BÁO CÁO BÀI TẬP LÝ THUYẾT

**Môn học: Pháp chứng kỹ thuật số**

**Bài tập: Email**

*GVHD: Nghi Hoàng Khoa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.O21.ATTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 2 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Nhung | 21521248 | 21521248@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

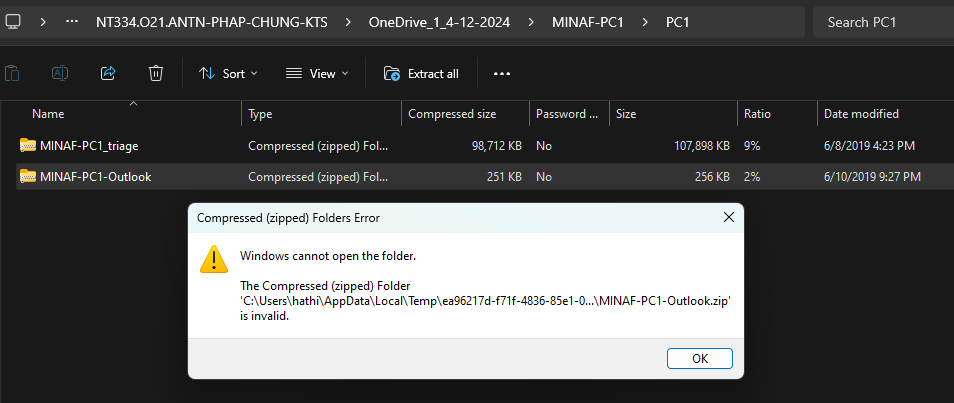
|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | 21 challenges | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Challenge 1: Một trong những việc đầu tiên của điều tra viên chính là kiểm tra mã băm của các chứng cứ mà MINAF cung cấp. Một trong các chứng cứ được cung cấp gặp vấn đề, đó là tập tin nào?**

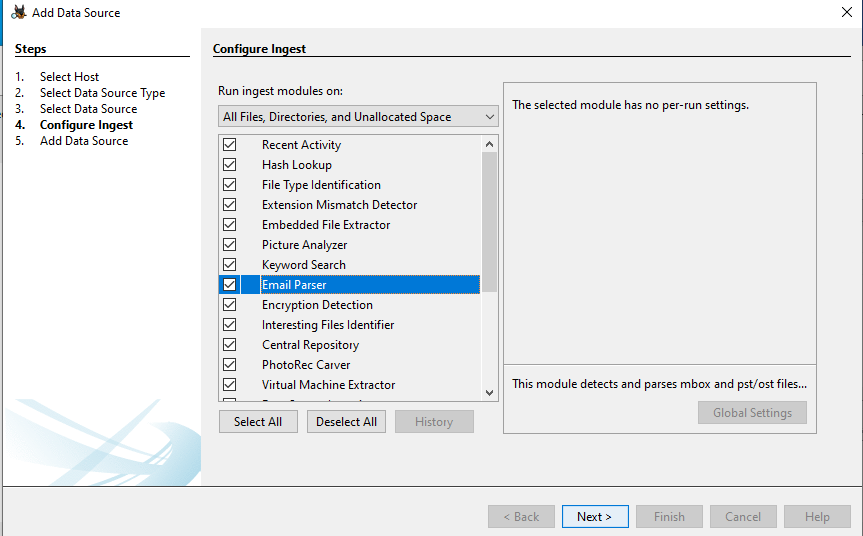
* Một trong những chứng cứ gặp vấn đề, nếu muốn tìm kiếm tập tin có vấn đề đó thì ta lần lượt thực hiện mở các file và thư mục tải về, thì nhận thấy rằng:



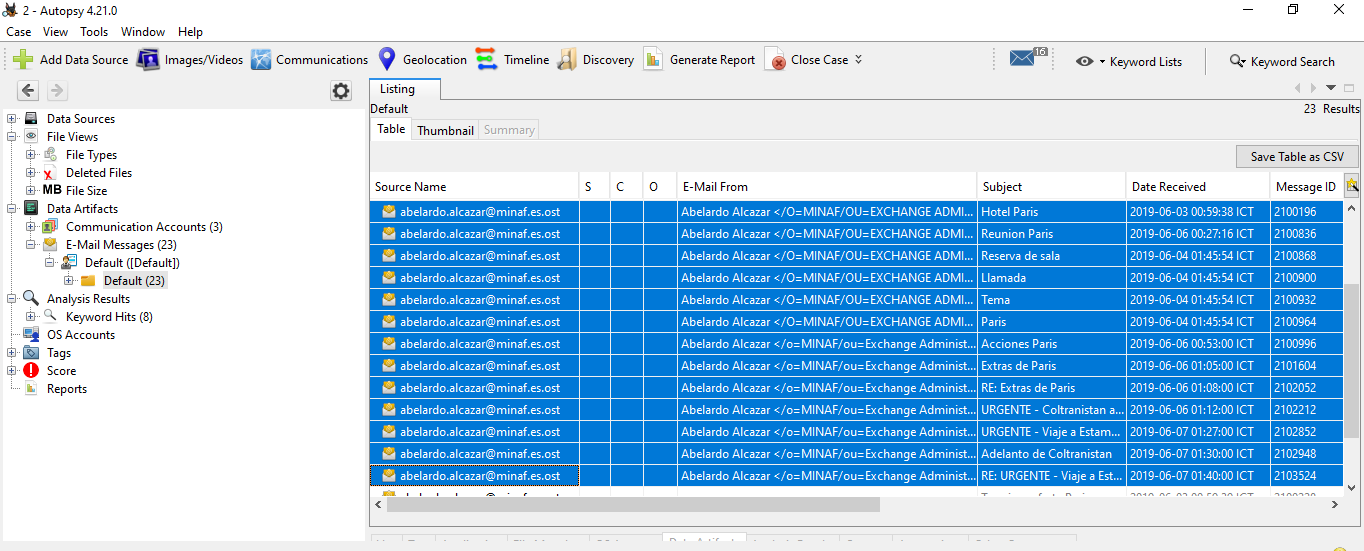
* **FLAG: inseclab{MINAF-PC1-Outlook.zip}**

