南京郵電大學
Nanjing University of Posts and Telecommunications

电子邮件取证分析

汇报人：10240411106戴芮昊

01

目录

CONTENT

Autopsy软件

1. Autopsy简介

AUTOPSY
DIGITAL FORENSICS

Autopsy 是一款开源数字取证平台，借助 Sleuth Kit 自动解析磁盘镜像中的文件系统和邮件数据，实现关键词搜索和时间线分析，从而迅速定位证据。

2. Autopsy的应用

- 执法人员利用 Autopsy 调查网络犯罪
- 企业安全专家利用 Autopsy 进行内部调查
- 网络安全分析师利用 Autopsy 分析恶意软件感染
- 人力资源部门利用 Autopsy 调查员工不当行为
- 法律顾问利用 Autopsy 支持诉讼中的电子证据分析

3. Autopsy取证分析电子邮件（.eml）

Autopsy 在取证分析 EML 文件时，主要依赖其内置的 Email Parser 模块以及底层的 Sleuth Kit 工具

- 文件识别与提取：

扫描存储介质，通过文件签名和元数据识别 EML 文件，同时利用文件剥离技术找出被删除或隐藏的邮件。

- MIME 格式解析：

根据 MIME 协议解析识别出的 EML 文件，将邮件头、正文和附件分离，并提取发送者、接收者、主题及时间戳等关键信息。

- 元数据提取与索引：

将解析后的邮件信息存入案件数据库，并建立索引，便于关键字搜索和时间线分析，同时附件作为派生文件进行处理。

- 数据展示与报告生成：

在图形界面中展示解析和索引结果，调查人员可直接查看邮件内容，并利用内置工具生成详细的取证报告。

南京郵電大學
Nanjing University of Posts and Telecommunications

02

