

HACKTIC

Tijdschrift voor
TECHNO-ANARCHISTEN

POSTCHEQUE
BIG BROTHER
giromaatpas
Carte de garantie
HACKTIC
BB2D031A
L37X507
6 02-93

Met in dit nummer

- Magneetkaarten
- Zelfbouw kostenteller
- Hacking IBM VM/CMS
- 5-ESS telefooncentrales
- en het Hack-Tic colofon !

Tijdschrift voor de alternatieve techneut

COLOFON

Hack-Tic is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1989.

UITGAVE: Met veel moeite door de Stichting Hack-Tic, een cover-up voor een groep individuen zonder enige kennis van zaken.

REDAKTIE: The Key, John D., Tx, Herman Acker, Peter Poelman, Rhincewind, Paul en Rop. Verder krijgen we informatie uit de gekste kringen.

ILLUSTRATIES: Koen Hottentot.

KONTAKT: De redactie is te bereiken via p.b. 22953, 1100 DL Amsterdam. UUCP: rop@neabbs.UUCP. Op het FIDO net 2:280/2 Hack Tic. Telex (modern 50 baud telecommunicatiecomfort van de PTT) 12969 neabs nl, telefax 020-763706. Zowel bij telex als bij fax even vermelden dat het voor Hack-Tic is. Ons telefoonnummer is 020-6001480 (ons superdeluxe antwoordapparaat staat 24 uur per dag tot uw beschikking).

PRIJS: Losse nummers kosten 4 gulden, een abonnement voor 10 nummers (hoe lang het ook duurt om die uit te geven) kost f 37,50. Abonnementsgelden kun je overmaken op bankrekeningnummer 98.72.84.541 t.n.v. Rop Gonggrijp. Rekening loopt bij de verenigde spaarbank, postrek. no. 15368. Abonnementen beginnen met het laatst uitgegeven nummer tenzij je bij de betaling een ander beginnummer aangeeft. Bedrijven en instellingen betalen f 100,- voor een jaarabonnement (maar kunnen de abonnementskosten dan weer van de belastingen aftrekken c.q. door de baas laten betalen).

PRIVACY: Het is natuurlijk via onze bankafschriften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan

kun je ook geld of girocheque en adres bijsluiten in een envelop en die aan onze postbus sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.

DISCLAIMER: Informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/ stout kunnen zijn. De redactie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt niet noodzakelijkerwijs de mening van de redactie of uitgever.

NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. etc. mogen zonder voorafgaande toestemming van de redactie (maar natuurlijk met bronvermelding) stukken overnemen uit de Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.

NABESTELLEN: Oude nummers kosten ook fl. 4,- en kunnen via de redactiepostbus besteld worden.

HOE: Hack-Tic werd met het WYSMRWYG (What You See Might Resemble What You Get) DTP pakket Ventura 2.0 gemaakt op een gammele AT. Print-outs van elke pagina werden met zo'n modern lasergeval gezoefd en daarna vermenigvuldigd. Dan nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

VERKRIJGBAAR: Erg moeilijk, maar wellicht bij: Het Computercollectief, Fort van Sjakoo en Athenaeum Boekhandel, allen in Amsterdam, De Rode Hond in Den Haag, De Rooie Rat in Utrecht, Dencker in Nijmegen en Athenaeum in Haarlem.

Tic-8

Zoals je ziet heeft de kافت een steunkleur en is onze mascotte eens een keertje niet op de kافت te zien. Ons nog niet 'afgetopte' redactie-hoofdkwartier in de Bijmermeer heeft de storm en de daarop volgende lekkage overleefd. Hier is Hack-Tic nummer 8; de eerste na de koude oorlog.

Na het publiceren van het schema van de "video-signaaloptimalisator" in Hack-Tic 5/6 zijn we overspoeld met brieven van mensen die dachten dat wij allemaal experts waren op het gebied van 'gestoorde videosignalen'. Wij horen van allerlei kanten dat het door ons gepubliceerde schema niet (meer?) werkt, dus bouw het nog niet na. Wij hebben inmiddels een ander schema en we gaan eens kijken of dat werkt, zo ja dan verschijnt het vanzelf wel in de Tic. Anders even bellen met 03480-14020, en vragen naar het schema voor een decoder.

Wat hebben wij zoal uitgevonden? We zijn druk bezig geweest met het bouwen van onze eigen magneetkaart lezer/schrijver/copier. De schema's om zoiets zelf te bouwen zie je op pagina 20. Verder hebben we een zeer goekope zelfbouw-kostenteller op pagina 10. Dit laatste project was niet mogelijk zonder de hulp van Billsf, de meest welkome loge die een stel hackers zonder noemenswaardige kennis van de

analoge electronica zich kunnen wensen. Bill zal in komende Hack-Tics nog wel van zich doen spreken.

Dan is er nog een groot artikel over de ins en outs van VM/CMS, een IBM operating system. Voor de phone-phreaks is het artikel over de "hidden extra's" van Sess centrales smulwerk.

Het volgende nummer is weer eens een dubbelnummer en komt volgens de planning voor de zomer uit. Abonnee's voor wie dat het laatste nummer van hun abonnement is ontvangen dan ook een acceptgiro om hun abonnementsgeld voor de volgende 10 nummers mee te betalen. Het verzenden van acceptgiro's kost echter geld. Als je ons deze kosten wilt besparen willen we je verzoeken je abonnementsgeld voor de nummer 11 1/m 20 nu al over te maken. Zie voor meer informatie het colofon.

In deze Tic

2.....	colofon
3.....	Tic 8
4.....	5-ESS features
7.....	Recensie Het Koekoeksei
8.....	Hack-Tic light
10.....	Zelfbouw kostenteller
12....	DKRV-BRIT computer PTT
14.....	Hacking IBM's VM/CMS
18.....	ANI in Nederland
19.....	Hekjes
20.....	Magneetkaarten
24...	Electriciteit voor beginners

5-ESS Diensten

Telefooncentrales zijn mooie apparaten. Hier in Nederland merken we daar weinig van omdat de PTT alle mooie ingebouwde foefjes op hun moderne centrales zorgvuldig uit heeft gezet. Nu wisten we al dat je voor het NIET UITZETTEN van kostenimpuls en toonkiesmogelijkheid moest betalen en is het dus waarschijnlijk op te vatten als PTT-beleid om niet de optimale service te verlenen. Hack-Tic beschrijft de verborgen mogelijkheden van de 5-ESS PRX centrale van APT, een zeer moderne centrale die op nogal wat plaatsen zijn intrede heeft gedaan.

Het idee niet optimaal over de eigen telefooncentrale te kunnen beschikken moet een gruwel zijn voor iedere rechtgeaarde phreak, hacker of wasmachine-reparateur. Niet om je te pesten, maar hier zijn de diensten die ze op de meeste centrales met een paar commando's op de system-console aan kunnen zetten. Imagine:

Malicious Call Identification

Je wordt gebeld door een hijger. Je tikt op de hookflash knop (dit is hetzelfde als ongeveer 0.8 sec neerleggen) en je drukt *39#. Je hoort vervolgens een indicatietoon en je zit weer in het gesprek met de hijger. Zijn nummer is echter in de telefooncentrale afgedrukt en kan door de abonnee worden opgevraagd. (minder leuk voor computerhackers, maar daarover later meer).

Alarm Call Service

Gebruik je telefoon als wekker. Tik *55*0730# als je om half acht gewekt wilt worden. Als je de wekker uit wilt zetten tik je #55*0730. De tijd moet je dan nog een keer opgeven omdat je tegelijkertijd meerdere 'wekkers' aan kunt hebben staan. Als we deze service zouden kunnen krijgen zou je waarschijnlijk elke maand een nieuwe wekker kunnen kopen voor het geld dat de PTT hiervoor zou willen hebben.

Abbreviated Dial

Na de geheugentelefoon nu ook de geheugentelefooncentrale. Voor veel geld krijg je straks tien te onthouden nummers, voor nog meer geld krijg je er maximaal 100. Als je *51*13*0206001480# tikt dan is Hack-Tic bij jou onder nummer 13 geprogrammeerd. Om dit verkorte nummer te kiezen druk je **13 en om nummer 13 te wissen toets je #51*13#.

Number Repetition

0# draait het laatst gekozen nummer nog een keer.

Do Not Disturb Service

De meest exotische service tot nu toe: je kiest *26*1600#. Belt iemand je dan voor 1600 uur dan krijgt hij/zij de beleefde mededeling dat je tot 16:00 onbereikbaar bent. Met #26# zet je dit grapje weer uit.

Wat er gebeurt als de Wekservice belt naar de Do Not Disturb service is helaas in de documentatie niet terug te vinden. Hoe dan ook, meer dan een leuke gadget wordt het niet.

Call Waiting

Jij bent in gesprek en iemand wil je bereiken. Je hoort een piepton en je drukt op de hookflash. Je krijgt dan een nieuwe kiestoon waarop je 1 of 2 kunt kiezen. 1 geeft je je oorspronkelijke gesprek en 2 schakelt naar het nieuwe inkomende gesprek.

Aanzetten van deze service doe je met *34# en uitzetten (dit moet als je met modem werkt of een antwoordapparaat gebruikt!) is #34#

Outgoing Call Barring

Hiermee kun je uitgaande gesprekken blokkeren voor iedereen die de code niet kent. Tik *34*XXXX*Y#. XXXX staat voor de code die je wilt instellen. Y is het type blokkering dat je wilt instellen.

0: blokkeert alle uitgaande gesprekken
1: blokkeert alle niet-lokale gesprekken
2: blokkeert alle internationale gesprekken
3: blokkeert alle intercontinentale gesprekken (landcode begint niet met 3 of 4)

Uitzetten doe je met #34*XXXX# waarbij XXXX de juiste code moet zijn. Als je toch op kosten van de eigenaar van deze lijn wilt bellen kun je je gesprekspartner natuurlijk collect laten bellen.

Divert Immediately

*21*Telefoonnummer# schakelt inkomende gesprekken door naar het ingetikte telefoonnummer. Met #21# zet je dit weer uit. In Hack-Tic 3 hebben we hier al het een en ander over geschreven.

