

Spion op eigen netwerk

Zo houdt u alles
in de gaten



Illustratie: SevenHeaven

Vlak voor de zomer besloten de populairste internetcommunity's de chatmogelijkheden te beperken, voornamelijk omdat er seks gesprekken tussen volwassen en kleine kinderen plaatsvonden. Er zijn gelukkig programma's om al het computerverkeer in de gaten te houden. Betrap die ontrouwe partner, voorkom sexchats en zet die luie medewerkers aan het werk.

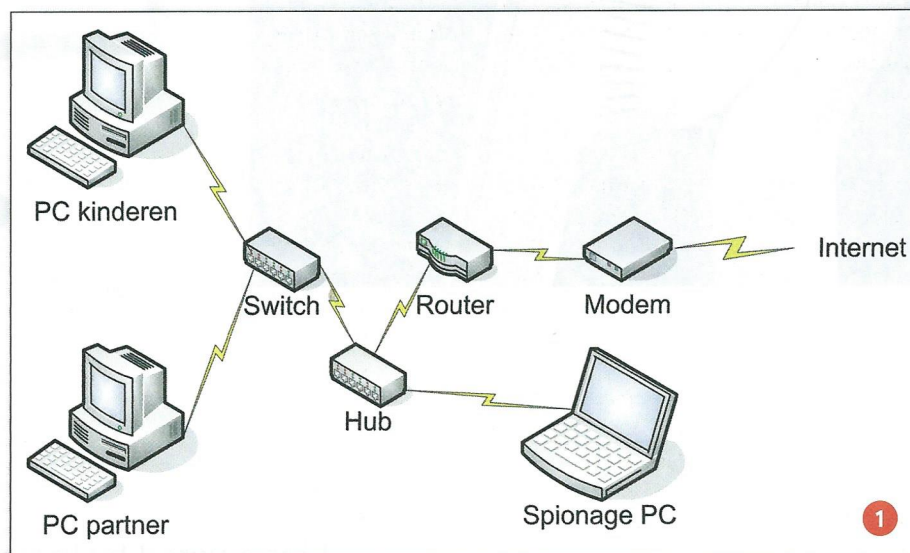
Steeds meer gezinnen beschikken over meer dan één pc. Handig wanneer iedereen ineens tegelijk op de computer wil. De keerzijde is dat u geen enkel idee meer hebt wat er op de laptop op zolder nu precies gebeurt. Weet u bijvoorbeeld wat uw familieleden op het internet uitspoken? Wat gebeurt er op die laptop op de kamer van uw kind? Met wie zit uw partner de hele avond te chatten? Welke websites bezoeken ze en is het wel allemaal even onschuldig?

De oplossing is even doeltreffend als simpel:

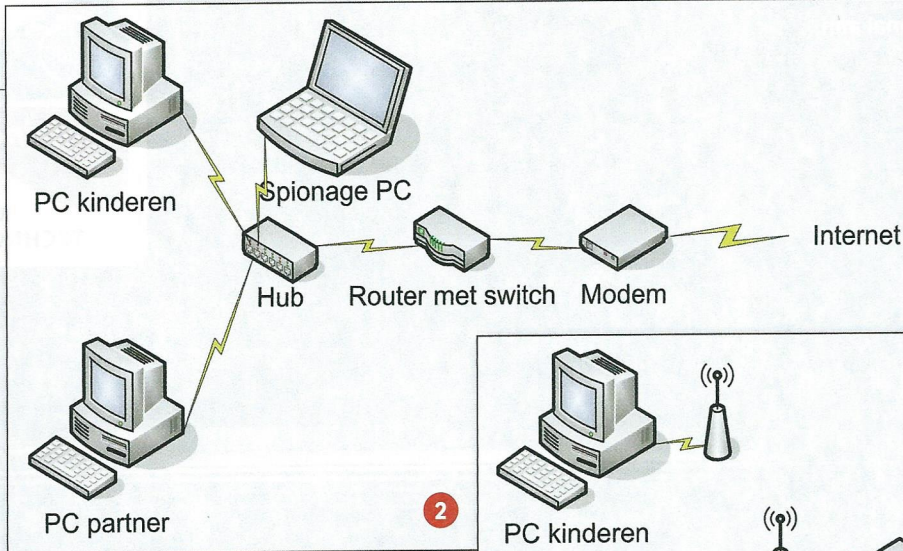
luister al het netwerkverkeer af met speciale programma's en u krijgt alle wachtwoorden, online gesprekken, e-mails en bezochte websites op een presenteerblaadje aangereikt. Ook als u over één losstaande pc beschikt, zijn er krachtige programma's om te ontdekken wat anderen uitspoken als u er niet bent. In dit artikel worden zowel de

