje snelladen brengt je dan 499 kilometer verder.

De prijs is nog niet bekend, maar die wil je mogelijk ook niet onder ogen zien wanneer je weet dat er slechts 155 exemplaren van geproduceerd worden.

Leuk om te weten, is dat James Bond (*Daniel Craig*) in de nieuwe Bond-film hoogstwaarschijnlijk in deze nieuwe Aston Martin Rapide E zal rondcrossen.

Bron: Techpulse.be

☸ NIEUWTJES

* Miljoen besmette Asus-laptops

Een beveiligingslek in de automatische updatetool van Asus laptops heeft ervoor gezorgd dat hackers in 2018 mogelijk toegang hadden tot meer dan een miljoen systemen van het merk.
Laptops van voor november 2018 kunnen besmet zijn.

Het programma Asus Live Update staat standaard op alle laptops van Asus. Het controleert en installeert updates voor Asus (*stuur*)programma's. Kaspersky ontdekte kwaadaardige code in eerdere versies van dit programma, die volgens het bedrijf tussen juni en november 2018 is verspreid naar laptops van Asus.

Het antivirusbedrijf schat dat in totaal meer dan een miljoen systemen getroffen zijn. Inmiddels wordt de malware niet meer verspreid. Nieuwe laptops lopen volgens Kaspersky dan ook geen gevaar.

- ***Reactie Asus***

In een reactie op de eigen site geeft Asus aan de beveiliging van de update-software te hebben verbeterd en contact te hebben gehad met getroffen gebruikers om de risico's weg te nemen.
Lees het bericht. http://tinyurl.com/y2yhjcq4

- ***Is mijn laptop besmet?***

Asus heeft een programmaatje met de naam ASUSDiagnosticTool beschikbaar gesteld dat controleert of je Asus-laptop getroffen is. Heb je een Asus-laptop en had je deze al tussen juni en november 2018? Dan is het aan te raden om de tool te gebruiken. *(ASUSDiagnosticTool, download via de opgegeven link)*

Bij een eventueel besmette laptop raadt Asus aan om het systeem te back-uppen en vervolgens terug te zetten naar de fabrieksinstellingen.

- ***Laptop-overzicht***

In principe lopen alle Asus-laptops voor november 2018 het risico om besmet te zijn. Weet je niet meer precies van wanneer je laptop is? Wij hebben tussen 2016 en november 2018 in totaal 165 laptops van Asus getest.

Als je laptop hiertussen staat, dan raden we je in ieder geval aan om het diagnostische tooltje van Asus uit te voeren. Zelf hebben we in onze kleine steekproef overigens geen geïnfecteerde machines gevonden.

- ***Gerichte aanval***

Dat het lek zo lang onopgemerkt is gebleven, ligt er waarschijnlijk aan dat de aanvallers officiële certificaten van Asus hebben bemachtigd. Daarvoor hebben zij ingebroken op servers van Asus waar de update-tool wordt verspreid. Zo lijkt het voor zowel Asus als voor de gebruiker alsof er niks aan de hand is.

Wat de kwaadwillenden precies met de aanval wilden bereiken, is niet duidelijk. Wel is bekend dat het ze uiteindelijk geïnteresseerd waren in maar 600 systemen. Volgens Asus was de aanval gericht op bepaalde internationale organisaties of entiteiten en niet op consumenten.

Bron: Consumentenbond.nl

☸ NIEUWTJES

* Gmail krijgt een nieuw R-muis menu

In het oude menu kunnen gebruikers maar een paar dingen doen zoals een e-mail verwijderen of archiveren.
In het nieuwe menu worden er veel meer opties toegevoegd. Zo kunnen gebruikers dan reageren op e-mails, of ze doorsturen. Ook verschijnen er betere zoekopties. Gebruikers kunnen dan alle e-mails van dezelfde afzender zoeken, of zoeken op onderwerp.

Die functies waren altijd al beschikbaar in Gmail, maar moesten in de mail zelf of via een aparte zoekbalk worden toe gepast.
Google rolt de nieuwe features binnenkort uit voor gebruikers. Zakelijke gebruikers kunnen er als eerste gebruik van maken.

Bron: NU.nl

* Microsoft Surface Laptop 2

Tot Microsofts lancering van vier nieuwe producten behoort ook Surface Laptop 2, de eerste opvolger van de traditionele Surface Laptop. Net zoals bij de Surface Pro 6 heeft Microsoft niet veel wijzigingen aangebracht aan zijn basisformule voor deze laptop. Toch lijkt deze nieuwe laptop zeker de moeite waard om eens van dichterbij te bekijken.

De grootste verandering die de Surface Laptop 2 aanbiedt, is de 8e generatie Intel Quad Core processor. Hiermee zou deze laptop 85% sneller moeten zijn dan de eerste reeks laptops in het Surface-gamma. Ook komt het toestel met PixelSense Touch Display en een ingebouwd toetsenbord dat een combinatie moet bieden van "stille schoonheid, prestatiekracht en draagbaarheid". Het batterijverbruik blijft, met een maximale gebruikstijd van 14,5 uur, tegelijkertijd hetzelfde als dat van de eerste Surface Laptop ondanks de sterkere prestaties. Verder blijft de grootte van de laptop ook hetzelfde met 13,5 inch, waardoor deze nog steeds zeer compact is.

