Greffe de cœur pour OpenSSL

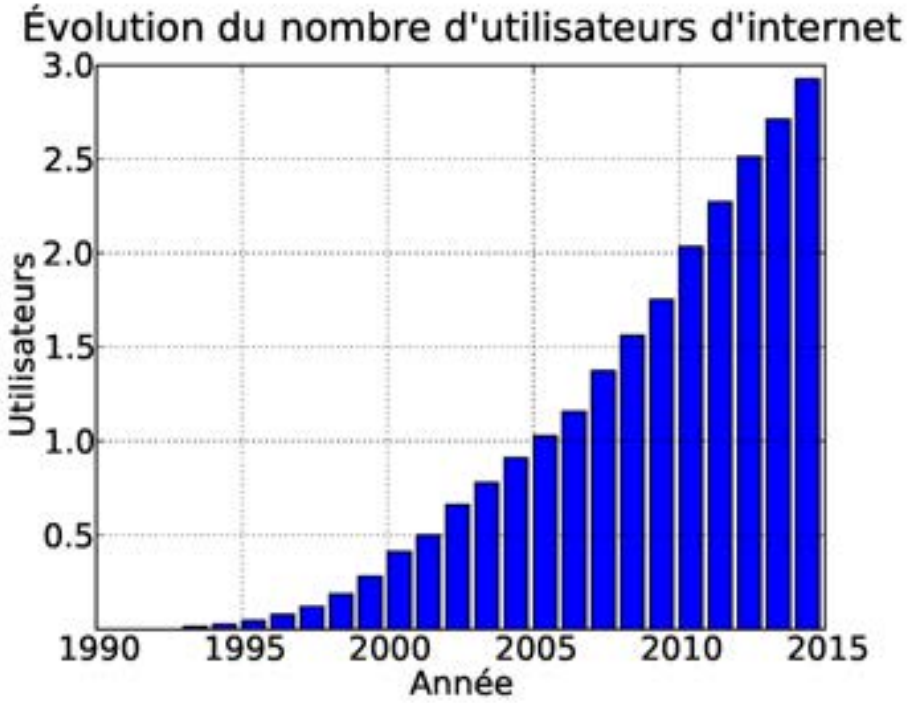
JSSI

Ministère de la Défense

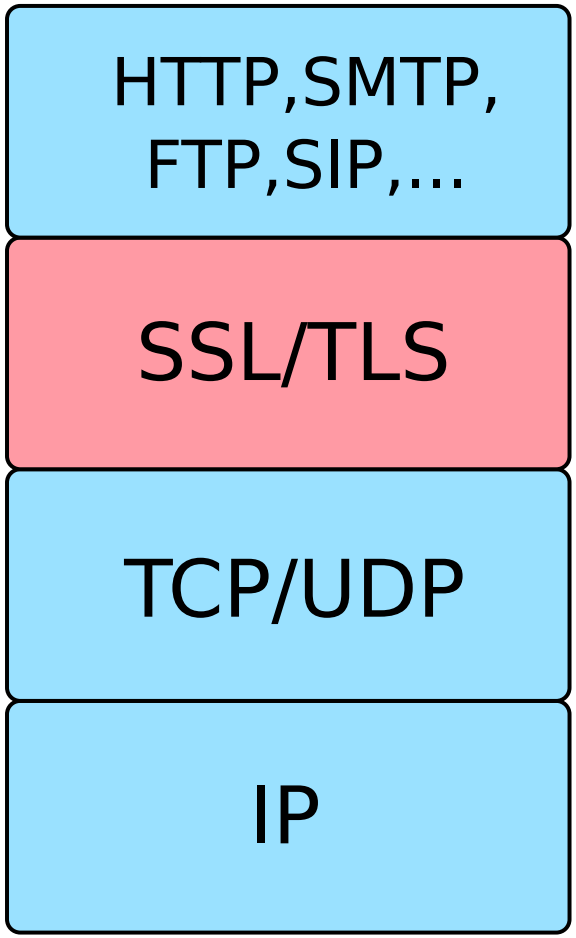
13 Novembre 2014

Évolution de l'exposition des utilisateurs

- Trafic total : $\sim$ 24 To/s
- Utilisateurs de plus en plus exposés :
  - Transactions financières
  - Mails
  - VoIP
  - Vie privée



SSL/TLS



- Authentification
- Confidentialité
- Intégrité

OpenSSL

Cryptography and SSL/TLS Toolkit

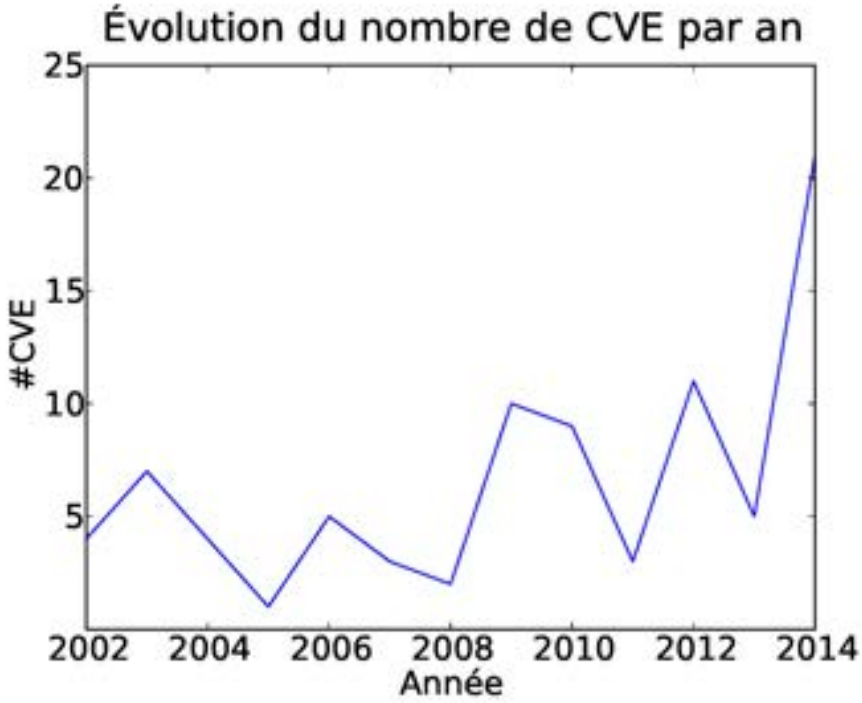
OpenSSL : petit rappel...

- Création : 23/12/98
- Bibliothèque cryptographique + implémentation SSL/TLS
- Open source - communauté mondiale
- Versions Unix/Linux, Microsoft Windows, OpenVMS
- Certification : FIPS 140-2
- Utilisation : Apache + Nginx = 66% du marché

La sécu dans tout ça

Quelques petites failles...

