Challenge Root Me

Réseau

FTP - Authentification

Énoncé

Un échange authentifié de fichier réalisé grâce au protocole FTP. Retrouvez le mot de passe utilisé par l'utilisateur.

La ressource fournit comprend un unique fichier ch1.pcap qui peut être lu par le logiciel Wireshark permettant d'analyser les paquets transmis sur le réseau.
On cherche un échange authentifié grâce au protocole FTP.
On y observe le mot de passe à trouver en brut.

TELNET - Authentification

Énoncé

Retrouvez le mot de passe de l'utilisateur dans cette capture réseau de session TELNET.

La ressource fournit comprend un fichier également en .pcap.
On récupère la capture et on l'ouvre avec Wireshark. On voit un échange entre 2 machines. Les 3 premiers segments TCP nous montre qu'il y a ouverture de connexion, grâce aux bytes : SYN, SYN/ACK, ACK. Les informations de connexions ne doivent donc pas être très loin.
Et pour se faciliter la chose, WireShark intègre une option, qui ici, va nous être super utile : le "Follow TCP Stream ». On y trouve le password.

TWITTER - Authentification

Énoncé

Une session d'authentification twitter a été capturée. Retrouvez le mot de passe de l'utilisateur dans cette capture réseau.

On analyse l'unique trame avec Wireshark, il est présenté une authentification sur le réseau social Twitter via le protocole HTTP.

En déroulant les menus notamment l'autorisation, on observe la méthode basic avec le mot de passe crypté en base 64. Il suffit alors de le décrypté mais Wireshark le fait automatiquement.

ETHERNET - Trame

Énoncé

Retrouvez les données normalement confidentielles contenues dans cette trame.

```
00 05 73 a0 00 00 e0 69 95 d8 5a 13 86 dd 60 00
00 00 00 9b 06 40 26 07 53 00 00 60 2a bc 00 00
00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00
00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1
d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e
69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74
69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a
6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d
0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73
61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74
3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67
0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d
0a
```

On observe une trame en hexadecimal, on retire tous les espaces puis on converti la trame en ASCII:

```
??s????i??Z???`??????@&?S??`*????????? ?A???B3?????????t?P??}?????????????????>i???~?GET / HTTP/
1.1??Authorization: Basic Y29uZmk6ZGVudGlhbA==??User-Agent: InsaneBrowser??Host: www.myipv6.org??
Accept: */*????
```

On repère : Authorization : Basic Y29uZmk6ZGVudGlhbA==
On tente de la décodé en base 64 puis on trouve: confi:dential

CISCO - Mot de passe

Énoncé

Trouvez le mot de passe « Enable".

La ressource nous fournit l'historique des lignes de commandes, nous y observons différents mots de passes.
Notamment avec des sécurités différentes. Grâce au ressource Cisco proposé nous savons que le: type 7 est un mot de passe avec un cryptage faible.
Les mots de passe de type 7 peuvent être décrypté à l'aide d'outils accessibles au public.
Sachant sa on cherche sur internet un décrypteur Cisco pour lire les mots de passes de niveau 7 on trouve ceux-ci:
username hub password 7 025017705B3907344E —> 6sK0_hub
username admin privilege 15 password 7 10181A325528130F010D24—> 6sK0_admin
username guest password 7 124F163C42340B112F3830 —> 6sK0_guest
On prend du recule et on observe la logique utiliser pour déterminer les mots de passes. On peut donc supposer: 6sK0_enable enfin cela est juste.

IP - Time to live

Énoncé

Retrouvez le TTL employé pour atteindre l'hôte ciblé par cet échange de paquets ICMP.

Dans ce challenge,on ouvre la capture réseau dans Wireshark.
En analysant la conversation, on observe que les requêtes du serveur meurent à chaque fois tandis que le TTL est incrémenté.
En parcourant la conversation, on voit que la conversation change radicalement à partir de TTL =13 alors qu'avant le serveur affichait que la requête expirait dans le transit

SIP - Authentification

Énoncé

Retrouvez le mot de passe utilisé pour s'authentifier sur l'infrastructure SIP.

```
172.25.105.3"172.25.105.40"555"asterisk"REGISTER"sip:172.25.105.40"4787f7ce"""PLAIN"1234
172.25.105.3"172.25.105.40"555"asterisk"INVITE"sip:1000@172.25.105.40"70fbfdae""""MD5"aa533f6efa2b2abac675c1ee6cbde327
172.25.105.3"172.25.105.40"555"asterisk"BYE"sip:1000@172.25.105.40"70fbfdae"""MD5"0b306e9db1f819dd824acf3227b60e07
```

La première ligne de code indique un mot de passe NON chiffré (plain) qui a pour fonction REGISTER(authentification) le mot de passe est donc 1234 comme indiqué