Three Party Service

Als je op deze service geabonneerd bent kun je tijdens een gesprek met een hookflash en een daarop volgend cijfer schakelen tussen twee uitgaande gesprekken. In een gesprek tik je 'flash' en dan het telefoonnummer om een nieuw gesprek te maken. Met 'flash' en dan 2 schakel je tussen de twee gesprekken. 'flash' 1 verbreekt het huidige gesprek en schakelt naar de andere lijn. 'flash' 0 verbreekt het wachtende gesprek en 'flash' 3 verbindt de 3 gesprekspartners met elkaar. Met 'flash' 2 kom je weer terug in privacy mode met 1 van de gesprekdeelnemers. 'flash' 4 verbindt de twee gesprekspartners met elkaar als in gesprek. Jij kunt dan neerleggen (!)

Calling Number Identification

Deze feature wordt ook vaak ANI (Automatic Number Identification) genoemd. De 5-ESS kan voor het rinkelen van je telefoon het nummer van de opbeller door middel van DTMF tonen op de lijn zetten. Als je apparatuur hebt om die piepjes te ontvangen kun je dus zien wie je opbelt. Het invoeren van deze service heeft in veel staten in de VS nogal wat stof doen opwaaien. De PTT heeft aangekondigd deze service ook hier in de toekomst te gaan bieden. Volgens velen is deze feature onder andere de doodsklap voor anonieme telefonische hulpverlening.

Hotline

De laatste feature waarmee de klant eventueel in aanraking kan komen is de 'hotline'. Geabonneerd op deze feature is het onmogelijk om uitgaande gesprekken te voeren. Zodra je de telefoon oppakt wordt een vastevoren vastgelegd nummer gebeld. Handig voor telefoons waarmee je alleen maar de brandweer/politie/portier etc. mag bellen. Ook beschikbaar als 'timed hotline'; je kunt wel uitgaand bellen maar als je gedurende X seconden niets intikt wordt je verbonden met het ingestelde nummer.

Standaard

De in- en uitschakelcodes voor deze diensten zijn internationaal genormeerd door het CEPT. Amerikaanse centrales (waar vaak veel van deze diensten al draaien) gebruiken andere codes. We kunnen niet garanderen dat alle diensten in Nederland dezelfde codes krijgen. Een groot deel van deze diensten krijgen we hier nooit omdat de PTT ze als 'niet rendabel' terzijde schuift. De PTT zal echter volhouden dat bepaalde dingen 'technisch onmogelijk' zijn. De Hack-Tic abonnee weet beter!

Politiek

Waarom noemen we al deze diensten? Omdat we vinden dat de samenleving zich zou moeten gaan bezig houden met de vraag welke diensten ze wel en welke ze niet in haar telefoonnet zou willen hebben. Het is volgens ons niet de bedoeling dat alleen PTT technici en managers beslissen over de mogelijkheden van ons telefoonnet. Neem nu bijvoorbeeld ANI: in Amerika is ANI in bepaalde staten niet ingevoerd. Om bijvoorbeeld hijgers dwars te zitten zijn andere manieren denkbaar. Zo kun je in Illinois met je telefoontoetsenbord een lijst opgeven met nummers van mensen die jou niet meer mogen bellen. Je kunt daarin behalve jou bekende nummers ook het nummer van de laatste opbeller plaatsen. Jij weet dan nog steeds

zijn/haar nummer niet maar hij/zij kan je niet meer bellen.

Ons zit niet zo zeer dwars dat we bepaalde diensten al dan niet hebben. Ons zit dwars dat de PTT beslist welke kenmerken ons telefoonnet heeft.

Peter Poelman

Clifford Stoll

HET KOEKOEKSEI, Over krakers en computerspionage

*vertaling van The cuckoo's egg:
Tracking a spy through the maze of
computer espionage*
ISBN 90-269-4167-6

In dit boek beschrijft de astronoom Cliff Stoll hoe hij een jacht organiseerde op een aantal computerkrakers die inbraken in zijn systeem. Hij schrijft boeiend en spannend en geeft d.m.v. een haast oneindig aantal anecdotes en voor de leek begrijpelijke technische beschrijvingen een goed beeld van de jacht op een hacker.

Misschien is het enige hindertje dat Stoll elke twee pagina's duidelijk laat merken dat hij zichzelf nog steeds als hippie ziet, al heeft hij in het boek samenwerking met de CIA, de NSA en (minder produktief) ook met de FBI. Hij beschrijft het uitzetten van vallen om de inbrekers in zijn computer te vangen en het uiteindelijk klemzetten van de indringer, die voor de KGB bleek te werken.

Hij vindt al die "spionnen" met wie hij samenwerkt ook maar eng, maar, zo redeneert hij: "Op onze computernetten heerst een sfeer van onderling vertrouwen en open-

Een samenleving is hooguit zo democratisch als de organisatie die de structuren en tarieven van haar telecommunicatie vaststelt.

S. Weméry



heid van informatie. Hackers ondermijnen dit vertrouwen en zijn dus een bedreiging voor de openheid van informatie". De wetenschappelijke computernetwerken zijn een schat van informatie, niet alleen voor wetenschappers. De redenatiefout die Stoll maakt is dat die "openheid van informatie" alleen geldt voor de wetenschappers wiens baas geld genoeg heeft om de toegang tot die netwerken te betalen.

In de filosofie van Stoll heeft de schooljongen, de gewone man, geen recht op de informatie op de computernetten. Het kwam Stoll natuurlijk wel goed uit dat zijn hacker een van de "guys with dark hats" was en de informatie wilde verkopen aan de KGB (dit is "slecht", het leveren van informatie aan de NSA/CIA/FBI is "goed").

Ikzelf heb meerdere malen illegaal gebruik gemaakt van wetenschappelijke computers juist om informatie van 'het net' te kunnen plukken. Ik weiger echter om me verantwoordelijk te voelen voor onderling wantrouwen dat binnen het net ontstaat. Stoll heeft het over zijn "computer-privacy" die is aangetast. Het komt er dus op neer of je eigendomsrechten over openbare informatie erkent. Zolang er voor mij geen goedkope wegen open staan om aan deze informatie te komen zal ik die informatie "stelen". Stoll of geen Stoll.

Rop Gonggrijp

Hack-Tic light

AT&T down



p 16 januari van dit jaar viel een groot gedeelte van het Amerikaanse telefoonnet uit. Bijna alle interlokale lijnen van AT&T, de grootste telefoonmaatschappij van Amerika, vielen uit doordat een 4-ess telefooncentrale niet helemaal overweg kon met zijn nieuwe software. Als een bepaald deel van de centrale ermee ophield was er niets aan de hand. Als het weer terug kwam gingen andere centrales down. Gevolg was een gigantische lading ups en downs op het telefoonnet en dus geen long-distance telefoonverkeer over AT&T lijnen. Over de andere telefoonmaatschappijen kon nog wel long-distance gebeld worden, helaas is men het publiek vergeten te vertellen hoe dat precies werkt.

AIDS-Virus

Onder andere via het tijdschrift PC-Business World werd eind vorig jaar het "AIDS-info virus" verspreid dat na een willekeurig aantal keren te zijn opgestart de harddisk formatteerde (en dus al je gegevens wiste). De uitgevers van dit virus wilden eerst geld zien alvorens zij

het virus ongedaan maakten. Stuur eens een kaartje naar de PC Cyborg Corporation, P.O. Box 871744, Panama 7, Panama. Zie voor de nu profetische cartoon ons dubbelnummer 5/6.

Pincode

Dat mooie pincode-onthoud kaartje dat we zonder uitleg op de achterkant van Tic-7 hadden is niet betrouwbaar. Het blijkt dat je meer emotie legt in het opschrijven van je PIN-code dan in al die andere cijfertjes en dus was bij veel kaartjes een handschriftonderzoek voldoende om het PIN te achterhalen.

De Menulijn

Hoewel er nog niets in het bestand zit is het wel leuk om eens een beetje te spelen met Voice-Mail achtige toepassingen. Als je een DTMF telefoon hebt moet je het maar eens proberen: 010-4291749. Het nummer is van het bedrijf Speechline en is 'gespot' door Robert C.

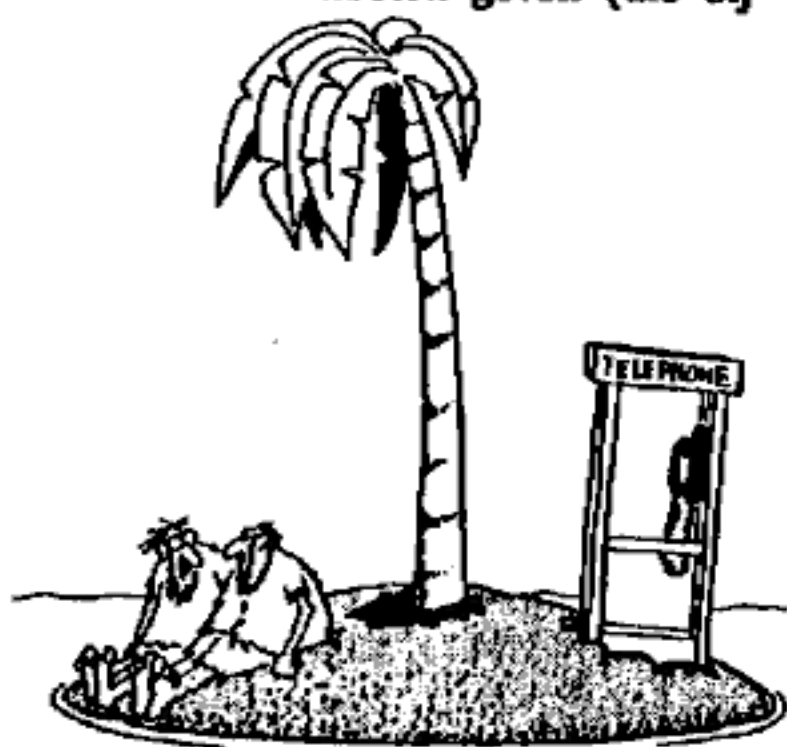


Internet Worm

De auteur van de internet-worm, Robert T. Morris (25) is schuldig bevonden aan 'federal computer tampering'. Hij zou nu 5 jaar de cel in moeten en \$250.000 dollar boete moeten betalen. Morris, die inmiddels heeft bekend de worm te hebben geschreven, zegt geen criminele bedoelingen te hebben. De beveiligingsgaten waarvan de internet-worm gebruik maakte waren al tijden gemeengoed in de internet-gemeenschap.