- Timing attacks
  - Clés privées RSA - 2003
  - Clés symétriques - 2013
- Deni de service
  - Parsing ASN.1 - 2003
  - OCSP stapling - 2011
- Affaiblissement cryptographique
  - Debian - 2008
  - Injection CCS - 2014



Heartbleed

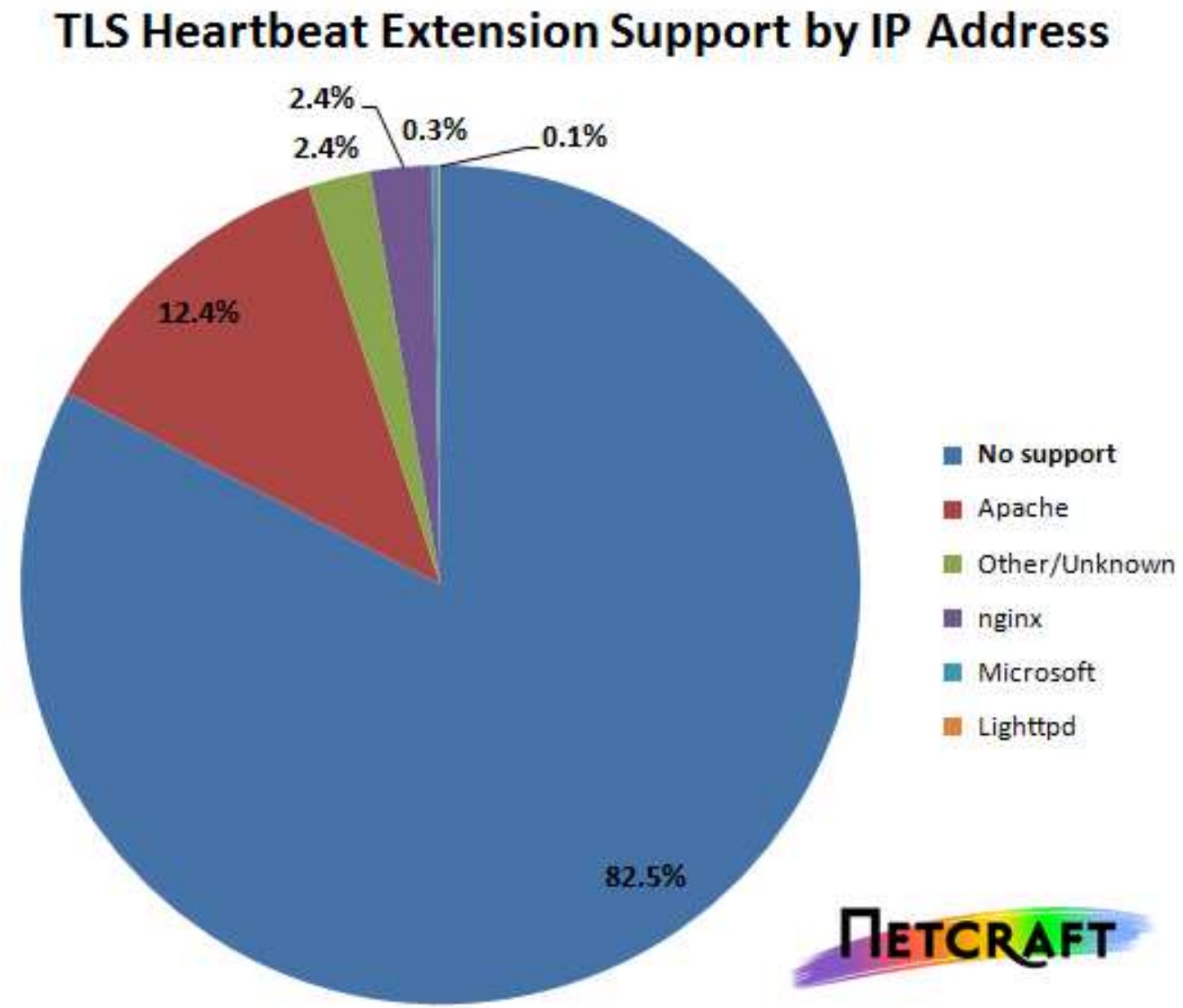
OpenSSL Heartbleed
Zero-day vulnerability

Heartbeat

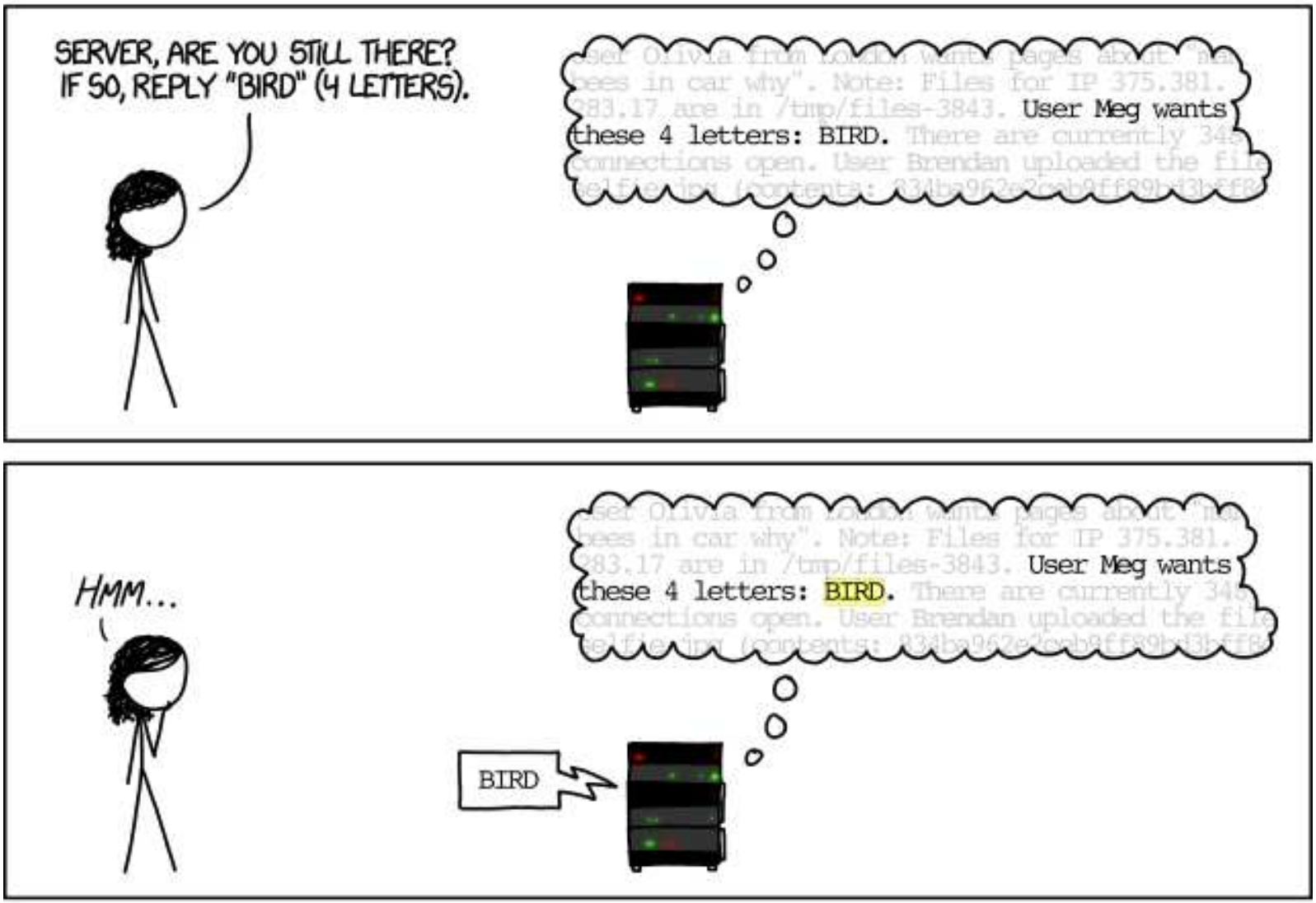
- DTLS : TLS sur UDP
- RFC 6520 : TLS/DTLS Heartbeat Extension
- Objectifs :
  - Éviter la renégociation : keep-alive
  - Path MTU discovery pour le DTLS