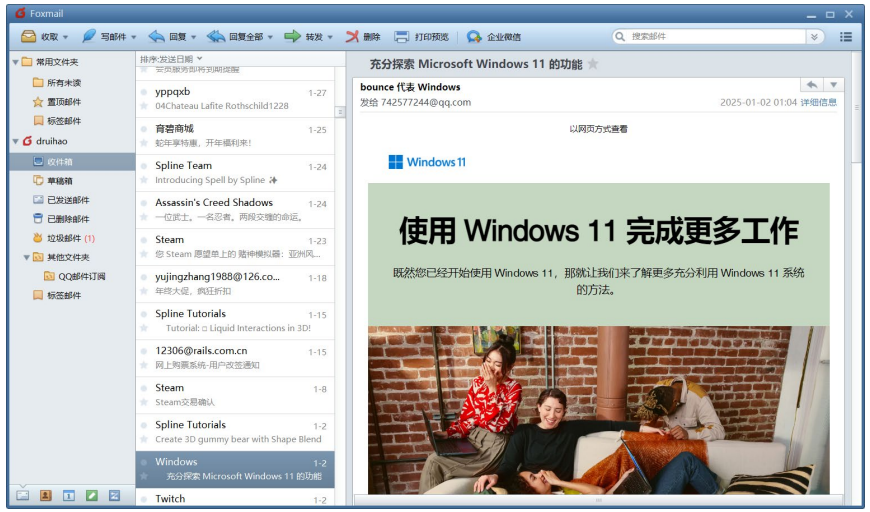
目录

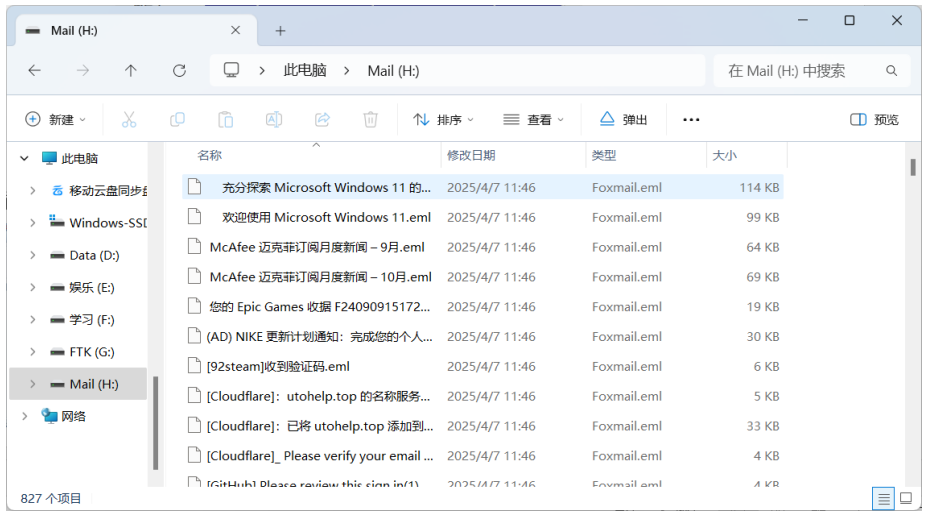
CONTENT

取证

创建一个虚拟磁盘，用来存放导出的邮件。

打开邮箱软件foxmail并登录，并且从该软件中将邮件以.eml文件形式导出至Mail（H:）





取证

打开FTK Imager软件，对虚拟磁盘Mail（H:）生成DD镜像。

mail.001　　2025/4/7 11:47　　WinRAR 压缩文件　　1,048,576 KB

创建时间 AccessData® FTK® Imager 4.2.0.13

案件信息:
采集方式: ADI4.2.0.13
案例编号:
证据编号:
唯一性描述: untitled
检查器:
注释:

Information for C:\Users\86133\Desktop\forensics\final\mail:

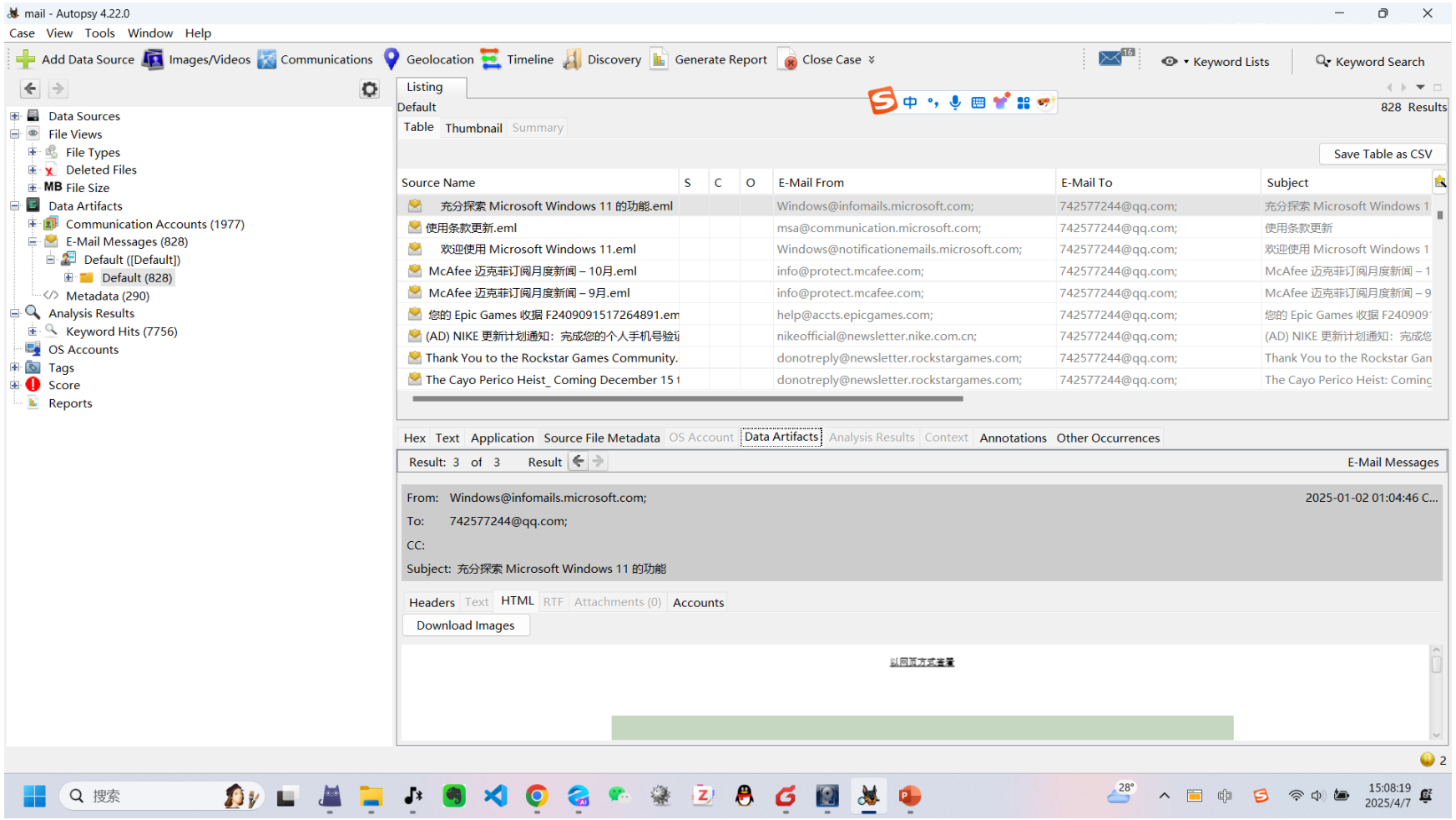
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[驱动器几何参数]
柱面数: 130
每柱面磁道数: 255
每磁道扇区数: 63
每扇区字节数: 512
扇区数: 2,097,152
[物理驱动器信息]
驱动器型号: Microsoft 虚拟磁盘
驱动器接口类型\n
连接驱动器的接口: SCSI
Removable drive: FALSE
Source data size: 1024 MB
Sector count: 2097152
[Computed Hashes]
MD5 checksum: a0507751fa3c41a0347d971450669ddc
SHA1 checksum: 898b52a3298ecc5784eea5dc110eba8e542c752b