WAARSCHUWING

In dit artikel worden krachtige programma's behandeld om het computergedrag van uw familie of medewerkers in kaart te brengen. Stel u zelf de vraag hoe u het zou vinden als anderen volledig inzicht hebben in uw surfgedrag, wachtwoorden en online gesprekken. Iedereen heeft recht op privacy, ook online. Ga eerst het gesprek aan met kinderen, partners of medewerkers voordat u deze programma's inzet. Bedenk dat computervredebreuk strafbaar is. Ga dus niet zomaar met achterhaalde wachtwoorden aan de slag. Alle gesprekken, e-mailadressen en wachtwoorden zijn speciaal voor dit artikel gemaakt. Ze dienen alleen ter illustratie van de mogelijkheden.



1



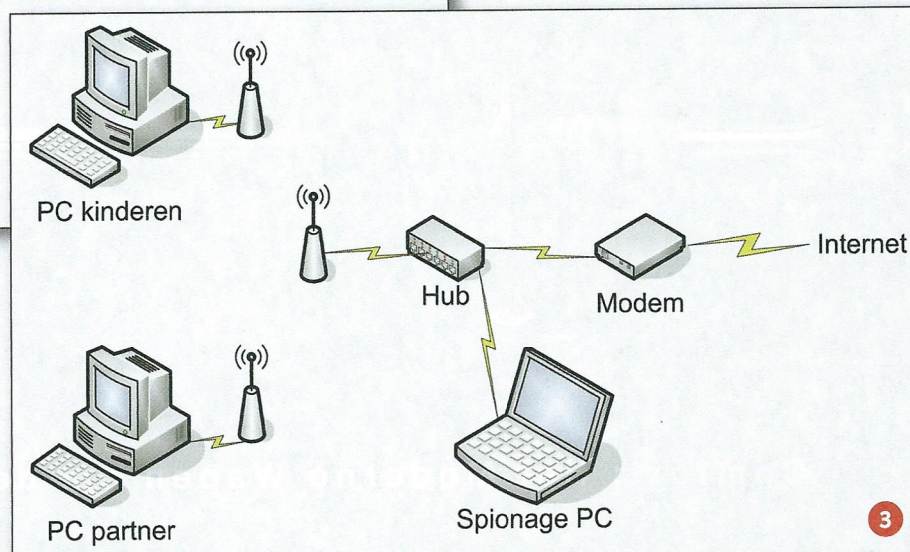
netwerkmethode als de losstaande computer behandeld. Het netwerk afluisteren is dé werkwijze van de echte spion. Het is voor anderen bijna onmogelijk het afluisteren te voorkomen en te ontdekken.

LUISTER HET NETWERK AF HET NETWERK

Tot een paar jaar geleden werden computers in een netwerk verbonden met hubs. Een hub is een netwerkapparaat waar u ook uw internetverbinding op aansluit. Het voordeel van een hub is dat het een dom apparaat is. Op het moment dat u een webpagina opvraagt op internet, wordt het verzoek niet alleen naar internet verzonden, maar ook naar alle aangesloten computers. Dat maakt aftappen erg eenvoudig. Tegenwoordig zijn switches meer gangbaar. Een switch is een intelligente hub. Het verzoek voor een webpagina wordt alleen naar internet verzonden en niet naar alle andere computers. Als u wilt aftappen, hebt u een dure switch met configuratiemogelijkheden nodig of een simpele hub. Haal die oude hub weer uit de kast of koop er een. Op www.marktplaats.nl is een groot aanbod van hubs met een prijs rond 10 euro. Een nieuwe hub koopt u voor ongeveer 35 euro. Bezoek de website www.tweakers.net/pricewatch/58120 voor de laagste prijs. Een tweedehands hub heeft meestal een maximale snelheid van 10Mbps. De nieuwe modellen kunnen 100Mbps aan. Dat laatste is handig als u veel bestanden kopieert tussen computers op uw netwerk.

MODEMS, SWITCHES, HUBS EN ROUTERS

Voor een breedbandinternetverbinding hebt u drie apparaten nodig. Het modem zorgt voor de omzetting van een adsl- of kabelsignaal naar een netwerkaansluiting; de router zorgt voor de scheiding van het internet en uw thuisnetwerk, en op de switch of hub sluit u de computers aan. In veel gevallen zijn deze functies gecombineerd in één apparaat. Dat is geen probleem. Bepaal de plaats in uw netwerk waar al het dataverkeer langs gaat. In het geval van een losse switch, router en modem, plaatst u de hub tussen de switch en de router (afbeelding 1). De spionagecomputer sluit u ook aan op de hub om al het



dataverkeer op te vangen. Bij een router met ingebouwde switch sluit u alle computers, inclusief de spionagecomputer aan op de hub en verbindt u de hub met de router (afbeelding 2). Bij een draadloze router plaatst u de hub tussen de router en het modem (afbeelding 3). Het nadeel van deze methode is dat u de spionagecomputer alleen nog voor spioneren kunt gebruiken en niet meer voor internettoegang. Met een draadloze router met ingebouwd modem kunt u de netwerk-methode niet gebruiken.

