KTH Technology and Health

Laboration 2 – Analys av nätverkstrafik

Syftet med laborationen är att ge dig kännedom om programmet Wireshark, samt hur man kan använda det för att analysera inspelad data. Wireshark används för att fånga in nätverkstrafik samt låter dig inspektera innehållet i de infångade paketen. Du kommer även all lära dig hur man använder sig av olika typer av filter, samt skapar egna för att få fram den information man är intresserad av.

Översikt

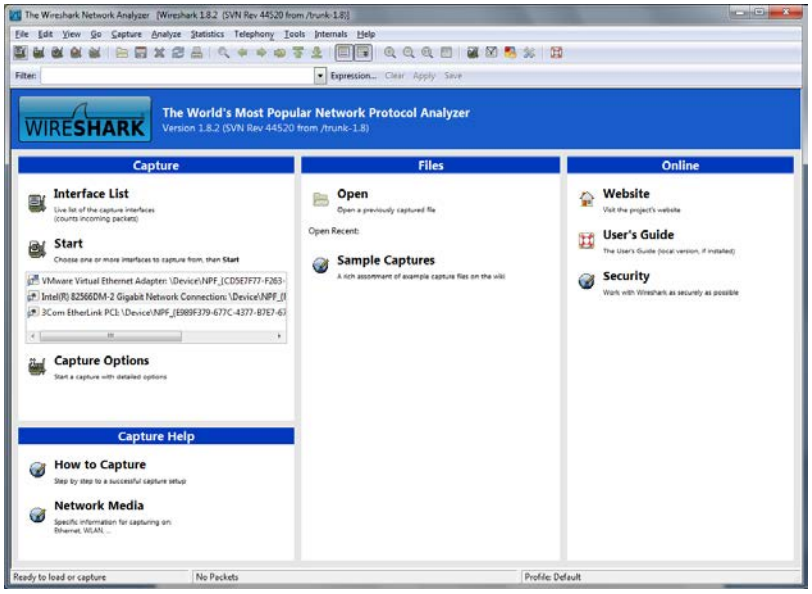
Du skall under laborationen analysera nätverkstrafik mellan en dator här i Haninge och en server i USA. Genom att inspektera/analysera den inspelade trafiken på lämpligt vis ska du kunna besvara frågor om vad som har hänt på nätet.

Sniffer

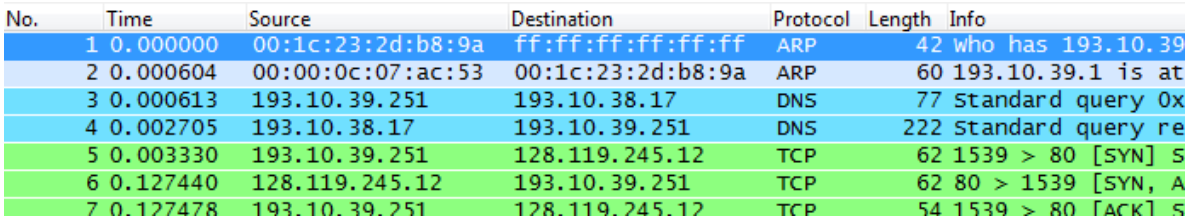
En sniffer är en programvara som kan användas för att övervaka och kontrollera ett nätverk på olika sätt. Till att börja med ställer den om nätverkskortet i så kallat ”promiscous mode”. Detta gör att nätverkskortet kan ta emot kopior av datapaket som är avsedda för andra nätverkskort. Sniffern känner på detta vis av nätverksaktiviteten. När detta är gjort kan många snifferprogram presentera det den har fångat upp på ett lättförståeligt sätt för användaren.

Lär känna Wiresharkl

Starta programmet Wireshark som du hittar under startmenyn. Du ska nu ha fått upp en sida med följande utseende. Ladda ner den färdinspelande filen labb2.pcap från bilda och öppna genom att välja *File* → *Open* i Wireshark.