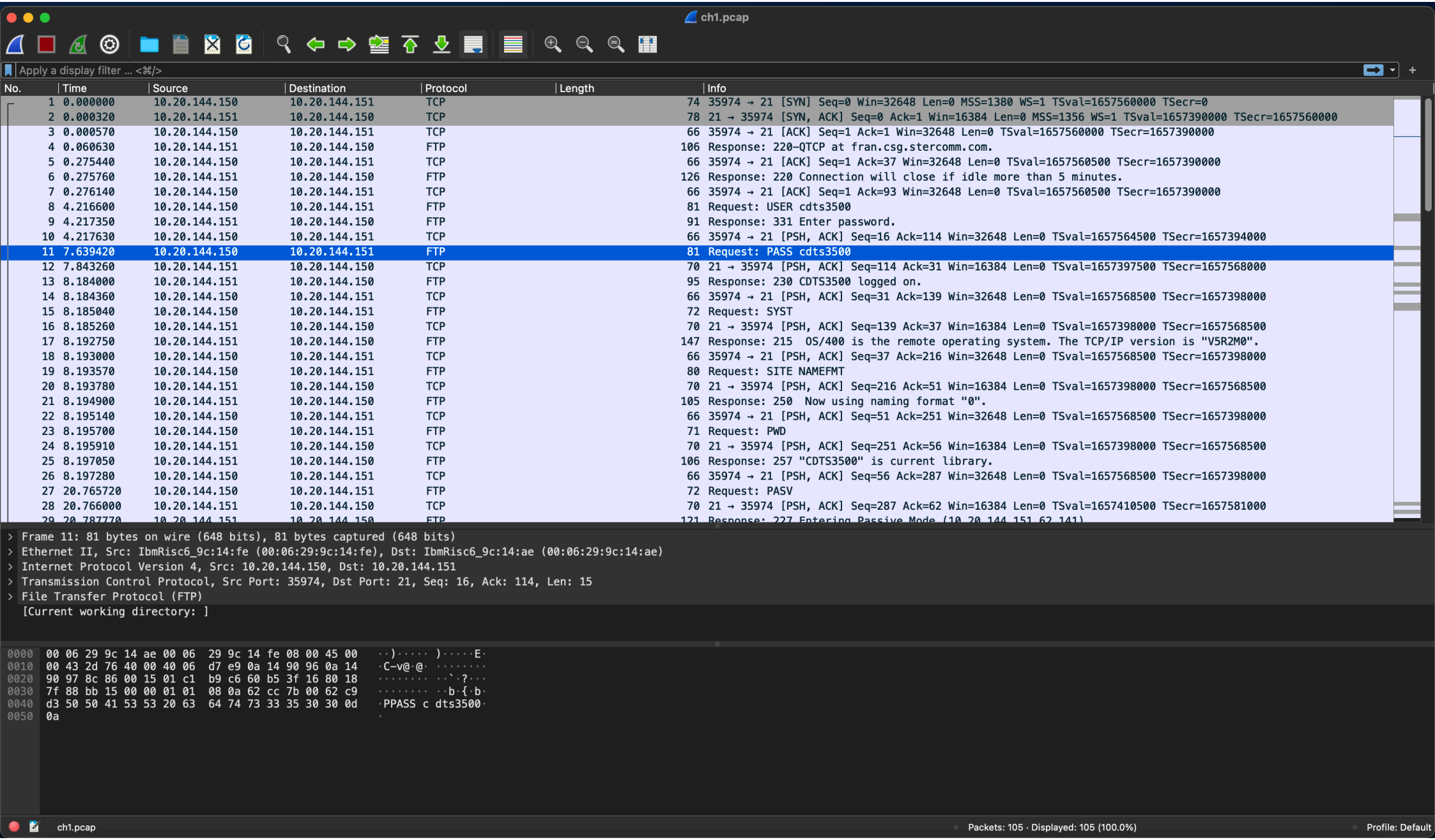
Bluetooth - Fichier inconnu

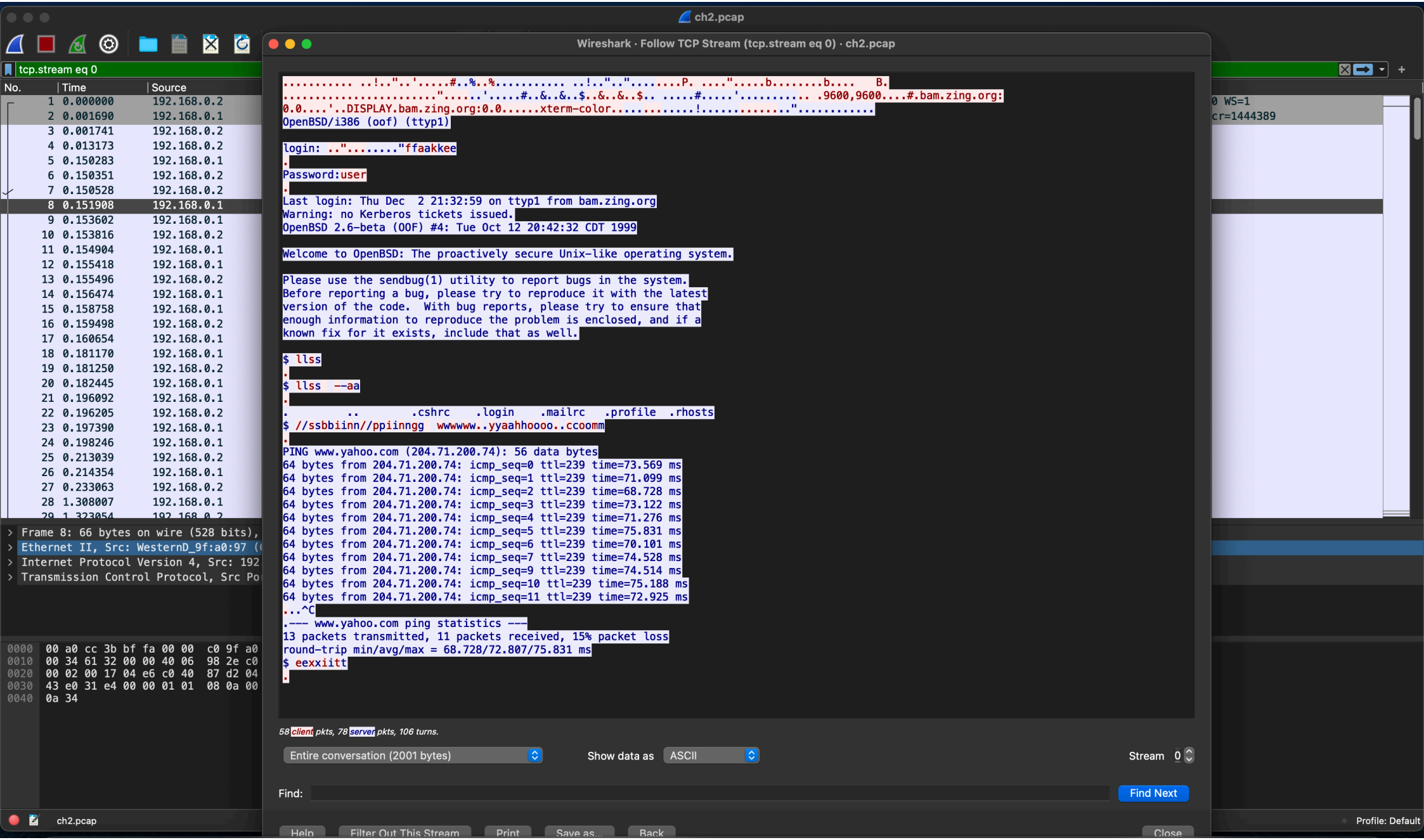
Énoncé

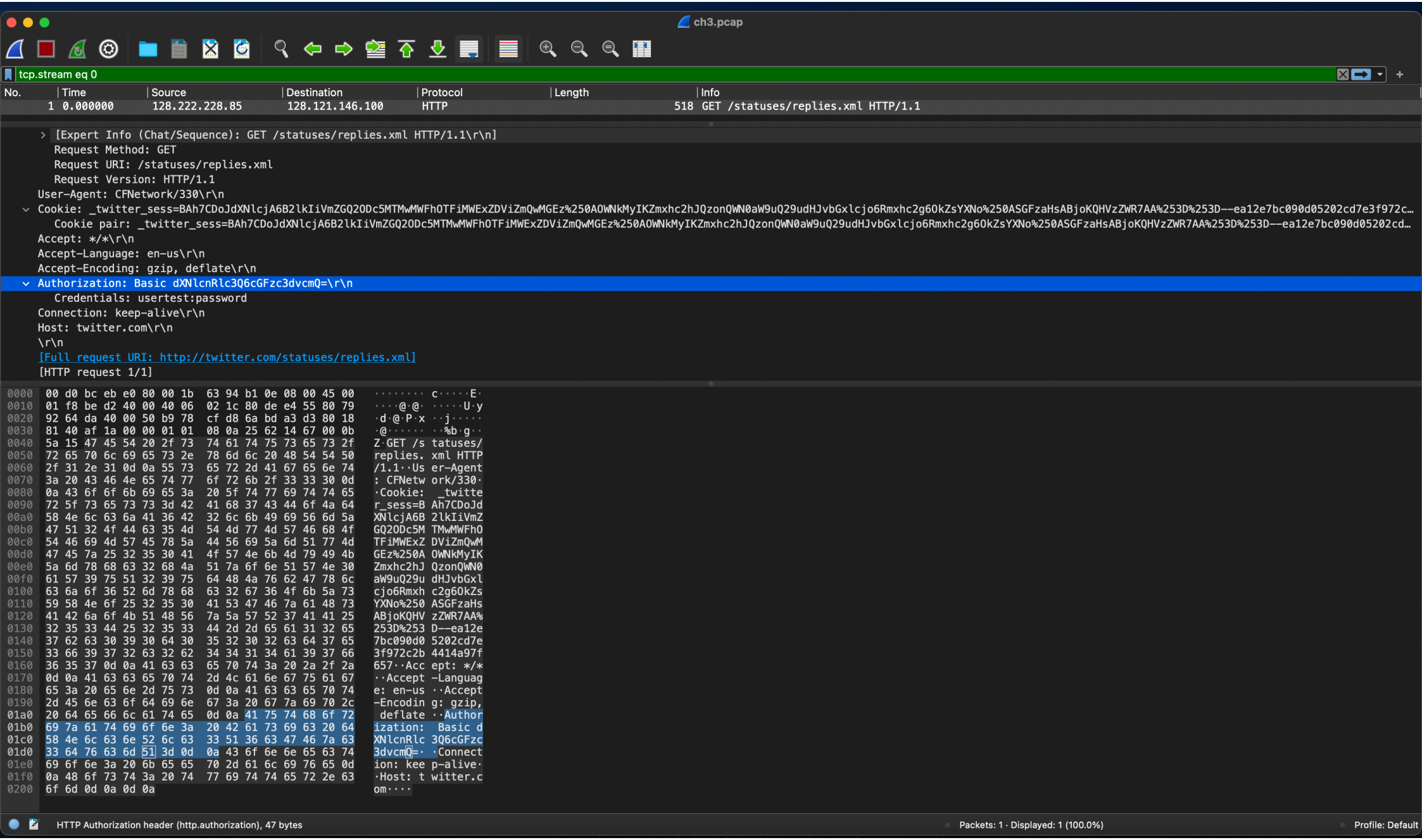
Votre ami travaillant à l'ANSSI a récupéré un fichier illisible dans l'ordi d'un hacker. Tout ce qu'il sait est que cela provient d'un échange entre un ordinateur et un téléphone. A vous d'en apprendre le plus possible sur ce téléphone.

La réponse est le hash SHA1 de la concaténation de l'adresse MAC (en majuscules) et du nom du téléphone.

J'ouvre le fichier .bin à l'aide de Wireshark. Un outil est disponible dans Wireshark, le menu Wireless puis Bluetooth devices. Une fenêtre apparait alors avec tous les appareils de l'échange contenant l'adresse MAC et le nom du téléphone. Je le hash en SHA1 à l'aide d'un convertisseur.