1. **Challenge 2: Sử dụng tập tin MINAF-PC2-Outlook.zip, xác định có tổng cộng bao nhiêu Email được gửi từ tài khoản abelardo.alcazar trong khoảng thời gian từ 02/06/2019 đến 07/06/2019?**

* Sử dụng autospy để xem thông tin tập tin **MINAF-PC2-Outlook.zip**



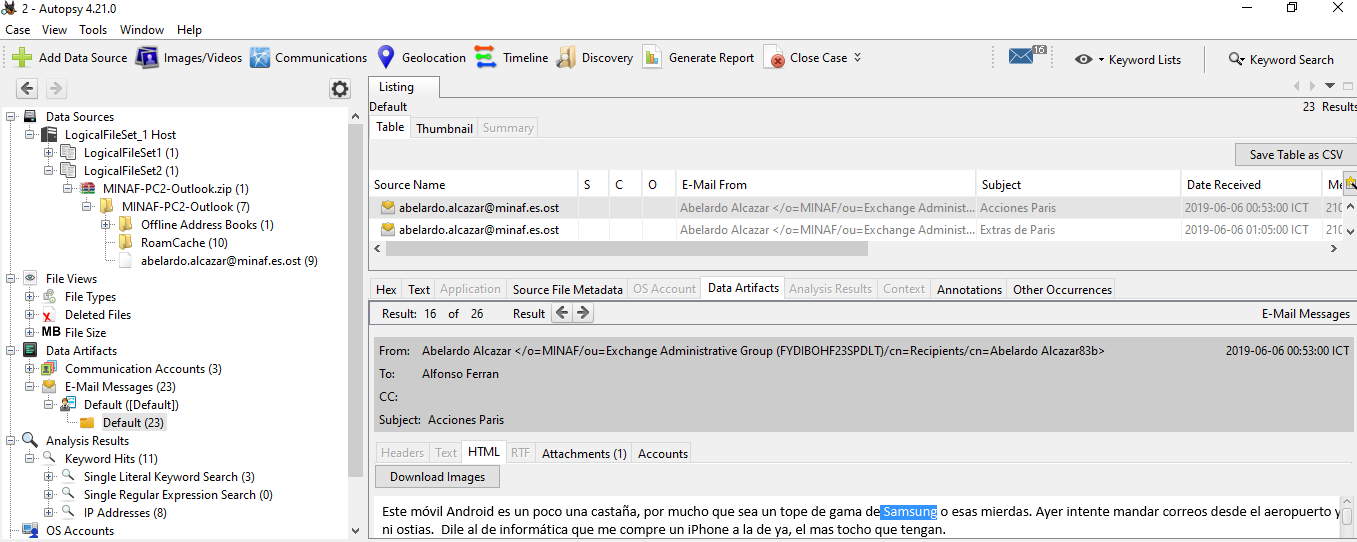
* Sau khi kiểm tra thì ta nhận thấy, có 13 email được gửi từ tài khoản abelardo.alcazar trong khoảng thời gian từ 02/06/2019 đến 07/06/2019



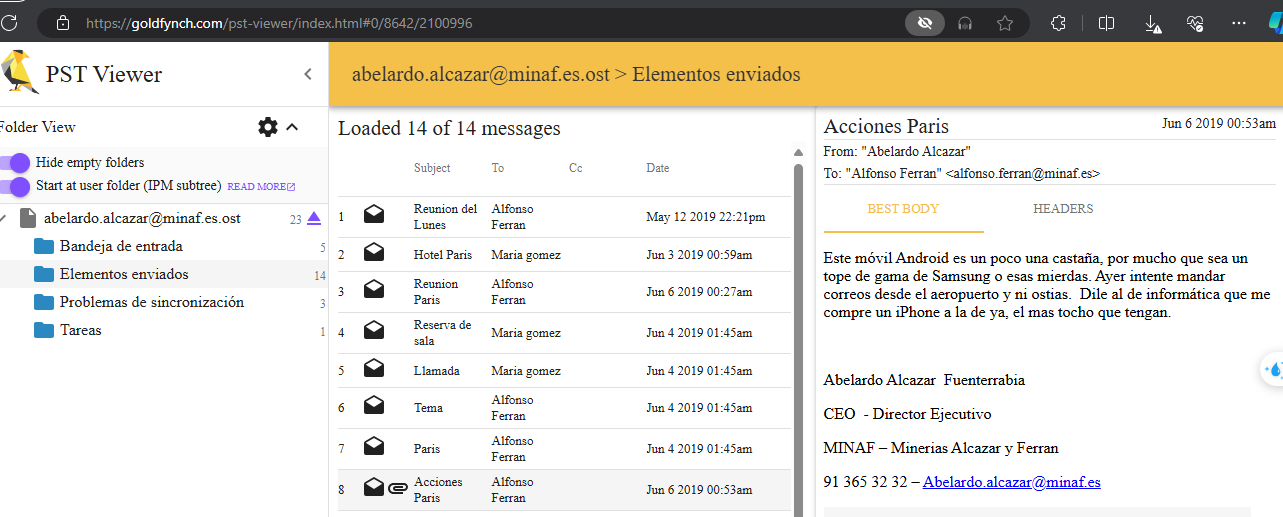
* **FLAG: inseclab{13}**

1. **Challenge 3: Sử dụng tập tin MINAF-PC2-Outlook.zip và cho biết tên hãng điện thoại mà Abelardo Alcazar sử dụng.**

* Tiếp tục sử dụng AutoSpy để kiểm tra tìm kiếm xem hãng điện thoại Abelardo Alcazar sử dụng, thì trong 1 email ngày 6/62019 ta thấy thông tin như sau:



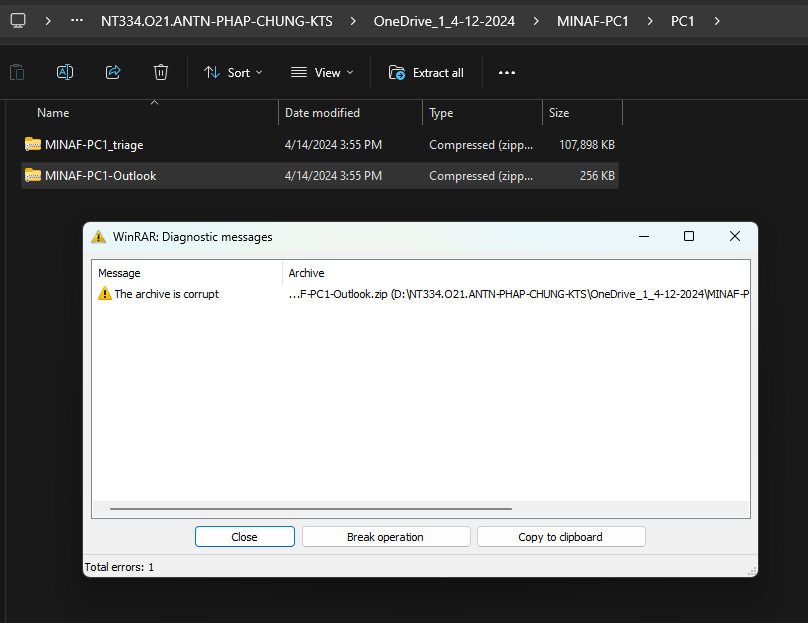
* Hoặc dùng PST Viewer để xem



* **FLAG: inseclab{Samsung}**

1. **Challenge 4: Kiểm tra sơ bộ tập tin MINAF- PC1-Outlook.zip, chúng ta phát hiện tập tin này đã bị …? (Gợi ý, đây là 1 từ tiếng Anh diễn tả trạng thái của tập tin đang sử dụng)**

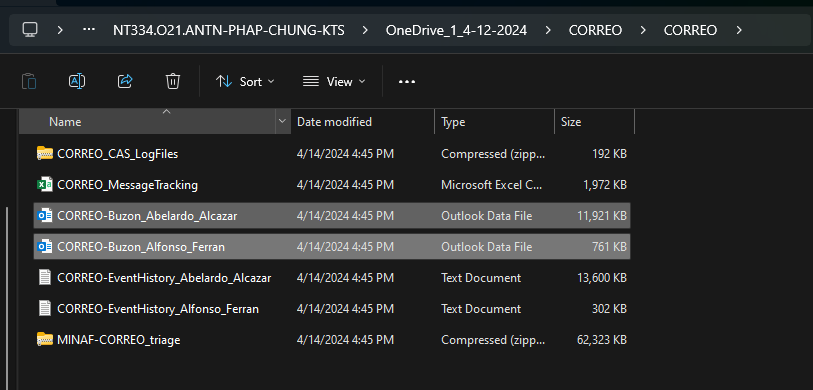
* Như challenge 1 ta đã biết có vấn đề xảy ra ở **MINAF- PC1-Outlook.zip,** vậy điều gì đang xảy ra với tập tin này (1 từ tiếng Anh diễn tả trạng thái của tập tin đang sử dụng), sử dụng winrar để giải nén xem hiện thông báo gì