Image Information:
Acquisition started: Mon Apr 7 11:47:29 2025
Acquisition finished: Mon Apr 7 11:47:48 2025
Segment list:
C:\Users\86133\Desktop\forensics\final\mail.001

Image Verification Results:
Verification started: Mon Apr 7 11:47:48 2025
Verification finished: Mon Apr 7 11:47:52 2025
MD5 checksum: a0507751fa3c41a0347d971450669ddc : verified
SHA1 checksum: 898b52a3298ecc5784eea5dc110eba8e542c752b : verified

取证

打开Autopsy软件，新建case，将Mail.001镜像文件作为数据源添加。



取证

数据源添加完毕后，可以在Autopsy图形界面中获取邮件头

-----HEADERS-----

Received: from r24.engage.microsoft.com (r24.engage.microsoft.com [172.82.208.24]) by newxmmxsza44-0.qq.com (NewMX) with SMTP id 16F1464A for <742577244@qq.com>; Thu, 02 Jan 2025 01:05:47 +0800
X-QQ-mid: xmmxza44-0t1735751158tsesmrvhp
Sender: bounce@infomails.microsoft.com
X-QQ-CSender: bounce@infomails.microsoft.com
X-QQ-XMAILINFO: M+O05MdVE3ttr4nFVZtCl/I+HGtE9EfYJ/ZUta6sYRDHu10/WEbDJCINAdVbUz 3CtrwOtYnriRmOvX/xXTrgvMgcNEF7c43iV4GNQOfB0WIz//DOadtv0MmvleveGh+EeqZhCSLf14
mAHnbZN9qgPbLCq9t3pROfQ8HNrDqhVJdhaef9E0+uNzhsSsPYWSCb4fqzovmNHyGDF/uGVqoFqa +P2feo600H7nTGj72V58F1X0titbWNV2iTx4z8bxjI0Yuh9LAAFIjkcdgZVp2xo9SsGVmMzfRihN
4pVfdyQzjYEZVKBIF+fAhFskAn9ER1HqhByMevodONJDT8mbvYKvRekQ9gvcn+RrJ+3q2cT8lwew kmdAyI+o3tQo8Xr15Y2fcQcJhDrymJawoP5D8NLub88nNrWJpMW4YIckCzz/yemcJ6lfJmLTLBdG
yH5N9JVi2pzYaIccGasHr9EKVa3p6CbEZqY28vA0EfYUQOLbJos3o2mTduGFSTI3wj3o8x6L0TRb WToWwbRLzK/DcrURhzZb+z+P//lll6IbVvJUYFCBGcyaBN6maA7YTTPfx7onqDoh35hSTCy3fzJX
IRg11UTjf4wlLkx/+vnYDT4npDfOoP+HgGo0zID2PZZadtHW/YELk0RxOCxs9ydSrNZwGwC+NZ/5 DAMkQMq4CbA3yXY13E+K4LxC/sng+wg8B1fXIN/Jz5bEXqgaNVVN+znMAGrRUlxGJZeTbB48C+zN
yVTw5UNLtxqg4NB4ECVjH4+5YlWXLULCzXiQg0zVPq5pjqUcktFGSFYbn0T//f5/lZUxLH3Zy2rD eQYrPQzpLdEQizjPMZ442Qn8ZvaUNMFbsn8wGVD3twOYLs9b9s+sK3yt2ZBlmkbyRtn2rPAkl/qw
SvVlVPyOSr+LCamdHtq8qA5COAxLCHC6y/kumlNrJMKCF1pAbmsV0GneN4faaE/iT44JhKoRPEql L3d7dliyaq+ncczgvdEq88SiFWB9QEsLszKuruIQAboZB+ecBkkwJMxPV8nNnqmRvTzDUIahpsT/
Jc5OaddLFeIESiMzK0B1tOMkm5X9vTCaH0Cn1j5wAVWwJuor1iwVUR+W2PNInLsPczHuKftWwnek klhmA5eg9sD9N0pDAZlJnFVN23odxmnMVMTDqC22iFuCxdyTE2iZgIgK7UuX6b/GScmz5zzOPfbK
1s/N1l/uInWtNqaITLVOdTx7zYgo8FEK60ImW8EyebZnD5SsrhMAUNE6g/ynUppN7mZZJjwwe3AP 6BX6LhN9PjLuT3RkD9ocROzDhpJtBCyz+qoph7uPUct9dJD/MzFG98TE+di8mjTKWhqaTnszhhJK
