

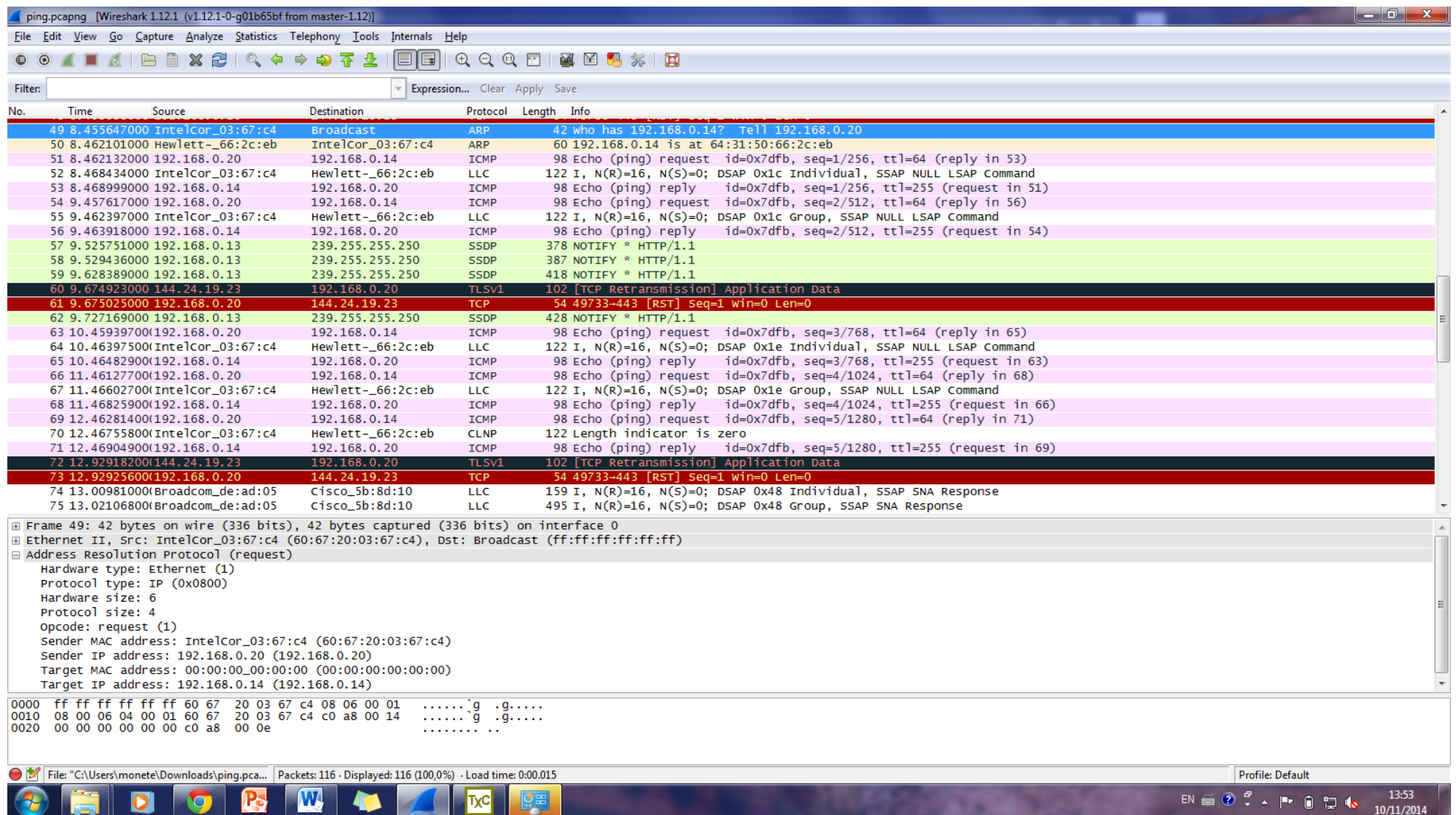


FIG 1 : Ping – Pong

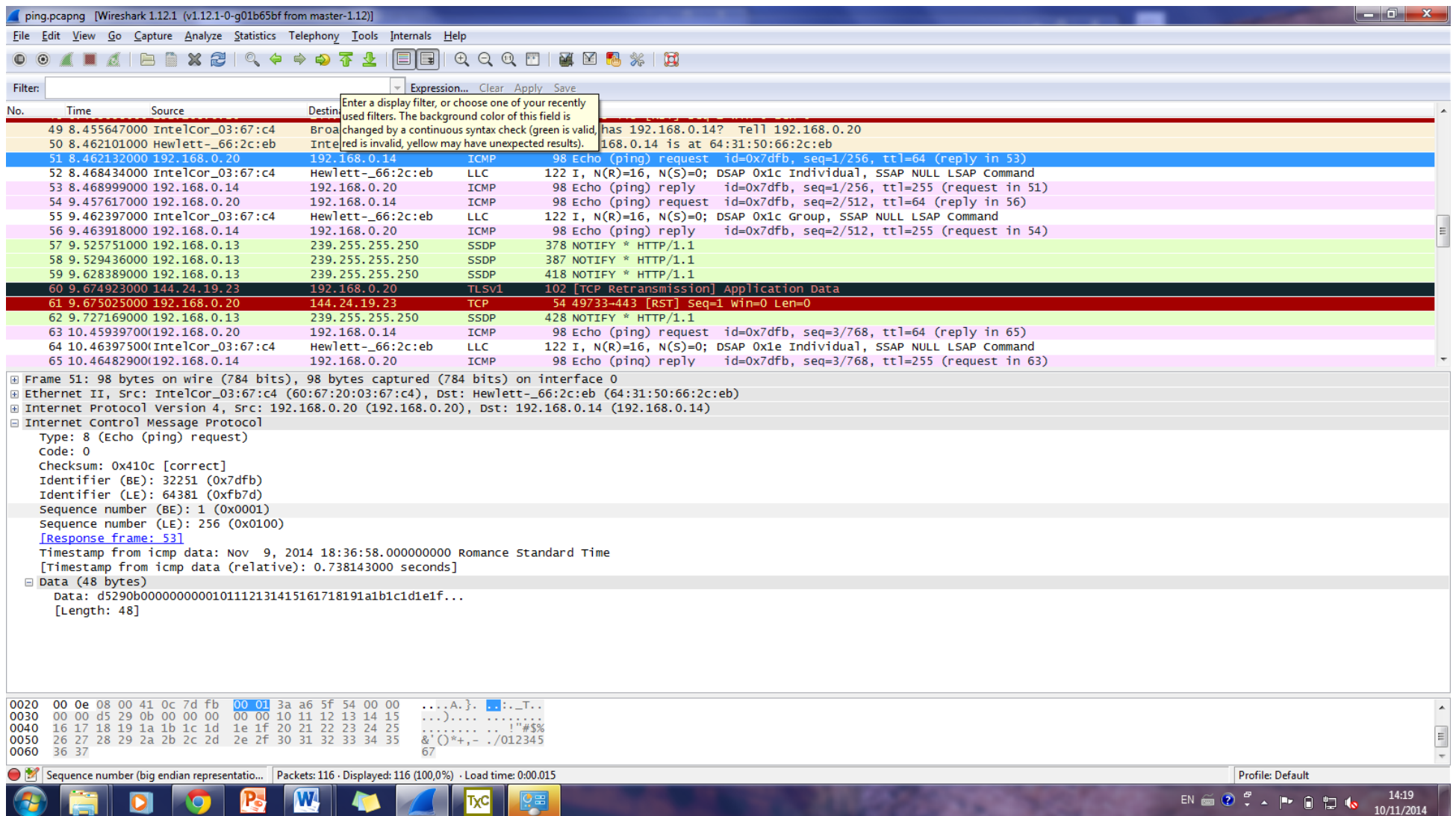