Sweep test

Als je eens wilt kijken of er filters in een internationale telefoonverbinding zitten moet je maar eens 09-1-415-552-0046 bellen. Dit is gratis en het zou een steeds hoger wordende toon moeten geven (die bij



"For the one-hundredth time in as many days ... I HAVEN'T GOT A QUARTER!"

Liam

het bereiken van zijn hoogtepunt weer bij laag begint). Zitten er gaten in deze toon dan heb je wat filters op de lijn zitten.



Extra cijfers

Ook de Amsterdamse telefoonnummers nummers die niet met zes beginnen maar wel zes cijfers hebben krijgen een extra zes voor het oude nummer geplakt. In 1991 hebben dan alle Amsterdamse nummers zeven cijfers. Wij continentals hebben echter geen werkelijk talent voor verwarring; in Engeland pakt men de zaken groter aan. Daar verandert British Telecom (of Bitch Telescum) het netnummer van Londen! Netnummer 01 wordt gesplitst, 071 voor het centrum en 081 voor al het andere dat nu onder netnummer 01 valt. Bij het bellen vanuit Nederland natuurlijk de nul weglaten. Stel je voor dat je veertig Londense telefoonnummers uit je hoofd kent, dan moet je van alle veertig uitzoeken WAAR in de stad die nummers zich bevinden. De Hack-Tic redactie neemt haar petje af voor de chaos die dit zal scheppen, hierbij vergeleken zijn wij amateurs.

Hack-Tic kostenteller

Hack-Tic presenteert de goedkoopste zelfbouw-kostenteller. Totale materiaalkosten voor deze teller bedragen ongeveer f2,- en een oud rekenmachientje met een herhalingsfunctie op de '='-toets.

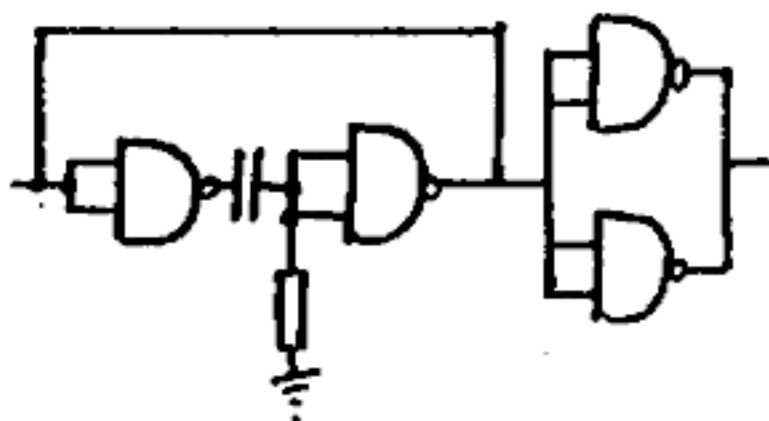
Speciaal voor Hack-Tic door Billsf

Het principe is simpel: de kostenpuls is een 50 Hz puls die in fase op zowel de a- als op de b-draad wordt gezet. Een normale telefoon die tussen a en b is aangesloten merkt dus niets van de kostentik. Als je echter de twee lijnen meet ten opzichte van aarde zie je dat alleen tijdens de kostentik het gemiddelde van a en b boven 0 Volt uitkomt.

Onze schakeling maakt gebruik van dit principe om de tik te detecteren. Zodra het gemiddelde boven ongeveer 15 Volt komt schakelt de transistor de ene ingang van de eerste NAND naar 0. De 1 μ F condensator is ontladen en dus gaan de inputs van de tweede NAND, hier als inverter gebruikt, ook hoog. De output hiervan wordt laag. Dit signaal wordt gebruikt als tweede input op de eerste NAND. Dit houdt de output van die NAND op 1, hoe lang of kort de input puls ook is. Als de condensator is opgeladen (150 milliseconden later) keert de hele mik weer terug in de begintoestand.

Het uitgangssignaal van de tweede NAND wordt door twee parallel geschakelde inverters geleid (dit om twee keer zoveel stroom te

kunnen leveren) om een mooie, 150 milliseconden lange, 5 Volt puls te leveren (50 mA maximaal). Dit signaal gooien we in een reed relais (of een ander relais dat met 50 mA toekan).



Het kontakt van dit relais knopen we vervolgens aan de draadjes naar de '=' toets van een goedkoop wegwerp-calculator. Op dit prul tik je '+.15' of '.15++' en vervolgens is de zaak klaar. Elke keer als er een kostentik binnenkomt 'drukt' de schakeling op de '=' toets en telt dus 0.15 op bij het getal op het display. Neem geen calculator met auto-off tenzij de '=' toets het ding 'wekt' zonder het getal op het display te wissen.

Nog even dit. Het IC loopt op alles tussen +2 en +7 Volt. Met een beetje mazzel zit de batterijspanning van je rekentuig hier er-

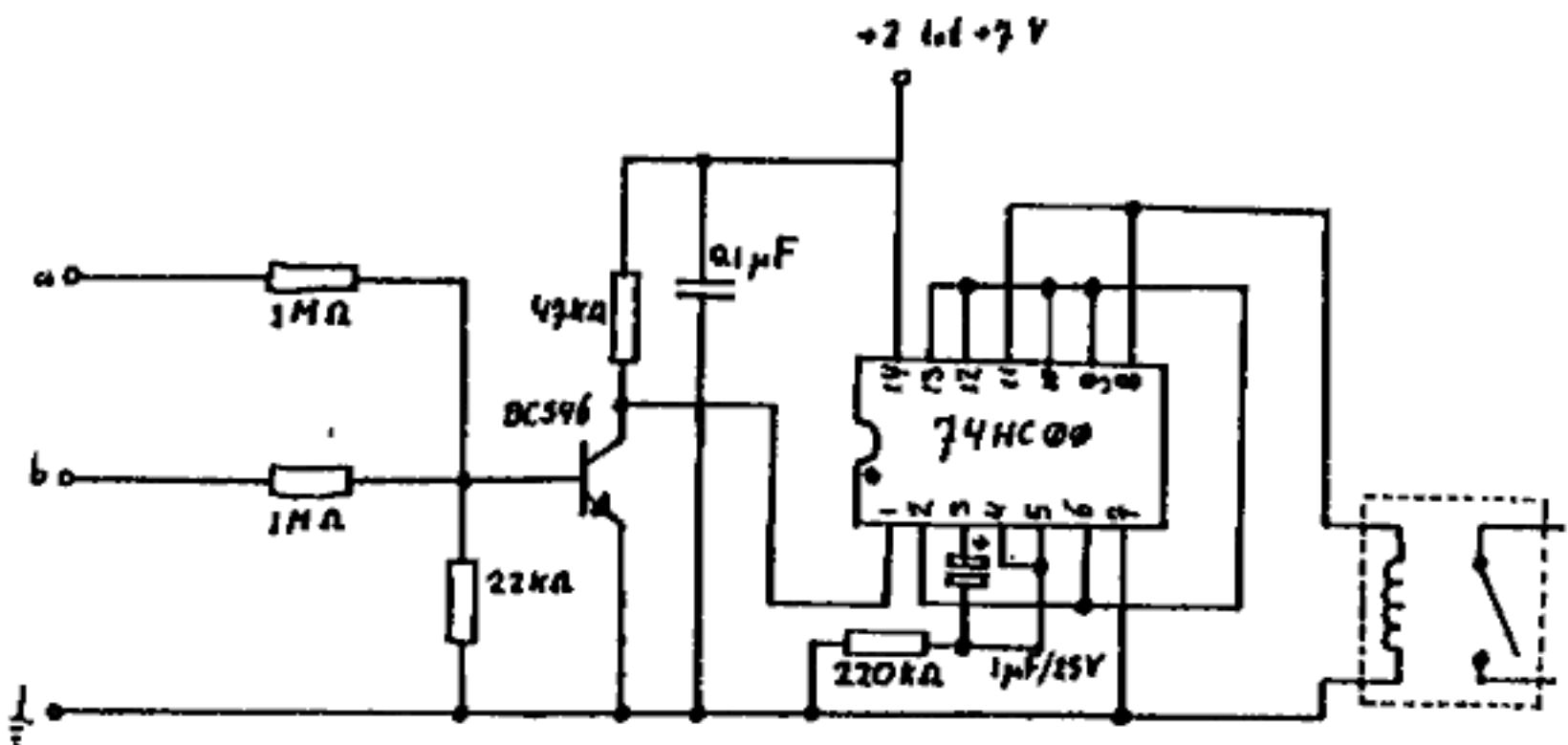
gens tussen en heb je dus geen aparte batterij nodig. Als je een 9 Volt rekenmachine hebt kun je een LED-je met z'n anode op de +9 en z'n kathode op de +2/+7 ingang van de schakeling hangen. Geeft ook geen leuk flitsje als de puls niet binnenkomt. Als je het zaakje op 2 of 3 volt laat lopen is het raadzaam even te checken of je relais bij die spanning nog wel schakelt.

Je kunt deze schakeling natuurlijk ook z'n eigen 9 Volt batterij geven. In dat geval houdt de schakeling met een 50 mA relais het ongeveer f36.000,- uit. Tegen die tijd kan een nieuw batterijtje er wel af.....

Vergeet de aarde niet aan te sluiten (zou eigenlijk op het penne-

tje linksonder in je telefoonstopkontakt moeten zitten maar de monteurs sluiten het nooit aan; het is de blanke draad in de PTT kabel). Verder is het leuk om te weten dat deze schakeling het niet doet als je op een moderne centrale bent aangesloten. De PTT levert in dat geval geen tel-puls totdat je er voor betaalt. Het leuke is dat mensen die niet weten dat ze op een oude centrale zijn aangesloten betalen voor een dienst die de burens gratis hebben! Affijn, eventueel aanvragen bij 004.

Als je er niet uit komt kun je een UUCP berichtje sturen naar billsf@well.UUCP (in het Engels). Je kunt een gelijkwaardige schakeling ook voor f190,25 door ome PTT thuis laten monteren.