Du bör nu kunna se ett antal inspelade ramar i Wireshark övre fönster.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:1c:23:2d:b8:9a	ff:ff:ff:ff:ff:ff	ARP	42	who has 193.10.39
2	0.000604	00:00:0c:07:ac:53	00:1c:23:2d:b8:9a	ARP	60	193.10.39.1 is at
3	0.000613	193.10.39.251	193.10.38.17	DNS	77	Standard query 0x
4	0.002705	193.10.38.17	193.10.39.251	DNS	222	Standard query re
5	0.003330	193.10.39.251	128.119.245.12	TCP	62	1539 > 80 [SYN] S
6	0.127440	128.119.245.12	193.10.39.251	TCP	62	80 > 1539 [SYN, A
7	0.127478	193.10.39.251	128.119.245.12	TCP	54	1539 > 80 [ACK] S

Varje rad i resultatlistan (i övre fönstret) är ett Ethernet-meddelande.

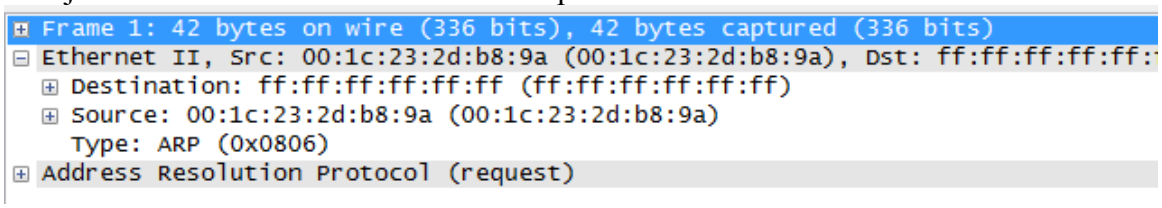
På varje rad ser man räknat från vänster:

- ram nr.
- tiden när ramen registrerades
- från vem ramen sändes
- till vem ramen skickas
- högsta nivå protokoll som används av ramen
- förklaring med information om ramen.

Kom ihåg att ALLA meddelanden är Ethernet-meddelanden som i sin tur innehåller ett meddelande (av typ ...) som i sin tur kan innehålla ett meddelande av typ ... som i sin tur etc. Det protokollnamn som man här redovisar är det som är mest intressant, dvs det som svarar mot det "innersta" meddelandet (högst upp på protokollstacken).

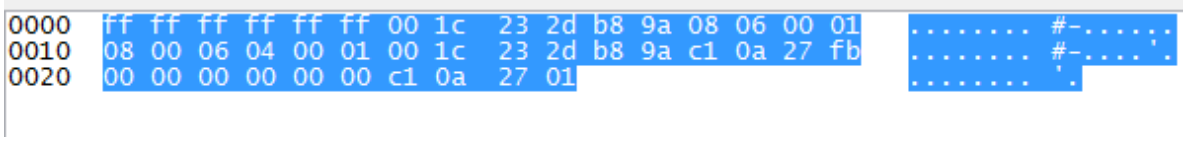
Om meddelandet innehåller ett IP-meddelande så finns det alltid IP-adresser och då redovisas dessa, annars finns inga IP-adresser och då redovisas MAC-adressen eller ett symboliskt namn på den nod i nätverket som har motsvarande MAC-adress.

Genom att klicka på ”pilen” (eller plus-tecken i Wireshark) på någon rad i mittenfönstret kan man steg för steg expandera ramen och inspektera ramens innehåll i detaljer. Här kan du t.ex. hitta header-information för protokollet, applikationsdata samt detaljerad information om olika inbäddade protokoll.



```
⊞ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
⊟ Ethernet II, Src: 00:1c:23:2d:b8:9a (00:1c:23:2d:b8:9a), Dst: ff:ff:ff:ff:ff:
  ⊞ Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  ⊞ Source: 00:1c:23:2d:b8:9a (00:1c:23:2d:b8:9a)
    Type: ARP (0x0806)
⊞ Address Resolution Protocol (request)
```

I det nedre fönstret hittar du detaljerad information för markerad ram i binär form.



```
0000  ff ff ff ff ff ff 00 1c  23 2d b8 9a 08 06 00 01   ........ #-......
0010  08 00 06 04 00 01 00 1c  23 2d b8 9a c1 0a 27 fb   ........ #-....'.
0020  00 00 00 00 00 00 c1 0a  27 01                     ........ '.
```

Det borde nu finnas två paket med protokollet ARP, två DNS, tre TCP, följt av ett HTTP (Info: GET), ett TCP till, och ett HTTP (Info: HTTP/1.1 200 OK).