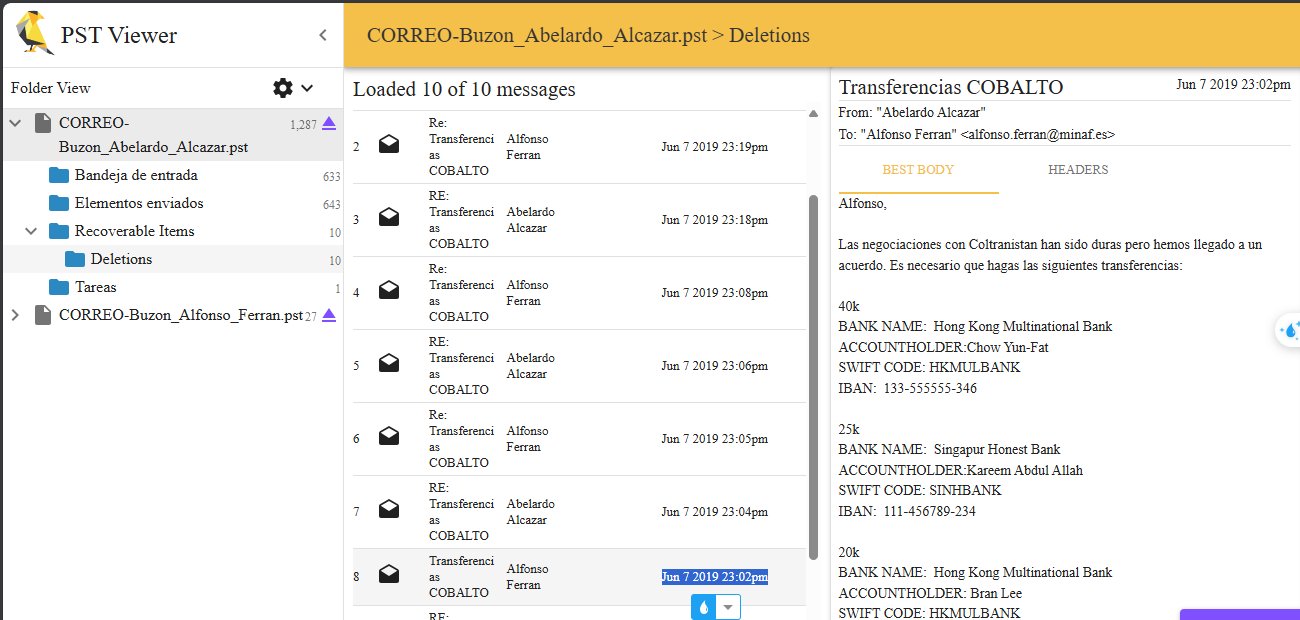


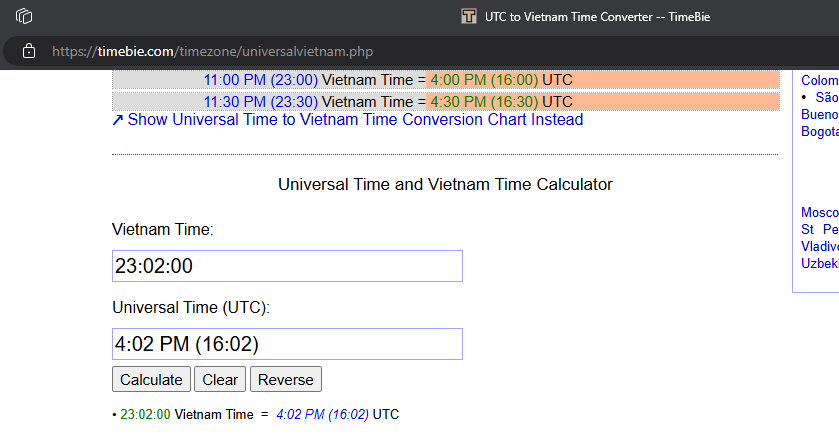
* **FLAG: inseclab{corrupted}**

1. **Challenge 5: Vào ngày 07/06/2019, có một vài Email được gửi với tiêu đề (subject) chứa từ khóa “COBALTO”. Hãy cho biết Email đầu tiên được gửi vào thời gian nào? (Ghi chú, trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS)**

* Dùng PST Viewer để xem



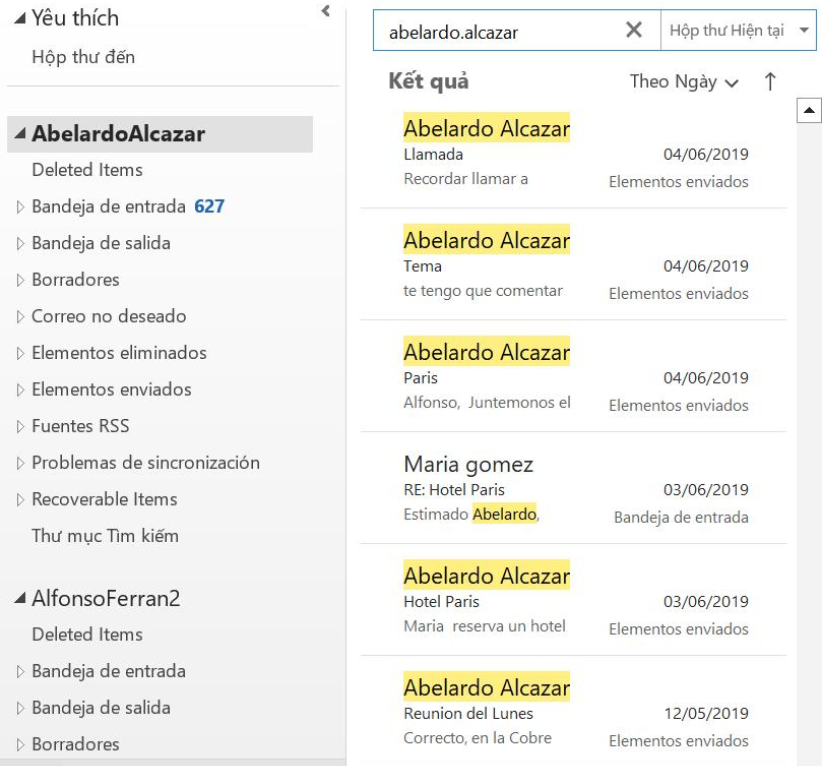




* **FLAG: inseclab{16:02:00}**

1. **Challenge 6: Có bao nhiêu Email THẬT SỰ được gửi bởi tài khoản abelardo.alcazar từ ngày 02/06/2019 đến ngày 07/06/2019? (Gợi ý, đừng đếm các Email yêu cầu xóa từ xa – remotewipe)**

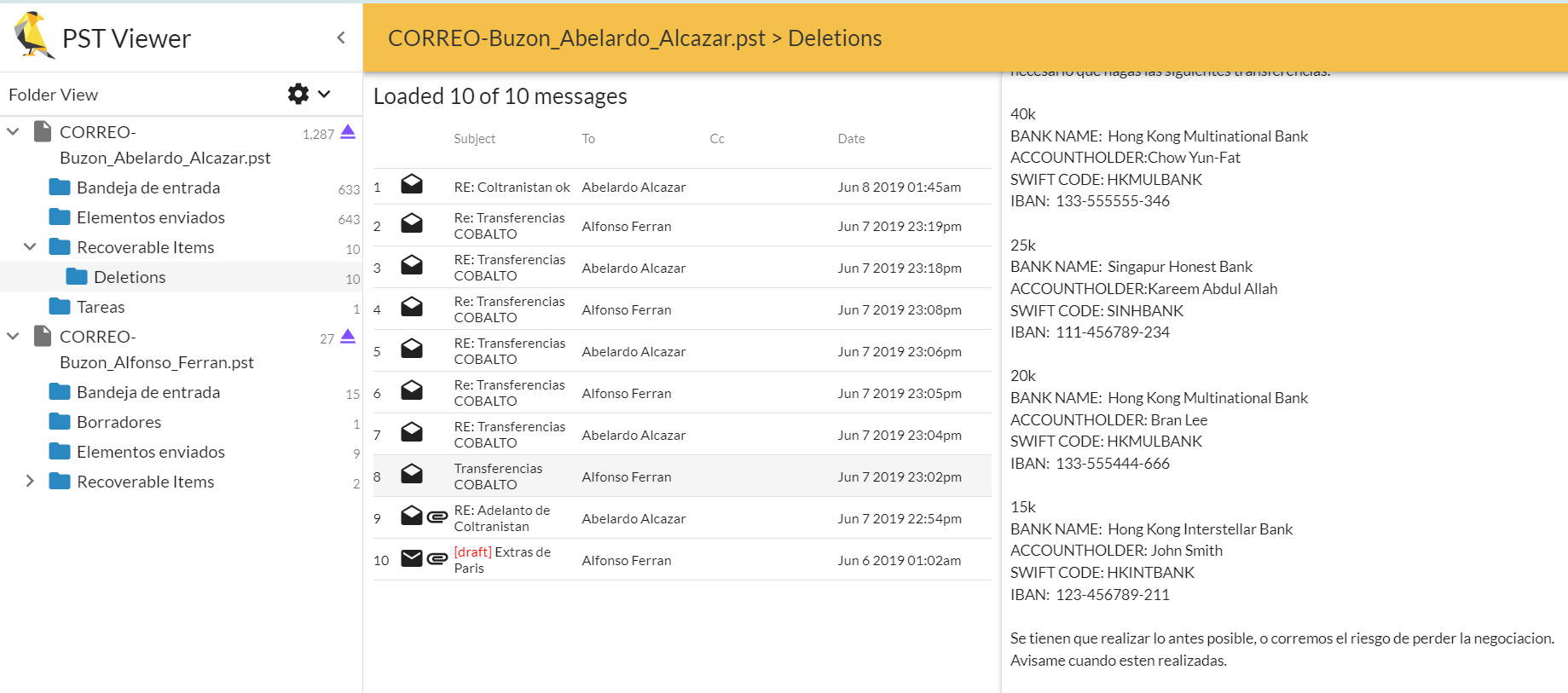
Tìm kiếm abelardo.alcazar trong hộp thư của Abelardo Alcazar, sau đó sắp xếp kết quả theo ngày.