Hack-Tic files

(Wat sommige mensen toch on-line laten slingeren). Bel voor meer informatie het Directoraat Kabel en Radio Verbindingen van PTT-Telecom.

PTT-TELECOM DATA-CENTRALE

ENTER CLASS

(0)

hello XXXX.brit

ENTER USER PASSWORD:

XXXXXX

HP3600 / MPE V G.0L.0L

AKTIEVE SYSTEEM

LIJST MET PROCEDURES

BR - BERICHTEN VOOR GEBRUIK
 EH - EINDE PROGRAMMA
 ?? - AFDrukKEN VAN DEZE L.
 RD - RAADPLEGEN EN OVERZ.
 ZR - ZOEKEN VAN ROUTER*

GB - GEGEVENS BLOK BINDELS
 GC - GEGEVENS CODELEIDINGEN
 GF - GEGEVENS FUNCTIELEIDINGEN
 GR - GESCHIEDEN ROUTERINGEN
 GS - GEGEVENS GROEPEN/SYSTEMEN
 GT - GEGEVENS TRANSMISSIE MEDIA
 KC - KOPPELING CODELEIDINGEN
 KF - KOPPELING FUNCTIELEIDINGEN
 KG - KOPPELING GROEPEN/SYSTEMEN
 KS - GEGEVENS LEIDINGEN/GROEPEN
 LV - L.I.C.

TABEL HP

HERSTELPRIORITEIT

HP	AA	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AB	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AC	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AD	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AE	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AF	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AG	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AH	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AI	NIET HERROUTEREN ZONDER TOESTEMMING CCSKD
HP	AL	RELATIEF
HP	AM	HERSTELPRIORITEIT IN VOORKEUR
HP	AN	CALAMITEITEN
HP	AO	VITAAL, HERSTEL HERGENTIE: 1
HP	AP	GEEN HERSTELPRIORITEIT
HP	AQ	NIG NIET BEKEND
HP	AR	NIET VIA STRAAL

TAST ONLY
 TAST THROUGH
 VITAAL

HP
 HP
 HP
 HP
 HP

DATANETNUMMERS EN LEIDINGNAMINGEN T.B.V. DNI

DNI	1170-141	GN-30/DN1
DNI	1170-206	GN-07/DN2
DNI	1170-207	GN-07/DN3
DNI	1170-251	GV-RT/DN4
DNI	1170-252	GV-RT/DN2
DNI	1170-253	GV-PT/DN7
"	"	254 GV

TABEL LS

LEIDINGSIGNALERING

LS
 LS
 LS
 LS
 LS
 LS
 LS
 LS
 LS
 LS

GEEN SIGNALERING
 HW) OP VSS (14KHZ) 3025 HZ CCITT Q21-A
 BASL. OV OP DC-KC (14KHZ) 3025 HZ CCITT Q21
 BASL. OV OP DC-KC (14KHZ) 3025 HZ CCITT Q21
 HW) OP VSS (6KHZ) 4300 HZ
 BASL. OV OP DC-KC (6KHZ) 4300 HZ
 BASL. OV OP DC-KC (6KHZ) 4300 HZ
 HW) OP VSS 2200 HZ CCITT Q8-A
 NI TEN HUIZE VAN ABONNEE 2200 HZ CCITT Q8A
 VOT OP DC-KC 2200 HZ CCITT Q8-A
 VOT TEN HUIZE VAN AB. EN/OP MIT BTFC 2300 HZ CCITT Q8
 VOT OP DC-KC 2300 HZ CCITT Q8E KIESRICHTING: A-->B
 VOT OP DC-KC 2300 HZ CCITT Q8E KIESRICHTING: B-->A
 VOT TEN HUIZE VAN ABONNEE 2200 HZ CCITT Q8E KIESRICHTING: A-->B
 VOT TEN HUIZE VAN ABONNEE 2200 HZ CCITT Q8E KIESRICHTING: B-->A
 VOT OP DC-KC 2200 HZ CCITT Q8E KIESRICHTING: A-->B
 VOT OP DC-KC 2200 HZ CCITT Q8E KIESRICHTING: B-->A

TOEV ASC
TOEV ATT
TOEV ITT
TOEV NCI

AMERICAN SATELLITE COMPANY
AMERICAN TELEGRAPH AND TELEPHONE
INTERNATIONAL TELEGRAPH AND TELEPHONE
1222222 (CARRIER IN USA)

(BASE G. 61. 6.)

STAD LEM
STAD LEMV
STAD LFDG
STAD LGB
STAD LGL

LEMELE NL
LEMERERVELE NL
LLAHFAIRPULLGWYNGYLLGGERYCHNYRHROBMLLLANTYILLJOGOGOOCH GB
LANGENKOM NL
LUIKSGESTEL NL

TABEL ET EXPLOITATIEVE TOEVOEGING

ET 153 SWIFT (HOOPDRIJTE PNL VIA GV1)
ET 154 SWIFT (HOOPDRIJTE PNL VIA GV2)
ET 303 NIEUW-APOSTOLISCHE KERK IN NEDERLAND
ET 360 KOPPELKEK KERKTELEFONNETTEN
ET 364 LUIDSPREKERNET TWEEDE KAMER DER STATEN GENERAAL
ET 371 DATA-NET F-16 PROJECT
ET 379 NATIONALE LEN BEWAKING BEZ-GOCH

BEHAGA DE REGISTRATIE INTERLOK EN INTERN. TRANSMISSIEMIDDELEN
COMPUTER UITWIJK CENTRUM TE LLS
INTELSAT BUSINESS SYSTEM
POSTBANK TE ASD
TIJDMELDING
DATANET T.B.V. DCC DE LIER EA
FACS NET T.B.V. KON. MARINE EA
IMN ZOETERMEER DATANET

ET CUC
ET IRS
ET POST
ET RCC
ET TMD

GD++RT2 60.2 DRRV G4V
60.7 DRRV G4A /000/10 ID (3)
60.8 DRRV G5V /000/04 ID (4)
60.10 DRRV G5V /000/03 ID (4)
60.12 DRRV G5V /000/06 ID (5)
RT2++ACHN 60.1 DRRV NCV /000/08 ID (5)
/001/02 ID (3-4-5)

ET 784 RIJKSBELASTINGEN T2 ROTTERDAM
ET 790 RIJKSBELASTINGEN TE EINDHOVEN
ET 801 VERENIGDE DEOP PARKIEKEN TE ETEN LEUR
ET 800 VERRE-MEETHEI LICHTVERONTFEINIGING Z-LIMBURG
ET 804 ALARMNET LIPS CHUUS ELECTRONIC
ET 874 ALARMNET DE POSTCHEQUE & GIBODIENST
ET ACS ALARMNET PTT DRRV LAAN EN MAN
ET KSON AUTOMATIC SWITCH COMMUNICATION NETWORK (ASCHN)
ET ATP1 AUTO TELEFON 1
ET ATP2 AUTO TELEFON 2
ET ATME AUTOMATIC TEST MESSURING EQUIPMENT
ET AUNS AUTOMATIC VOICE NETWORK SWITCHING (AUTOVON)
ET BJC BANK GINA CENTRALE BV
ET BPT

ET 2000
ET 2001
ET 2100
ET 2101
ET 2102
ET 2103
ET 2104
ET 2105

ATM INTERNATIONAL
ATM INTERNATIONAL MFC
ATM INTERNATIONAL MFC FDM
ATM INTERNATIONAL MFC NIET TELLERS
ATM INTERNATIONAL MFC TELLERS

ADERS VOOR DIGITAL VERKEER

TABEL EA
ETORNAAR VAN DE APPARAAT
CYFTELE AANVULLENDE VERIEDIJDING
DIJESTUKAAT KABEL- EN KALIVERBODINGEN
MINISTERIE VAN DEFENSIE
MEKEN KAN HENDEN

Een introductie op VM/CMS

Of je trekt de stekker er uit

Vandaag de dag is de helft van alle mainframes afkomstig van IBM. De IBM-mainframes worden vooral gebruikt bij de verzekeringen en banken. Om een of andere reden zijn de systemen van Big Blue niet erg in trek bij hackers. Ergens is het ook wel logisch, want het operating systeem van IBM (VM/CMS dus) is ontzettend complex. Ook is het zo dat elk systeem een net even iets andere versie heeft van VM/CMS. VM/CMS kan namelijk helemaal aan de wensen van de klant worden aangepast. En je raad het natuurlijk al, documentatie van al die aanpassingen is er nauwelijks. Vergeleken met de andere systemen van IBM is VM/CMS makkelijk maar vergeleken met bv. UNIX of VMS is het moeilijk te leren en omslachtig.

Afkortingen

Hieronder volgt een lijst met afkortingen die je nodig zult hebben om dit artikel een beetje te begrijpen. Ook zul je ze regelmatig terugvinden in IBM-computers.

