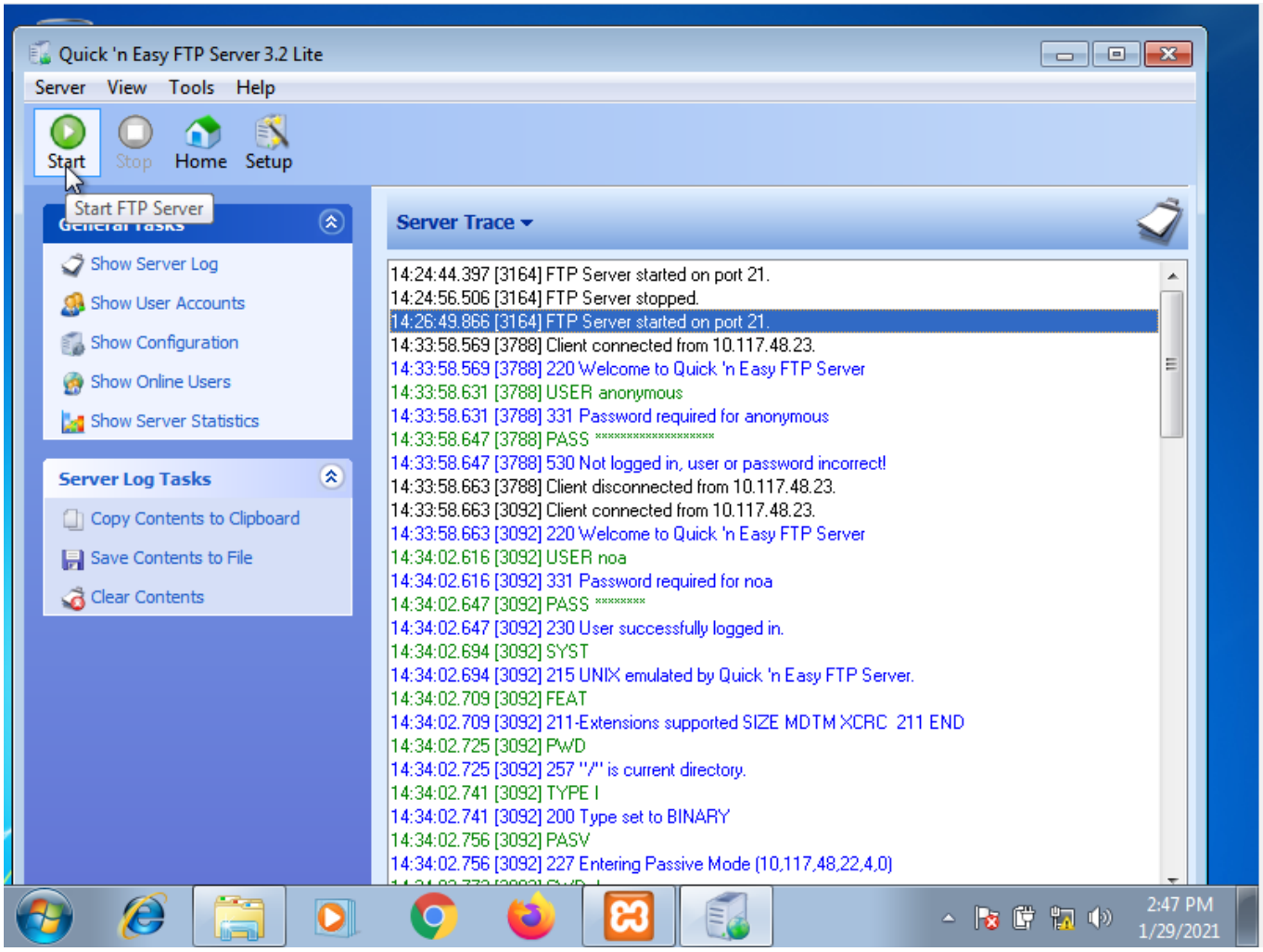
Wireshark- harjoitus



Käynnistettiin FTP-palvelin painamalla start-painiketta.

Aloitettiin skannaus Wiresharkissa.

Pingattiin tietokoneita keskenään.

Pingaus Windows 7-tietokoneelta :

```
C:\Users\noa>ping 10.117.48.23

Pinging 10.117.48.23 with 32 bytes of data:
Reply from 10.117.48.23: bytes=32 time=1ms TTL=128
Reply from 10.117.48.23: bytes=32 time=1ms TTL=128
Reply from 10.117.48.23: bytes=32 time=1ms TTL=128
Reply from 10.117.48.23: bytes=32 time<1ms TTL=128

Ping statistics for 10.117.48.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pingaus Windows 10-tietokoneelta :

```
C:\Users\noa>ping 10.117.48.22

Pinging 10.117.48.22 with 32 bytes of data:
Reply from 10.117.48.22: bytes=32 time<1ms TTL=128
Reply from 10.117.48.22: bytes=32 time=1ms TTL=128
Reply from 10.117.48.22: bytes=32 time<1ms TTL=128
Reply from 10.117.48.22: bytes=32 time=1ms TTL=128

Ping statistics for 10.117.48.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tarkasteltiin tuloksia Wiresharkissa suodattamalla tuloksia ehdolla ”icmp”

icmp

No.	Time	Source	Destination	Protocol	Length	Info
49	54.401218981	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 50)
50	54.401618340	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in…
52	55.399504420	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 53)
53	55.399912149	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (request in…
55	56.382730542	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 56)
56	56.383100768	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (request in…
58	57.391487749	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in …
59	57.391817352	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (request i…
86	77.659085779	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 87)
87	77.659452958	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in…
90	78.682551069	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 91)
91	78.682790267	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (request in…
92	79.698019548	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 93)
93	79.698344289	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (request in…
94	80.714022147	10.117.48.23	10.117.48.22	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in …
95	80.714446588	10.117.48.22	10.117.48.23	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (request i…

Request = lähetetään pyyntö.