PROFESSIELE SWITCHES

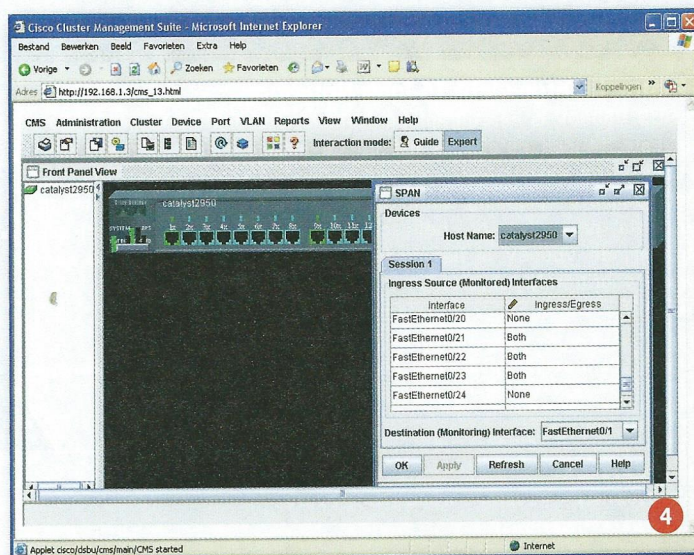
Een switch die u voor een paar tientjes aanschaft bij een computerwinkel heeft geen configuratiemogelijkheden. U stopt de stekker erin en de switch werkt. Dat is anders voor de duurdere 'manageable' switches. Deze bieden vaak de mogelijkheid om al het verkeer naar één poort te kopiëren (afbeelding 4). Op deze poort sluit u de spionagecomputer aan. U kunt deze alleen nog voor spionage gebruiken, normaal netwerkverkeer is meestal onmogelijk. Door de prijs van honderden euro's komen dergelijke switches meestal in een zakelijke omgeving voor.

SNIFFERS

Normaal gesproken zal uw eigen pc het netwerkverkeer dat niet voor u is bestemd, niet accepteren en dat is juist wel de bedoeling als u anderen wilt bespioneren. U hebt hiervoor een zogenaamde sniffer of logger nodig. Al deze programma's (zie tabel) maken overigens gebruik van hetzelfde hulpprogramma, WinPcap, dat bij alle programma's wordt meegeleverd. Gebruikt u meerdere sniffers, dan hoeft u WinPcap maar één keer te installeren, bij alle volgende slaat u het over. Meer informatie over winpcap staat op www.winpcap.org.

MSN MESSENGER

MSN Messenger is razend populair, vooral onder jongeren. Het programma beschikt over



uitgebreide mogelijkheden om te chatten en videobeelden te versturen en kan behoorlijk verslavend werken. De keerzijde van MSN Messenger is dat het programma ook wordt gebruikt door volwassenen die onder valse voorwendselen minderjarigen uit de kleren proberen te krijgen voor een webcam. Planet Internet heeft al aangetoond hoe geraffineerd dit wordt gedaan. Daarnaast staat het internet, en met name de shocklogs, vol met Messenger-filmpjes van jaloerse ex-vriendjes/vriendinnetjes die na het verbreken van een relatie privéfilmpjes openbaar maken. Als u wilt gaan spioneren, begin dan met Messenger als het om kinderen gaat.

Download en installeer MSN Sniffer. De evaluatieversie van het programma toont de eerste vijftien berichten van iedere chat. Klik na het starten op de configuratieknop. MSN Sniffer toont nu een lijstje met beschikbare netwerkadapters (afbeelding 5). De informatie die in dit scherm staat, is meestal niet correct, maar dat staat een goede werking van het programma niet in de weg. Kies als eerste de adapter waar een ip-adres achter staat en klik op OK. Het geeft niet als dit ip-adres niet het juiste is. Klik nu op start en zet een vinkje in het vakje voor Auto Refresh. U kunt de werking testen door met MSN Messenger een gesprek te starten met iemand anders. Als er geen gegevens verschijnen, hebt u de verkeerde adapter geselecteerd. Stop het loggen van gegevens en kies met de configuratieknop een andere adapter en start het loggen opnieuw. In het bovenste deel van het scherm verschijnen nu alle gesprekken die gevoerd worden (afbeelding 6). Klik op een gesprek om de inhoud te kunnen lezen. In tegenstelling tot MSN Messenger worden nieuwe gespreksregels onderaan worden toegevoegd, leest u hier het gesprek van beneden naar boven. Als een chat gedurende langere tijd onderbroken wordt, toont MSN Sniffer deze weer als een nieuwe. Loop daarom alle regels in de conversatielijst langs om een goed