VM/SP: Virtual Machine / System Product
CP: Control Program
CMS: Conversational Monitoring System
HPO: High Performance Option
VSE: Virtual Storage Extended
MVS: Multiple Virtual Storage
TSO: Time Sharing Option

JES: Job Entry System
CICS: Customer Information Control System
VSAM: Virtual Storage Access Method
VTAM: Virtual Telecommunications Access Method
IX: Interactive Executive
IPL: Initial Program Load
IVP: Installation Verification Program
RSCS: Remote Spooling Communications Subsystem
EREP: Environmental Recording Editing and Printing
SNA: Systems Network Architecture
NCCF: Network Communications Control Facility
REXX: Restructured Extended Executive Language
VTOC: Volume Table of Contents
DOCS: Display Operator Console System
JCL: Job Control Language
ACF: Advanced Communications Functions
SQL/DS: Structured Query Language / Data System
DBA: Data Base Administrator
GCS: Group Control System
SCP: System Control Program
FDP: Field Development Program
CNA: Communications Network Application
POF: Programmable Operator Facility
PSW: Program Status Word
SSCP: Subsystem Services Control Point
IPCS: Interactive Problem Control System
DCSS: Discontiguous Shared Segments
VMCF: Virtual Machine Comm. Facility
AP: Attached Processor
MP: Multi-Processor
R/O: Read/Only
W/O: Write/Only
I/O: Input/Output

Inloggen

Als je inlogt op een oudere versie van CMS dan krijg je de boodschap "VM/370 ONLINE". Eigenlijk klopt dit niet want een VM/CMS draait nauwelijks meer op een 370 machine. Tegenwoordig draaien ze allemaal op the 43XX en 30XX series. De allernieuwste versies geven een lijstje van mogelijkheden:

- LOGON userid (b.v.: LOGON VMUSER1)
- MSG userid message (b.v.: MSG VMUSER3 HELLO)
- LOGOFF

Dit menuutje kan van systeem tot systeem verschillen, want, zoals al gezegd, de systeem manager kan ontzettend veel veranderen en toevoegen. Drie andere boodschappen voor het inloggen kunnen zijn "Ready to Host", "Press break key to begin session" of "Invalid Switch Characters". Als je de laatste boodschap tegenkomt zit je waarschijnlijk in een poortselector van IBM. Je moet dan eerst nog kiezen naar welk systeem je wilt gaan. "VM" wordt meestal gebruikt voor VM/CMS, "TSO" voor MVS/TSO systemen. Als dat niet werkt kan je ook "LOGON" of "LOGON VM" proberen. LOGON kun je afkorten tot "L". Een userid is meestal 1 tot 8 tekens lang. Elk teken mag gebruikt worden. Een password moet meestal ook 1 tot 8 tekens zijn. Sommige systemen hebben andere voorwaarden voor het aantal tekens, daar moeten

passwords bijvoorbeeld minimaal 6 tekens zijn. In sommige systemen mag je het password niet op dezelfde regel zetten als de username. Dus niet ".L USERNAME PASSW ", maar ".L USERNAME". Het systeem vraagt daarna vanzelf om het password. Het systeem maakt geen onderscheid tussen hoofd en kleine letters.

Noipl

NOIPL is een zgn. "login qualifier", dwz. dat het iets extra meegeeft tijdens het inloggen. De enige login qualifier die VM/CMS kent is NOIPL. IPL zorgt ervoor dat een programmaatje wordt gerund. Dat programmaatje is te vergelijken met de *autoexec.bat* bij pc's. Het zorgt er dus voor dat automatisch bepaalde programma's worden gestart. De bedoeling van dit geheel kan zijn er voor te zorgen dat niemand op "command level" kan komen. NOIPL zorgt er dus voor dat je niet automatisch in een programma wordt gegooid. Helaas werkt dit niet altijd.

Foutmeldingen

De grootste blunder van VM/CMS zit in de foutmelding tijdens het inloggen. Als je namelijk een username hebt geprobeerd en die werkt niet, dan geeft het systeem dat mooi aan met de melding "Userid not in CP directory". Als je een goede username hebt ingetypt maar

een verkeerd password dan krijg je de melding "Logon unsuccessful - incorrect password". Oudere systemen zeggen "Password incorrect - reinitiate logon procedure".

Standaardlogins

Zoals altijd bestaan er ook op dit systeem standaardlogins, ze werken hier zelfs veel vaker dan op andere systemen. Hier volgen er een paar:

OPERATOR, SMART,
CMSBATCH, VTAM, AUTO-
LOG1, EREP, OPERATNS, RSCS,
VMTEST, CMS, VMUTIL, SNA,
MAINT

Je raad het al, in al deze gevallen is het password gelijk aan de username.

Dial

Het DIAL commando is er om allerlei soorten lijnen aan elkaar te verbinden. De namen of nummers van de lijnen zijn niet via een commando op te roepen, maar staan vaak in files. De syntax is simpel, gewoon "DIAL *adres lijnumnummer*". Soms moet het lijn-nummer gegeven worden, omdat die computer niet zelf kan ruiken welke lijnen vrij zijn voor dat gebruik. Iets slimmere systemen doen dat automatisch.

Op IBM-systemen komt het heel vaak voor dat er meerdere operating-systemen draaien op één enkel systeem. Ze kunnen naast elkaar maar ook onder elkaar draaien. Een

paar operating-systemen zijn VM/CMS, MVS/TSO, DOS/VSE, OS/VS1, MUSIC, JES en IX/370. IX/370 is IBM's versie van UNIX.

Het is zelfs mogelijk userid's te dialen. Dit moet soms zelfs om andere systemen binnen te kunnen komen. Om je verbinding te beindigen typ je gewoon RESET in.

Message

Uiteraard kun je ook je sociale kontakten op peil houden met VM/CMS. Het commando hiervoor is MSG. De syntax is: MSG *userid boodschap*. Een sterretje ipv een userid zorgt ervoor dat er een bericht naar jezelf wordt gestuurd. Dit is makkelijk als je niet weet welke user je bent.

Logoff

Uitloggen doet je met het commando LOGOFF, afgekort LOG. Je krijgt tijdens het uitloggen een statistiekje met wat info over je sessie. Met LOG HOLD kun je uitloggen, maar heb je nog de mogelijkheid om, zonder het systeem opnieuw te bellen, weer in te loggen.

Beveiligings-software

Omdat VM/CMS niet bepaald lekvrij is, heeft men wat beveiligingspakketjes gemaakt om het een klein beetje dicht te stoppen. De twee meest gebruikte pakketten zijn VMSECURE en ACF2. TOP SECRET en RACF komen minder

vaak voor. Hoe kom je er nou achter of VMSECURE of ACF2 aanwezig is? Simpel. Als VMSECURE draait moet er een userid VMSECURE bestaan. Voor ACF2 ligt het iets anders. Als je een verkeerd password hebt ingetypt, moet het systeem reageren met:

- ACFV1012 PASSWORD NOT
MATCHED

- ACFV0044 ACF2 ENTER
PASSWORD

Enkele dingen die deze software kan zijn: laatste inlog-tijd/datum en password-vervaldatum vastleggen, regels geven voor het formaat van een password, userid's of terminals uitschakelen als hackers geprobeerd hebben ze te hacken, file-veiligheid opvoeren en laten zien of en hoe vaak een verkeerd password is gebruikt.

Ingelogd

Nadat je hebt ingelogd zie je waarschijnlijk iets over het scherm flitsen dat op het volgende lijkt.

```
DASD 190 LINKED R/O;R/W
BY MAINT; R/O BY 030
USERS
LOGMSG 10:40:25 EST FRI-
DAY 05/22/87
WELCOME TO MISCELLANEOUS
COMPUTER SERVICES
VM1
SYSTEM WILL BE DOWN FROM
10:00 TO 10:30 EST SUN-
DAY MAY 24, 1987
```

```
Logon at 13:22:59 EST
FRIDAY 05/22/87
VM/SP REL 4 04/20/86
11:33
```

```
R;T=0.01/0.01 13:23:10
```

Regel 1: DASD 190 laat zien dat de disk op lijn 190 zit en dat jij daar R/O, MAINT(enance) R/W, en de overige 30 gebruikers R/O rechten hebben

Regel 2: De login-message is gemaakt om 10:40 op 22 mei 1987.

Regel 3-5: Een berichtje dat elke gebruiker van de systeembeheerder krijgt (the message of the day).

Regel 6: De eigenlijke tijd en datum

Regel 7: De 4e Release van VM/SP die genstalleerd is op 20 april

Regel 8: R betekent Ready, de computer is dus klaar voor input. T=0.01/0.01 betekent dat de computer over de laatste opdracht één honderdste seconde heeft gedaan. De tijd daarna is de tijd op dat moment.

Query

Met het commando QUERY kan je kleine beetjes informatie opvragen. Vergelijk het met het SHOW-commando op VMS.

.Q NAMES geeft een lijst van userid's die op het systeem zijn geweest. Deze lijst bevat honderden userid's, dus als je op zoek bent naar

een bepaalde userid dan kan daarnaar zoeken dmv .Q NAMES.

.Q USERS geeft aan hoeveel users ingelogd zijn via een lokale terminal, hoeveel verbonden zijn met een multi-user systeem en hoeveel ingelogd zijn via een SNA netwerk.

.Q LOGMSG laat je het loginbericht nog een keer lezen.

.Q CMSLEVEL vertelt je welke versie dit is van VM/CMS Er zijn nog veel meer onderwerpen die je kan query-en. Voor een volledige lijst zie de help-file (aan te roepen met HELP HELP)

Oh ja: als je een foutmelding krijgt maar je snapt niet waarom, typ dan .HELP DMS000000 of DMK000000 in. Je krijgt dan een volledige uitleg over het hoe, wat en waar van je fout.

De rest van dit artikel volgt in de volgende Tic.

Taco

Bewerking van een artikel uit 2600-Magazine van Lex Luthor and The Legion of Hackers.