FIG 2 : Ping Request

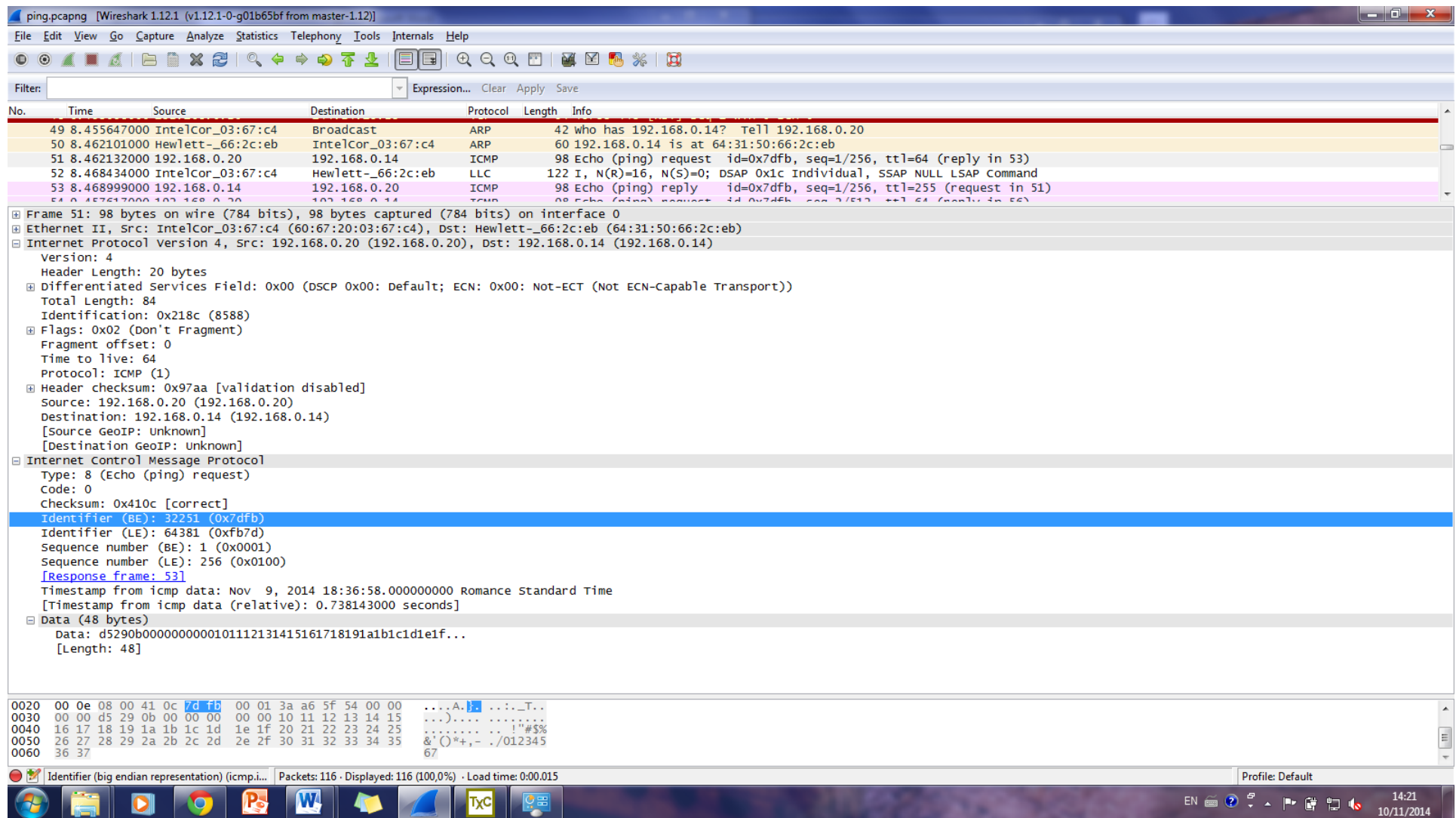


Fig 3 : Ping Request (2)