Reply = vastaus pyyntöön.

Seuraavaksi otettiin FTP-yhteys Windows 10-tietokoneelta kirjoittamalla selaimen url-kenttään ”ftp://10.117.48.22”. Avautui lomakeruutu, johon syötettiin käyttäjätunnus ja salasana jotka oli määritelty FTP-sovelluksen asetuksissa.

Tarkasteltiin tuloksia Wiresharkissa suodattamalla tuloksia ehdolla ”ftp”

ftp

No.	Time	Source	Destination	Protocol	Length	Info
12	3.211701720	10.117.48.22	10.117.48.23	FTP	95	Response: 220 Welcome to Quick 'n Easy FTP Server
13	3.244303287	10.117.48.23	10.117.48.22	FTP	70	Request: USER anonymous
14	3.244775668	10.117.48.22	10.117.48.23	FTP	91	Response: 331 Password required for anonymous
15	3.247045158	10.117.48.23	10.117.48.22	FTP	80	Request: PASS mozilla@example.com
16	3.247586082	10.117.48.22	10.117.48.23	FTP	102	Response: 530 Not logged in, user or password incorrect!
24	3.257913797	10.117.48.22	10.117.48.23	FTP	95	Response: 220 Welcome to Quick 'n Easy FTP Server
32	6.670567003	10.117.48.23	10.117.48.22	FTP	64	Request: USER noa
33	6.670984910	10.117.48.22	10.117.48.23	FTP	85	Response: 331 Password required for noa
34	6.707367505	10.117.48.23	10.117.48.22	FTP	69	Request: PASS salasana
35	6.707954779	10.117.48.22	10.117.48.23	FTP	88	Response: 230 User successfully logged in.
36	6.770023967	10.117.48.23	10.117.48.22	FTP	60	Request: SYST
37	6.770575737	10.117.48.22	10.117.48.23	FTP	102	Response: 215 UNIX emulated by Quick 'n Easy FTP Server.
38	6.809592883	10.117.48.23	10.117.48.22	FTP	60	Request: FEAT
39	6.810278411	10.117.48.22	10.117.48.23	FTP	109	Response: 211-Extensions supported
40	6.814119127	10.117.48.23	10.117.48.22	FTP	60	Request: PWD
41	6.816600437	10.117.48.22	10.117.48.23	FTP	85	Response: 257 "/" is current directory.
42	6.824341478	10.117.48.23	10.117.48.22	FTP	62	Request: TYPE I
43	6.825234974	10.117.48.22	10.117.48.23	FTP	78	Response: 200 Type set to BINARY
44	6.826555540	10.117.48.23	10.117.48.22	FTP	60	Request: PASV
45	6.827277462	10.117.48.22	10.117.48.23	FTP	100	Response: 227 Entering Passive Mode (10,117,48,22,4,0)
46	6.830101466	10.117.48.23	10.117.48.22	FTP	61	Request: CWD /
49	6.832109384	10.117.48.22	10.117.48.23	FTP	85	Response: 250 "/" is current directory.
51	6.834155328	10.117.48.23	10.117.48.22	FTP	60	Request: LIST
52	6.835786178	10.117.48.22	10.117.48.23	FTP	114	Response: 150 Opening ASCII mode data connection for directory…
59	6.958354817	10.117.48.22	10.117.48.23	FTP	77	Response: 226 Transfer complete
67	11.074292583	10.117.48.23	10.117.48.22	FTP	60	Request: PASV
68	11.074959666	10.117.48.22	10.117.48.23	FTP	100	Response: 227 Entering Passive Mode (10,117,48,22,4,0)
69	11.078889865	10.117.48.23	10.117.48.22	FTP	75	Request: SIZE /tiedosto1.txt
72	11.080660715	10.117.48.22	10.117.48.23	FTP	61	Response: 213 9
74	11.090588802	10.117.48.23	10.117.48.22	FTP	75	Request: MDTM /tiedosto1.txt
75	11.092258847	10.117.48.22	10.117.48.23	FTP	78	Response: 213 20210129142313.000
76	11.094497896	10.117.48.23	10.117.48.22	FTP	75	Request: RETR /tiedosto1.txt
77	11.095922279	10.117.48.22	10.117.48.23	FTP	114	Response: 150 Opening BINARY mode data connection for file tra…
84	11.182102412	10.117.48.22	10.117.48.23	FTP	77	Response: 226 Transfer complete

Request = Pyyntö suorittaa joku toimenpide.

Response = Lupa suorittaa toimenpide (tai jos jokin menee pieleen niin virheilmoitus).

Yhteenveto

Ideana oli tarkastella Wiresharkilla tapahtumia, kun laitteet kommunikoivat keskenään.

Huomataan että Wiresharkin tuloksissa nähdään useita tietoja

No. = tapahtuman numero

Time = Aika, milloin tapahtuma on suoritettu.

Source = Mistä pyyntö lähetettiin.

Destination = Määränpää pyynnölle.

Protocol = Protokolla, vaikka FTP tai icmp.

Lenght = Pyynnön pituus.

Info = Tietoa pyynnöstä selväkielisenä tekstinä.