

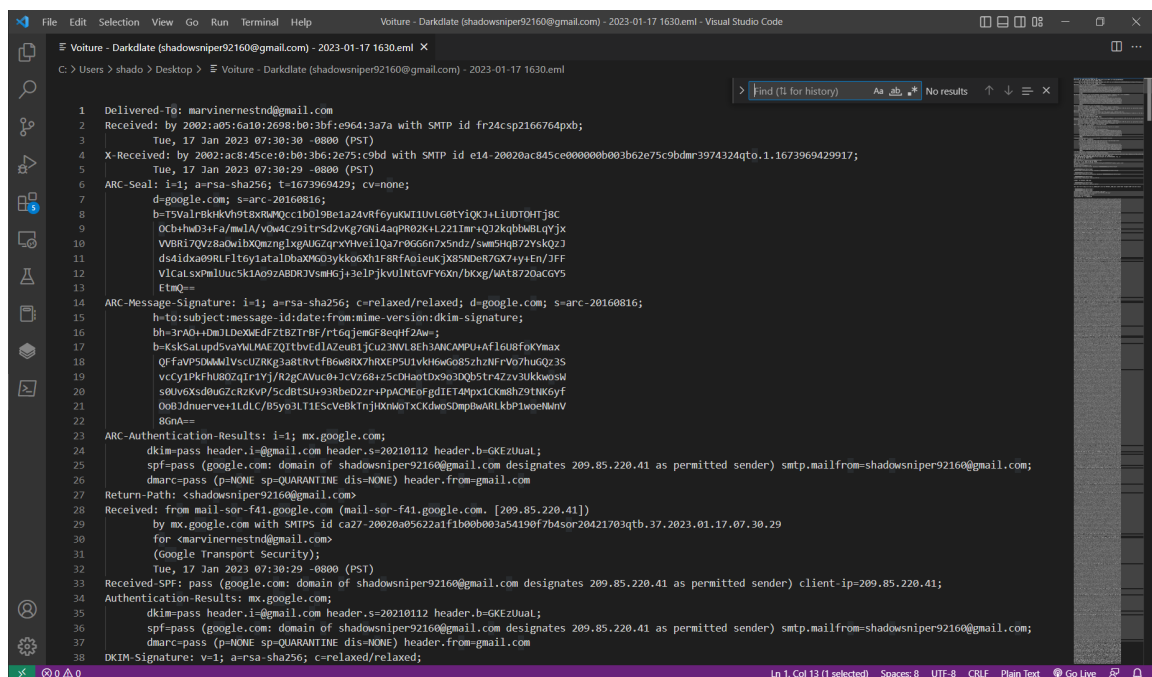
Phishing

STOP 1 :