Type (1 octet)	Taille du payload (2 octets)	payload	padding

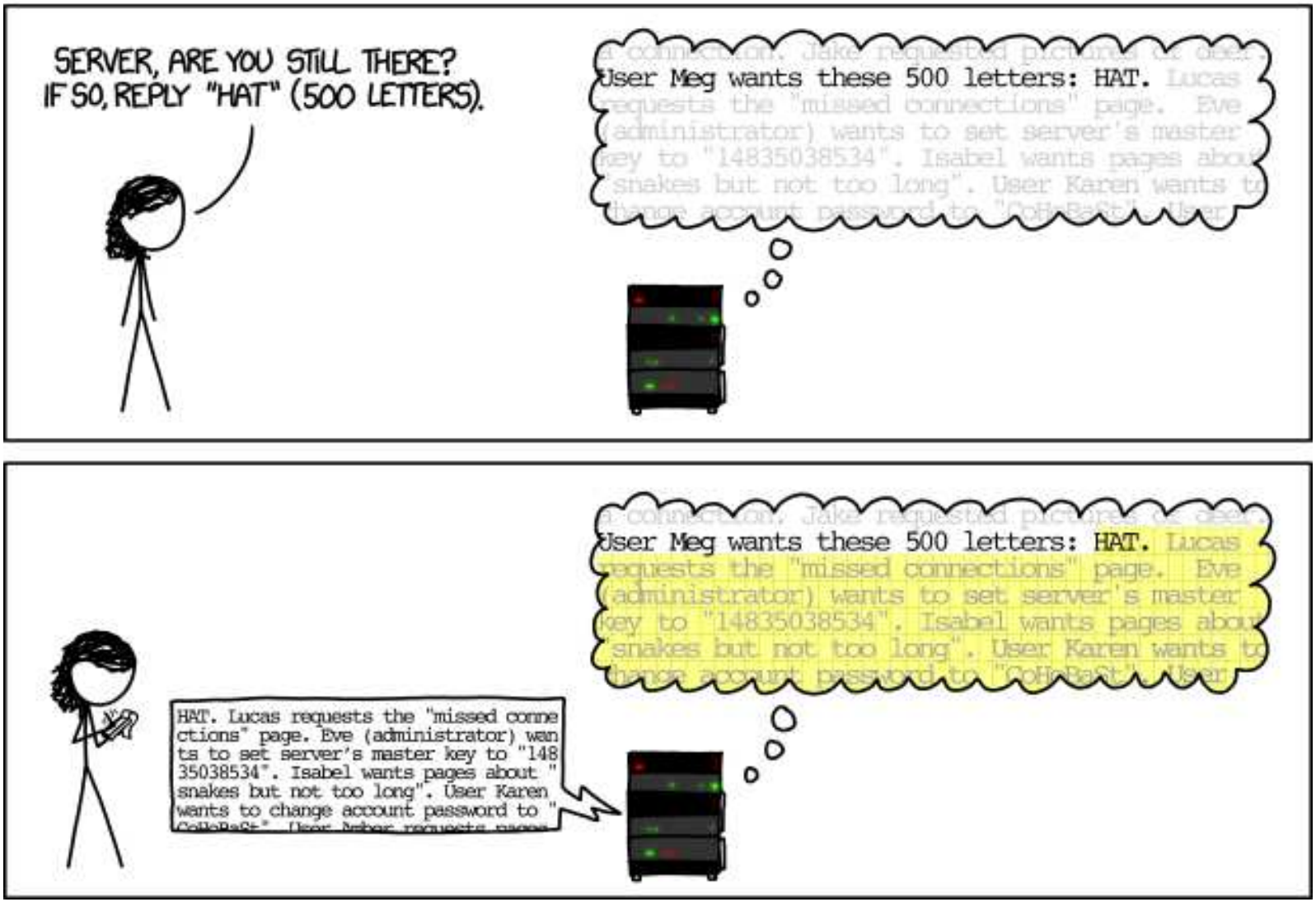
Support Heartbeat



Heartbleed expliqué par xkcd



Heartbleed expliqué par xkcd



Le petit bug

```
/* Read type and payload length first */


hbtype = *p++;
n2s(p, payload);


pl = p;
```

Le petit bug

```
/* Read type and payload length first */

if (1 + 2 + 16 > s->s3->rrec.length)
    return 0; /* silently discard */

hbtype = *p++;
n2s(p, payload);

if (1 + 2 + payload + 16 > s->s3->rrec.length)
    return 0; /* silently discard per RFC 6520 */

pl = p;
```