Dags att gräva lite.

Observera: Datorn i Haninge som gör en http-förfrågan till en server i USA har följande information. Denna information behöver du för att kunna besvara frågorna.
IP-adressen: 193.10.39.251,
MAC-adressen: 00:1c:23:2d:b8:9a
DNS-server: 193.10.38.17

Address Resolution Protocol (ARP)
Vad frågas i ARP-paketen? who has 193.10.39.1

Och vilket svar fås i ARP-svaret? 193.10.39.1 is at 00:00:0c:07:ac:53

Varför skickas dessa ARP? för att 193.10.39.251 vill veta

Vilken information innehåller första ARP-paketet? frågan och vem vill ha svaret

Vilken information innehåller andra ARP-paketet? svaret

Domain Name System (DNS)
Vad frågas i DNS-paketen? vilken address ligger urlen på

Och vilket svar fås i DNS-svaret? urlen ligger på 128.119.245.12

Varför skickas dessa DNS? för att översätta url till ip

Vilken information innehåller första DNS-paketet? urlen

Vilken information innehåller andra DNS-paketet? ip addressen till urlen

Vilket transport-protokoll använder DNS? UDP

Vilka transport-portar används? 55112 samt 53

Vad innebär port 53? domain

Vilka IP-adresser används?

193 . 10 . 38 . 17 Vems adress? dns server

193 . 10 . 39 . 251 Vems adress? dell

Vilken typ av Ethernet används? (IEEE 802.3 eller Ethernet II)? e2

Tranmission Control Protocol (TCP)

Vad betyder de 3 TCP-segmenten? sync sync-ack ack

Vilka TCP-portar används? 80 samt 1539

Vad innebär port 80? http

Vad är första TCP-segmentets uppgift? skickar förfrågan om connection A

Vilket sekvensnummer innehåller första TCP-segmentet? 609192698

Hur stort är första TCP-huvudet? 28 bytes

Vad innehåller första TCP-huvudet för options? max nop nop tcp sack true

Hur stort är Maximum segment size (MSS)? 1460 bytes

Hur stort är Window size? 65535

Hur många MSS-segment motsvarar denna Window size (beräkna)? 45 st

Vilken flagga är satt till 1 i första TCP-segmentet? sack_perm

Vad är andra TCP-segmentets uppgift? B accepterar och skickar egen förfrågan till A

Vilket sekvensnummer innehåller andra TCP-segmentet? 2156302665

Vilket kvittensnummer innehåller andra TCP-segmentet? 609192698

Hur stort är andra TCP-huvudet? 28 bytes

Vad innehåller andra TCP-huvudet för options? samma som första

Hur stort är Maximum segment size (MSS)? 1460 bytes

Hur stort är Window size? 5840

Hur många MSS-segment motsvarar denna Window size (beräkna)? 4 st

Vilka flaggor är satta till 1 i andra TCP-segmentet? sackperm

Vad är tredje TCP-segmentets uppgift? A acceptera Bs förfrågan

Vilket sekvensnummer innehåller tredje TCP-segmentet? 609192699

Vilket kvittensnummer innehåller tredje TCP-segmentet? 2156302666

Hur stort är tredje TCP-huvudet? 28

Vilken flagga är satt till 1 i tredje TCP-segmentet? null

Mellan vilka IP-adresser skickas TCP-segmenten?

193 . 10 . 39 . 251 Vems adress? dell A

128 . 119 . 245 . 12 Vems adress? http B

Vilkas MAC-adresser motsvarar det? 00:00:0c:07:ac:53

HyperText Transfer Protocol (HTTP)
Vi skall nu titta på det paket som innehåller vår HTTP GET-förfråga till gaia.cs.umass.edu

Vi börjar med transportskiktet.