* Bỏ qua các email yêu cầu xoá từ xa, tìm kiếm các email từ ngày 02/06/2019 đến ngày 07/06/2019 (vì tính theo múi giờ UTC+0 nên 1:39 AM 08/06 vẫn là ngày 07/06), chúng ta đếm được 18 email.
* **FLAG: inseclab{18}**

1. **Challenge 7: Vào ngày 07/06/2019, có một vài yêu cầu chuyển khoản ngân hàng được yêu cầu. Hãy cho biết số tài khoản? (Định dạng: sắp xếp theo thứ tự từ bé đến lớn, cách nhau bởi dấu ‘,’ và không có khoảng trắng)**

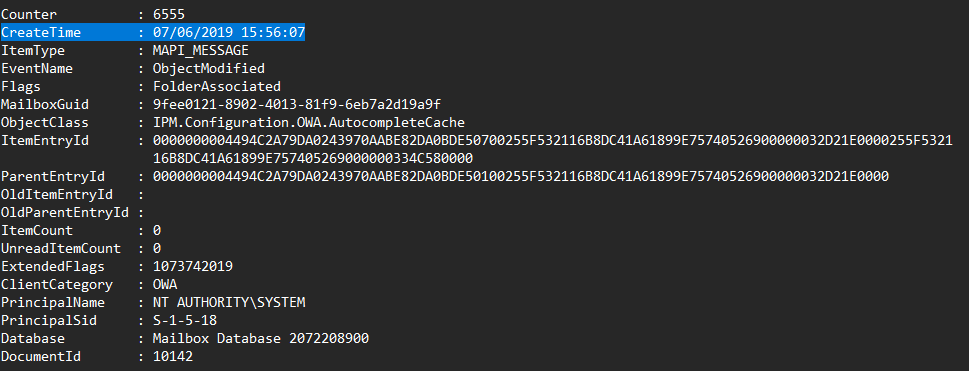
* Trong phần thư đã xoá, có một email đề cập đến thông tin chuyển khoản. Nhấn vào để xem nội dung thì chúng ta nhận được thông tin về 4 số tài khoản.



* **FLAG: inseclab{111-456789-234,123-456789-211,133-555444-666,133-555555-346}**

1. **Challenge 8: Vào ngày 07/06/2019, có một vài Email được gửi với tiêu đề (subject) chứa từ khóa “COBALTO”. Bạn hãy cho biết thời gian chính xác mà lá thư đầu tiên được gửi bắt đầu từ lúc soạn thư? Trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS. (Gợi ý, tùy thuộc vào chứng cứ mà bạn sử dụng, số giây có thể sai số trong khoảng “+1/-1”, vì vậy hãy bình tĩnh)**

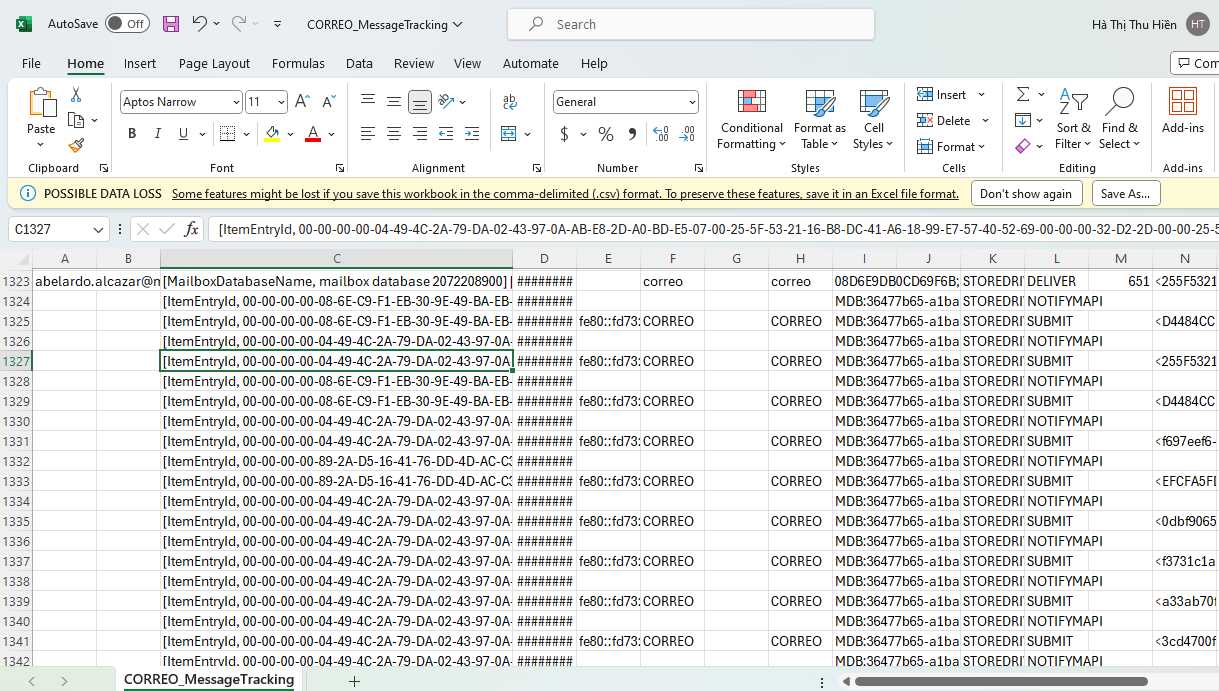
* Ta có thể dùng EventHistory để tìm lần đầu tiên xuất hiện của documentID ứng với mail này