Net zoals bij de Surface Pro-reeks lijkt Microsoft hetzelfde patroon aan te houden bij zijn reeks Surface Laptops. Het bedrijf gebruikt hierbij een sterke en succesvolle basisformule en brengt kleine, maar effectieve wijzigingen aan bij elke update van het product. Wanneer we dus de opvolger van de Surface Laptop 2 (*waarschijnlijk de Surface Laptop 3*) te zien krijgen, zal deze hoogstwaarschijnlijk ook een touchscreen hebben van 13,5 inch.

Bron: Techpulse.be

❁ NIEUWTJES

* Audacity geluidsbewerkingssoftware

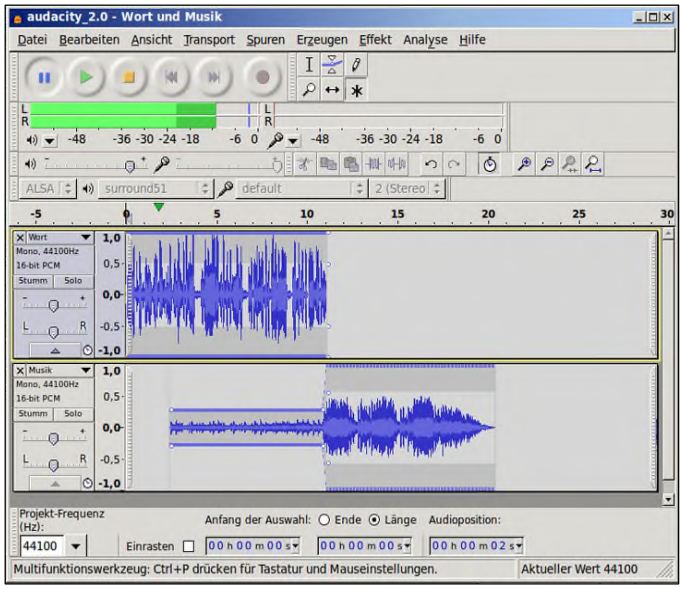
Audacity is een vrije en gebruiksvriendelijke audio-editor voor Windows, Mac OS X, GNU/Linux en andere besturingssystemen.
Deze geluidsbewerkingssoftware is niet alleen in het Engels, maar ook in het Nederlands beschikbaar.

De functies van Audacity zijn zeer uitgebreid. Zo kunt u niet alleen delen uit geluidsbestanden knippen of juist erbij plakken, het is ook mogelijk om effecten zoals een echo toe te voegen en de geluidskwaliteit aan te passen. Audacity heeft alles in huis om van verschillende losse nummers of zelf opgenomen geluidsbestanden uw eigen muziekmix te creëren.
Handige functies hierbij zijn het in- en uitfaden van nummers en het op elkaar afstemmen van het tempo van twee nummers.

Verschillende bestandsformaten voor audio kunnen geïmporteerd en geëxporteerd worden waaronder AIFF, AU, FLAC, Ogg Vorbis, WAV en na installatie van de libmad audio decoder ook MP2 en MP3.

U heeft volledige controle over de toonhoogte, het tempo en het volume van de bewerkte audiobestanden. Standaard bevat het programma een aantal veelgebruikte geluidseffecten die u in uw mix kunt gebruiken. Zo kunt u kiezen uit onder andere echo, afkappen van stilte en Paulstretch (*het extreem uitrekken van een geluidsbestand*). Het in dj-sets en podcasts veelgebruikt Auto Duck effect maakt ook onderdeel uit van de meegeleverde effecten. Dit effect zorgt ervoor dat het volume van de muziek automatisch een aantal decibel omlaag gaat op het moment dat de voice-over spreekt. Wanneer u aan de standaard selectie van effecten niet voldoende heeft kunt u nieuwe toevoegen met behulp van LADSPA, Nyquist, VST en Audio Unit plugins.

Audacity heeft geen problemen met het gebruik van hele grote audiobestanden. Alle bewerkingen kunnen uitgevoerd worden met de muis, maar ook volledig via het toetsenbord en sneltoetsen die u zelf kunt instellen. Dit maakt het programma toegankelijk voor zowel beginnende als professionele gebruikers.



- ***Audacity heeft de volgende kenmerken:***
  - geluid opnemen via ingebouwde microfoon van laptop of USB/Firewire apparaat,
  - verschillende audioformaten importeren en exporteren,
  - geluidskwaliteit van geluidsbestanden instellen en verbeteren,
  - bewerkingen zoals knippen, plakken en kopiëren uitvoeren,
  - bediening via de muis of volledige via het toetsenbord mogelijk,
  - effecten zoals toonhoogte, tempo, echo, Paulstretch, omkeren, etc. toepassen,
  - onbeperkt nieuwe effecten toevoegen met LADSPA, Nyquist, VST en Audio Unit,
  - effecten in batches aan meerdere audiobestanden toevoegen,
  - digitaliseren van cassettebandjes en vinylplaten, visualisatie van frequenties via spectogram weergavemods,
  - beschikbaar voor Linux, Mac en Windows.

Bron: Gratissoftware.nu/
https://www.audacityteam.org/