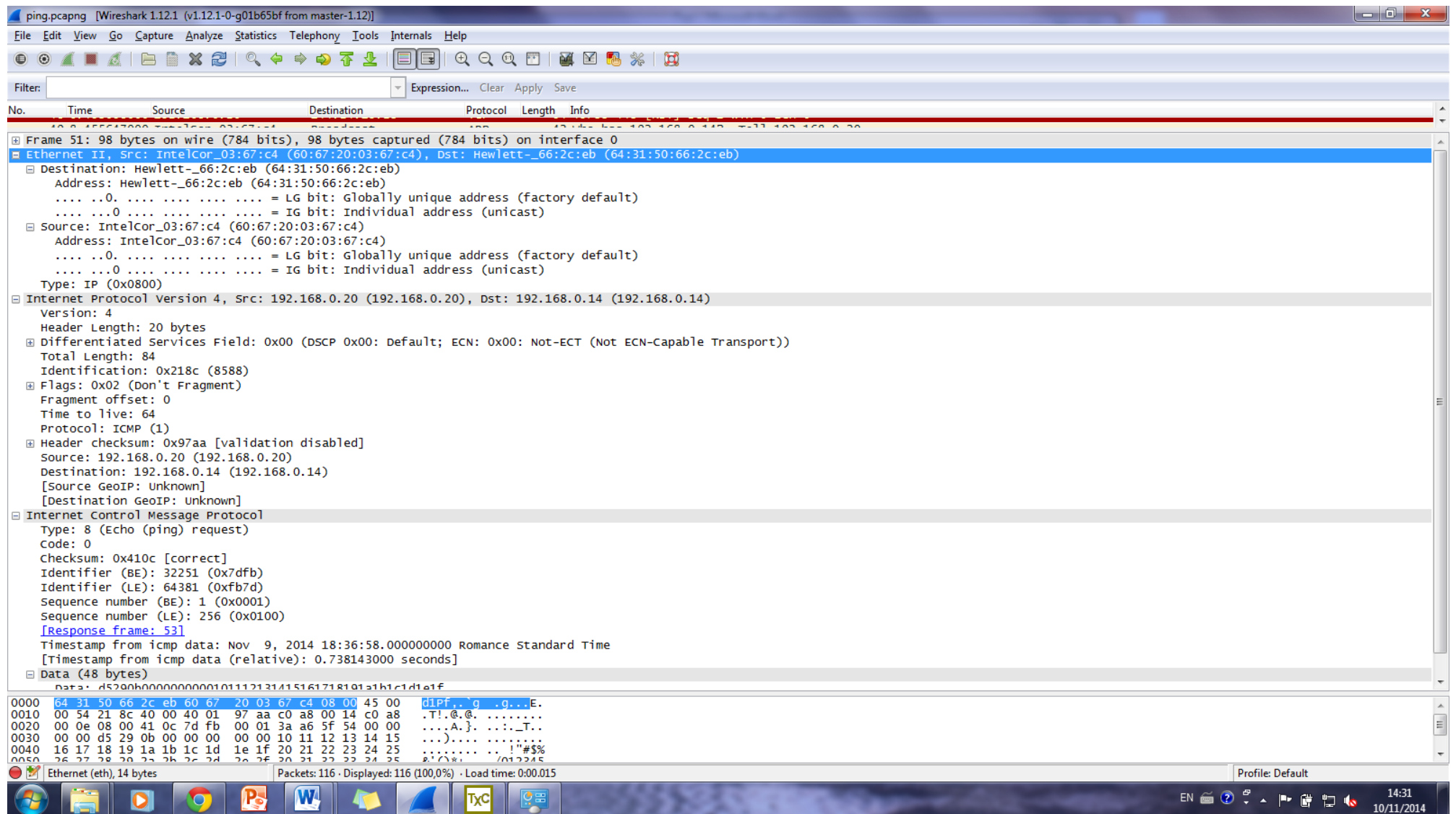


Fig 4 : Ping Request (3)