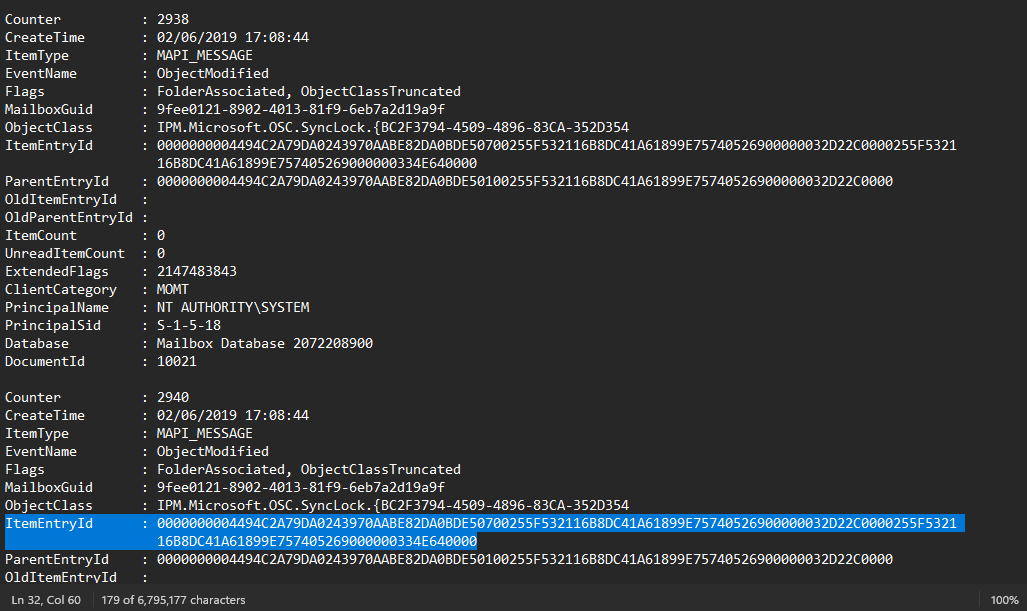


* **FLAG: inseclab{15:56:06}**

1. **Challenge 9: Mỗi Exchange email đều có một trường nào đó duy nhất cho phép máy chủ email xác định chúng. Hãy cho biết tên của trường đó? (Gợi ý, trường đó được hiển thị ở cả 2 vị trí MessageTracking và EventHistoryDB)**

* Như gợi ý, cùng xem thử trong 2 file MessageTracking và EventHistoryDB xem phát hiện ra trường duy nhất cho phép máy chủ email xác định chúng:

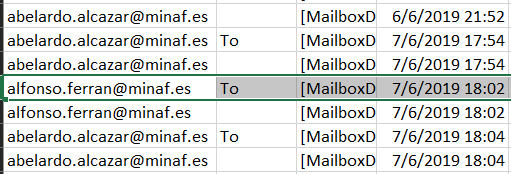


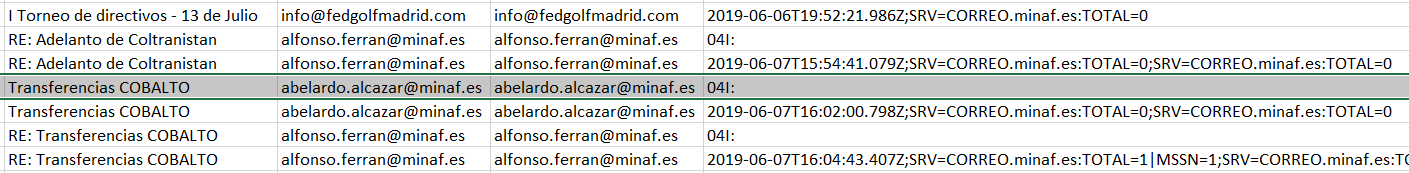


* **FLAG: inseclab{ItemEntryId}**

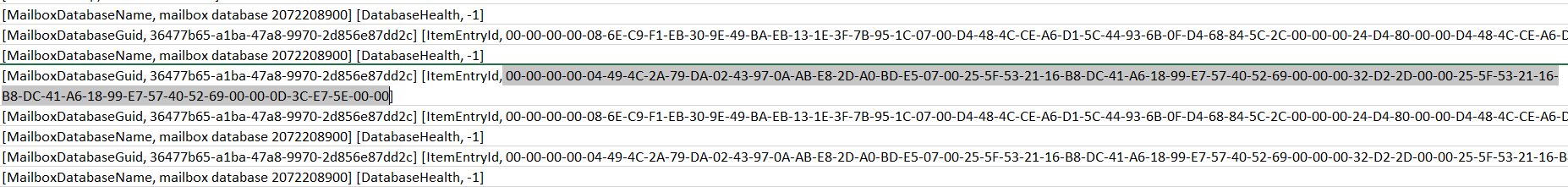
1. **Challenge 10: Cho biết giá trị của trường đó đối với Email đầu tiên được gửi bởi tài khoản abelardo.alcazar vào ngày 07/06/2019 với tiêu đề (subject) chứa từ khóa “COBALTO”? (Lưu ý, bỏ dấu “-” trong câu trả lời).**

* Tìm trong file excel CORREO\_MessageTracking với yêu cầu sender abelardo.alcazar, thời gian 7/6/2019, subject có “COBALTO”, tìm được:



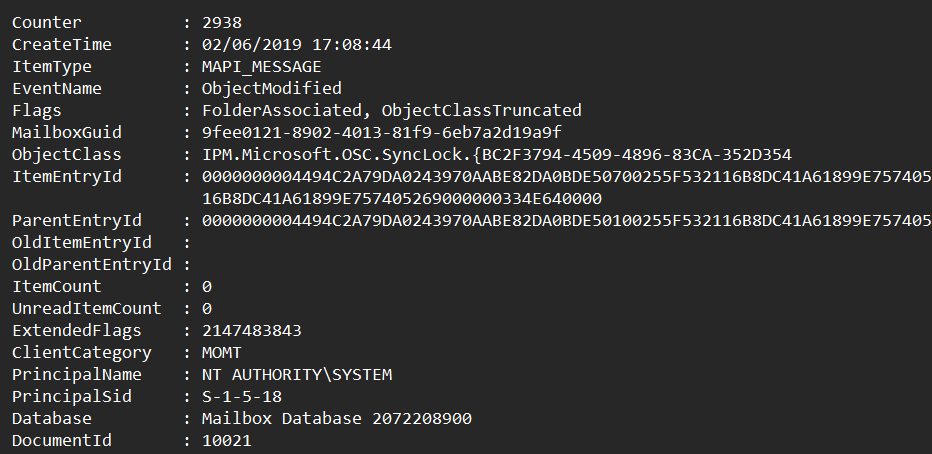


* Kết quả flag là ItemEntryId:

Flag: inseclab{00000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E75740526900000032D22D0000255F532116B8DC41A61899E75740526900000D3CE75E0000}

1. **Challenge 11: Email khá là quan trọng. Hãy cho biết giá trị của trường DocumentId?**

* Thông tin của mỗi email được lưu dưới định dạng như sau trong file CORREO-EventHistory\_Abelardo\_Alcazar.txt:



* Do ItemEntryId là duy nhất nên em sẽ tìm DocumentId thông qua ItemEntryId. Chỉ lấy một số kí tự ở cuối ItemEntryId để search vì ItemEntryId bị ngắt dòng, nên copy full thì sẽ tìm không được:

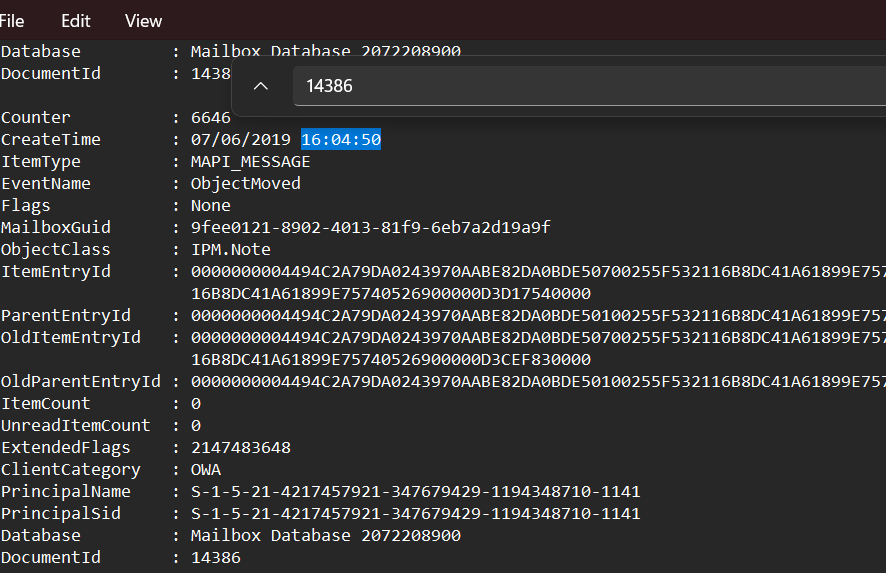
Flag: inseclab{14386}

1. **Challenge 12: Email này đã hoàn thành nhiệm vụ của nó. Hãy cho biết thời gian mà Email này được xóa? Trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS.**

* Em tìm thời gian email được xóa thông qua DocumentId và dựa vào EventName, tìm được ObjectDeleted:

Tuy nhiên, nhập 16:02:01 lại không chính xác.

* Thực hiện tiếp, lần cuối cùng email xuất hiện trên log là 16:20:41, tuy nhiên đây vẫn không phải flag cho challenge này:
* Tại câu 13 đã cho biết email bị xóa trong 2 lần và lần 2 mới bị xóa hoàn toàn, nên lần cuối cùng này sẽ là flag cho challeng 13. Còn flag cho câu 12 là mốc thời gian của sự kiện kế cuối:



Flag: inseclab{16:04:50}

1. **Challenge 13: Thật buồn cười nhưng Email đó không hoàn toàn bị xóa sạch ngay lần đầu tiên nó bị xóa. Bạn có thể đoán được thời gian mà Email này chắc chắn bị xóa khỏi hộp thư của người dùng không? Trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS.**

Như em đã trình bày ở câu 12, câu 13 sẽ có flag là inseclab{16:20:41}.

1. **Challenge 14: Email này (và các email liên quan) đã thu hút được rất nhiều sự chú ý. Nhưng, nó thực sự đến từ đâu? Các tùy chọn: Outlook, Mobile, ECP, OWA, PigeonCarrier.**

Các email này đến từ OWA:

Flag: inseclab{OWA}

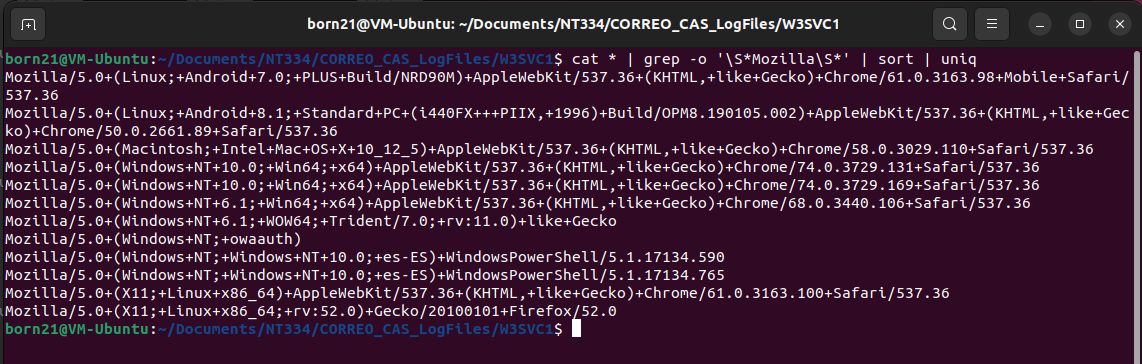
1. **Challenge 15: Abelardo Alcazar chỉ gửi 1 email duy nhất vào ngày 07/06/2019. Anh ấy đã gửi nó khi nào?**

