## Bài 1

“Một trong những chứng cứ đang gặp vấn đề”, mở file PC1-Outlook không được thì nghĩ file được đề cập là nó. Thử flag đúng luôn.

A screenshot of a computer

Description automatically generated

Flag: inseclab{MINAF-PC1-Outlook.zip}

## Bài 2

1. Từ bài này trở đi em dùng Kernel OST Viewer. Vào thư mục Elementos enviados (Sent):

A screenshot of a computer

Description automatically generated

Xem số mail được gửi ở trên từ 2/6 đến 7/6. Có tổng cộng 13 mail. Flag: inseclab{13}

## Bài 3

Ban đầu tìm thấy iphone tưởng đáp án là apple:

A screenshot of a computer

Description automatically generated

Nhưng đó không phải đáp án. Hóa ra mail này gửi từ tháng 5 nên không phải. Có thể CEO đã đổi dt.

Trong những metadata của nhiều email, ta thấy android. Đó là 1 gợi ý.

Trong 1 mail gửi ngày 6/6/2019 lúc 00:53 chứa nội dung về điện thoại mới:

A screenshot of a computer

Description automatically generated

Flag: inseclab{samsung}

## Bài 4

A screenshot of a computer

Description automatically generated

Thử hết các từ “crashed”, “damaged”, “corrupted” thì Flag là inseclab{corrupted}

## Bài 16

Import file “CORREO-Buzon\_Abelardo\_Alcazar.pst” vào Outlook rồi tình cờ thấy device id trong các mail remote wipe (tình cờ thật).

A white background with text

Description automatically generated

flag: inseclab{ androidc1290513397}

## Bài 9

Lúc đầu tưởng là tên các thuộc tính trong MessageTracking. Nhưng mà các thuộc tính đó không có trong EventHistory. Ta search các trường có từ “id” trong eventhistory coi có trong MessageTracking không.

A computer code on a white background

Description automatically generated

Lúc đầu tưởng là trường DocumentId, nhưng không có trong file csv. Kết quả là trường ItemEntryID.

Flag: inseclab{ItemEntryId}

## Bài 10

Cùng mail với wu câu 5. Lấy giá trị của trường ItemEntryID rồi bỏ gạch nối như yêu cầu. Flag: inseclab{ 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E75740526900000032D22D0000255F532116B8DC41A61899E75740526900000D3CE75E0000}

## Bài 5

Dựa vào email đầu tiên được gửi ngày 7/6/2019:

A screenshot of a computer

Description automatically generated

Múi giờ của Úc là UTC+2 nên phải trừ 2h.

flag: inseclab{14:02:00}

Dù messageTracking ghi giây 01 nhưng flag là giây 0. Em đã thử +/- 1 giây dựa vào gợi ý của bài 8 (dù đây là bài 5):

A white background with black text

Description automatically generated

## Bài 11

Trường DocumentID nằm trong EventHistory. Để tìm email này, ta dựa vào ItemEntryID. ItemEntryID có 2 hàng, cũng không phải vấn đề khi việc tìm kiếm trong EventHistory khi ta đã có ItemEntryID của email này từ bài 10. Email cần tìm trong EventHistory:

A screenshot of a computer

Description automatically generated

Flag: inseclab{14386}

## Bài 15

Để giải được bài 15, ta cần phải hiểu toàn bộ nội dung trao đổi của CEO với ông CFO vào ngày 7/6. Nhưng phần đó đã được tóm tắt:

A close up of a document

Description automatically generated

Đây là những mail gửi từ CEO ngày 7/6 (cột 43652.75 là giá trị 7/6 nhưng chuyển lỗi):

A close-up of a computer screen

Description automatically generated

Vào lúc 20:30 UTC+2, CEO đã nhắn với CFO rằng đã thực hiện đàm phán xong (xem bằng Outlook file pst của CFO):

A close-up of a message

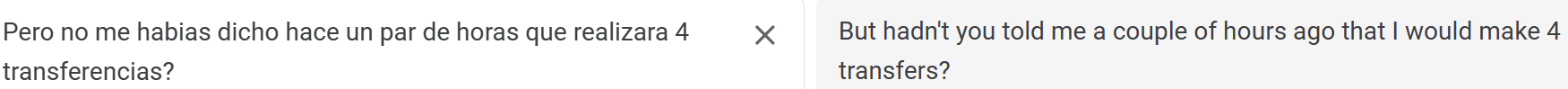
Description automatically generated

Dịch tiếng anh:

A screenshot of a computer

Description automatically generated

CEO bảo là không COBALT. Rồi sau đó CFO hỏi lại:



CFO hỏi là “Nhưng không phải nãy sếp kêu chuyển khoản sao?”.