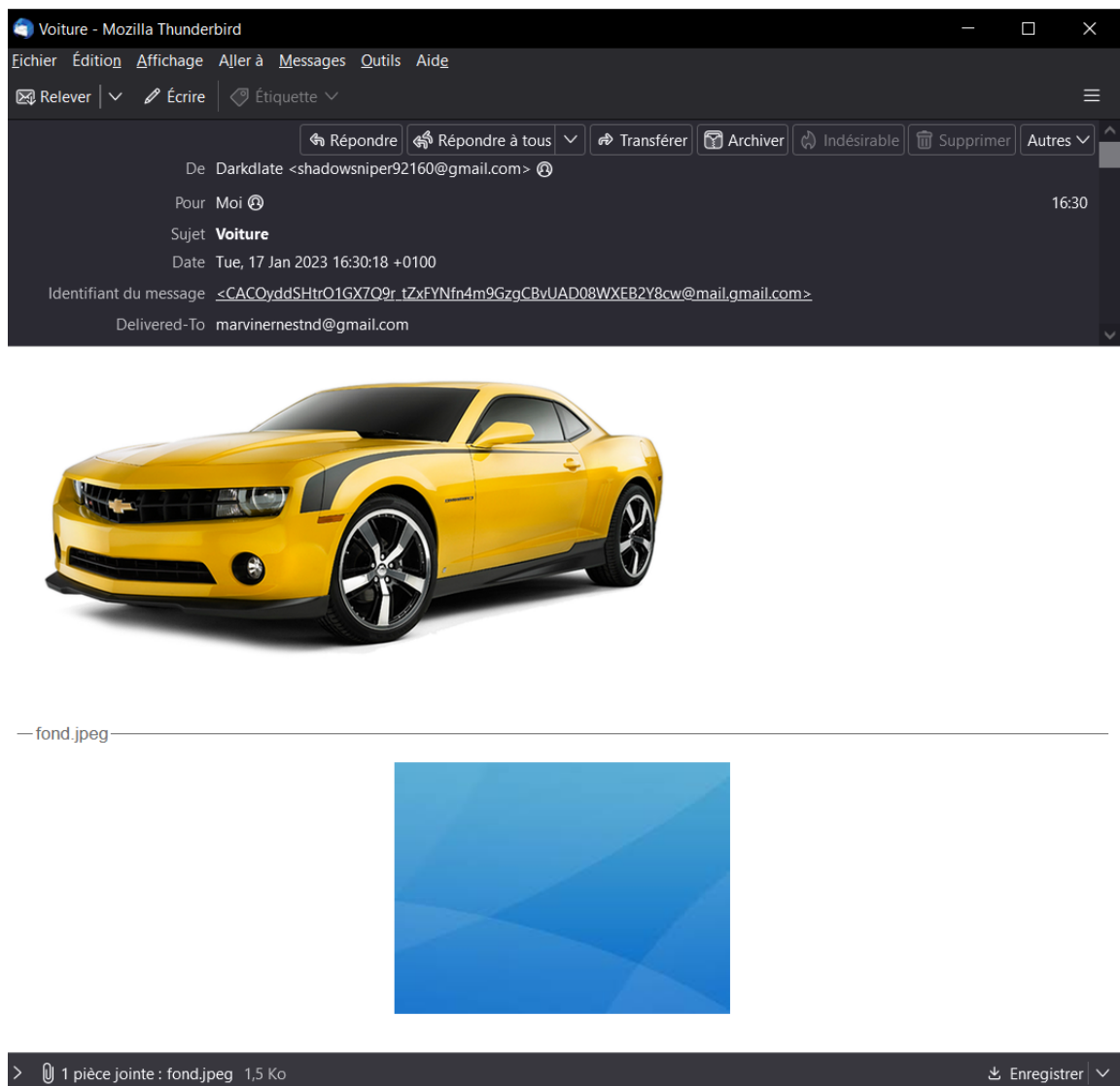
▼ 1

Travail à faire :
✓ Enregistrer le fichier IMF associé à un mail de votre choix contenant au moins une pièce jointe ainsi qu'une image. Le fichier doit avoir pour extension EML.
✓ Tester l'ouverture de ce fichier avec un éditeur de texte de votre choix puis avec le logiciel thunderbird.

Visual Studio Code :

A screenshot of the Visual Studio Code editor interface. The main window displays the source code of an email file named 'Voiture - Darkdate (shadowsniper92160@gmail.com) - 2023-01-17 1630.eml'. The code is a raw email message in Internet Message Format (IMF). It includes headers such as 'Delivered-To: marvinernestnd@gmail.com', 'Received: by 2002:a05:6a10:2698:b0:3bf:e964:3a7a with SMTP id fr24csp2166764pxb;', 'X-Received: by 2002:ac8:45ce:81b0:3b6:2e75:c9bd with SMTP id e14-20020ac845ce000000003b62e75c9bdm3974324q0.1.1673969429917;', 'ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=to:subject:message-id:date:from:mime-version:dkim-signature; bh=3ra0+DmJLDXMEFZt8TrBF/rT6qJewG8eqHf2Aw; b=skskatup5vaymWACZQ1t0vrdIAZm81Jc023WV1B83ANCAMPJH-AF1G8fXKmax Qf fapSPDmAlNscUz8KgaabLvt f8w88X7HXP5U1v6HwG885thJNFv87hUGQ33S vccy1PkhU80Zq1r1Yj/R2gCAVuc0-JcYz68+5cDhaotDx90J0Qb5tr4Zv3UkKwosM sLUV6XSd0UGZrKv9/ScdBtSu+938be02zr4pPAChEofgdIFET4Mpx1CKa8hZ9TNG6yf Q0Bjduerve+1ldLC/B5y03L1IEScVeBktNj0Xm07xCKdwoSDmp0wARLkbp1w0eManV 8GnA==', and 'ARC-Authentication-Results: i=1; mx.google.com; dkim=pass header.i=@gmail.com header.s=20210112 header.b=GKEZUuat; spf=pass (google.com: domain of shadowsniper92160@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=shadowsniper92160@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com'. The code is line-numbered from 1 to 38. The status bar at the bottom indicates 'Ln 1, Col 13 (1 selected) Spaces: 8 UTF-8 CRLF Plain Text Go Live'.