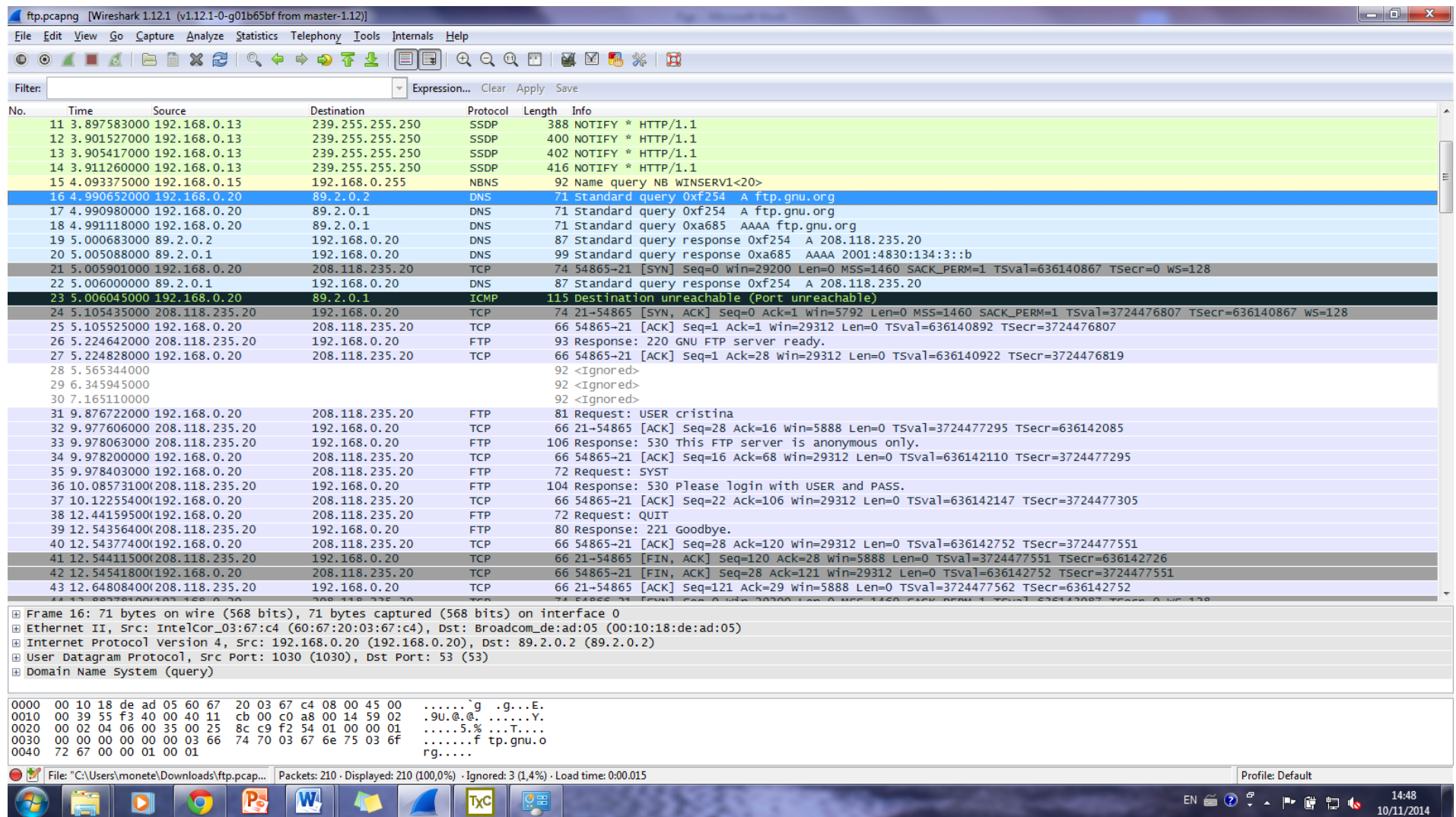


Fig. 5 : FTP capture

ftp.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
45	13.98712700	208.118.235.20	192.168.0.20	TCP	74	21-54866 [SYN, ACK] Seq=0 Ack=1 win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3724477695 TSecr=636143087 WS=128
46	13.98727000	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=1 Ack=1 win=29312 Len=0 TSval=636143113 TSecr=3724477695
47	14.10770100	208.118.235.20	192.168.0.20	FTP	93	Response: 220 GNU FTP server ready.
48	14.10787700	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=1 Ack=28 win=29312 Len=0 TSval=636143143 TSecr=3724477707
49	16.27114800	192.168.0.20	208.118.235.20	FTP	82	Request: USER anonymous
50	16.37597900	208.118.235.20	192.168.0.20	TCP	66	21-54866 [ACK] Seq=28 Ack=17 win=5888 Len=0 TSval=3724477934 TSecr=636143684
51	16.37950000	192.168.0.20	208.118.235.20	FTP	138	Response: 230-Due to U.S. Export Regulations, all cryptographic software on this
52	16.37963300	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=17 Ack=100 win=29312 Len=0 TSval=636143711 TSecr=3724477935
53	16.38029000	208.118.235.20	192.168.0.20	FTP	118	Response: 230-site is subject to the following legal notice:
54	16.38033800	208.118.235.20	192.168.0.20	FTP	72	Response: 230-
55	16.38040300	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=17 Ack=152 win=29312 Len=0 TSval=636143711 TSecr=3724477935
56	16.38049100	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=17 Ack=158 win=29312 Len=0 TSval=636143711 TSecr=3724477935
57	16.48190800	208.118.235.20	192.168.0.20	FTP	599	Response: 230- This site includes publicly available encryption source code
58	16.48202200	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=17 Ack=691 win=30336 Len=0 TSval=636143736 TSecr=3724477945
59	16.48245000	192.168.0.20	208.118.235.20	FTP	72	Request: SYST
60	16.58814600	208.118.235.20	192.168.0.20	FTP	85	Response: 215 UNIX Type: L8
61	16.62655800	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=23 Ack=710 win=30336 Len=0 TSval=636143773 TSecr=3724477956
62	17.91895700	192.168.0.1	239.255.255.250	SSDP	384	NOTIFY * HTTP/1.1
63	17.92220400	192.168.0.1	239.255.255.250	SSDP	329	NOTIFY * HTTP/1.1
64	17.92542400	192.168.0.1	239.255.255.250	SSDP	320	NOTIFY * HTTP/1.1
65	17.92930400	192.168.0.1	239.255.255.250	SSDP	394	NOTIFY * HTTP/1.1
66	18.22371700	192.168.0.20	208.118.235.20	FTP	92	Request: PORT 192,168,0,20,155,62
67	18.32862900	208.118.235.20	192.168.0.20	FTP	117	Response: 200 PORT command successful. Consider using PASV.
68	18.32874000	192.168.0.20	208.118.235.20	TCP	66	54866-21 [ACK] Seq=49 Ack=761 win=30336 Len=0 TSval=636144198 TSecr=3724478130
69	18.32892600	192.168.0.20	208.118.235.20	FTP	72	Request: LIST
70	18.43628400	208.118.235.20	192.168.0.20	TCP	74	20-39742 [SYN] Seq=0 win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3724478140 TSecr=0 WS=128
71	18.43639500	192.168.0.20	208.118.235.20	TCP	74	39742-20 [SYN, ACK] Seq=0 Ack=1 win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=636144225 TSecr=3724478140 WS=128
72	18.46766800	208.118.235.20	192.168.0.20	TCP	66	21-54866 [ACK] Seq=761 Ack=55 win=5888 Len=0 TSval=3724478144 TSecr=636144198
73	18.53768300	208.118.235.20	192.168.0.20	TCP	66	20-39742 [ACK] Seq=1 Ack=1 win=5888 Len=0 TSval=3724478151 TSecr=636144225
74	18.53818500	208.118.235.20	192.168.0.20	FTP	105	Response: 150 Here comes the directory listing.
75	18.53948800	208.118.235.20	192.168.0.20	FTP-DAT	1330	FTP Data: 1264 bytes
76	18.53965000	192.168.0.20	208.118.235.20	TCP	66	39742-20 [ACK] Seq=1 Ack=1265 win=31488 Len=0 TSval=636144251 TSecr=3724478151
77	18.53994500	208.118.235.20	192.168.0.20	TCP	66	20-39742 [FIN, ACK] Seq=1265 Ack=1 win=5888 Len=0 TSval=3724478151 TSecr=636144225