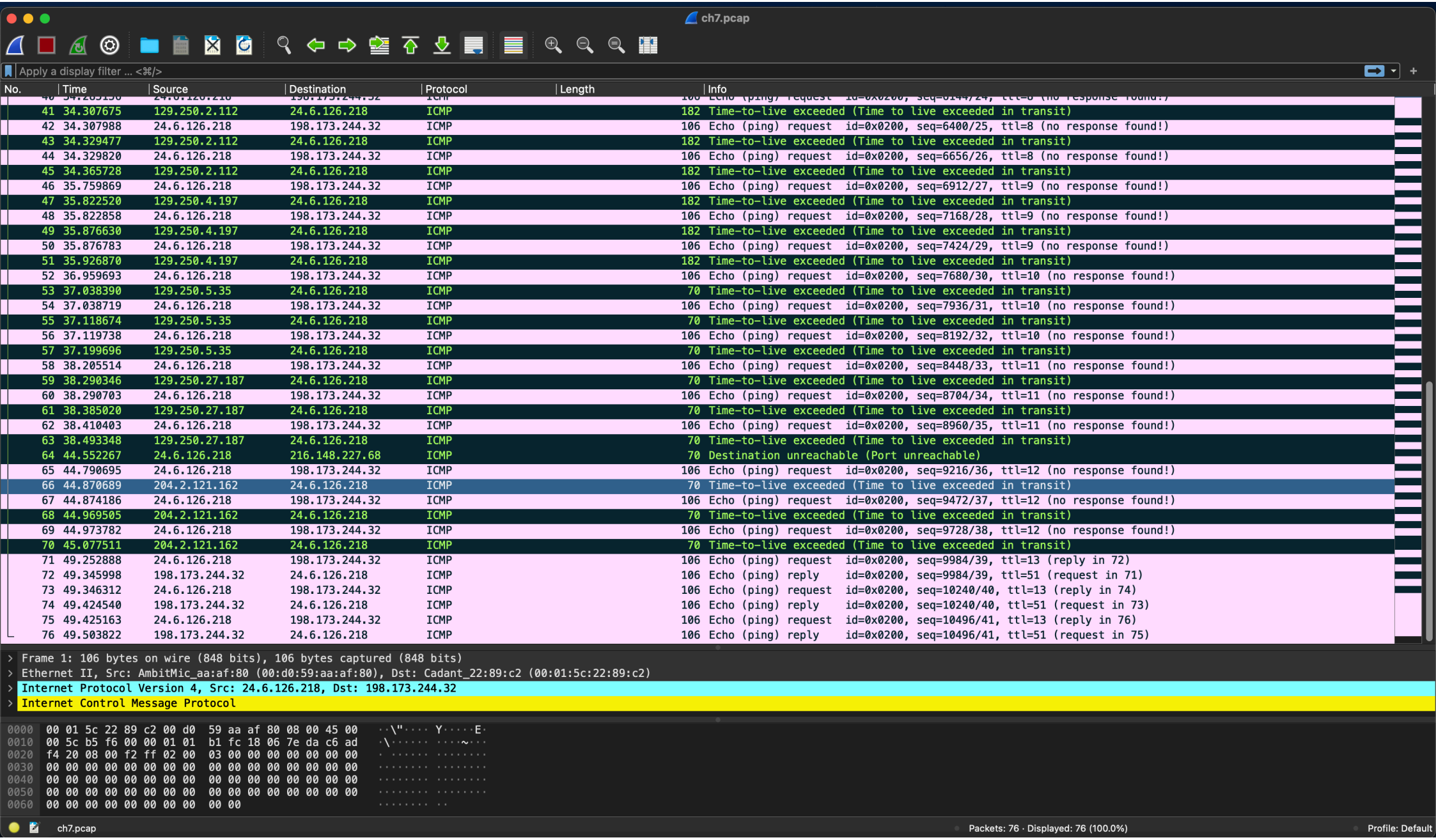

ch1.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.20.144.150 10.20.144.151 TCP 74 35974 → 21 [SYN] Seq=0 Win=32648 Len=0 MSS=1380 WS=1 TSval=1657560000 TSecr=0
2 0.000320 10.20.144.151 10.20.144.150 TCP 78 21 → 35974 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1356 WS=1 TSval=1657390000 TSecr=1657560000
3 0.000570 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [ACK] Seq=1 Ack=1 Win=32648 Len=0 TSval=1657560000 TSecr=1657390000
4 0.060630 10.20.144.151 10.20.144.150 FTP 106 Response: 220-QTCP at fran.csg.stercomm.com.
5 0.275440 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [ACK] Seq=1 Ack=37 Win=32648 Len=0 TSval=1657560500 TSecr=1657390000
6 0.275760 10.20.144.151 10.20.144.150 FTP 126 Response: 220 Connection will close if idle more than 5 minutes.
7 0.276140 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [ACK] Seq=1 Ack=93 Win=32648 Len=0 TSval=1657560500 TSecr=1657390000
8 4.216600 10.20.144.150 10.20.144.151 FTP 81 Request: USER cdts3500
9 4.217350 10.20.144.151 10.20.144.150 FTP 91 Response: 331 Enter password.
10 4.217630 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [PSH, ACK] Seq=16 Ack=114 Win=32648 Len=0 TSval=1657564500 TSecr=1657394000
11 7.639420 10.20.144.150 10.20.144.151 FTP 81 Request: PASS cdts3500
12 7.843260 10.20.144.151 10.20.144.150 TCP 70 21 → 35974 [PSH, ACK] Seq=114 Ack=31 Win=16384 Len=0 TSval=1657397500 TSecr=1657568000
13 8.184000 10.20.144.151 10.20.144.150 FTP 95 Response: 230 CDTS3500 logged on.
14 8.184360 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [PSH, ACK] Seq=31 Ack=139 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
15 8.185040 10.20.144.150 10.20.144.151 FTP 72 Request: SYST
16 8.185260 10.20.144.151 10.20.144.150 TCP 70 21 → 35974 [PSH, ACK] Seq=139 Ack=37 Win=16384 Len=0 TSval=1657398000 TSecr=1657568500
17 8.192750 10.20.144.151 10.20.144.150 FTP 147 Response: 215 OS/400 is the remote operating system. The TCP/IP version is "V5R2M0".