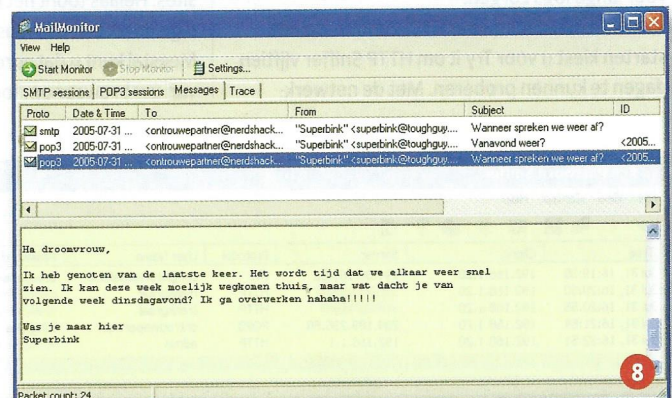
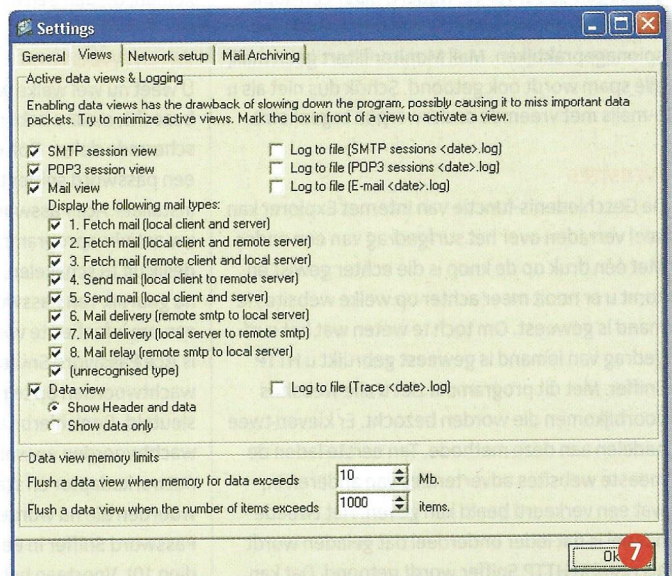
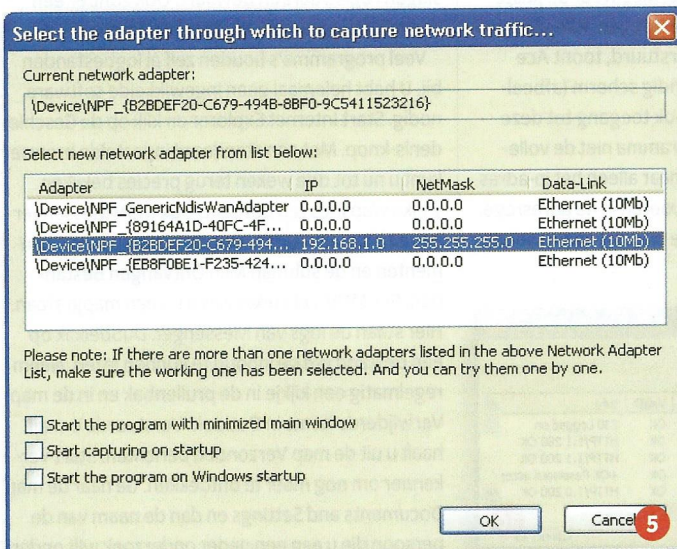
beeld te krijgen van alle MSN-gesprekken. Met de Save-knop slaat u uw bewijsmateriaal op als html-bestand. U kunt deze bekijken met een browser. Het grote broertje van dit programma is EtherBoss Network Monitor. Door de extra functies is dit programma erg geschikt voor bedrijven, maar er hangt wel een prijskaartje van bijna 300 dollar aan.