Découverte

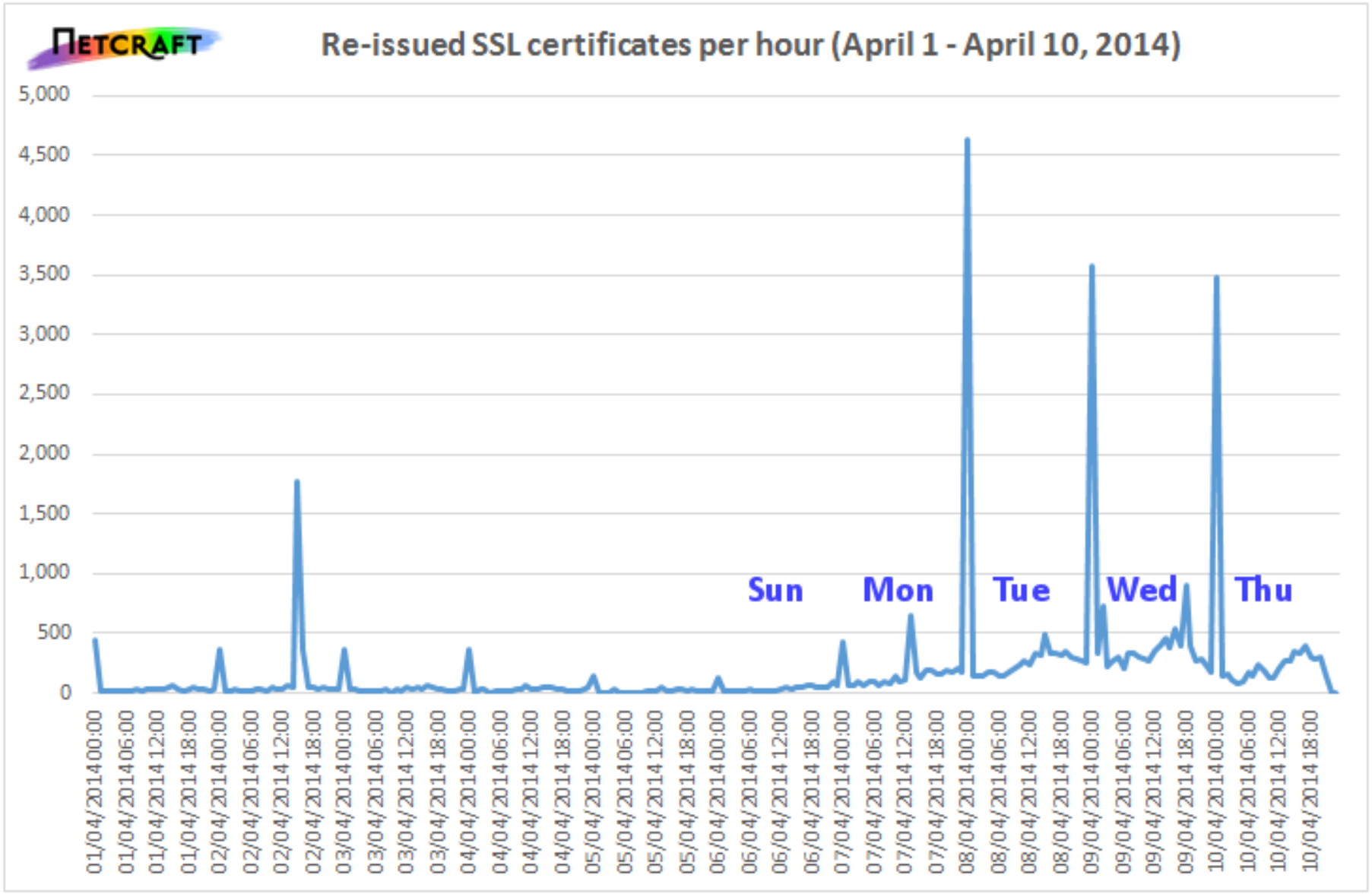
- Codenomicon et Google
- Fuzzing : Codenomicon's Defensic SafeGuard

- openssl-1.0.1[a-f]

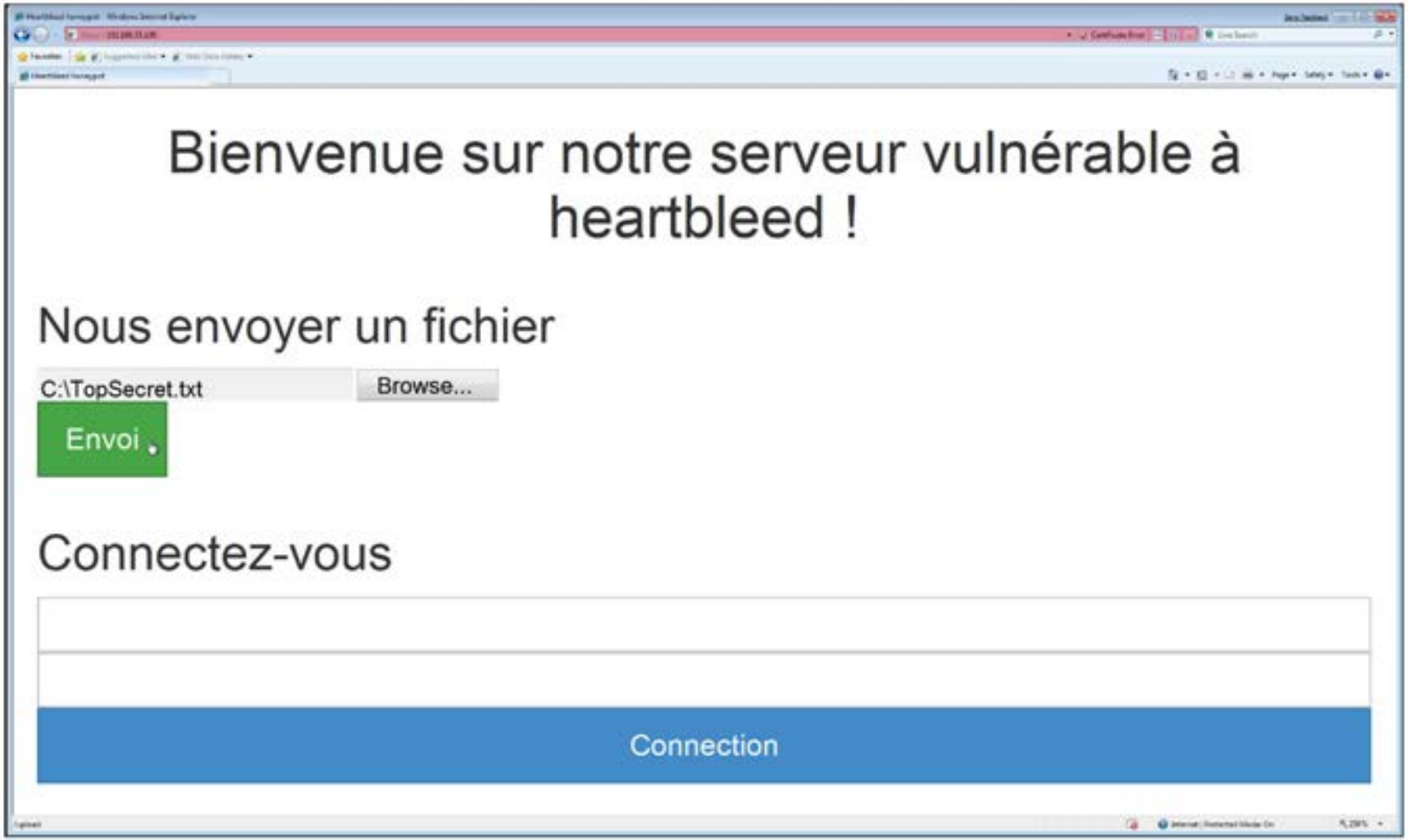
Chronologie des événements

18 Juin 2010	Draft RFC 6520
31 Décembre 2011	Rajout du code pour Heartbeat
14 Mars 2012	OpenSSL 1.0.1
3 Décembre 2013	Réservation du CVE
5 Avril 2014	Heartbleed.com enregistré
7 Avril 2014	Annonce de la faille, nouvelle version d'OpenSSL
8 Avril 2014	RHEL, CentOS, Ubuntu, Debian, etc
11 Avril 2014	Vol de la clé privée de Cloudflare
17 Juin 2014	Sites populaires encore exposés $> 10^4$

