

Imgur

Capture d'une session http grâce à Wireshark.

Nous pouvons voir les fichiers qui ont été échangés via :

imgur.pcap

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Ouvrir Ctrl+O
Dernier fichier ouvert
Fusionner...
Importer depuis Dump Hex...
Fermer Ctrl+W
Sauvegarder Ctrl+S
Sauvegarder Sous Ctrl+Maj+S
Fichier
Exporter Paquets Spécifiques...
Exporter analyse des paquets
Exporter Paquets Octets... Ctrl+H
Exporter PDU vers un Fichier...
Exporter Clés de Session SSL...
Exporter Objets
Imprimer... Ctrl+P
Quitter Ctrl+Q

DICOM...
HTTP...
SMB...
TFTP

	Destination	Protocol	Length	Info
	Broadcast	ARP	60	Who has 192.168.78.2? T
	Broadcast	ARP	60	Who has 192.168.78.2? T
	192.168.78.2	DNS	95	Standard query 0x38ad A
	192.168.78.2	DNS	95	Standard query 0x0236 A
	192.168.78.2	DNS	83	Standard query 0xb566 A
	192.168.78.2	DNS	83	Standard query 0x3f60 A
	192.168.78.128	DNS	531	Standard query response
	192.168.78.128	DNS	531	Standard query response
	192.168.78.128	DNS	287	Standard query response
	35.167.223.122	TCP	74	34726 → 443 [SYN] Seq=0
	192.168.78.128	DNS	215	Standard query response
	52.84.86.166	TCP	74	49346 → 443 [SYN] Seq=0
	192.168.78.128	TCP	60	443 → 49346 [SYN, ACK] S
	52.84.86.166	TCP	54	49346 → 443 [ACK] Seq=1
	52.84.86.166	TLSv1.2	278	Client Hello
	35.167.223.122	TCP	74	34730 → 443 [SYN] Seq=0
	192.168.78.128	TCP	60	443 → 49346 [ACK] Seq=1
	192.168.78.128	TLSv1.2	2974	Server Hello, Certificat
	192.168.78.128	TCP	54	49346 → 443 [ACK] Seq=2
	192.168.78.128	TLSv1.2	586	Certificate StatusServer
	52.84.86.166	TCP	54	49346 → 443 [ACK] Seq=2
	52.84.86.166	TLSv1.2	180	Client Key Exchange, Cha
	192.168.78.128	TCP	60	443 → 49346 [ACK] Seq=3
	35.167.223.122	TCP	60	443 → 34726 [SYN, ACK] S
	192.168.78.128	TCP	54	34726 → 443 [ACK] Seq=1
	35.167.223.122	TLSv1.2	266	Client Hello
	192.168.78.128	TCP	60	443 → 34726 [ACK] Seq=1

Wireshark · Exporter · Liste d'objets HTTP					
Paquet	Nom d'hôte	Type de contenu	Taille	Nom du fichier	
299	clients1.google.com	application/ocsp-request	75 bytes	ocsp	
301	clients1.google.com	application/ocsp-request	75 bytes	ocsp	
313	clients1.google.com	application/ocsp-response	463 bytes	ocsp	
315	clients1.google.com	application/ocsp-response	463 bytes	ocsp	
365	clients1.google.com	application/ocsp-request	75 bytes	ocsp	
368	clients1.google.com	application/ocsp-response	463 bytes	ocsp	
404	ocsp.digicert.com	application/ocsp-request	83 bytes	\	
406	p.imgur.com	image/gif	4 bytes	lumbar.gif?a=%7B%22UID%22%3A%22405c440...	
420	ocsp.digicert.com	application/ocsp-request	83 bytes	\	
422	ocsp.digicert.com	application/ocsp-response	471 bytes	\	
432	ocsp.digicert.com	application/ocsp-response	471 bytes	\	
447	aax.amazon-adsystem.com	text/javascript	19 bytes	bid?src=3079&u=http%3A%2F%2Fimgur.com%	
503	pixel.quantserve.com	image/gif	35 bytes	pixel;r=866446160;a=p-f8oruOqDFIMel;rf=0;fpar	
554	p.imgur.com	image/gif	4 bytes	lumbar.gif?a=%7B%22UID%22%3A%22405c440...	
562	ocsp.digicert.com	application/ocsp-request	83 bytes	\	
564	ocsp.digicert.com	application/ocsp-response	471 bytes	\	
583	imgur.com	application/x-www-form-urlencoded	33 bytes	checkcaptcha	
590	p.imgur.com	image/gif	4 bytes	lumbar.gif?a=%7B%22UID%22%3A%22405c440...	
596	imgur.com	application/json	126 bytes	checkcaptcha	
635	imgur.com	multipart/form-data	53 kB	upload	
660	imgur.com	text/html	248 bytes	upload	
702	p.imgur.com	image/gif	4 bytes	imageview.gif?a=E2r3d8e&r=http%3A%2F%2Fi	
720	p.imgur.com	image/gif	4 bytes	lumbar.gif?a=%7B%22UID%22%3A%22405c440...	
791	i.imgur.com	image/png	53 kB	E2r3d8e.png	
920	imgur.com	image/png	53 kB	E2r3d8e	