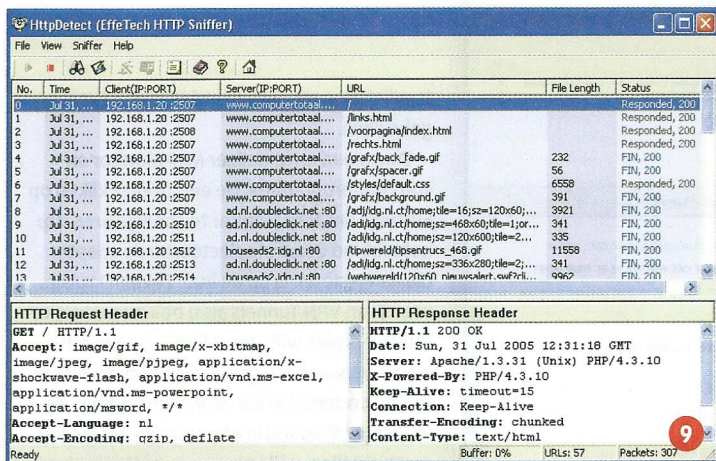
E-MAIL

E-mail onderscheppen is een fluitje van een cent met Mail Monitor. Het programma onderschept alle verzonden en ontvangen e-mails met één uitzondering. Als er gebruik gemaakt wordt van webgebaseerde e-maildiensten als Hotmail, Gmail of Yahoo-mail hebt u een ander programma nodig. Deze e-mails worden via Internet Explorer (of een andere browser) verstuurd en werken anders. Mail Monitor is bij uitstek geschikt voor het afvangen van e-mail in een zakelijke omgeving of voor

familieleden die Outlook of Outlook Express gebruiken.

Download en installeer Mail Monitor en start het programma. De eerste keer klikt u op Settings om Mail Monitor te configureren. Op het tabblad General selecteert u de adapter die aangesloten is op de hub. Zet een kruisje voor Scan VPN Tunnels als u ook een zakelijke thuiswerkplek wilt controleren. Op het tabblad Views wordt u gewaarschuwd om niet al te veel onderdelen aan te vinken (afbeelding 7). Dat geldt vooral in een zakelijke omgeving met tientallen mails per uur, voor thuisgebruik selecteert u ze allemaal. Eventueel kiest u ook voor de mogelijkheid om de logs naar een bestand weg te schrijven. U kunt het dan later op uw gemak nalezen. Bij Network Setup hoeft u niets te wijzigen en eventueel archiveert u alle mails met de selectie op het laatste tabblad. Klik op OK om de instellingen op te slaan en begin met onderscheppen door op Start Monitor te klikken. U kunt nu de juiste werking testen door met bijvoorbeeld Outlook Express een testmailtje te sturen. Ook hier geldt weer: als u niets ziet, controleer dan of u de juiste adapter hebt geselecteerd in het configuratiescherm.





Op het tabblad Messages ziet u nu alle verzonden en ontvangen e-mails voorbij komen. Klik op een mail en de inhoud wordt in het onderste deel van het scherm getoond (afbeelding 8). In sommige gevallen is het onderste deel niet zichtbaar. Maximaliseer het scherm dan en sleep de scheidingsbalk naar boven. Wachtwoorden achterhalen is ook simpel. Op het tabblad POP3 sessions worden alle e-mails nogmaals getoond, maar nu met gebruikersnaam en wachtwoord. Dat is handig als u vanaf een andere locatie zonder Mail Monitor toch e-mails van anderen wilt inzien. Zorg er in dat geval wel voor dat u niet de e-mail van de server verwijdert, maar een kopie achterlaat, anders wordt u snel betrapt met uw spionagepraktijken. Mail Monitor filtert geen mail, alle spam wordt ook getoond. Schrik dus niet als u e-mails met vreemde onderwerpen tegenkomt.