ANI in Nederland

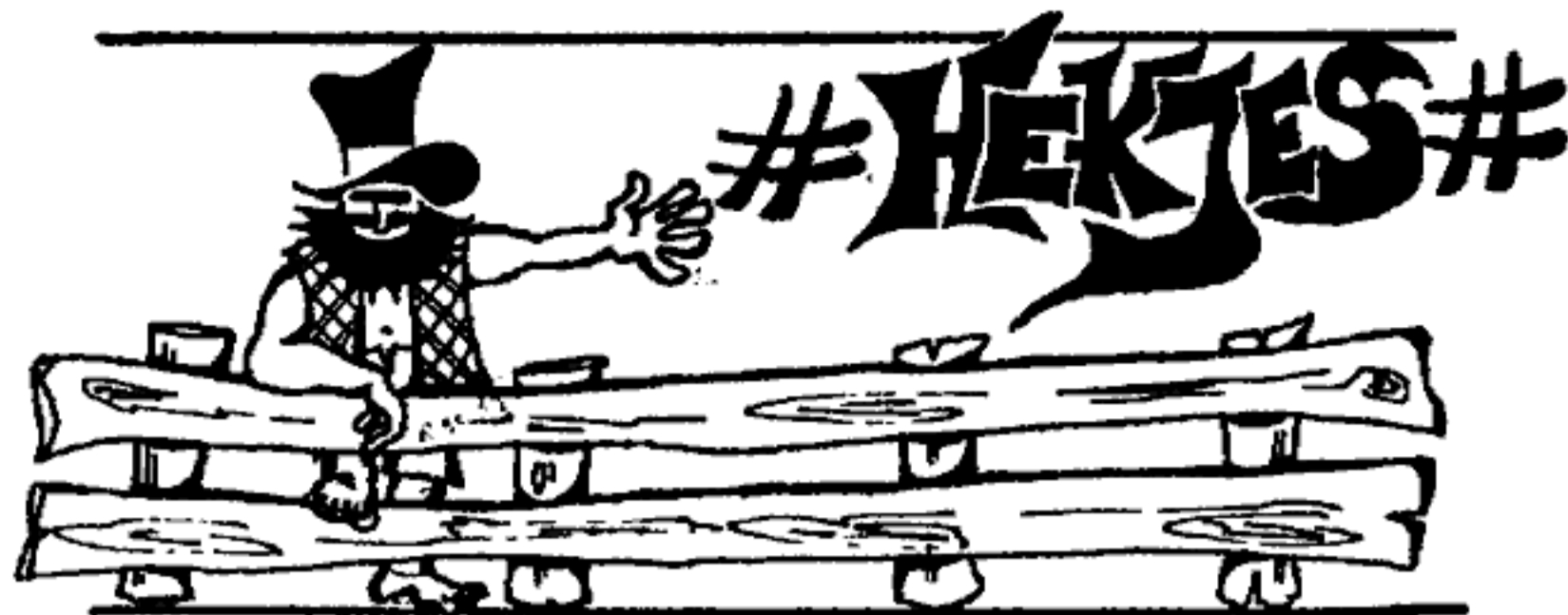
Wij kregen van iemand het nummer 085-430652. Toen we dit nummer belden nam een modem op, het gaf een connect op 1200 of 2400 baud full-duplex en hing vervolgens na 5 seconden weer op, wat we ook intikten.

Twintig seconden later rinkelde de lijn waarmee we dit nummer hebben gebeld. Het was een PTT functionaris die ons verzocht om ONMIDDELIJK op te houden met 'hacken'. Toen we hem eraan herinnerden dat iedereen in principe vrij is om te draaien wat hij wil kregen we een nors; "Ja, en als U dit nummer nog een keer belt stellen we Uw telefoonaansluiting buiten dienst." Klak, tuut-tuut-tuut.

Deze man beschikte over ANI, Automatic Number Identification. Hij had, in andere woorden, een schermje waarop hij ons nummer kon aflezen. Dit lijkt alleen te werken als de opbeller op een tamelijk moderne centrale is aangesloten. Hoewel je het nog niet kunt bestellen kun je er van uitgaan dat de PTT het levert aan "goede vrienden".

Bel dus nooit direct naar computers die je hackt, zeker niet als je op een moderne centrale bent aangesloten en helemaal niet als het doelwit eigendom van de PTT is!

Welkom in de negentiger jaren. Deze techniek gaat de manier waarop wij van de telefoon gebruik maken drastisch veranderen.



Hier adverteren is gratis. Stuur je advertentie op naar Hack-Tic Hekjes, Postbus 22953, 1100 DL Amsterdam. Adverteren onder nummer is mogelijk, de redactie behoudt zich het recht voor advertenties te weigeren.

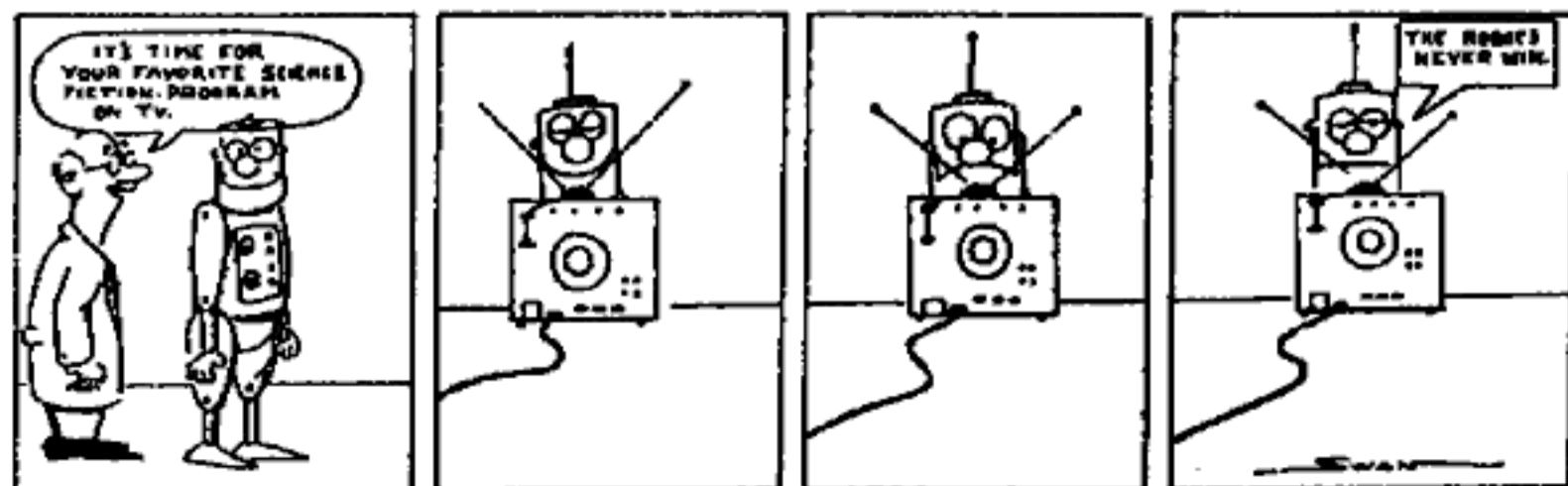
Ik zoek brief-vrienden, om brief (of e-mail) contacten met landgenoten te hebben. Mijn naam is Jan, ik kom uit Rotterdam (Overschie) en ik woon nu sinds drie jaar in Berlijn (WEST). Na al die tijd heb ik geen zin meer, alleen nog in het Duits (vreselijke taal, keelziekte) te communiceren. De reden, waarom ik toch hier woon, is omdat ik hier een informatica opleiding volg. Ik werk op een PC/XT onder MS-DOS {good adventure :-)}, dus voldoende voor de communicatie... Other skills: ik ben in (para-)psychologie geïnteresseerd. Schrijf naar: remke@netmbx.uucp (UUCP-mail) of Jan K. Remke, Postfach 304041, D-1000 Berlin/W.30, EG (de ouderwelse methode).

Hacker zoekt advocaat met ervaring / op zoek naar ervaring met credit card fraude en telefoonzaken. Reacties onder #8/1

Heb je problemen of heb je stress gekregen van het hacken. Neem dan wat ontspanning en log eens in bij The Hitch-Hiker BBS. Your Sysops: The Blues Brothers. 070-3636330 300/1200/2400 8n1

Wie heeft er voor mij een kleine DTMF toonkiezer (tegen vergoeding) of het schema ervan. AUB een briefje naar: Eric, Kamgras 17, 2804 NP Gouda.

We hebben beslag weten te leggen op een kopie van de 'teruggelaste' source-code van de Internet-worm. Dit in C geschreven verhaal is voor abonnees verkrijgbaar door een aan jezelf geadresseerde envelop aan ons op te sturen die 20 of 30 velletjes A4 kan bevatten en die voor de zekerheid (we hebben nog wat meer leuk spul) met f2,25 gefrankeerd is. Opsturen aan Hack-Tic.



Magneetkaarten

Contant geld is out, plastic-money is in! Het zal er in de nineties om gaan wie de beste kaarten in handen heeft. Hack-Tic helpt hackers aan een vijfde aas om mee te kunnen spelen in het grote magneetkaartenspel.

door Dr. Mabuse

Iedereen heeft wel eens staan kijken naar magneetkaartjes en zich afgevraagd wat er precies op zou staan. Wie het durfde heeft zelfs geïnformeerd naar magneetkaart lezer/schrijvers, alleen maar om na het horen van de prijs weer met andere dingen bezig te gaan. En dat terwijl je zo graag de bits en bytes van de kaart zou willen plukken.

Hack-Tic brengt nu een aantal zelfbouw-projecten. Om gewoon eens met de techniek te spelen is er voor een paar tientjes de magneetkaartcopier. Dit apparaat leest van de ene magneetkop en beschrijft met die informatie tegelijkertijd een andere kaart. Voor de gevorderde electronica-hobbyist is er de magneetkaart lezer/schrijver. Iedereen die weet wat TTL is en die zoiets ook middels een soldeerbout uit zijn/haar computer kan bevrijden kan met deze schema's een magneetkaart lezer/schrijver op de computer aansluiten.

Veel belangrijker dan alle elektronische hokus-pokus is het om eerst te zien wat er werkelijk op de magneetstrip staat. Hiervoor het eerste beetje techniek in dit artikel.