vixD67fAIuiV9bNoKdM4De8+wZmV0UID9917+VRbZTdHs4JkxTdjBA23ZLq+RweTVrn2yQfomlm9 /eLCf1XB27aQ==
X-QQ-XMRINFO: NS+P29fieYNw95Bth2bWPxk=
Authentication-Results: mx.qq.com; spf=pass(172.82.208.24) smtp.mailfrom=<boun ce@infomails.microsoft.com>; dkim=pass(signature was verified) header.d=info mails.microsoft.com; dmarc=pass(p=NONE sp=NONE pct=100) header.from=infomail
s.microsoft.com
Return-Path: <bounce@infomails.microsoft.com>
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=infomails.microsoft.com; s=mscom; t=1735751117; bh=Pfix8CZySIt6MUmaxmyztlUVjq0X3iZfV734KTEDk+Y=; h=From:Date:Subject:To:MIME-Version:Message-ID:List-
Unsubscribe: List-Unsubscribe-Post:Content-Type; b=o89uyvAzh+xqXefukIJlTr9atxcCWsgUpAdfYqEJ8yREstQ/q7VTY7S6moUu9KNJ4 nvJ59tk3VN2EP/1iBQv8ZIA088pCU4ublk7CorUz4srjhpb/HGImCFePf9gNiG2l6V
6/x1DDPhfwRgCfSoz8g9wtG5mRlKwFcej6FnaFQ4vgdYEOWj2+LbB9MgL48HvgPYI+ anZ7o0K+94fLgRKpGNp7leydhgdWVrSGX0zS1m40c3+1eaKFOrbGW7UgnNTy//GebL
rFfHzqVGxBbnoKFw2XYzsVUtHqlodVfM8i2b0ANCQbv7GpBLviPGJzCpmv2elWNVBz 18talgX+3ye3g==
X-MSFBL: zsGjYHA7xinEKVwxDjnHnpQLJgzUUV8fewjZSfUV1Vo=|eyJnIjoiYmF0Y2h0cml nZ2VybWFya2V0aW5nXzFlNzVjMzNhLTk3YTQtNDczYy1hYThjLTk4YWRmNWFhYWM
yMyIsImliOiJhenVyZV9tc2NvbV9wcm9kNzhfYmF0Y2h0cmlnZ2VybWFya2V0aW5 nX21vbWVudHVtNTlfbXRhMDA0XzE3Mi44Mi4yMDguMjQiLCJyY3B0X21ldGEiOns
gImluIjogIm1zY29tX21rdF9wcm9kNzgiLCAiciI6ICI3NDI1NzcyNDRAcXEuY29 tliwgIm0iOiAiMzEzMzg0MTM5OCIsICJkIjogIjE0OTQyMDMwNjciLCAiaSI6ICJ
FQTc2QURFOTU3NzZEMkVDN0YwMDAxMDFAQWRvYmVPcmciIH0slnliOiI3NDI1Nzc yNDRAcXEuY29tIn0=
Received: from [10.182.126.227] ([10.182.126.227:46397] helo=r33.engagemail.microsoft.com) by momentum59.or1.cpt.adobe.net (envelope-from <bounce@infomails.microsoft.com>) (ecelerity 4.2.38.999 r(:)) with ESMTP id
68/43-01300-CC575776; Wed, 01 Jan 2025 09:05:17 -0800
From: "Windows" <Windows@infomails.microsoft.com>
Date: Wed, 01 Jan 2025 09:04:46 -0800
Subject: =?utf-8?B?ICAgICDIhYXIiIbmjqLntKIgTWIjcm9zb2Z0IFdpbmRvd3MgMQ==?= =?utf-8?B?MSDnmoTIip/og70=?=
To: <742577244@qq.com>
Reply-To: "noreply" <replies@microsoft.com>
MIME-Version: 1.0
X-mailer: nlserver, Build 7.0.0.10695
Message-ID: <AC700000000BACA9FF6590FBABBmscom_mkt_prod78@infomails.microsoft.com>
List-Unsubscribe:
List-Unsubscribe-Post: List-Unsubscribe=One-Click
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: quoted-printable