Vilket TCP-segmentnummer anges? 609192699

Hur långt är TCP-segmentet? 505

Stämmer det med vilket nummer som vi förväntar i nästa TCP-segment? ja

Vi går till Applikationsskiktet.

Vilken fil efterfrågas? ethreal-labs/intro-ethereal-file1.html

Vilken host tillfrågas? gaia.cs.umass.edu

Vad tror du Keep-Alive innebär? döda inte uppkopplingen

Nästa paket innehåller ett TCP-segment med en kvittens.

Vilket är TCP-kvittensnumret? 6091926204

Vilket TCP-segmentnummer anges? 2156302666

Varför ändras inte TCP-segmentnumret? kvittot har inte skickat någon data

Vi går vidare till nästa HTTP-paket och tittar i TCP-informationen.

Vilket TCP-segmentnummer anges? 215136302666

Hur långt är TCP-segmentet? 380

Stämmer det med vilket nummer som vi förväntar i nästa TCP-segment? ja

Vi går till Applikationsskiktet.

Vad innehåller HTTP-data? text du har tankat labfiler

Hur många bytes nyttodata innehåller HTTP-data (Content-length)? 80

När modifierades innehållet senast? 11 mars 2013

Vilken server användes? apache

Vilken version av servern körs? apache/2.2.3 (centOS)

Vi tittar på sista TCP-segmentet.

Vilket är TCP-kvittensnumret? 609193204

Har Window size ändrats? 65155

Med hur mycket? 58723

Kan du förklara skillnaden första skickade bara en förfrågan till en sida, andra skickade hela

---

Avsluta
När du är klar med alla uppgifter, skall du skriva ditt namn och dagens datum på raden härunder, samt få lärarens signatur, vilket är ditt kvitto på att laborationen är genomförd.

Namn: _____ Datum: _____

Lärarens signatur: _____

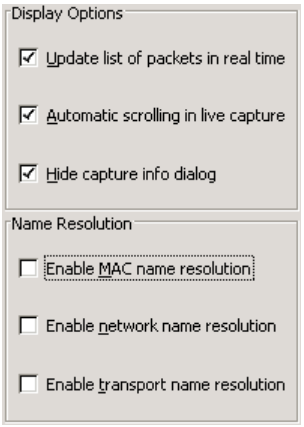
Extra uppgift – Vill du avlyssna vad som skickas på nätet just nu och varför inte se hur enkelt det är att få tag på login och lösenord?

Starta programmet Wireshark som du hittar under startmenyn. Du ska nu ha fått upp en sida med följande utseende.

Nu är det dags att starta Wireshark paketsniffning samt göra en del grundinställningar.

Gå till menyn **Capture** och välj **Options** och gör följande inställningar i dialogrutan (se bild till höger). Välj det nätverkskort som har **3Com** i namnet.

Klicka därefter på Start-knappen för att påbörja inspelningen av Ethernet ramar.



Stoppa avlyssningen efter ett tag. Det blir lätt många tusen paket som man har avlyssnat och för att begränsa till det man är intresserad av kan man lägga till ett filter.

Ställ in display-filter
Skriv in ”**ip.addr ==** ” (utan citattecken) följt av datorns IP-adress i displayfiltret (i menyn finns ett fält där det står Filter). Tryck sedan Enter. Detta gör att vi nu endast ser trafik som berör din dator. Lägg till t.ex. ”**and http**” för att få enbart http trafik till och från din dator.

Dags att snappa upp login och lösenord
Prova surfa in på www.spray.se , starta sniffern efteråt och logga in på deras e-post tjänst med ett påhittat namn och lösenord.
Stoppa sniffern och lägg in ett filtret: ” ip.src==193.10.39.1XX && http” byt ut 1XX till den IP-adress din dator har.
Leta nu efter ett paket där det står POST (där det står GET på de flesta). Markera det paketet och klicka på plustecknet vid ”Hypertext Transfer Protocol”. Leta nu och se om du kan hitta något användarnamn och/eller lösenord. Du kan också prova om grannen loggar in och du kan se hans/hennes login och lösenord.