Frame 77: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: Broadcom_de:ad:05 (00:10:18:de:ad:05), Dst: IntelCor_03:67:c4 (60:67:20:03:67:c4)

Internet Protocol Version 4, Src: 208.118.235.20 (208.118.235.20), Dst: 192.168.0.20 (192.168.0.20)

Transmission Control Protocol, Src Port: 20 (20), Dst Port: 39742 (39742), Seq: 1265, Ack: 1, Len: 0

0000 60 67 20 03 67 c4 00 10 18 de ad 05 08 00 45 08 .g.g... ..E.
0010 00 34 cd ae 40 00 2b 06 05 c6 d0 76 eb 14 c0 a8 .4..@.+...V....
0020 00 14 00 14 9b 3e e7 7b d0 08 1e 16 35 a4 80 11>.{...5....
0030 00 2e 7e a2 00 00 01 01 08 0a dd ff 06 c7 25 ea ..~.....%..
0040 ca 61 .a

File: "C:\Users\monete\Downloads\ftp.pcapng" Packets: 210 · Displayed: 210 (100,0%) · Ignored: 3 (1,4%) · Load time: 0:00.015

Profile: Default

14:55 10/11/2014

Fig. 6 : FTP capture (2)

ftp.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
69	18.32892600	192.168.0.20	208.118.235.20	FTP	72	Request: LIST
70	18.43628400	208.118.235.20	192.168.0.20	TCP	74	20→39742 [SYN] Seq=0 win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3724478140 TSecr=0 WS=128
71	18.43639500	192.168.0.20	208.118.235.20	TCP	74	39742→20 [SYN, ACK] Seq=0 Ack=1 win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=636144225 TSecr=3724478140 WS=128
72	18.46766800	208.118.235.20	192.168.0.20	TCP	66	21→54866 [ACK] Seq=761 Ack=55 win=5888 Len=0 TSval=3724478144 TSecr=636144198
73	18.53768300	208.118.235.20	192.168.0.20	TCP	66	20→39742 [ACK] Seq=1 Ack=1 win=5888 Len=0 TSval=3724478151 TSecr=636144225
74	18.53818500	208.118.235.20	192.168.0.20	FTP	105	Response: 150 Here comes the directory listing.
75	18.53948800	208.118.235.20	192.168.0.20	FTP-DAT	1330	FTP Data: 1264 bytes
76	18.53965000	192.168.0.20	208.118.235.20	TCP	66	39742→20 [ACK] Seq=1 Ack=1265 win=31488 Len=0 TSval=636144251 TSecr=3724478151
77	18.53994500	208.118.235.20	192.168.0.20	TCP	66	20→39742 [FIN, ACK] Seq=1265 Ack=1 win=5888 Len=0 TSval=3724478151 TSecr=636144225
78	18.54051500	192.168.0.20	208.118.235.20	TCP	66	39742→20 [FIN, ACK] Seq=1 Ack=1266 win=31488 Len=0 TSval=636144251 TSecr=3724478151
79	18.57455100	192.168.0.20	208.118.235.20	TCP	66	54866→21 [ACK] Seq=55 Ack=800 win=30336 Len=0 TSval=636144260 TSecr=3724478151

Frame 74: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0

Ethernet II, Src: Broadcom_de:ad:05 (00:10:18:de:ad:05), Dst: Intelcor_03:67:c4 (60:67:20:03:67:c4)

Internet Protocol Version 4, Src: 208.118.235.20 (208.118.235.20), Dst: 192.168.0.20 (192.168.0.20)

Transmission Control Protocol, Src Port: 21 (21), Dst Port: 54866 (54866), Seq: 761, Ack: 55, Len: 39

Source Port: 21 (21)

Destination Port: 54866 (54866)

[Stream index: 2]

[TCP Segment Len: 39]

Sequence number: 761 (relative sequence number)

[Next sequence number: 800 (relative sequence number)]

Acknowledgment number: 55 (relative ack number)

Header Length: 32 bytes

... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)

window size value: 46

[calculated window size: 5888]

[window size scaling factor: 128]

Checksum: 0x4a18 [validation disabled]

Urgent pointer: 0

Options: (12 bytes), No-operation (NOP), No-operation (NOP), Timestamps

[SEQ/ACK analysis]

[iRTT: 0.104489000 seconds]

[Bytes in flight: 39]

File Transfer Protocol (FTP)

150 Here comes the directory listing.\r\n

Response code: File status okay; about to open data connection (150)

Response arg: Here comes the directory listing.