18 8.193000 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [PSH, ACK] Seq=37 Ack=216 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
19 8.193570 10.20.144.150 10.20.144.151 FTP 80 Request: SITE NAMEFMT
20 8.193780 10.20.144.151 10.20.144.150 TCP 70 21 → 35974 [PSH, ACK] Seq=216 Ack=51 Win=16384 Len=0 TSval=1657398000 TSecr=1657568500
21 8.194900 10.20.144.151 10.20.144.150 FTP 105 Response: 250 Now using naming format "0".
22 8.195140 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [PSH, ACK] Seq=51 Ack=251 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
23 8.195700 10.20.144.150 10.20.144.151 FTP 71 Request: PWD
24 8.195910 10.20.144.151 10.20.144.150 TCP 70 21 → 35974 [PSH, ACK] Seq=251 Ack=56 Win=16384 Len=0 TSval=1657398000 TSecr=1657568500
25 8.197050 10.20.144.151 10.20.144.150 FTP 106 Response: 257 "CDTS3500" is current library.
26 8.197280 10.20.144.150 10.20.144.151 TCP 66 35974 → 21 [PSH, ACK] Seq=56 Ack=287 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
27 20.765720 10.20.144.150 10.20.144.151 FTP 72 Request: PASV
28 20.766000 10.20.144.151 10.20.144.150 TCP 70 21 → 35974 [PSH, ACK] Seq=287 Ack=62 Win=16384 Len=0 TSval=1657410500 TSecr=1657581000
Frame 11: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
Ethernet II, Src: IbmRisc6_9c:14:fe (00:06:29:9c:14:fe), Dst: IbmRisc6_9c:14:ae (00:06:29:9c:14:ae)
Internet Protocol Version 4, Src: 10.20.144.150, Dst: 10.20.144.151
Transmission Control Protocol, Src Port: 35974, Dst Port: 21, Seq: 16, Ack: 114, Len: 15
File Transfer Protocol (FTP)
[Current working directory:]
0000 00 06 29 9c 14 ae 00 06 29 9c 14 fe 08 00 45 00
0010 00 43 2d 76 40 00 40 06 d7 e9 0a 14 90 96 0a 14
0020 90 97 8c 86 00 15 01 c1 b9 c6 60 b5 3f 16 80 18
0030 7f 88 bb 15 00 00 01 01 08 0a 62 cc 7b 00 62 c9
0040 d3 50 50 41 53 53 20 63 64 74 73 33 35 30 30 0d
0050 0a
ch1.pcap
Packets: 105 · Displayed: 105 (100.0%)
Profile: Default