Từ đó ta có thể đây là nội dung duy nhất trong ngày của CEO. Nhưng file outlook không có giây, phải vào MessageTracking coi Subject “Coltrasion OK” giống của Outlook rồi trừ đi 2h để thành UTC+0:

A screenshot of a computer

Description automatically generated

Flag: inseclab{18:39:16}

## Bài 12 – 13

Sử dụng Kernel Outlook PST Viewer, nếu file chưa bị xóa thì nó sẽ nằm trong thư mục Recoverable Items/Deletions:

A screenshot of a computer

Description automatically generated

Xem thời gian lần cuối được chỉnh sửa: 11:20:41 PM. Để biết nó đang ở UTC nào, ta xem giờ nó gửi đi là 23:02. Ở bài 5, file này được gửi đi lúc 16:02:01 UTC+0. Vậy file này đang ở UTC+7. Vậy UTC+0 của lần cuối sửa là 16:20:41. Nhập flag này không đúng cho bài 12. Hóa ra đây là lần cuối file này xuất hiện trước khi xóa, nên nó là của flag 13. Flag13: inseclab{16:20:41}.

Chắc tool này không lưu các phiên bản chỉnh sửa khác. Buộc phải vào xem EventHistory. Từ bài trước, DocumentID của mail này là 14386. Đúng là lần cuối xuất hiện thì là vào 16:20:4. Trường EventName của nó là ObjectMoved (lần 2 là xóa vĩnh viễn):

A screenshot of a computer

Description automatically generated

Vậy lần kế cuối xuất hiện là: 16:04:50. Đây là lần xóa file không thành. Nên trường EventName của nó là ObjectMoved (lần 1 là đưa vào thùng rác):

A screenshot of a computer

Description automatically generated

flag12: inseclab{16:04:50}

## Bài 8

Với cách giải của bài 12-13, ta có thể dùng EventHistory để giải bài 8 bằng cách tìm lần xuất hiện đầu tiên của documentID ứng với mail này:

A screenshot of a computer

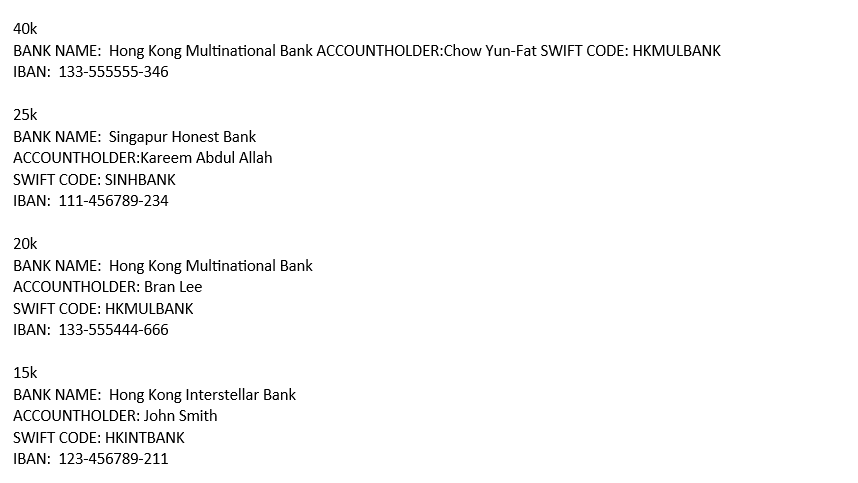
Description automatically generated

Đúng thật, trường EventName là “ObjectCreated”

Đề bài nói thời gian thực tế chậm hoặc nhanh hơn 1s. flag: inseclab{15:56:06}

## Bài 7

Có một mail từ tài khoản tên Abelardo Alcazar yêu cầu chuyển tiền



Sắp xếp theo thứ tự từ lớn đến bé là ra flag: inseclab{111-456789-234,123-456789-211,133-555444-666,133-555555-346}