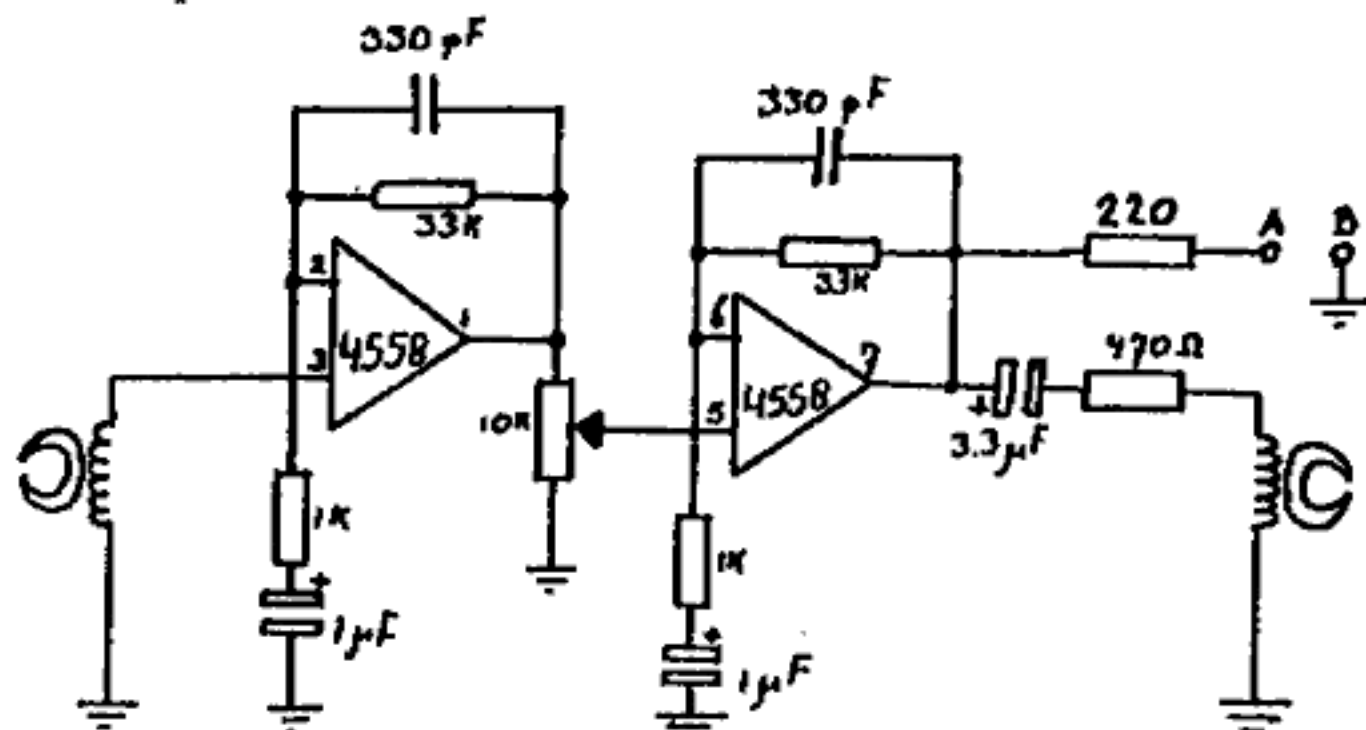
De informatie op de meeste kaarten is binair opgeslagen. Deze enen en nullen zijn weggeschreven door de richting van het schrijvende magneetveld te variëren. Om te zien wat er op de kaart staat strooi je een beetje ijzervijlsel op de magneetstrip en tik je een paar keer zachtjes met de rand van de kaart op tafel (wel even een papiertje er onder; het heeft genoeg moeite gekost om al dat ijzer te vijlen). Presto: daar staat je magnetische informatie, duidelijk zichtbaar voor het blote oog. Sommige kaartjes hebben zulke grote bits dat je met een gemagnetiseerd scheermes (!) de informatie zou kunnen veranderen (Parijse metrokaartjes zijn een goed voorbeeld). Op andere kaartjes staan de bits zo dicht tegen elkaar aan dat je alleen een gemagnetiseerde 'balk' zult zien.

Voor het opslaan van informatie op magneetkaartjes zijn internationaal een paar standaards vastgelegd. Zo zijn er de 'tracks' (sporen) 1, 2 en 3, zoals vastgelegd door de International Standards Organisation. Veel fabrikanten gebruiken echter andere plaatsen en coderingen om

de kaarten te beschrijven. Alleen ijzervijzel geeft uitsluitel.

Het eerste zelfbouwproject, zoals gezegd, is een copier voor de magnetische informatie op de kaart. Dit betekent dat het niets uitmaakt op wat voor manier de informatie gecodeerd is. Alles wat je moet weten is de plaats en de breedte van

het track met de informatie die je wilt dupliceren. Zolang de schrijfkop van je copier een breder spoor schrijft dan het spoor dat je wilt copieren is er waarschijnlijk niets aan de hand. (Is het spoor smaller dan is het waarschijnlijk handiger om een nieuwe schrijfkop te zoeken.) Hier is het schema.



De Magneetkaart-copier

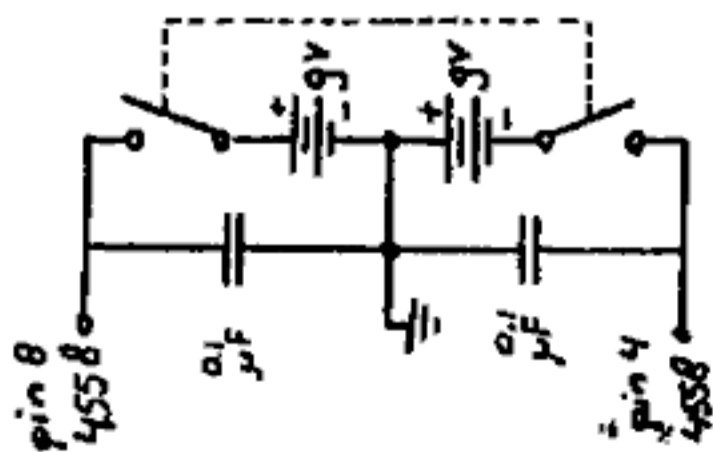
Links in het schema is de leeskop. Hiervoor kun je elke magneetkop gebruiken. Als de gekozen kop breder is dan het spoor dat je wilt dupliceren zul je extra ruis oppikken. Is de kop al te smal dan wordt het signaal misschien te zwak. Veel experimenteren (en dus taperecorders slopen of dumpzaken aflopen) is hier geboden. De schrijfkop (rechts in het schema) liefst zo breed mogelijk kiezen, tenzij je meer dan twee smalle sporen naast elkaar wilt schrijven.

Tussen de punten A en B kun je een koptelefoon (de twee luidsprekers van een walkmankoptelefoon in serie bijvoorbeeld) zetten. Als je de leeskop langs de te lezen informatie haalt zul je het soort geluid horen dat de 'oudere' hobbyisten nog wel kennen van hun data-cassettes. Nu zul je nog een manier moeten vinden om de lees- en de schrijfkop op hetzelfde moment langs de kaarten te halen. De truk is om beide koppen op een eindje hout te monteren, ongeveer 10 cm. uit elkaar. Vervolgens gebruik je een ander stuk hout waar je met lijmklemmen o.i.d. de kaartjes

(orgineel en kopie) tegenaan klemt. Dit tweede stuk hout beweeg je langs het stuk met de koppen en presto.

Er zijn echter kaartjes waarbij de informatie niet onder een rechte hoek wordt geschreven. Als je d.m.v. het ijzervijlsel zoiets ziet zul je dus de hoek waaronder de koppen zijn gemonteerd moeten veranderen. Een truukje om de koppen af te stellen is de 220Ω weerstand voor de koptelefoon te vervangen door een $0.1\ \mu\text{F}$ condensator en dan te luisteren welke stand van de kop de meeste hoge tonen geeft.

Schrijven doe je alleen naar een kaart die je van te voren met een wisselstroommagneet of demagnetisator hebt gewist! Om te controleren of je een kans hebt dat de gemaakte kopie werkt kun je ernaar luisteren door de aangehechte koptelefoon. Het menselijk gehoor blijkt een hele aardige meter te zijn voor de kwaliteit van de kopie. Nog een laatste woord tenslotte over de voeding: de pennen 4 en 8 van de chip (2 OPAMPS in 1 chip) zijn voor de negatieve en positieve voedingsspanning (onder).