---END HEADERS--

03

目录

CONTENT

分析


```
Received: from r24.engage.microsoft.com (r24.engage.microsoft.com [172.82.208.24])        by newxmmxsza44-0.qq.com (NewMX) with SMTP id 16F1464A                for
<742577244@qq.com>; Thu, 02 Jan 2025 01:05:47 +0800
X-QQ-mid: xmmxza44-0t1735751158tsesmrvhp
```

发送节点： 邮件最初从 r24.engage.microsoft.com 发出，其对应 IP 地址为 172.82.208.24。

接收节点： 邮件由 QQ 邮箱服务器 newxmmxsza44-0.qq.com 接收。

时间戳： 邮件被接收的时间标记为 2025 年 1 月 2 日 01:05:47（+0800 时区）。

SMTP id： 16F1464A 是 QQ 邮件服务器分配给这封邮件的内部标识号，有助于追踪和诊断传输问题。

```
Received: from [10.182.126.227] ([10.182.126.227:46397] helo=r33.engagemail.microsoft.com)        by momentum59.or1.cpt.adobe.net (envelope-from
<bounce@infomails.microsoft.com>)        (ecelerity 4.2.38.999 r(:)) with ESMTP        id 68/43-01300-CC575776; Wed, 01 Jan 2025 09:05:17 -0800
```

后续received字段：显示邮件在传输过程中经过了多个中继服务器（Microsoft 与 Adobe 的服务器）。

内部 IP 地址：通常表示在内部网络或专用网络内使用，说明邮件处理过程中还涉及内部通信环节。

分析

Sender: bounce@infomails.microsoft.com

From: "Windows" <Windows@infomails.microsoft.com>

Sender：指出实际负责发送邮件的邮箱地址，这里是bounce@infomails.microsoft.com，通常用于退信或系统通知。

From：显示邮件的发件人名称和地址，这里显示为 “Windows”，来自相同的域infomails.microsoft.com，表明邮件主题与 Windows 产品相关，可能与微软的系统通知或推广信息有关。