WEBSITES

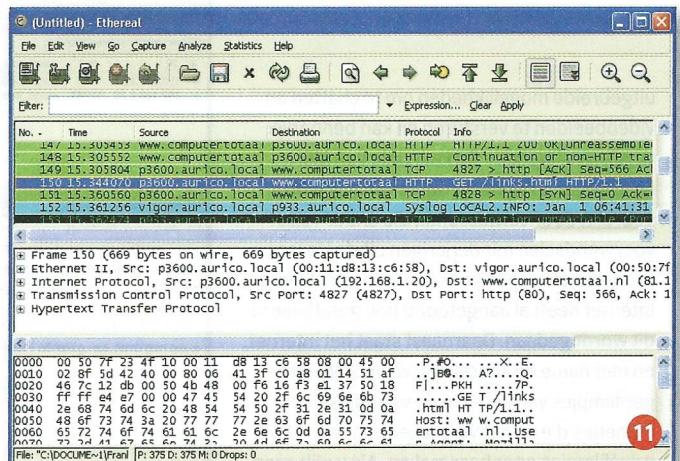
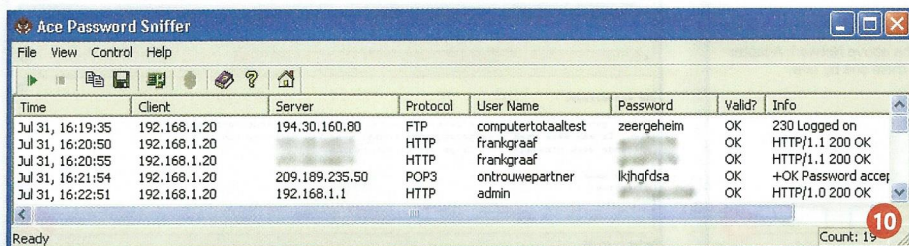
De Geschiedenis-functie van Internet Explorer kan veel verraden over het surfgedrag van een ander. Met één druk op de knop is die echter gewist en komt u er nooit meer achter op welke websites iemand is geweest. Om toch te weten wat het surfgedrag van iemand is geweest gebruikt u HTTP Sniffer. Met dit programma ziet u alle websites voorbijkomen die worden bezocht. Er kleven twee nadelen aan deze methode. Ten eerste laden de meeste websites advertenties van anderen in, wat een verkeerd beeld kan geven. Het tweede nadeel is dat ieder onderdeel dat geladen wordt als regel in HTTP Sniffer wordt getoond. Dat kan voor lange logs zorgen.

Download en installeer HTTP Sniffer. Na het starten kiest u voor Try it om HTTP Sniffer vijftien dagen te kunnen proberen. Met de netwerk-

knop selecteert u de juiste netwerkkaart. Klik op de startknop en bezoek wat websites. Het scherm vult nu als u de juiste adapter hebt geselecteerd (afbeelding 9). Klik op een regel om extra informatie op te vragen door vervolgens de verrijkerknop te kiezen. U krijgt nu alle details te zien. De saveknop zorgt voor het opslaan van bewijsmateriaal, maar de vraag is of u hier iets mee kunt. Alleen het inladen van de homepage van Computer!Totaal zorgt al voor 56 regels. In zulke grote logs wordt het moeilijk om iets terug te vinden. Het beste overzicht krijgt u door te scrollen door de resultaten. Url's die vaak terugkomen, duiden een bezochte website aan.

WACHTWOORDEN

U weet nu wel welke websites iemand heeft bezocht, maar u hebt nog geen toegang tot afgeschermd delen. Ook dat kunt u achterhalen door een password sniffer te gebruiken. Download en installeer Ace Password Sniffer en voorkom dat uw antivirusprogramma alarm slaat door het tijdelijk uit te schakelen. Zet uw virusbescherming na gebruik van Password Sniffer direct weer aan om infecties te voorkomen. Naast websites is Ace Password Sniffer in staat om vrijwel alle wachtwoorden op te pikken die niet worden versleuteld. Denk hierbij aan ftp-inloggegevens, mailwachtwoorden en websites. Kies weer de juiste netwerkadaptor en start het loggen. Alle wachtwoorden die nu worden verstuurd, toont Ace Password Sniffer in een handig scherm (afbeelding 10). Voortaan hebt u ook toegang tot deze sites. Helaas toont het programma niet de volledige naam van de website maar alleen het ip-adres. Meestal kunt u dat adres invoeren in de adresregel van uw browser om toch de website te bezoeken.



De probeerversie toont alleen de mogelijkheid tot onderscheppen, voor echte wachtwoorden hebt u de volledige versie nodig.