0000 60 67 20 03 67 c4 00 10 18 de ad 05 08 00 45 00 .g.g... ..E.

0010 00 5b 27 80 40 00 2b 06 ab d5 d0 76 eb 14 c0 a8 .L'.@.+..V...

0020 00 14 00 15 d6 52 82 b4 25 75 87 f8 bf 60 80 18R..%....

0030 00 2e 4a 18 00 00 01 01 08 0a dd ff 06 c7 25 ea .J.....%.

0040 ca 46 31 35 30 20 48 65 72 65 20 63 6f 6d 65 73 .F150 He re comes

0050 20 74 68 65 20 64 60 72 65 62 74 6f 72 20 60 6c the dir ectory l

File: C:\Users\monet\Downloads\ftp.pcapng... Packets: 210 · Displayed: 210 (100,0%) · Ignored: 3 (1,4%) · Load time: 0:00.015

Profile: Default

18:42 10/11/2014

Fig. 7 : Paquet 74 en détail

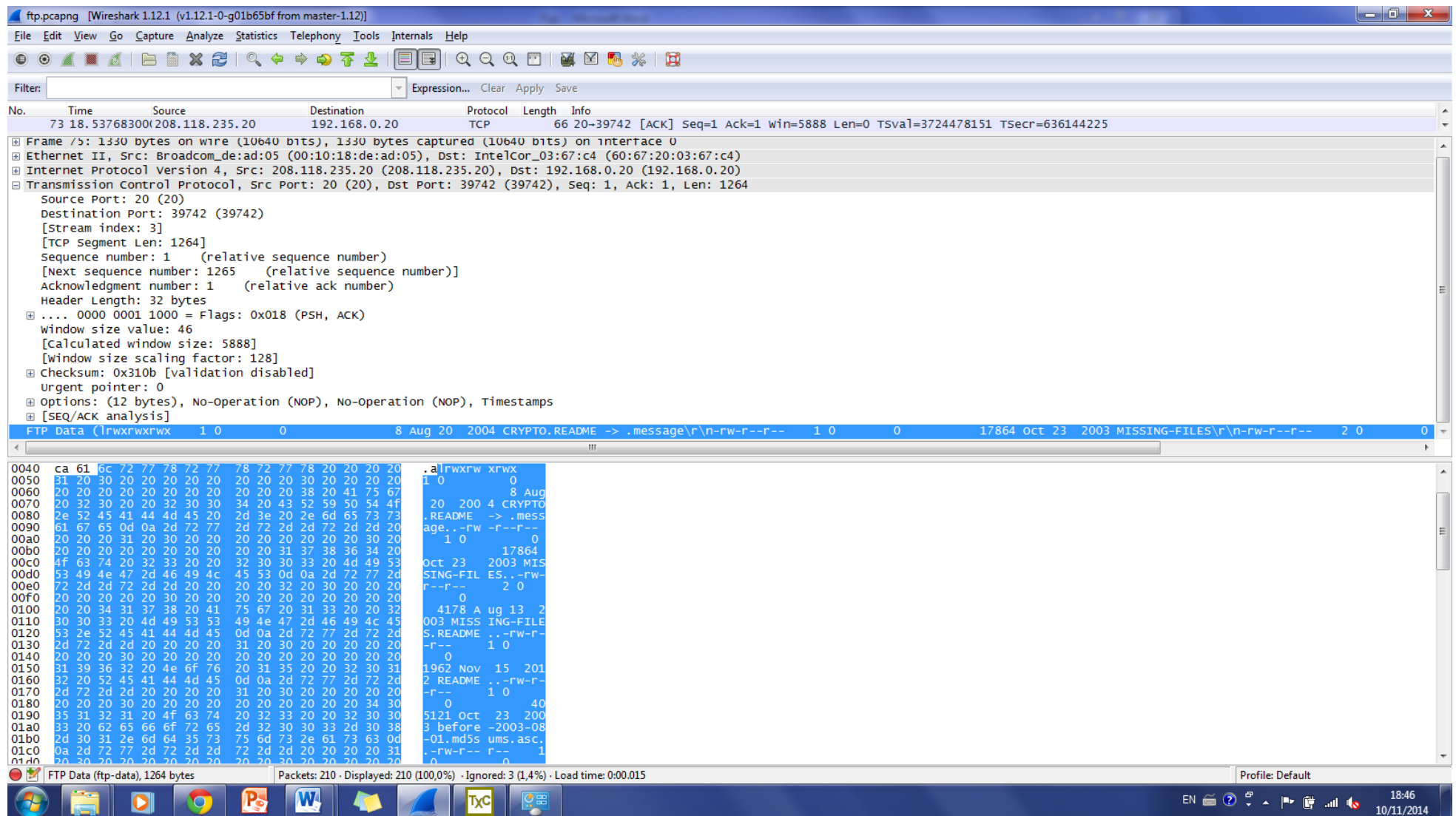


Fig. 8 : Paquet 75 en détail

ftp.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
73	18.53768300	208.118.235.20	192.168.0.20	TCP	66	20→39742 [ACK] Seq=1 Ack=1 win=5888 Len=0 TSval=3724478151 TSecr=636144225
74	18.53818500	208.118.235.20	192.168.0.20	FTP	105	Response: 150 Here comes the directory listing.
75	18.53948800	208.118.235.20	192.168.0.20	FTP-DATA	1330	FTP Data: 1264 bytes
76	18.53965000	192.168.0.20	208.118.235.20	TCP	66	39742→20 [ACK] Seq=1 Ack=1265 win=31488 Len=0 TSval=636144251 TSecr=3724478151
77	18.53994500	208.118.235.20	192.168.0.20	TCP	66	20→39742 [FIN, ACK] Seq=1265 Ack=1 win=5888 Len=0 TSval=3724478151 TSecr=636144225
78	18.54051500	192.168.0.20	208.118.235.20	TCP	66	39742→20 [FIN, ACK] Seq=1 Ack=1266 win=31488 Len=0 TSval=636144251 TSecr=3724478151
79	18.57455100	192.168.0.20	208.118.235.20	TCP	66	54866→21 [ACK] Seq=55 Ack=800 win=30336 Len=0 TSval=636144260 TSecr=3724478151
80	18.64596600	208.118.235.20	192.168.0.20	TCP	66	20→39742 [ACK] Seq=1266 Ack=2 win=5888 Len=0 TSval=3724478161 TSecr=636144251
81	18.64659900	208.118.235.20	192.168.0.20	FTP	90	Response: 226 Directory send OK.