Thunderbird :



▼ 2

Travail à faire :

✓ Utiliser cette ressource afin de compléter le tableau suivant sur le mail extrait précédemment.

Champs	Signification	Valeur
X-Originating-IP		
Return-path		
Date		

Champs	Signification	Valeur
X-Originating-IP	L'adresse ip	2002:a05:6a10:2698:b0:3bf:e964:3a7a
Return-Path	l'email	shadowsniper92160@gmail.com
Date	la date	Tue, 17 Jan 2023 16:30:18 +0100

▼ 3

Travail à faire :

- ✓ Utiliser cette ressource afin d'obtenir des renseignements sur l'adresse IP extraite dans le champ X-Originating-IP. Conserver sur votre documentation les informations obtenues.

```

NetRange:      2002:: - 2002:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
CIDR:          2002::/16
NetName:       IANA-V6-6T04
NetHandle:     NET6-2002-1
Parent:        ()
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:       2001-02-01
Updated:       2008-11-14
Comment:       2002::/16 is reserved for use in 6to4 deployments [RFC3056]
Ref:           https://rdap.arin.net/registry/ip/2002::

```

```

OrgName:       Internet Assigned Numbers Authority
OrgId:         IANA
Address:       12025 Waterfront Drive
Address:       Suite 300
City:          Los Angeles
StateProv:     CA
PostalCode:    90292
Country:       US
RegDate:
Updated:       2012-08-31
Ref:           https://rdap.arin.net/registry/entity/IANA

```

```

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

```

```

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

```

▼ 4

Travail à faire :

- ✓ Toujours depuis le fichier IMF précédemment extrait, compléter le tableau suivant.

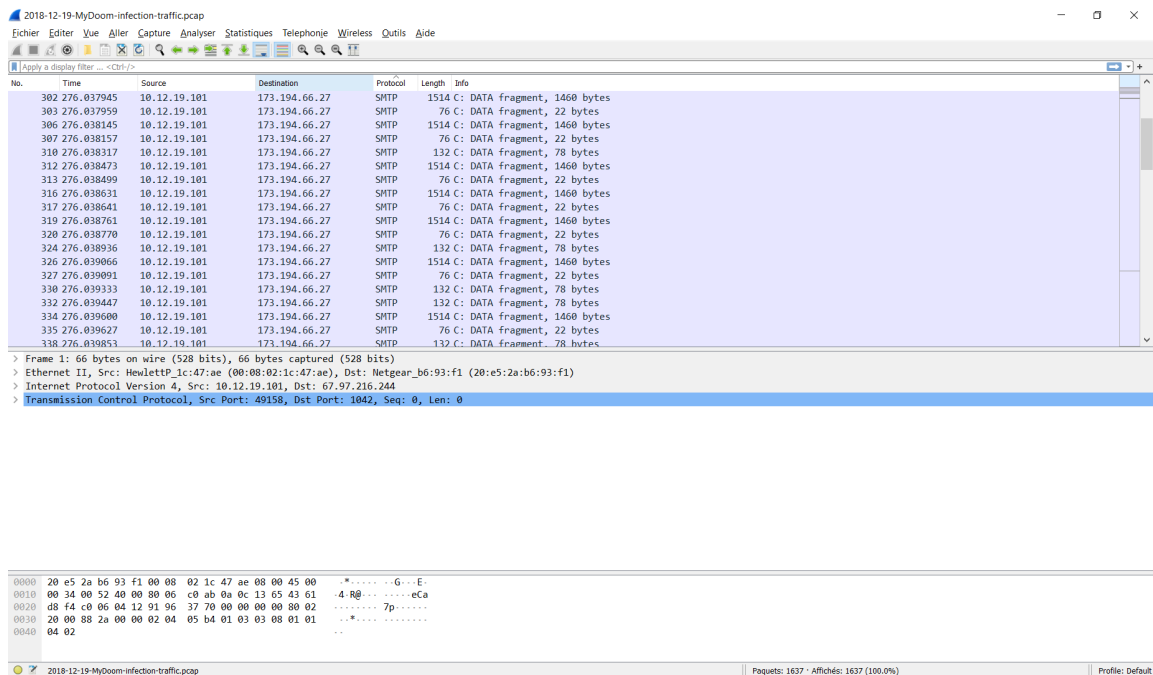
Champs	Signification	Contenu
Content-type		
Content-Disposition		
Content-Transfer-Encoding		

Champs	Signification	Contenu
Content-type	ce que ca contient	image/png; name="car-967387__480.png"
Content-Disposition	si le contenu devrait etre affiche en ligne	inline; filename="car-967387__480.png"
Content-Transfer-Encoding	en quoi le contenu est encode (base64/8-bit/binary)	base64