ALLES SNIFFEN

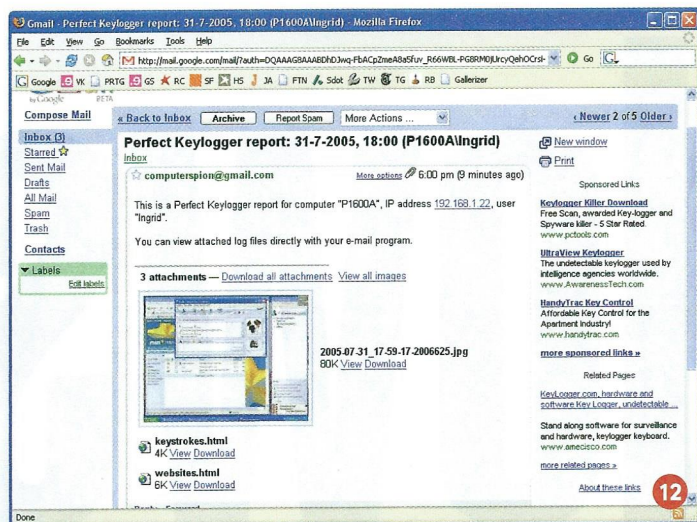
Alle netwerkprogramma's luisteren de stroom dataverkeer af en filteren daar de relevante gegevens uit. Met het opensource-programma Ethereal krijgt u inzicht in al het verkeer. Download en installeer het programma. In het menu Capture kunt u aangeven op welke netwerkadaptor het programma moet luisteren en kunt u het sniffen starten. Ethereal slaat alles op, wat bij druk internetverkeer erg grote logs oplevert. Als het loggen is gestopt, kunt u de resultaten bekijken en filters toepassen (afbeelding 11). Ethereal is zeker niet bedoeld voor beginners, maar door de vele filtermogelijkheden een prachtig programma voor netwerkanalyse. U kunt er gericht mee zoeken, maar bedenk wel dat de log onwerkbaar lang wordt als iemand anders op het netwerk bijvoorbeeld een dvd aan het downloaden is.

LOSSTAANDE COMPUTER

LOGBESTANDEN DOORZOEKEN

Ook op een losstaande computer kunt u goed achterhalen wat er precies gebeurt. Het krachtigste hulpmiddel is een keylogger dat alle toetsaanslagen registreert en bewaart. Ook zonder een dergelijk programma kunt u al ver komen.

Veel programma's houden zelf al logbestanden bij. U hebt helemaal geen ingewikkelde software nodig. Start Internet Explorer en klik op de Geschiedenis-knop. Met een standaard ingestelde browser kunt u nu tot drie weken terug precies bekijken welke websites zijn bezocht. Ook MSN Messenger kan een log bijhouden. Ga naar de map Mijn Documenten en de submap Mijn Ontvangen Bestanden. Per MSN-gebruiker ziet u nu een mapje staan. Hier staan de logs van Messenger. Dubbelklik op een bestand om de inhoud te kunnen lezen. Neem regelmatig een kijkje in de prullenbak en in de map Verwijderde items in Outlook. Verstuurde e-mail haalt u uit de map Verzonden berichten. Start Verkenner om nog meer te ontdekken. Ga naar de map Documents and Settings en dan de naam van de persoon die u aan een nader onderzoek wilt onder-



werpen. In de map Cookies vindt u verwijzingen naar bezochte websites (afbeelding 14) terwijl in de map Onlangs Geopend snelkoppelingen staan naar bestanden waar mee gewerkt is.

KEYLOGGER

Let op voordat u met keyloggers aan de slag gaat. Ze worden vaak als virus gebruikt en een kwaadwillende krijgt volledig inzicht in alle wachtwoorden die u gebruikt. Denk hierbij ook aan online bankieren. Het is geen prettig vooruitzicht als een onbevoegde toegang krijgt. Gelukkig vangen de meeste antivirusprogramma's keyloggers af. Download Perfect Keylogger en installeer het. Er zijn drie versies beschikbaar. Alleen bij de duurste zal niets erop wijzen dat u alles in de gaten houdt. De gratis versie toont een banner tijdens het starten, wat nogal opvalt. Tijdens de installatie kunt u de naam van het programma wijzigen en kiezen tussen een normale installatie en een onzichtbare. In het laatste geval wijst niets erop dat er een keylogger geïnstalleerd is. Als u de betaalde versie aanschaft, kunt u zelfs op afstand keyloggers installeren. Weet wat u doet als u dit overweegt en onthoud dat u wel degelijk strafbare feiten achter een pc kunt plegen. De eerste stap na de installatie is uw Perfect Keylogger configureren. U kunt ervoor kiezen alleen toetsaanslagen op te slaan, maar ook kunt u periodiek schermafbeeldingen

maken. Deze logs en afbeeldingen kunt u vervolgens versturen via e-mail (afbeelding 12) of uploaden naar een ftp-server. Maak alerts aan als u direct een e-mail wilt ontvangen op het moment dat de naam van een persoon of een ander woord wordt ingetoetst. U kunt dan meteen ingrijpen. In de bijlage van de mailtjes vindt u alle toetsaansla-

gen. Perfect Keylogger houdt woordengroepen bij elkaar. Iemand die inlogt op Hotmail of een ander webbased e-mailprogramma geeft met Perfect Keylogger alles prijs (afbeelding 13). Dankzij de bijlage in het mailtje hebt u overal inzicht in. Houd er wel rekening mee dat ook e-mail alles behalve veilig is. Een andere spion kan deze e-mails weer onderscheppen en heeft dan ook toegang tot dezelfde websites.