82	18.64672700	192.168.0.20	208.118.235.20	TCP	66	54866→21 [ACK] Seq=55 Ack=824 win=30336 Len=0 TSval=636144278 TSecr=3724478161
83	19.96701500	192.168.0.13	239.255.255.250	SSDP	378	NOTIFY * HTTP/1.1
84	20.17164700	192.168.0.13	239.255.255.250	SSDP	387	NOTIFY * HTTP/1.1
85	20.17550800	192.168.0.13	239.255.255.250	SSDP	418	NOTIFY * HTTP/1.1

Frame 76: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

- Ethernet II, Src: IntelCor_03:67:c4 (60:67:20:03:67:c4), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
- Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: 208.118.235.20 (208.118.235.20)
- Transmission Control Protocol, Src Port: 39742 (39742), Dst Port: 20 (20), Seq: 1, Ack: 1265, Len: 0
 - Source Port: 39742 (39742)
 - Destination Port: 20 (20)
 - [Stream index: 3]
 - [TCP Segment Len: 0]
 - Sequence number: 1 (relative sequence number)
 - Acknowledgment number: 1265 (relative ack number)
 - Header Length: 32 bytes
 - 0000 0001 0000 = Flags: 0x010 (ACK)
 - Window size value: 246
 - [Calculated window size: 31488]
 - [Window size scaling factor: 128]
 - Checksum: 0x7dc1 [validation disabled]
 - Urgent pointer: 0
 - Options: (12 bytes), No-operation (NOP), No-operation (NOP), Timestamps
 - [SEQ/ACK analysis]
 - [This is an ACK to the segment in frame: 75]
 - [The RTT to ACK the segment was: 0.000162000 seconds]
 - [RTT: 0.101399000 seconds]

```

0000  00 10 18 de ad 05 60 67 20 03 67 c4 08 00 45 08  ....`g .g...E.
0010  00 34 ff de 40 00 40 06 be 95 c0 a8 00 14 d0 76  .4.@.@.....V
0020  eb 14 9b 3e 00 14 1e 16 35 a4 e7 7b d0 08 80 10  .>...5.{...
0030  00 f6 7d c1 00 00 01 01 08 0a 25 ea ca 7b dd ff  .}.....%{...
0040  06 c7

```

Frame (frame), 66 bytes Packets: 210 · Displayed: 210 (100.0%) · Ignored: 3 (1.4%) · Load time: 0:00.015 Profile: Default