▼ 5

Travail à faire :

- ✓ Extraire le fichier pcap de capture de trames associé à la ressource suivante puis l'enregistrer sur votre ordinateur. Le mot de passe de l'archive est **infected**.
<https://www.malware-traffic-analysis.net/2018/12/19/index.html>
- ✓ En utilisant les deux ressources suivantes, répondre aux questions suivantes.
<https://www.wireshark.org/docs/dfref/s/smtp.html>
<https://www.wireshark.org/docs/dfref/i/imf.html>
 - ✓ Quel est le port utilisé pour le trafic SMTP ?
 - ✓ Combien de paquets liés au trafic SMTP la capture de trames contient-elle ?
 - ✓ Quelle est l'adresse IP du serveur SMTP ?
 - ✓ Comment se nomme la pièce jointe ?
 - ✓ Quel est son extension de cette pièce jointe ?



- Le port utilise pour le traffic SMTP est le port 25
- Il ya 512 paquets liés au trafic SMTP
- L'IP du serveur SMTP est : 10.12.19.101
- La piece jointe se nomme : document.zip
- L'extension de la piece jointe est zip

STOP 2 :

▼ 1

Spam	Envoi répété d'un message électronique, souvent publicitaire, à un grand nombre d'internautes sans leur consentement.
Spear fishing	Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée.
Whaling	Se faire passer pour un supérieur au sein d'une entreprise et de cibler directement la haute direction ou d'autres membres importants, dans le but de voler de l'argent, des informations sensibles ou d'avoir accès à leurs systèmes informatiques, le tout bien sûr à des fins criminelles.
Smishing	Le smishing est une forme de <u>phishing</u> dans laquelle un attaquant utilise un SMS convaincant pour inciter les destinataires ciblés à

	cliquer sur un lien et à envoyer à l'attaquant des informations privées ou à télécharger des programmes malveillants sur un smartphone
Vishing	Phishing se déroulant par un appel téléphonique

▼ Fichiers EML

Ce qui peut permet de constater que ce mail est frauduleux est le nom de 'adresse mail ainsi que le manque d'interface graphique du mail

▼ Fichiers PCAP

▼ 2

Cette attaque relève du phishing

Login : brad@malware-traffic-analysis.com

MDP : this-is-not-a-real-password

▼ 3



▼ 4

Analyse du mail :

Mail header analysis



Address Details

Mail From:	sales@maxsgmail.top	Mail To:	brad@malware-traffic-analysis.net
Mail From Name:	malware-traffic-analysis.net	Reply To:	

Message Details

Subject:	brad@malware-traffic-analysis.net Kindly Re-Validate	Content-Type:	text/html
Date:	05 May 2020 09:03:36 -0700	UTC Date	
MessageID:			


Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	maxsgmail.top([117.50.10.134])	Mail Server To:	
Mail Server From IP:	117.50.10.134	Mail Server To IP:	
Mail Country From:	China 	Mail Country To:	 Country/Code/Continent: // Longitude/Latitude:
AS Name From:	China Mobile Communications Group Co., Ltd.	AS Name To:	
AS Number From:	AS9808	AS Number To:	
Distance (All Hops/Summary):	0/ KM	Hops (All/Public):	1 /
MTA Encryption	Good (*)	Delivery Time:	0
Your IP:	87.88.163.37	Your GeoLoc:	Lat:48.8611 Lon:2.3269

Spam Scoring Details

Score	Spam Description
Total Score (Max:5)	Spamassassin prediction
0	No Spam = Good!

Hop Details

Hop 1/1	Public / Internal Mail Routing		
By MTA		By IP	UNKNOWN (*)
From MTA	maxsgmail.top([117.50.10.134])	From IP	117.50.10.134 (*) 
From AS Nbr	AS9808	From AS Name	China Mobile Communications Group Co., Ltd.
From Geo	Lat:39.9143 Lon:116.3861	From Next City	(*)
Date MTA	Tue, 05 May 2020 16:03:13 +0000	UTC Date	Tue May 5 16:03:13 2020
Epoch	1588690993	UTC Epoch	1588690993
MTA Encryption	Not encrypted (internal)		
For	UTC		
RAW	Received: from maxsgmail.top([117.50.10.134]) by [removed] for brad@malware-traffic-analysis.net; Tue, 05 May 2020 16:03:13 +0000 (UTC)		

X-Header

Mail header