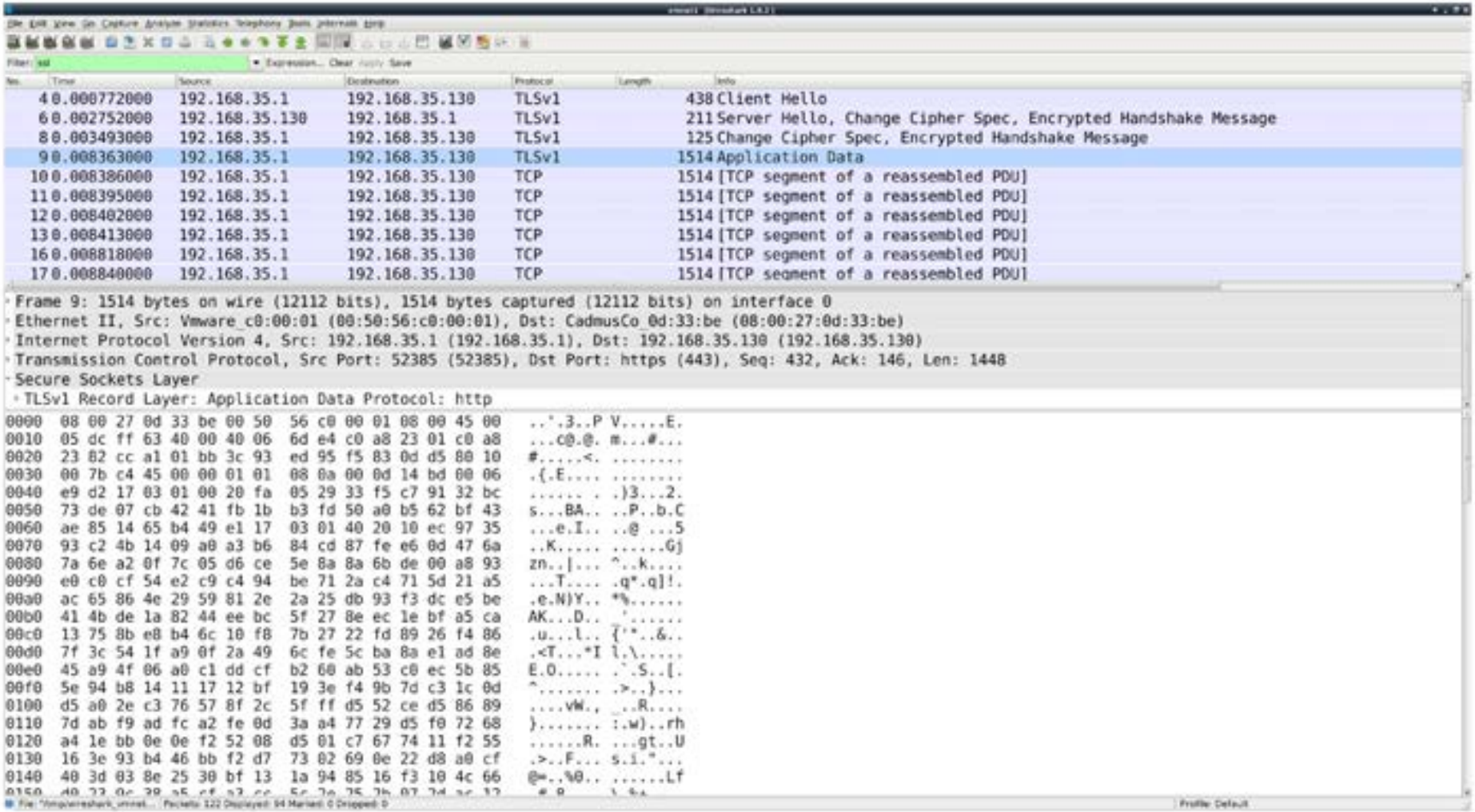
Ré-émission de certificats début Avril



Exploitation : envoi de fichier



Exploitation : envoi de fichier

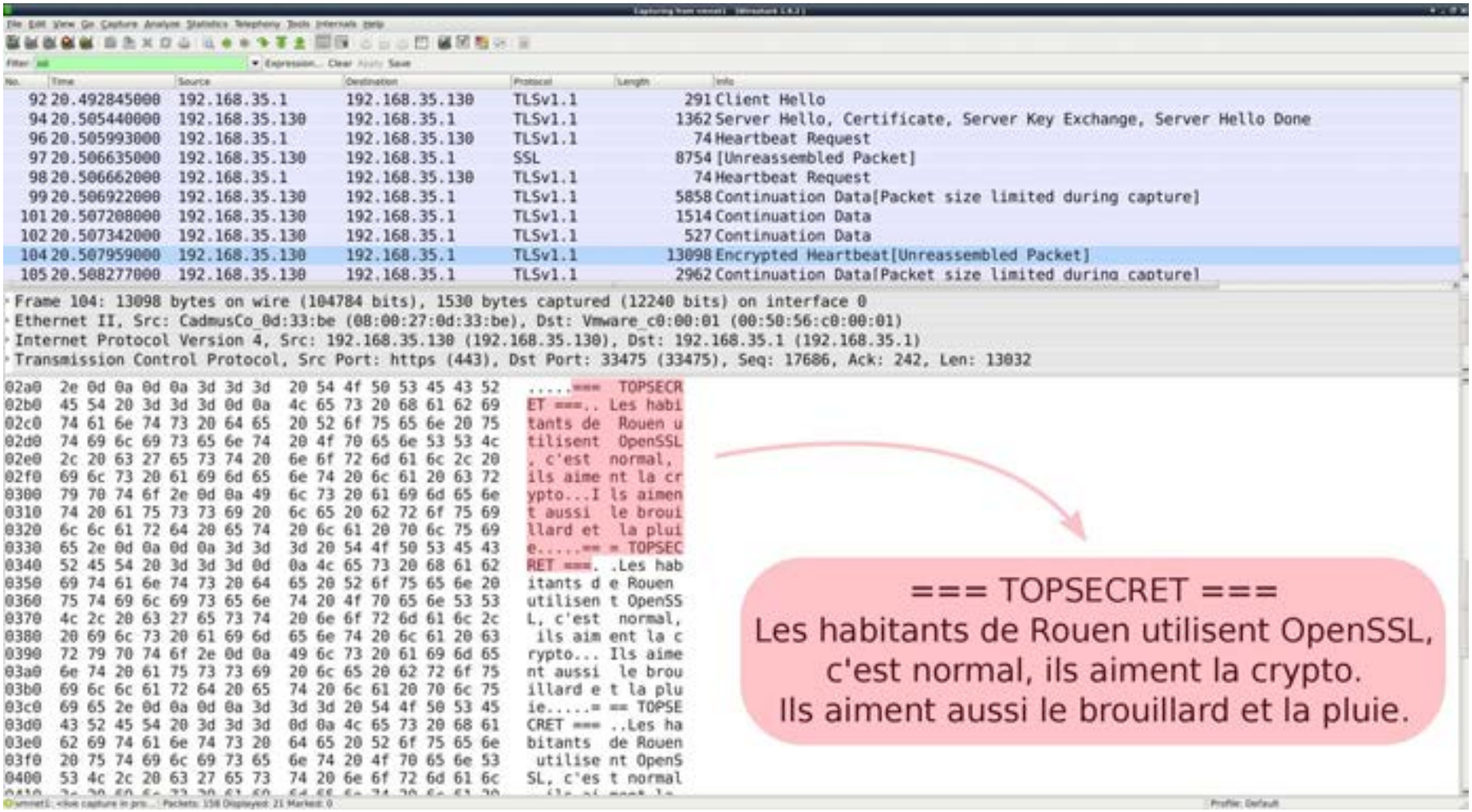


No.	Time	Source	Destination	Protocol	Length	Info
4	0.000772000	192.168.35.1	192.168.35.130	TLSv1	438	Client Hello
6	0.002752000	192.168.35.130	192.168.35.1	TLSv1	211	Server Hello, Change Cipher Spec, Encrypted Handshake Message
8	0.003493000	192.168.35.1	192.168.35.130	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message
9	0.008363000	192.168.35.1	192.168.35.130	TLSv1	1514	Application Data
10	0.008386000	192.168.35.1	192.168.35.130	TCP	1514	[TCP segment of a reassembled PDU]
11	0.008395000	192.168.35.1	192.168.35.130	TCP	1514	[TCP segment of a reassembled PDU]
12	0.008402000	192.168.35.1	192.168.35.130	TCP	1514	[TCP segment of a reassembled PDU]
13	0.008413000	192.168.35.1	192.168.35.130	TCP	1514	[TCP segment of a reassembled PDU]
16	0.008818000	192.168.35.1	192.168.35.130	TCP	1514	[TCP segment of a reassembled PDU]
17	0.008840000	192.168.35.1	192.168.35.130	TCP	1514	[TCP segment of a reassembled PDU]

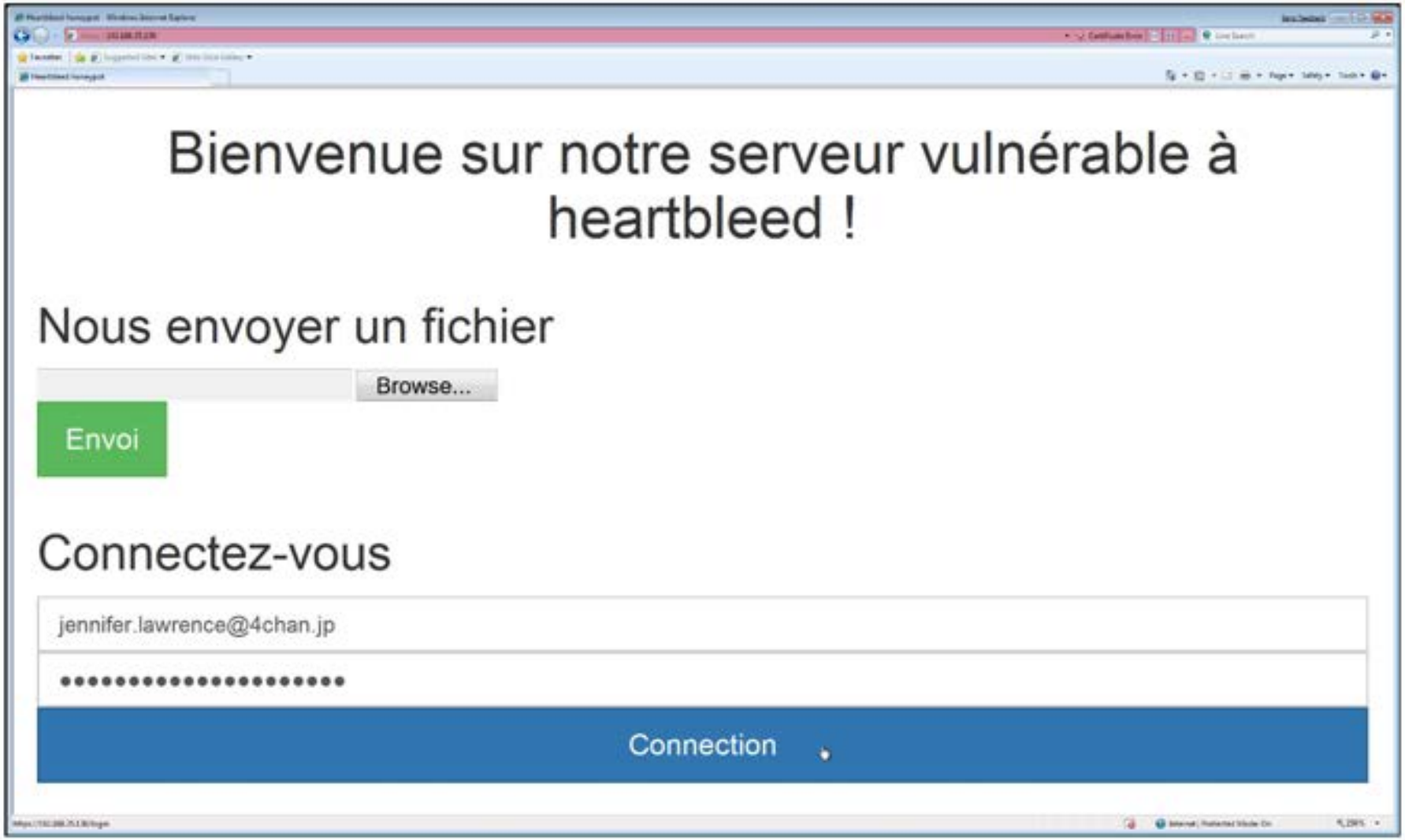
```
▸ Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: CadmusCo_0d:33:be (08:00:27:0d:33:be)
▸ Internet Protocol Version 4, Src: 192.168.35.1 (192.168.35.1), Dst: 192.168.35.130 (192.168.35.130)
▸ Transmission Control Protocol, Src Port: 52385 (52385), Dst Port: https (443), Seq: 432, Ack: 146, Len: 1448
▾ Secure Sockets Layer
  ▸ TLSv1 Record Layer: Application Data Protocol: http
```

```