VANG DE SPION

Leuk natuurlijk al die spionagehulpmiddelen, maar hoe voorkomt u nu dat u zelf het slachtoffer wordt? Beveilig allereerst uw computer. De meeste wachtwoordsniffers en keyloggers worden herkend door antivirus- en antispywareprogramma's. Van de website van Microsoft kunt u gratis een antispywareprogramma downloaden. Scan geregeld uw gehele computer met deze software. Tegen af luisteren op netwerkniveau kunt u erg weinig doen. U kunt het netwerk bekijken om te onderzoeken of er geen vreemde apparaten tussen zijn geplaatst. Als dat wel het geval is, zoek dan verder. Probeer de vermoedelijke spion uit z'n tent te lokken door vragen te stellen waar de spion normaal gespro-

ken geen antwoord op kan hebben. De ultieme oplossing is de installatie van een keylogger op de computer van de verdachte. Als u dit doet en ook schermafbeeldingen maakt, ziet u onmiddellijk of er verdachte programma's op draaien.

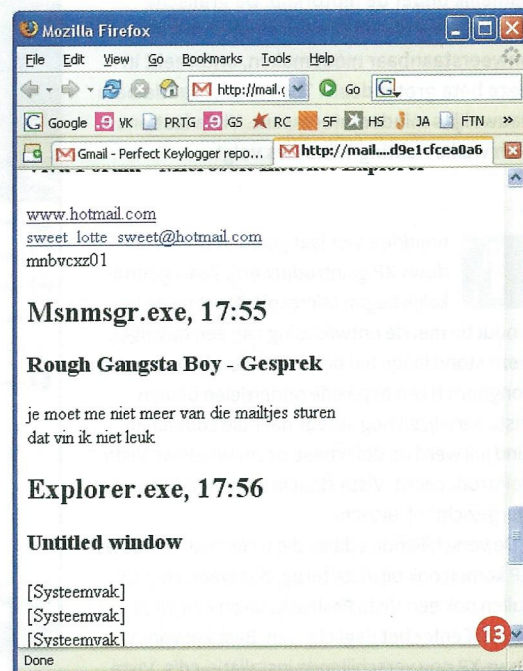
TOT SLOT

Weet wat u doet. Denk ook na over de vervolgstappen. Wat gaat u doen als u dingen ontdekt waar u niet blij van wordt? Wat gebeurt er als u ontmaskerd wordt als spion? Beantwoord eerst deze vragen voordat u spionageprogramma's gebruikt. Iedereen heeft recht op privacy, ook online.

EERDER VERSCHENEN

In onze online shop op Computertotaal.nl vindt u de volgende gerelateerde artikelen:

GLUREN MET GOOGLE
(Computer!Totaal 7/8, juli/augustus 2005)
WACHTWOORD KRAKEN? ZO DOET U DAT
(Computer!Totaal 6, juni 2005)



SOFTWARE

Sniffers en loggers	Prijs	Taal	Proefversie	Omvang	Besturingssysteem	Maker	Website
ACE Password Sniffer v1.2 *	\$ 30	EN	15 dagen	896kB	Windows 9x/NT4/2000/XP	Effetech	www.effetech.com
Ethereal v0.10.12	gratis	EN	n.v.t.	11MB	Windows 98/Me/2000/XP/2003	Ethereal.com	www.ethereal.com
HTTP Sniffer v3.6	\$ 30	EN	15 dagen	1,5MB	Windows 9x/NT4/2000/XP	Effetech	www.effetech.com
Mail Monitor	€ 49	EN	30 dagen	1,8MB	Windows 98/NT4/2000/XP	Digital Architects	www.digiarch.org
MSN Messenger Conversation Monitor & Sniffer	\$ 295	EN	15 dagen	969kB	Windows 9x/NT4/2000/XP	Etherboss	www.etherboss.com
MSN Sniffer v1.2 **	\$ 79	EN	15 dagen	885kB	Windows 9x/NT4/2000/XP	Effetech	www.effetech.com
Perfect Keylogger	\$ 45	EN	3 dagen	681kB	Windows 9x/Me/NT4/2000/XP	Blazingtools	www.blazingtools.com
WinPcap v3.1 beta 4 ***	gratis	EN	n.v.t.	474kB	Windows 9x/Me/NT/2000/XP/2003	NetGroup	www.winpcap.org

* Wachtwoorden worden niet weergegeven met de proefversie ** Maximaal 15 berichten per gesprek voor de proefversie *** Wordt meegeleverd met alle netwerkprogramma's