De lezer/schrijver

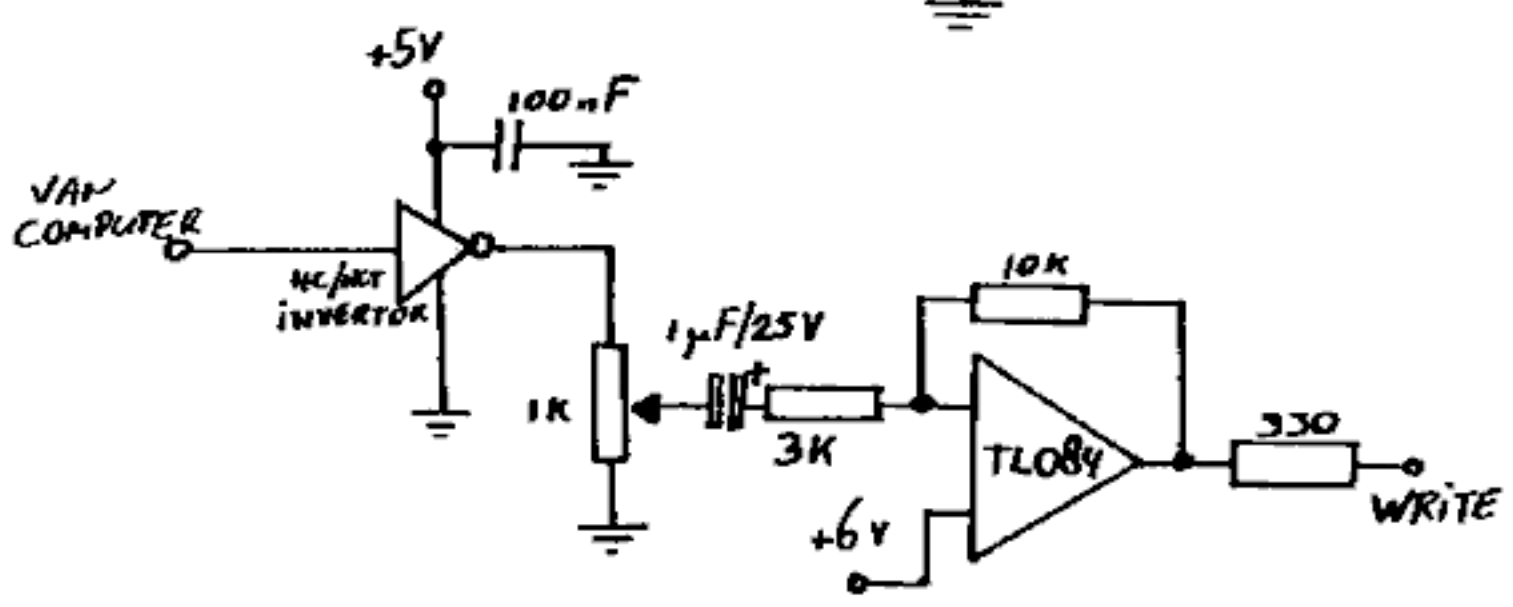
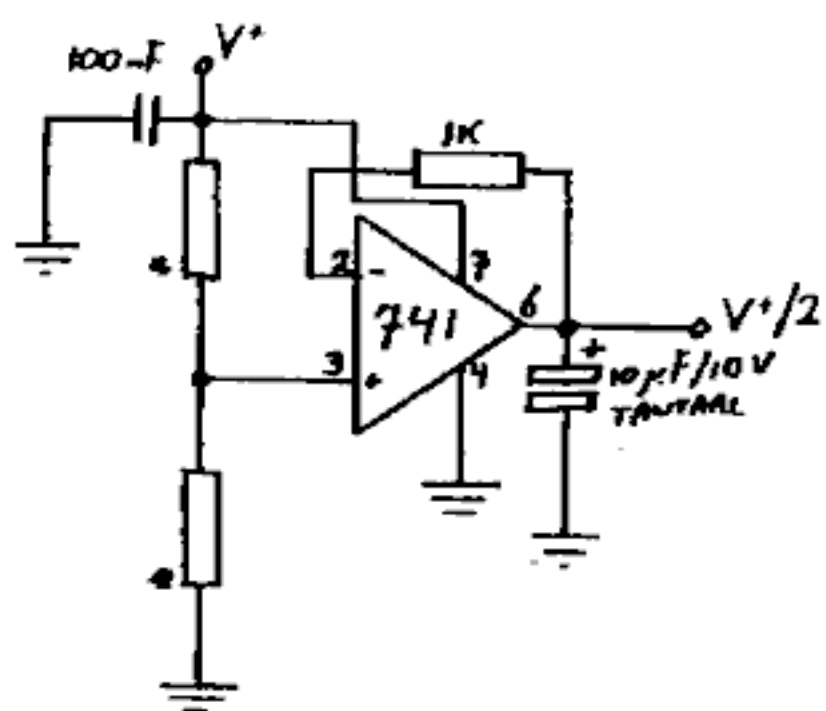
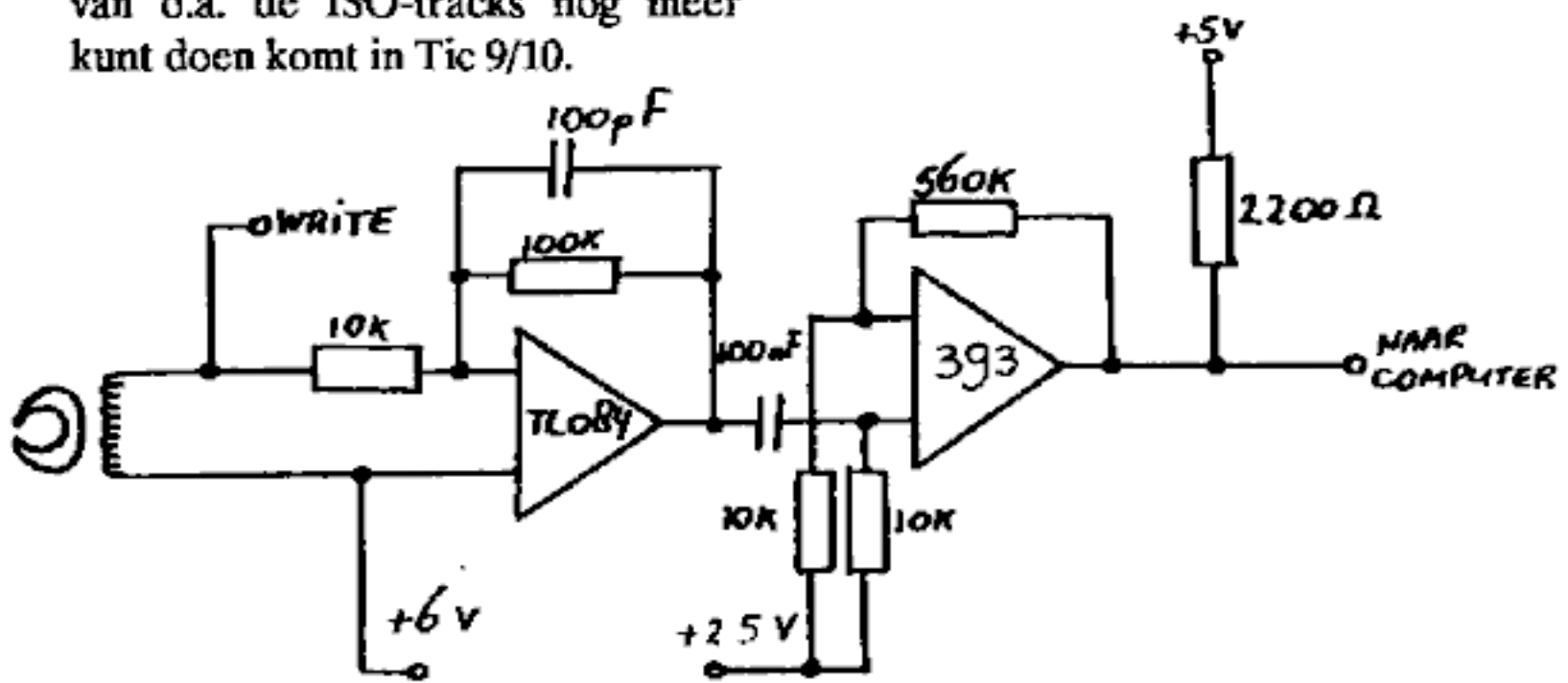
Deze schakeling leest en schrijft van en naar dezelfde kop. Als je met deze schakeling iets wilt schrijven zul je dus wel een mechanisme moeten hebben dat deze kop een zeer constante snelheid t.o.v. de kaart kan geven. Eigenlijk alleen het mechanisme van een oude magneetkaart lezer/schrijver komt hiervoor in aanmerking, tenzij je werkelijk een genie bent met draaibanken en andere fijne mechanica.

De gebruikte OPAMPS hebben behoefte aan een positieve en negatieve voedingsspanning, maar door middel van een actieve spanningsdeler (waarvan een schema is bijgevoegd) kunnen we de hele hap vanaf $+12\text{V}$ voedingsspanning laten lopen. De actieve spanningsdeler komt in de lezer schrijver 2 maal voor. Allereerst om $+12$ te splitsen naar $+6\text{V}$. Hiervoor zet je $6.8\text{ k}\Omega$ weerstanden op de met een sterretje gemarkeerde plaatsen in de deler. De tweede deler gebruikt $3.3\text{ k}\Omega$ weerstanden op de plaatsen met een sterretje om van 5 Volt (uit de computer?) 2.5 Volt te maken.

Het beste is om een relais te plaatsen tussen het write signaal van de schrijf-schakeling en de kop (dit om niet te storen bij het lezen).

Nu nog een interface die de motor van je lees/schrijfunit kan besturen en die bitjes kan uitwisselen met de zojuist beschreven schakelingen. Je kunt dan bitcopies maken van de

informatie. Wat je met de informatie van o.a. de ISO-tracks nog meer kunt doen komt in Tic 9/10.



De Hack-Tic gids voor electro-technici

1. Electriciteit wordt gemaakt in een fabriek, waar het in kabels wordt opgeslagen. Daarom zijn de kabels zo lang. Soms worden ze op haspels gewonden om meer kiloWatt te krijgen.

2. Sommige soorten electriciteit maken geen gebruik van kabels, zoals bij onweer en in draagbare radiotoestellen. Deze soorten worden niet opgewekt, maar worden in de lucht aangetroffen.

3. Electriciteit maakt een laag zoemend geluid. Dit kan worden gebruikt voor deurbellen, telefoneren en elektrische orgels. Men kan er ook de buurman mee pesten, hoewel dat enige studie vereist.

4. Electriciteit moet geaard worden, behalve bij vliegtuigen.

5. Electriciteit wordt gemaakt uit twee ingrediënten, negatief en positief. Eén ingrediënt heeft de voorkeur voor rode draden, de andere voor zwarte. Wanneer deze draden elkaar ontmoeten in wat een stekker wordt genoemd, komen de twee bij elkaar en vormen electriciteit.

6. Electriciteit kan in batterijen worden opgeslagen. Grote batterijen bevatten niet altijd meer dan kleine. In grote batterijen wordt de electriciteit met een schop aangebracht, in kleine transistorbatterijen met een pincet.

7. Niet nieuwsgierige mensen draaien aan een schakelaar en denken er verder nooit over na. Ik heb daar nooit genoeg mee genomen. Ik wil weten wat er achter steekt. Daarom kan ik U het volgende vertellen: Een lichtsakelaar is zoiets als een klem die de draad zo hard dichtknijpt dat de electriciteit er niet doorheen kan. Als de schakelaar wordt bediend, verlicht men deze druk en de electriciteit stroomt naar de lamp waar een stukje gloeidraad een soort strip-tease uitvoert. In elk geval is de draad daar naakt. Hier zien we dan ook de pure electriciteit in de vorm van een vonk, welke versterkt wordt door het bolvormige glas, dat als een vergrootglas werkt.

8. Waarom hebben lampen een beperkte levensduur? Omdat de hitte de aanwezige zuurstof in water verandert. Op den duur raakt de lamp vol water en dooft uit.

9. Het heeft me altijd verbaast dat de industrie, die zo vooruitstrevend is op alle gebied (uitvinding van gekleurde electriciteit voor TV en verkeerslichten, uitvinding van negatieve electriciteit voor koelkasten) toch 200 jaar nadat James Watt de elektrische ketel uitvond, nog steeds te dun zekeringsdraad maakt.

10. De industrie maakt zeker goed stevig draad dat onder andere in de kippe-industrie (gaasvormig) wordt gebruikt. Dat is beter dan de rommel die de electriciens verkopen, hoewel die ook moeten leven.

11. Ik heb nu een zekeringskast vol kippegaas, die al zes maanden lang geen enkele moeilijkheid meer oplevert. Zelfs niet toen de meter uit elkaar barstte omdat de centrale er te veel electriciteit in stopte.

12. Waarom zekeringen? Een transistor die je afzekert beschermt zijn zekering door altijd als eerste de geest te geven.

13. Ik zit nog met de automatische toaster. Pop, een gaar toastje. Hoe weet die electriciteit dat ie gaar is? Nou ja, je kunt niet alles weten.

14. Ik zou nog enkele logische antwoorden kunnen geven, maar... Het licht gaat uit. Zeker een haspel op de centrale leeggelopen.