0000  08 00 27 0d 33 be 00 50  56 c0 00 01 08 00 45 00   ..'.3..P V.....E.
0010  05 dc ff 63 40 00 40 06  6d e4 c0 a8 23 01 c0 a8   ...c@.@. m...#...
0020  23 82 cc a1 01 bb 3c 93  ed 95 f5 83 0d d5 80 10   #.....<. ........
0030  00 7b c4 45 00 00 01 01  08 0a 00 0d 14 bd 00 06   .{.E.... ........
0040  e9 d2 17 03 01 00 20 fa  05 29 33 f5 c7 91 32 bc   ...... . .)3...2.
0050  73 de 07 cb 42 41 fb 1b  b3 fd 50 a0 b5 62 bf 43   s...BA.. ..P..b.C
0060  ae 85 14 65 b4 49 e1 17  03 01 40 20 10 ec 97 35   ...e.I.. ..@ ...5
0070  93 c2 4b 14 09 a0 a3 b6  84 cd 87 fe e6 0d 47 6a   ..K..... ......Gj
0080  7a 6e a2 0f 7c 05 d6 ce  5e 8a 8a 6b de 00 a8 93   zn..|... ^..k....
0090  e0 c0 cf 54 e2 c9 c4 94  be 71 2a c4 71 5d 21 a5   ...T.... .q*.q]!.
00a0  ac 65 86 4e 29 59 81 2e  2a 25 db 93 f3 dc e5 be   .e.N)Y.. *%......
00b0  41 4b de 1a 82 44 ee bc  5f 27 8e ec 1e bf a5 ca   AK...D.. _'......
00c0  13 75 8b e8 b4 6c 10 f8  7b 27 22 fd 89 26 f4 86   .u...l.. {'"..&..
00d0  7f 3c 54 1f a9 0f 2a 49  6c fe 5c ba 8a e1 ad 8e   .<T...*I l.\.....
00e0  45 a9 4f 06 a0 c1 dd cf  b2 60 ab 53 c0 ec 5b 85   E.O..... .`.S..[.
00f0  5e 94 b8 14 11 17 12 bf  19 3e f4 9b 7d c3 1c 0d   ^....... .>..}...
0100  d5 a0 2e c3 76 57 8f 2c  5f ff d5 52 ce d5 86 89   ....vW., _..R....
0110  7d ab f9 ad fc a2 fe 0d  3a a4 77 29 d5 f0 72 68   }....... :.w)..rh
0120  a4 1e bb 0e 0e f2 52 08  d5 01 c7 67 74 11 f2 55   ......R. ...gt..U
0130  16 3e 93 b4 46 bb f2 d7  73 02 69 0e 22 d8 a0 cf   .>..F... s.i."...
0140  40 3d 03 8e 25 30 bf 13  1a 94 85 16 f3 10 4c 66   @=..%0.. ......Lf
```