Reply-To: "noreply" <replies@microsoft.com>

Reply-To：表明接收者如果回复邮件时，邮件会发送到 replies@microsoft.com。通常，“noreply” 表示不接受回复或自动处理回复。

分析


```
Authentication-Results: mx.qq.com; spf=pass(172.82.208.24) smtp.mailfrom=<boun
mails.microsoft.com; dmarc=pass(p=NONE sp=NONE pct=100) header.from=infomail
ce@infomails.microsoft.com>; dkim=pass(signature was verified) header.d=info
s.microsoft.com
```

SPF（发件人策略框架）： 表示 QQ 邮箱服务器经过验证，发现发件 IP（172.82.208.24）被授权发送来自 infomails.microsoft.com 域的邮件。

DKIM（域密钥识别邮件）： 邮件上附带了数字签名，经验证证明邮件内容在传输过程中未被篡改，且与发送域匹配。

DMARC（基于域的消息身份验证、报告和一致性）： 显示 DMARC 检查也通过，说明该邮件符合发送域的政策设置。

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  d=infomails.microsoft.com; s=mscom; t=1735751117;  bh=Pfix8CZySIt6MUmaxmyztIUVjq0X3iZfV734KTEDk+Y=;
h=From:Date:Subject:To:MIME-Version:Message-ID:List-Unsubscribe:  List-Unsubscribe-Post:Content-Type;
b=o89uyvAzh+xqXefukIJITr9atxcCWsgUpAdfYqEJ8yREstQ/q7VTY7S6moUu9KNJ4  nvJ59tk3VN2EP/1iBQv8ZIA088pCU4ublk7CorUz4srjhpb/HGlmCFePf9gNiG2I6V
6/x1DDPhfwRgCfSoz8g9wtG5mRIKwFcej6FnaFQ4vgdYEOWj2+LbB9MgL48HvgPYl+  anZ7o0K+94fLgRKpGNp7leydhgdWVrSGX0zS1m40c3+1eaKFOrbGW7UgnNTy//GebL
rFfHzqVGxBbnoKFw2XYzsVUtHqlodVfM8i2b0ANCQbv7GpBLviPGJzCpmv2eIWNVBz  18talgX+3ye3g==
```

v, a（版本和算法）： 使用 DKIM v1 与 rsa-sha256 算法，确保签名的安全性。

d（域名）： 说明签名来自 infomails.microsoft.com。

s（选择器 ）： mscom，用于查找公开的公钥，验证签名。

t（时间戳 ）： 邮件签名的时间。

bh（消息摘要）： 邮件体内容生成的哈希值，确保内容完整。

b（签名值）： 包含经过加密的签名数据，用于后续验证整个邮件头中指定字段的完整性。

分析

X-QQ-mid: xmmxza44-0t1735751158tsesmrvhp
X-QQ-CSender: bounce@infomails.microsoft.com
X-QQ-XMAILINFO: M+O05MdVE3ttr4nFVZtCI/I+HGtE9EfYJ/ZUta6sYRDHu10/WEbDJCINAdVbUz
3CtrwOtYnriRmOvX/xXTrgvMgcNEF7c43iV4GNQOfB0Wlz//DOadtv0MmvleveGh+EeqZhCSLf14
mAHnbZN9qgPbLCq9t3pROfQ8HNrDqhVJdhaef9E0+uNzhsSsPYWSCb4fqzovmNHyGDF/uGVqoFqa
+P2feo600H7nTGj72V58F1X0titbWNV2iTx4z8bxjI0Yuh9LAAFljkcdgZVp2xo9SsGVmMzfRihN
4pVfdyQzjYEZVKBlF+fAhFskAn9ER1HqhByMevodONJDT8mbvYKvRekQ9gvcn+RrJ+3q2cT8lwew
kmdAyl+o3tQo8Xr15Y2fcQcJhDrymJawoP5D8NLub88nNrWJpMW4YIckCzz/yemcJ6lfJmLTLBdG
yH5N9JVi2pzYalccGasHr9EKVa3p6CbEZqY28vA0EfYUQOLbJos3o2mTduGFSTl3wj3o8x6L0TRb
WToWwbRLzK/DcrURhzZb+z+P//lll6lbVvJUYFCBGcyaBN6maA7YTTPfx7onqDoh35hSTCy3fzJX
IRg11UTjf4wlLkx/+vnYDT4npDfOoP+HgGo0zID2PZZadtHW/YELk0RxOCxs9ydSrNZwGwC+NZ/5
DAMkQMq4CbA3yXY13E+K4LxC/sng+wg8B1fXlN/Jz5bEXqgaNVVN+znMAGrRUlxGJZeTbB48C+zN
yVTw5UNLtxqg4NB4ECVjH4+5YlWXLULCzXiQg0zVPq5pjqUcktFGSFYbn0T//f5/IZUxLH3Zy2rD
eQYrPQzpLdEQizjPMZ442Qn8ZvaUNMFbsn8wGVD3twOYLs9b9s+sK3yt2ZBlmkbyRtn2rPAkl/qw
SvVlVPyOSr+LCamdHtq8qA5COAxLCHC6y/kumlNrJMKCF1pAbmsV0GneN4faaE/iT44JhKoRPEql
L3d7dliyaq+ncczgvdEq88SiFWB9QEsLszKuruIQAboZB+ecBkkwJMxPV8nNnqmRvTzDUIahpsT/
Jc5OaddLFelESiMzK0B1tOMkm5X9vTCaH0Cn1j5wAVWwJuor1iwVUR+W2PNlnLsPczHuKftWwnek
klhmA5eg9sD9N0pDAZlJnFVN23odxmnMVMTDqC22iFuCxdyTE2iZgIgK7UuX6b/GScmz5zzOPfbK
1s/N1l/uInWtNqalTLVOdTx7zYgo8FEK60lmW8EyebZnD5SsrhMAUNE6g/ynUppN7mZZJjwwe3AP
6BX6LhN9PjLuT3RkD9ocROzDhpJtBCyz+qoph7uPUct9dJD/MzFG98TE+di8mjTKWhqaTnszhhJK
vixD67fAIuiV9bNoKdM4De8+wZmV0UID9917+VRbZTdHs4JkxTdjBA23ZLq+RweTVrn2yQfomlm9 /eLCf1XB27aQ==
X-QQ-XMRINFO: NS+P29fieYNw95Bth2bWPxk=

X-QQ 系列（例如 X-QQ-mid、X-QQ-CSender、X-QQ-XMAILINFO 等）：这些字段是 QQ 邮箱系统内部使用的标识和追踪信息，用于邮件的归类、日志记录以及判断邮件是否属于垃圾邮件或异常邮件。

分析