Fig.9 : Paquet 76 en détail

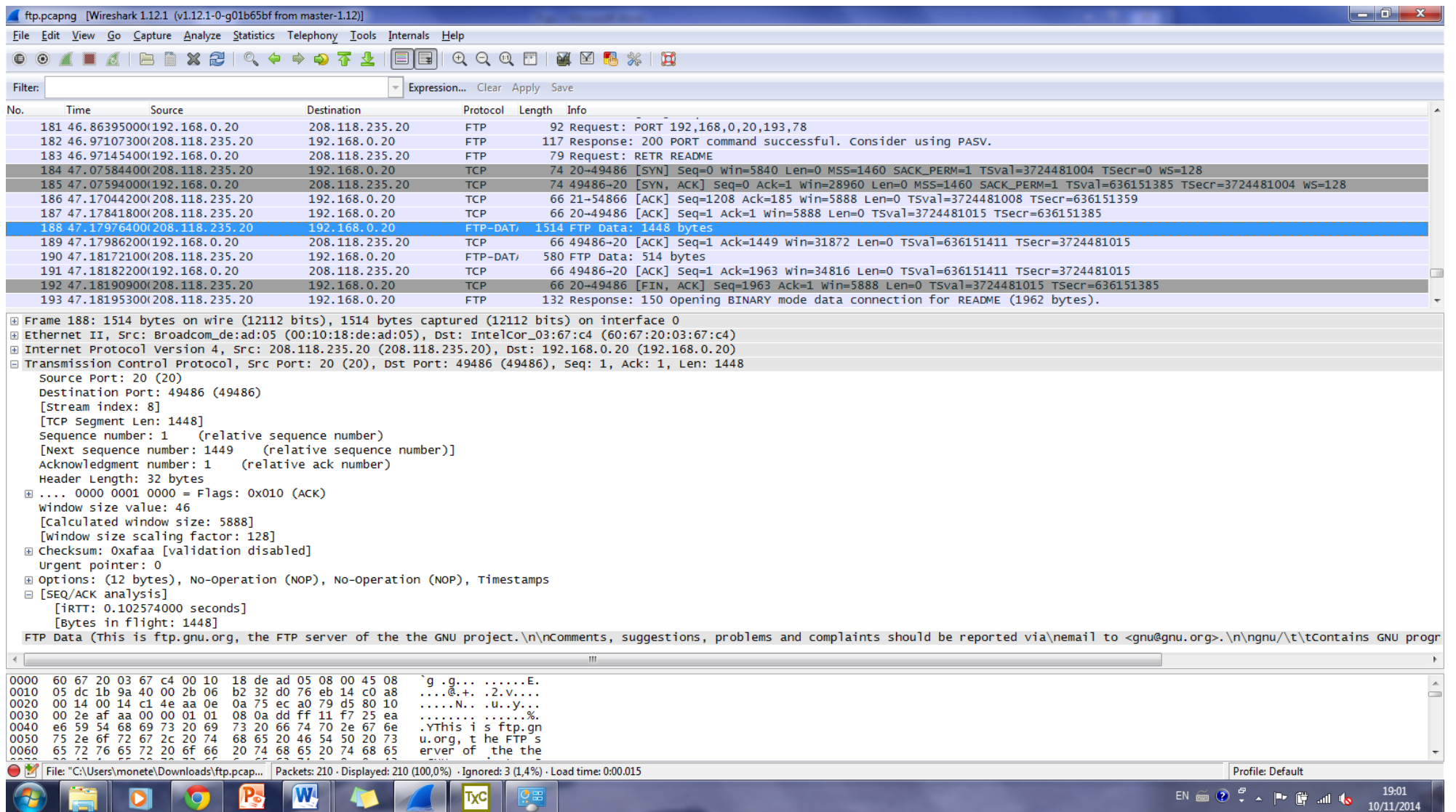


Fig. 10 : Capture Paquets sur FTP

ftp.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
189	47.17986200	192.168.0.20	208.118.235.20	TCP	66	49486→20 [ACK] Seq=1 Ack=1449 win=31872 Len=0 TSval=636151411 TSecr=3724481015
190	47.18172100	208.118.235.20	192.168.0.20	FTP-DAT	580	FTP Data: 514 bytes
191	47.18182200	192.168.0.20	208.118.235.20	TCP	66	49486→20 [ACK] Seq=1 Ack=1963 win=34816 Len=0 TSval=636151411 TSecr=3724481015
192	47.18190900	208.118.235.20	192.168.0.20	TCP	66	20→49486 [FIN, ACK] Seq=1963 Ack=1 win=5888 Len=0 TSval=3724481015 TSecr=636151385
193	47.18195300	208.118.235.20	192.168.0.20	FTP	132	Response: 150 Opening BINARY mode data connection for README (1962 bytes).
194	47.18314400	192.168.0.20	208.118.235.20	TCP	66	49486→20 [FIN, ACK] Seq=1 Ack=1964 win=34816 Len=0 TSval=636151412 TSecr=3724481015
195	47.21862900	192.168.0.20	208.118.235.20	TCP	66	54866→21 [ACK] Seq=185 Ack=1274 win=30336 Len=0 TSval=636151421 TSecr=3724481015
196	47.28883800	208.118.235.20	192.168.0.20	TCP	66	20→49486 [ACK] Seq=1964 Ack=2 win=5888 Len=0 TSval=3724481026 TSecr=636151412
197	47.29158100	208.118.235.20	192.168.0.20	FTP	90	Response: 226 Transfer complete.

Frame 193: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0

Ethernet II, Src: Broadcom_de:ad:05 (00:10:18:de:ad:05), Dst: IntelCor_03:67:c4 (60:67:20:03:67:c4)

Internet Protocol Version 4, Src: 208.118.235.20 (208.118.235.20), Dst: 192.168.0.20 (192.168.0.20)

Transmission Control Protocol, Src Port: 21 (21), Dst Port: 54866 (54866), Seq: 1208, Ack: 185, Len: 66

Source Port: 21 (21)

Destination Port: 54866 (54866)

[Stream index: 2]

[TCP Segment Len: 66]

Sequence number: 1208 (relative sequence number)

[Next sequence number: 1274 (relative sequence number)]

Acknowledgment number: 185 (relative ack number)

Header Length: 32 bytes

.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)

Window size value: 46

[Calculated window size: 5888]

[Window size scaling factor: 128]

Checksum: 0xeea5 [validation disabled]

Urgent pointer: 0

Options: (12 bytes), No-operation (NOP), No-operation (NOP), Timestamps

[SEQ/ACK analysis]

[RTT: 0.104489000 seconds]

[Bytes in flight: 66]

File Transfer Protocol (FTP)

150 Opening BINARY mode data connection for README (1962 bytes).\r\n

Response code: File status okay; about to open data connection (150)

Response arg: Opening BINARY mode data connection for README (1962 bytes).

0020 00 14 00 15 d6 52 82 b4 27 34 87 f8 bf e2 80 18R.. '4.....

0030 00 2e ee ae a5 00 00 01 01 08 0a dd ff 11 f7 25 ea%.....

0040 e6 3f 31 35 30 20 4f 70 65 6e 69 6e 67 20 42 49 .?150 Op ening BI

0050 4e 41 52 59 20 6d 6f 64 65 20 64 61 74 61 20 63 NARY mod e data c

0060 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 72 20 52 45 onnectio n for RE

0070 41 44 4d 45 20 28 31 39 36 32 20 62 79 74 65 73 ADME (19 62 bytes

0080 29 2e 0d 0a)..

Response arg (ftp.response.arg), 60 bytes

Packets: 210 · Displayed: 210 (100.0%) · Ignored: 3 (1.4%) · Load time: 0:00.015

Profile: Default

19:07 10/11/2014

Fig. 11 : Paquet 194 en détail.