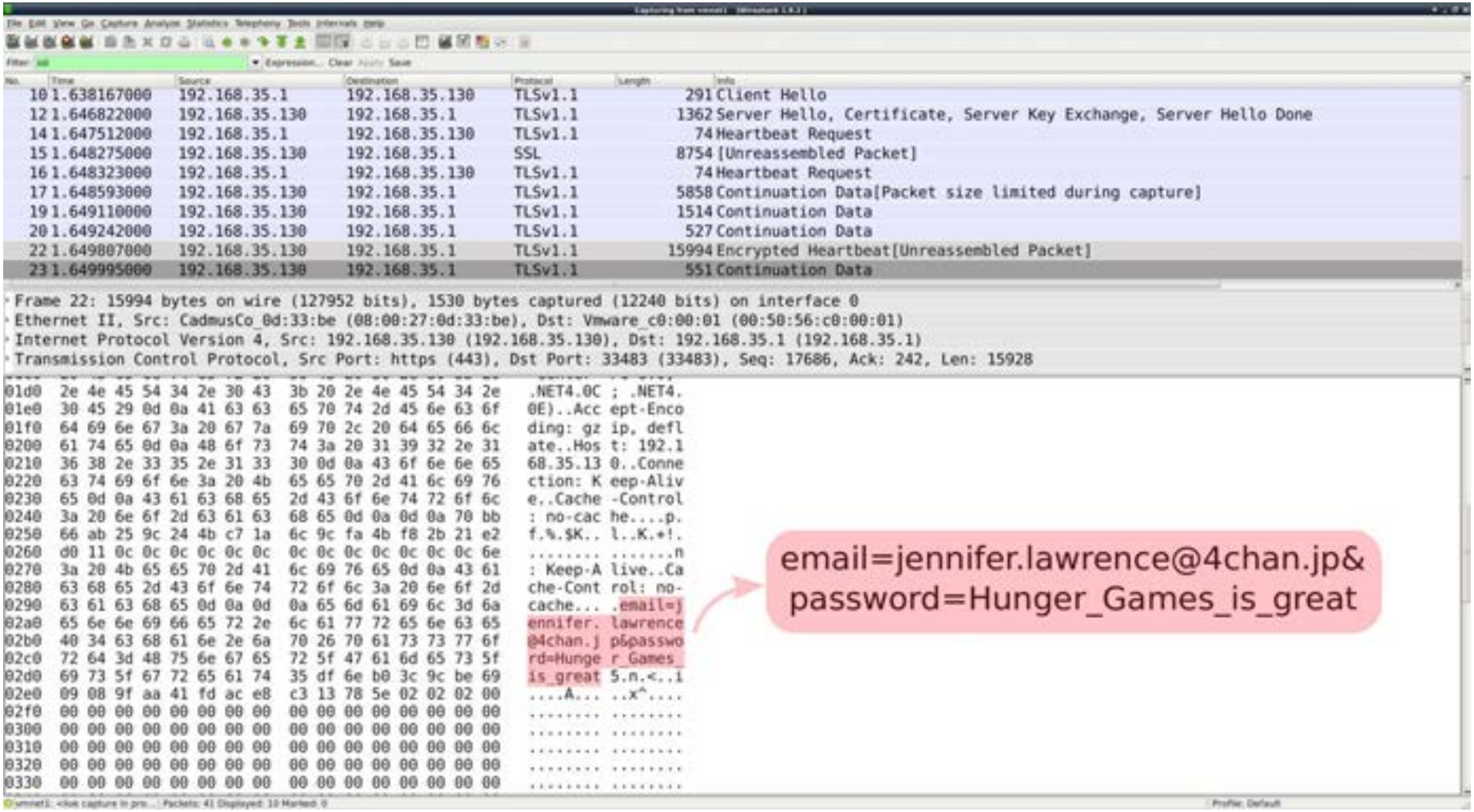
Exploitation : envoi de fichier



Exploitation : identifiants

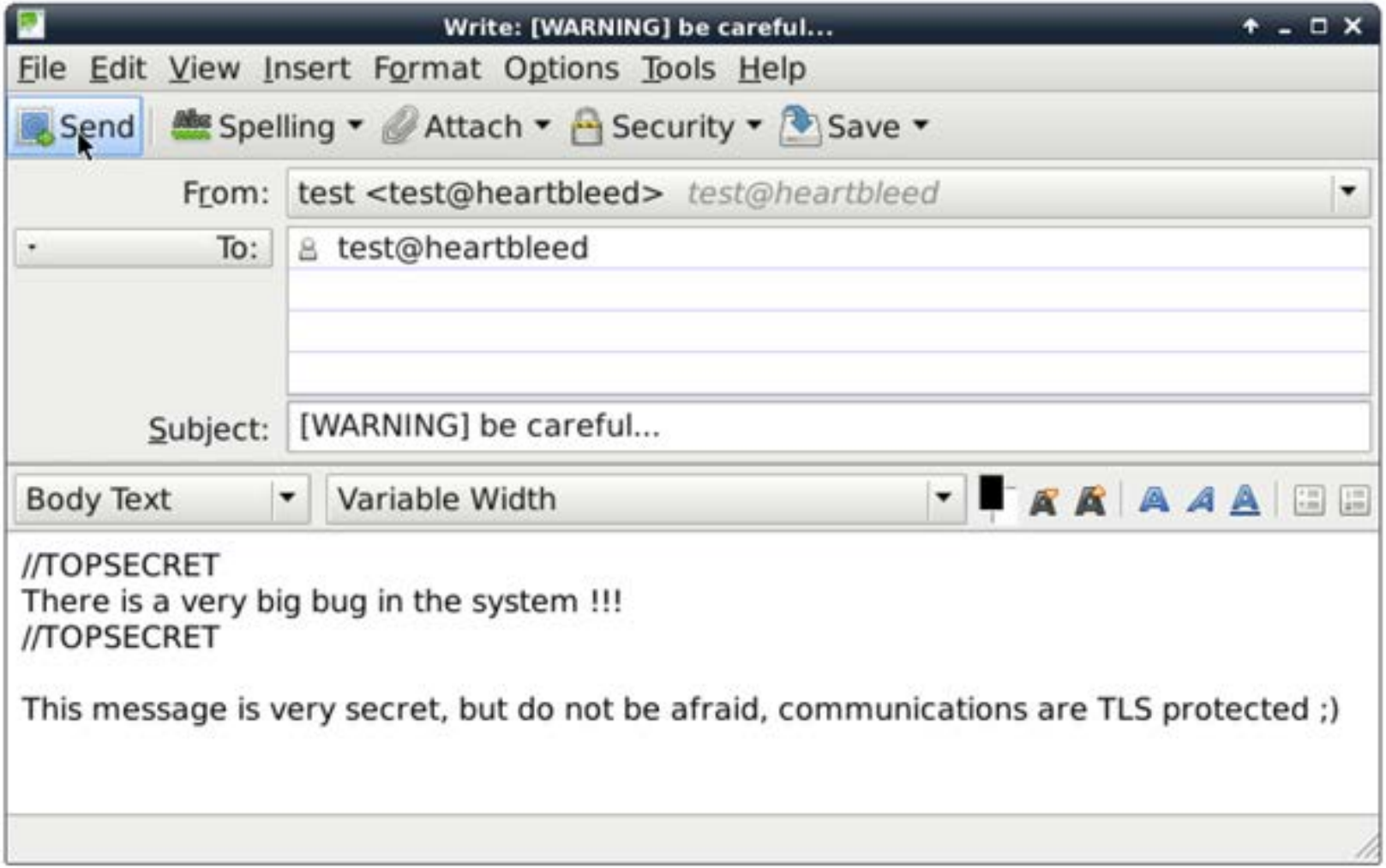


Exploitation : identifiants

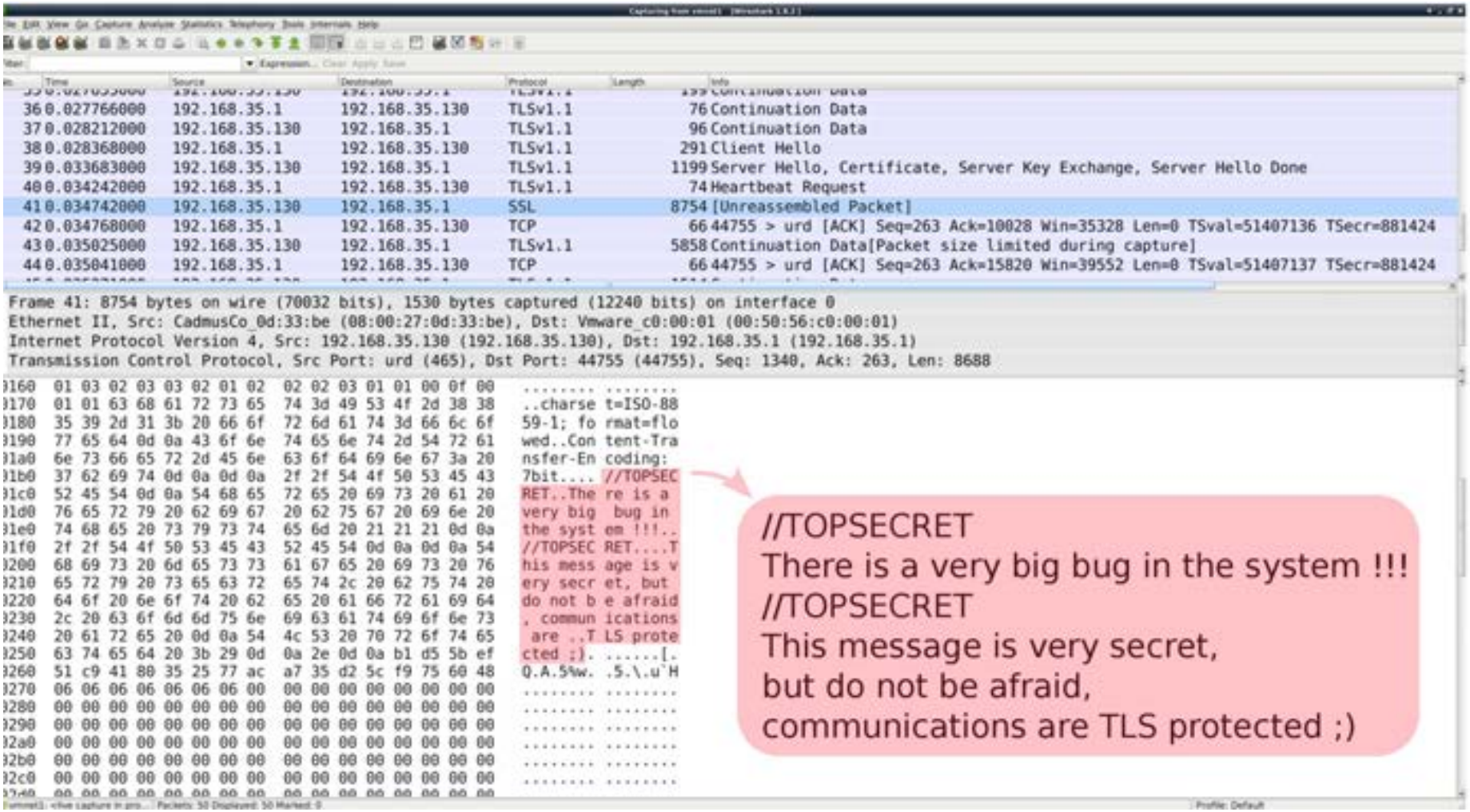


$$regexp = "email=([^&/]+)&password=([^&/]+)/"$$

Exploitation : mails (SMTPS)



Exploitation : mails (SMTPS)



Exploitation : clé privée du serveur

- RSA :
  - On récupère le certificat et donc $N = pq$
  - Pour chaque bloc P de $|N|/2$ octets consécutifs, on regarde si $P|N$
- ECDSA :
  - On récupère le certificat et donc $D_s = [d_s].G$
  - Pour chaque bloc d de $|d_s|$ octets consécutifs, on regarde si $[d].G = D_s$

- Grand nombre de réponses nécessaires (plusieurs Go)
- "Stresser" le serveur

Impact

Quoi ?

- Serveurs (HTTP, FTP, SMTP, ...)
- VPN
- TOR : 380 noeuds bloqués (12%)
- Applications mobiles
- Set top boxes

Qui ?

- $\sim$ 17% des 10000 plus gros sites web
- $\sim$ 500000 sites en tout
- Facebook, Google, Yahoo, Wikipedia, etc

Que faire ?

Utilisateur d'un site affecté

1. Une fois le site sûr : changer de mot de passe
2. Mettre à jour sa liste de révocation de certificats

Entreprise

1. Mise à jour
2. Ré-émission du certificat
3. Imposer le changement de mot de passe pour tous les utilisateurs

À l'avenir

- Analyse de code : clint, valgrind
- Tests :
  - Unitaires
  - Fuzzing

- Plus de relecteurs
- Aider la communauté OpenSSL : 1300 bugs ouverts, 500000 lignes

- Réduire la surface d'attaque, enlever des fonctionnalités
- LibreSSL, BoringSSL, polarSSL