```
Content-Type: text/html;        charset="utf-8"
Content-Transfer-Encoding: quoted-printable
```

Content-Type：指示邮件内容的格式为 HTML 格式，且字符编码为 UTF-8。

Content-Transfer-Encoding：“quoted-printable”表示邮件内容经过特定编码处理，以确保传输过程中的数据完整性（例如特殊字符会被编码）。

```
Subject: =?utf-8?B?ICAgICDlhYXlilbmjqLntKIgTWljcm9zb2Z0IFdpbmRvd3MgMQ==?= =?utf-8?B?MSDnmoTlip/og70=?=
```

Subject：邮件主题被编码为 Base64 格式。解码后可以看到主题中包含“微软”字样以及一些其他信息（可能与 Windows 或相关产品有关）。这种编码主要用于支持非 ASCII 字符集（如中文）。

04

目录

CONTENT

总结

邮件头信息：

传输路径：追踪每一跳的服务器、IP 地址、时间戳、使用的传输协议等信息，以重建邮件从发出到接收的完整路径。

身份验证与安全信息：检查 SPF、DKIM、DMARC 认证结果以及相关的 Authentication-Results、DKIM-Signature 等字段，判断邮件是否经过授权服务器发送、是否存在伪造或篡改的情况。

基础标识字段：分析 From、Sender、Reply-To、Message-ID、Date 等字段，了解邮件的来源、发送时间、唯一标识以及回复指向。

自定义与附加字段：检查各平台的 X- 开头的自定义字段（如 X-QQ、X-Microsoft-Antispam 等），这些字段可能记录了内部处理、反垃圾邮件判断、追踪或过滤的相关信息。

南京郵電大學 Nanjing University of Posts and Telecommunications

汇报结束，谢谢！

汇报人：1024041106戴芮昊