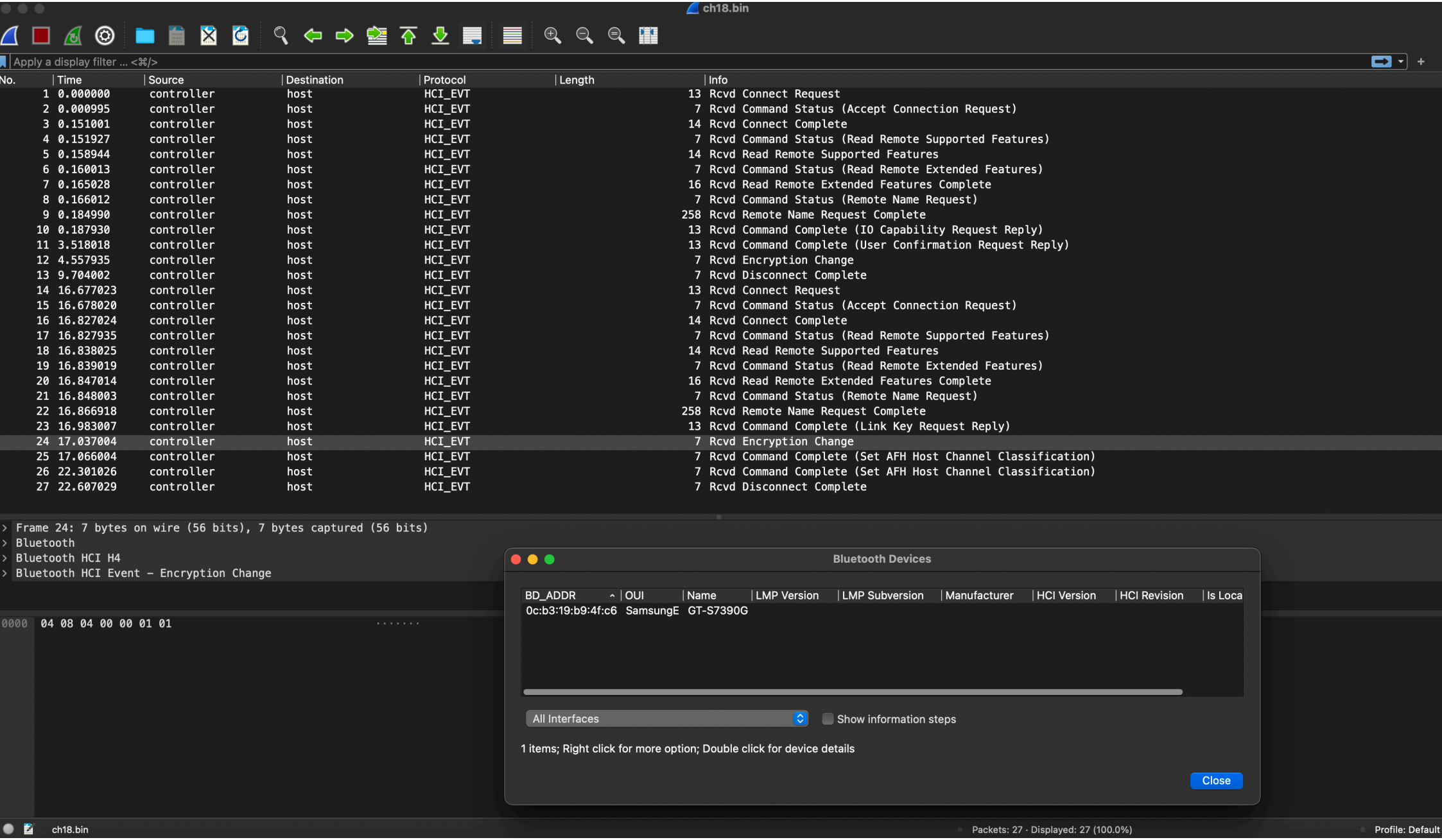

ch2.pcap
Wireshark · Follow TCP Stream (tcp.stream eq 0) · ch2.pcap
tcp.stream eq 0
No. Time Source
1 0.000000 192.168.0.2
2 0.001690 192.168.0.1
3 0.001741 192.168.0.2
4 0.013173 192.168.0.2
5 0.150283 192.168.0.1
6 0.150351 192.168.0.2
7 0.150528 192.168.0.2
8 0.151908 192.168.0.1
9 0.153602 192.168.0.1
10 0.153816 192.168.0.2
11 0.154904 192.168.0.1
12 0.155418 192.168.0.1
13 0.155496 192.168.0.2
14 0.156474 192.168.0.1
15 0.158758 192.168.0.1
16 0.159498 192.168.0.2
17 0.160654 192.168.0.1
18 0.181170 192.168.0.1
19 0.181250 192.168.0.2
20 0.182445 192.168.0.1
21 0.196092 192.168.0.1
22 0.196205 192.168.0.2
23 0.197390 192.168.0.1
24 0.198246 192.168.0.1
25 0.213039 192.168.0.2
26 0.214354 192.168.0.1
27 0.233063 192.168.0.2
28 1.308007 192.168.0.1
OpenBSD/i386 (oof) (ttyp1)
login: ..".....".ffaakkee
Password:user
Last login: Thu Dec 2 21:32:59 on ttyp1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999
Welcome to OpenBSD: The proactively secure Unix-like operating system.
Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.
$ llss
$ llss --aa
. .. .cshrc .login .mailrc .profile .rhosts
$ //ssbbiinn//ppiinngg wwwwww..yyaahhoooo..ccoomm
PING www.yahoo.com (204.71.200.74): 56 data bytes
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
...^C
.--- www.yahoo.com ping statistics ---
13 packets transmitted, 11 packets received, 15% packet loss
round-trip min/avg/max = 68.728/72.807/75.831 ms
$ eexxiitt
58 client pkts, 78 server pkts, 106 turns.
Entire conversation (2001 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close
Frame 8: 66 bytes on wire (528 bits),
Ethernet II, Src: WesternD_9f:a0:97 (
Internet Protocol Version 4, Src: 192
Transmission Control Protocol, Src Po
0000 00 a0 cc 3b bf fa 00 00 c0 9f a0
0010 00 34 61 32 00 00 40 06 98 2e c0
0020 00 02 00 17 04 e6 c0 40 87 d2 04
0030 43 e0 31 e4 00 00 01 01 08 0a 00
0040 0a 34
ch2.pcap
Profile: Default