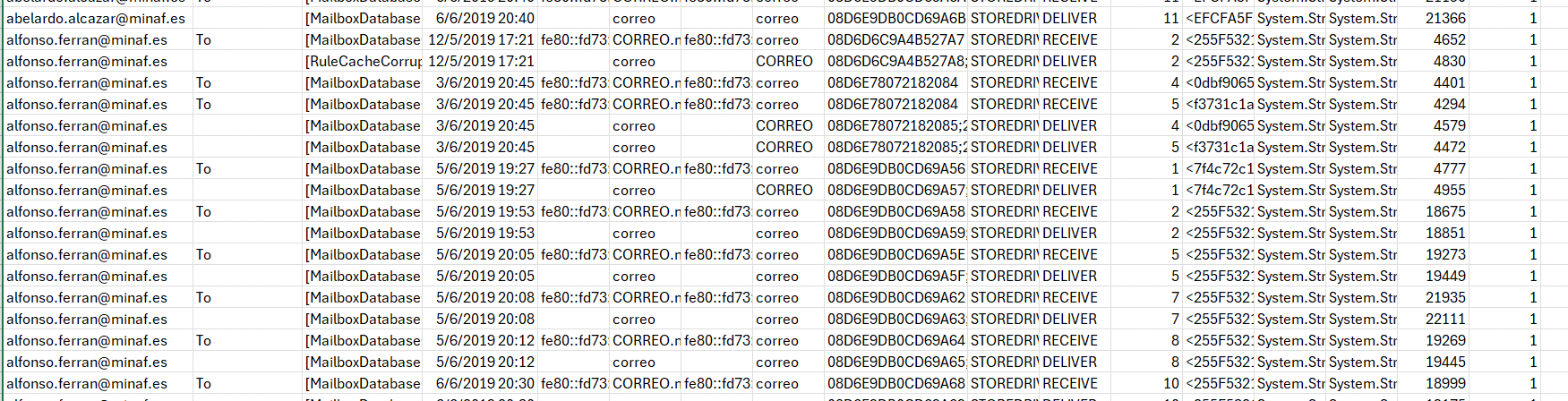
## Bài 14

Ta quan sát email có COBALTO gửi lần đầu tiên, với DocumentID là 14386 trong EventHistory. Phần lớn chúng đều có ClientCatagory (loại client dùng để thực hiện) là OWA (Outlook Web Access) – 1 loại mail dạng web.

Flag: inseclab{OWA}

## 16. Bài 6

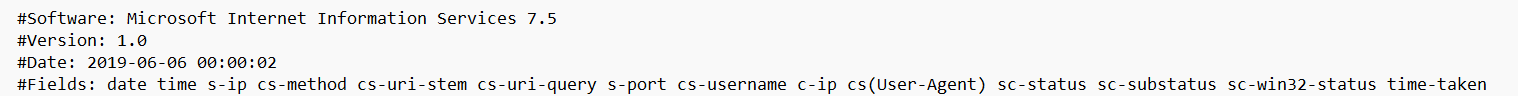
Kiểm tra trong MessageTracking, đếm các mail gửi từ abelardo.alcazar đến địa chỉ mail khác thì thấy có 18 mail



Flag: inseclab{18}

## Bài 18

Cú pháp log:



ip của mạng 10.x.x.x có thể là ip của doanh nghiệp như vpn. IP 101.132.122.100 khả năng cao là của attacker. Điều này càng có thể đúng khi địa chỉ ip này truy cập tới /owa thay vì ActiveSync như hình dưới (file u\_ex190604.log):

A screenshot of a computer

Description automatically generated

20:33:30 ngày 4/6/2019 cũng là lần đầu ghi nhận sự xuất hiện của ip này, khi host mang ip này đang tìm cách login vào owa.

flag: inseclab{2019-06-04 20:33:30}

## Bài 19

Mở file u\_ex190606.log:

A close-up of a computer screen

Description automatically generated

Ở những log trên, ta thấy attacker đang cố gắng login vào OWA, có thể qua bruteforce nhưng bị thất bại (nhận về 401). Tới 2019-06-06 20:05:25 (hình dưới) thì mới login thành công (trả về 302).

A blue and black text

Description automatically generated

Flag: inseclab{ 2019-06-06 20:05:32}

## Bài 20-21

Sử dụng Recovery Toolbox để đổi file ost trong PC2-Outloo sang pst rồi import vào Outlook. Mở phần inbox, mail này:

A screenshot of a computer

Description automatically generated

Nội dung mail có ý nghĩa là “click vào link này để đăng ký 1 sự kiện”:

A screenshot of a phone

Description automatically generated

Nghe rất giống phising, đặc biệt là khi mà mail này gửi vào 21:52 ngày 6/6/2019, trước ngày diễn ra vụ việc. Mà bài 20 cần một tên miền giả mạo. flag20: inseclab{www.federgolfmadrid.com}

Tới bài 21, ta đã có gần như toàn cảnh vụ việc (trừ bài 17), tóm tắt lại các bước cuộc tấn công:

1. Attacker spoofing 1 email đến CEO với nội dung về golf trong 1 trang phishing web.
2. Attacker dùng password của vị CEO (do trùng password) để login vào exchange.
3. Lợi dụng lúc CEO đàm phán, Attacker liên lạc với CFO yêu cầu chuyển khoản.
4. Xóa những cái mail để đảm bảo cuộc tấn công thuận lợi.

Thay vì search google về MITRE ATT&CK, em đã hỏi ChatGPT:

A white paper with black text

Description automatically generated

flag: inseclab{BEC}

## Bài 17

In ra cột User-agent



Load lên file notebook:

A screenshot of a computer program

Description automatically generated

Thử hết các giá trị (trừ c-ip). Flag: inseclab{Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36}