ch3.pcap
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
1 0.000000 128.222.228.85 128.121.146.100 HTTP 518 GET /statuses/replies.xml HTTP/1.1
[Expert Info (Chat/Sequence): GET /statuses/replies.xml HTTP/1.1\r\n]
Request Method: GET
Request URI: /statuses/replies.xml
Request Version: HTTP/1.1
User-Agent: CFNetwork/330\r\n
Cookie: _twitter_sess=BAh7CDoJdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWFhOTFiMWExZDViZmQwMGEz%250AOWNkMyIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGFzaHsABjoKQHVzZWR7AA%253D%253D--ea12e7bc090d05202cd7e3f972c…
Cookie pair: _twitter_sess=BAh7CDoJdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWFhOTFiMWExZDViZmQwMGEz%250AOWNkMyIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGFzaHsABjoKQHVzZWR7AA%253D%253D--ea12e7bc090d05202cd…
Accept: */*\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
Authorization: Basic dXNlcnRlc3Q6cGFzc3dvcmQ=\r\n
Credentials: usertest:password
Connection: keep-alive\r\n
Host: twitter.com\r\n
\r\n
[Full request URI: http://twitter.com/statuses/replies.xml]
[HTTP request 1/1]
0000 00 d0 bc eb e0 80 00 1b 63 94 b1 0e 08 00 45 00 ···· ···· c·····E·
0010 01 f8 be d2 40 00 40 06 02 1c 80 de e4 55 80 79 ····@·@· ·····U·y
0020 92 64 da 40 00 50 b9 78 cf d8 6a bd a3 d3 80 18 ·d·@·P·x ··j·····
0030 81 40 af 1a 00 00 01 01 08 0a 25 62 14 67 00 0b ·@····· ··%b·g··
0040 5a 15 47 45 54 20 2f 73 74 61 74 75 73 65 73 2f Z·GET /s tatuses/
0050 72 65 70 6c 69 65 73 2e 78 6d 6c 20 48 54 54 50 replies. xml HTTP
0060 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 /1.1··Us er-Agent
0070 3a 20 43 46 4e 65 74 77 6f 72 6b 2f 33 33 30 0d : CFNetw ork/330·
0080 0a 43 6f 6f 6b 69 65 3a 20 5f 74 77 69 74 74 65 ·Cookie: _twitte
0090 72 5f 73 65 73 73 3d 42 41 68 37 43 44 6f 4a 64 r_sess=B Ah7CDoJd
00a0 58 4e 6c 63 6a 41 36 42 32 6c 6b 49 69 56 6d 5a XNlcjA6B 2lkIiVmZ
00b0 47 51 32 4f 44 63 35 4d 54 4d 77 4d 57 46 68 4f GQ2ODc5M TMwMWFhO
00c0 54 46 69 4d 57 45 78 5a 44 56 69 5a 6d 51 77 4d TFiMWExZ DViZmQwM
00d0 47 45 7a 25 32 35 30 41 4f 57 4e 6b 4d 79 49 4b GEz%250A OWNkMyIK
00e0 5a 6d 78 68 63 32 68 4a 51 7a 6f 6e 51 57 4e 30 Zmxhc2hJ QzonQWN0
00f0 61 57 39 75 51 32 39 75 64 48 4a 76 62 47 78 6c aW9uQ29u dHJvbGxl
0100 63 6a 6f 36 52 6d 78 68 63 32 67 36 4f 6b 5a 73 cjo6Rmxh c2g6OkZs
0110 59 58 4e 6f 25 32 35 30 41 53 47 46 7a 61 48 73 YXNo%250 ASGFzaHs
0120 41 42 6a 6f 4b 51 48 56 7a 5a 57 52 37 41 41 25 ABjoKQHV zZWR7AA%
0130 32 35 33 44 25 32 35 33 44 2d 2d 65 61 31 32 65 253D%253 D--ea12e
0140 37 62 63 30 39 30 64 30 35 32 30 32 63 64 37 65 7bc090d0 5202cd7e
0150 33 66 39 37 32 63 32 62 34 34 31 34 61 39 37 66 3f972c2b 4414a97f
0160 36 35 37 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 657··Acc ept: */*
0170 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 ··Accept -Languag
0180 65 3a 20 65 6e 2d 75 73 0d 0a 41 63 63 65 70 74 e: en-us ··Accept
0190 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,
01a0 20 64 65 66 6c 61 74 65 0d 0a 41 75 74 68 6f 72 deflate ··Author
01b0 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 64 ization: Basic d
01c0 58 4e 6c 63 6e 52 6c 63 33 51 36 63 47 46 7a 63 XNlcnRlc 3Q6cGFzc
01d0 33 64 76 63 6d 51 3d 0d 0a 43 6f 6e 6e 65 63 74 3dvcmQ=· ·Connect
01e0 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: kee p-alive·
01f0 0a 48 6f 73 74 3a 20 74 77 69 74 74 65 72 2e 63 ·Host: t witter.c
0200 6f 6d 0d 0a 0d 0a om····
HTTP Authorization header (http.authorization), 47 bytes
Packets: 1 · Displayed: 1 (100.0%)
Profile: Default

```
!
! Last configuration change at 13:41:43 CET Mon Jul 8 2013 by
admin
! NVRAM config last updated at 11:15:05 CET Thu Jun 13 2013
by admin
!
version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname rmt-paris
!
security passwords min-length 8
no logging console
enable secret 5 $1$p8Y6$MCdRLBzuGlfOs9S.hXOp0.
!
username hub password 7 025017705B3907344E
username admin privilege 15 password 7 10181A325528130F010D24
username guest password 7 124F163C42340B112F3830
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
interface BRI0/0
 ip address 192.168.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 dialer map ip 192.168.1.1 name hub broadcast 5772222
 dialer-group 1
 isdn switch-type basic-5ess
 ppp authentication chap callin
 no shutdown
!
!
interface GigabitEthernet1/15
 ip address 192.168.2.1 255.255.255.0
 no shutdown
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 bgp dampening
```

```
 network 192.168.2.0 mask 255.255.255.0
 timers bgp 3 9
 redistribute connected
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line con 0
 password 7 144101205C3B29242A3B3C3927
 session-timeout 600
line vty 0 4
 session-timeout 600
 authorization exec SSH
 transport input ssh
```


ch7.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
41 34.307675 129.250.2.112 24.6.126.218 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
42 34.307988 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=6400/25, ttl=8 (no response found!)
43 34.329477 129.250.2.112 24.6.126.218 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
44 34.329820 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=6656/26, ttl=8 (no response found!)
45 34.365728 129.250.2.112 24.6.126.218 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
46 35.759869 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=6912/27, ttl=9 (no response found!)
47 35.822520 129.250.4.197 24.6.126.218 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
48 35.822858 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=7168/28, ttl=9 (no response found!)
49 35.876630 129.250.4.197 24.6.126.218 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
50 35.876783 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=7424/29, ttl=9 (no response found!)
51 35.926870 129.250.4.197 24.6.126.218 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
52 36.959693 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=7680/30, ttl=10 (no response found!)
53 37.038390 129.250.5.35 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
54 37.038719 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=7936/31, ttl=10 (no response found!)
55 37.118674 129.250.5.35 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
56 37.119738 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=8192/32, ttl=10 (no response found!)
57 37.199696 129.250.5.35 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
58 38.205514 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=8448/33, ttl=11 (no response found!)
59 38.290346 129.250.27.187 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
60 38.290703 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=8704/34, ttl=11 (no response found!)
61 38.385020 129.250.27.187 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
62 38.410403 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=8960/35, ttl=11 (no response found!)
63 38.493348 129.250.27.187 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
64 44.552267 24.6.126.218 216.148.227.68 ICMP 70 Destination unreachable (Port unreachable)
65 44.790695 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=9216/36, ttl=12 (no response found!)
66 44.870689 204.2.121.162 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
67 44.874186 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=9472/37, ttl=12 (no response found!)
68 44.969505 204.2.121.162 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
69 44.973782 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=9728/38, ttl=12 (no response found!)
70 45.077511 204.2.121.162 24.6.126.218 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
71 49.252888 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=9984/39, ttl=13 (reply in 72)
72 49.345998 198.173.244.32 24.6.126.218 ICMP 106 Echo (ping) reply id=0x0200, seq=9984/39, ttl=51 (request in 71)
73 49.346312 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=10240/40, ttl=13 (reply in 74)
74 49.424540 198.173.244.32 24.6.126.218 ICMP 106 Echo (ping) reply id=0x0200, seq=10240/40, ttl=51 (request in 73)
75 49.425163 24.6.126.218 198.173.244.32 ICMP 106 Echo (ping) request id=0x0200, seq=10496/41, ttl=13 (reply in 76)
76 49.503822 198.173.244.32 24.6.126.218 ICMP 106 Echo (ping) reply id=0x0200, seq=10496/41, ttl=51 (request in 75)
Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: AmbitMic_aa:af:80 (00:d0:59:aa:af:80), Dst: Cadant_22:89:c2 (00:01:5c:22:89:c2)
Internet Protocol Version 4, Src: 24.6.126.218, Dst: 198.173.244.32
Internet Control Message Protocol
0000 00 01 5c 22 89 c2 00 d0 59 aa af 80 08 00 45 00
0010 00 5c b5 f6 00 00 01 01 b1 fc 18 06 7e da c6 ad
0020 f4 20 08 00 f2 ff 02 00 03 00 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00
ch7.pcap
Packets: 76 · Displayed: 76 (100.0%)
Profile: Default


ch18.bin
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 controller host HCI_EVT 13 Rcvd Connect Request
2 0.000995 controller host HCI_EVT 7 Rcvd Command Status (Accept Connection Request)
3 0.151001 controller host HCI_EVT 14 Rcvd Connect Complete
4 0.151927 controller host HCI_EVT 7 Rcvd Command Status (Read Remote Supported Features)
5 0.158944 controller host HCI_EVT 14 Rcvd Read Remote Supported Features
6 0.160013 controller host HCI_EVT 7 Rcvd Command Status (Read Remote Extended Features)
7 0.165028 controller host HCI_EVT 16 Rcvd Read Remote Extended Features Complete
8 0.166012 controller host HCI_EVT 7 Rcvd Command Status (Remote Name Request)
9 0.184990 controller host HCI_EVT 258 Rcvd Remote Name Request Complete
10 0.187930 controller host HCI_EVT 13 Rcvd Command Complete (IO Capability Request Reply)
11 3.518018 controller host HCI_EVT 13 Rcvd Command Complete (User Confirmation Request Reply)
12 4.557935 controller host HCI_EVT 7 Rcvd Encryption Change
13 9.704002 controller host HCI_EVT 7 Rcvd Disconnect Complete
14 16.677023 controller host HCI_EVT 13 Rcvd Connect Request
15 16.678020 controller host HCI_EVT 7 Rcvd Command Status (Accept Connection Request)
16 16.827024 controller host HCI_EVT 14 Rcvd Connect Complete
17 16.827935 controller host HCI_EVT 7 Rcvd Command Status (Read Remote Supported Features)
18 16.838025 controller host HCI_EVT 14 Rcvd Read Remote Supported Features
19 16.839019 controller host HCI_EVT 7 Rcvd Command Status (Read Remote Extended Features)
20 16.847014 controller host HCI_EVT 16 Rcvd Read Remote Extended Features Complete
21 16.848003 controller host HCI_EVT 7 Rcvd Command Status (Remote Name Request)
22 16.866918 controller host HCI_EVT 258 Rcvd Remote Name Request Complete
23 16.983007 controller host HCI_EVT 13 Rcvd Command Complete (Link Key Request Reply)
24 17.037004 controller host HCI_EVT 7 Rcvd Encryption Change
25 17.066004 controller host HCI_EVT 7 Rcvd Command Complete (Set AFH Host Channel Classification)
26 22.301026 controller host HCI_EVT 7 Rcvd Command Complete (Set AFH Host Channel Classification)
27 22.607029 controller host HCI_EVT 7 Rcvd Disconnect Complete
> Frame 24: 7 bytes on wire (56 bits), 7 bytes captured (56 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI Event – Encryption Change
0000 04 08 04 00 00 01 01 ....
Bluetooth Devices
BD_ADDR OUI Name LMP Version LMP Subversion Manufacturer HCI Version HCI Revision Is Loca
0c:b3:19:b9:4f:c6 SamsungE GT-S7390G
All Interfaces
Show information steps
1 items; Right click for more option; Double click for device details
Close
ch18.bin
Packets: 27 · Displayed: 27 (100.0%)
Profile: Default