* Thông tin tìm được:
* Flag: inseclab{18:39:15}

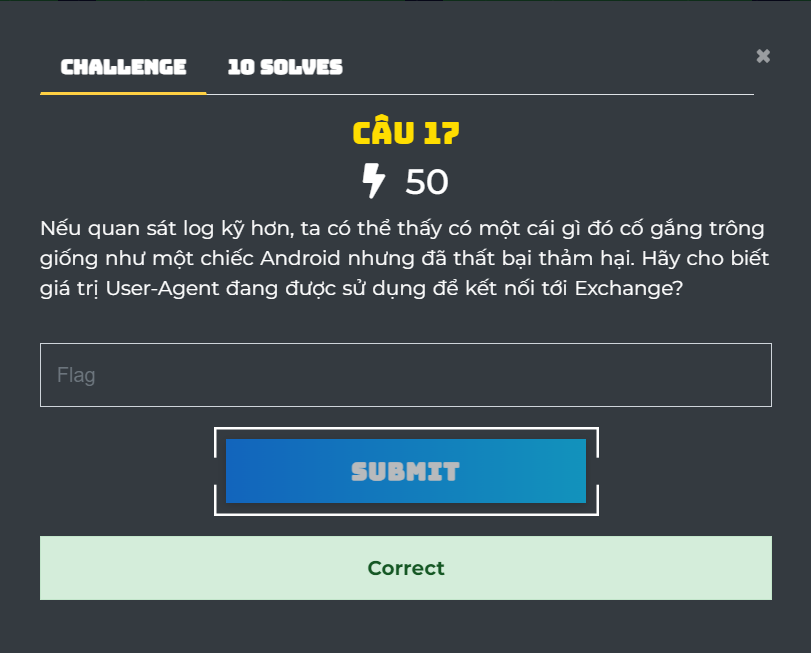
1. **Challenge 16: Điện thoại của Abelardo Alcazar có DeviceID là bao nhiêu?**

* Em dùng Outlook để mở các file Outlook Data file mà thầy đã cung cấp, tìm được thông tin về điện thoại của Abelardo Alcazar như sau:
* Flag: inseclab{androidc1290513397}

1. **Challenge 17: Nếu quan sát log kỹ hơn, ta có thể thấy có một cái gì đó cố gắng trông giống như một chiếc Android nhưng đã thất bại thảm hại. Hãy cho biết giá trị UserAgent đang được sử dụng để kết nối tới Exchange?**



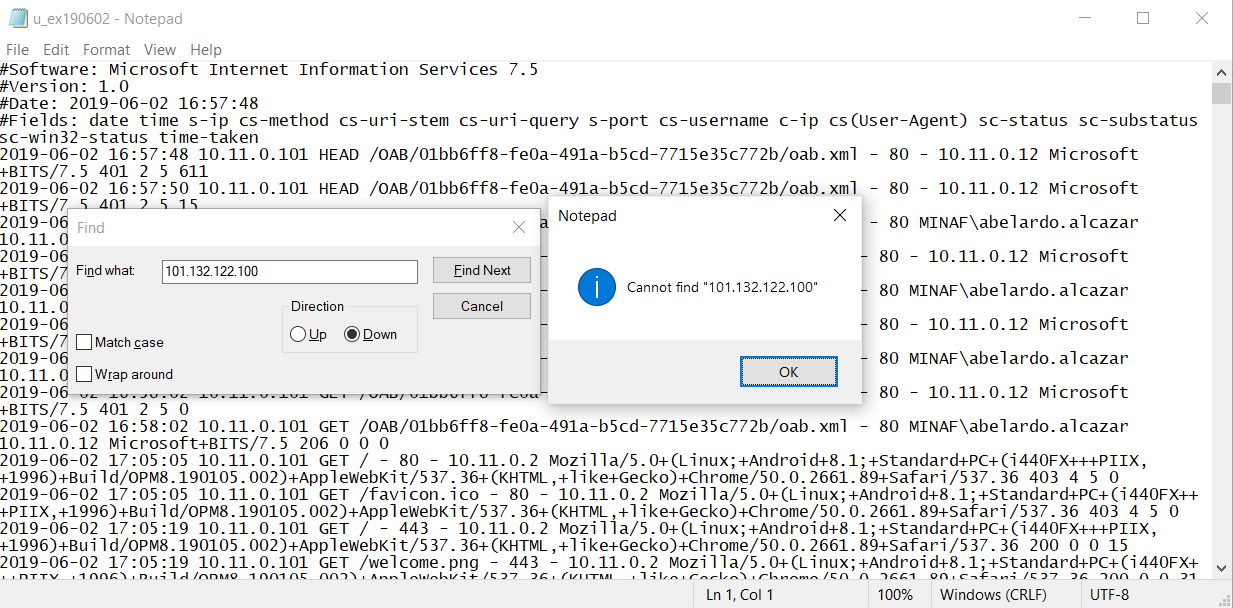
* Em nghĩ đến một cách là thử tất cả user agent được lưu lại trong các file .log. Kết quả sẽ cho chúng ta một danh sách các từ chứa "Mozilla" mà không có từ nào trùng lặp, được sắp xếp theo thứ tự từ điển.
* Khi em nộp flag với user agent đầu tiên thì hệ thống đã thông báo flag đúng, nhưng vì hết thời gian submit nên kết quả này không được lưu lại.



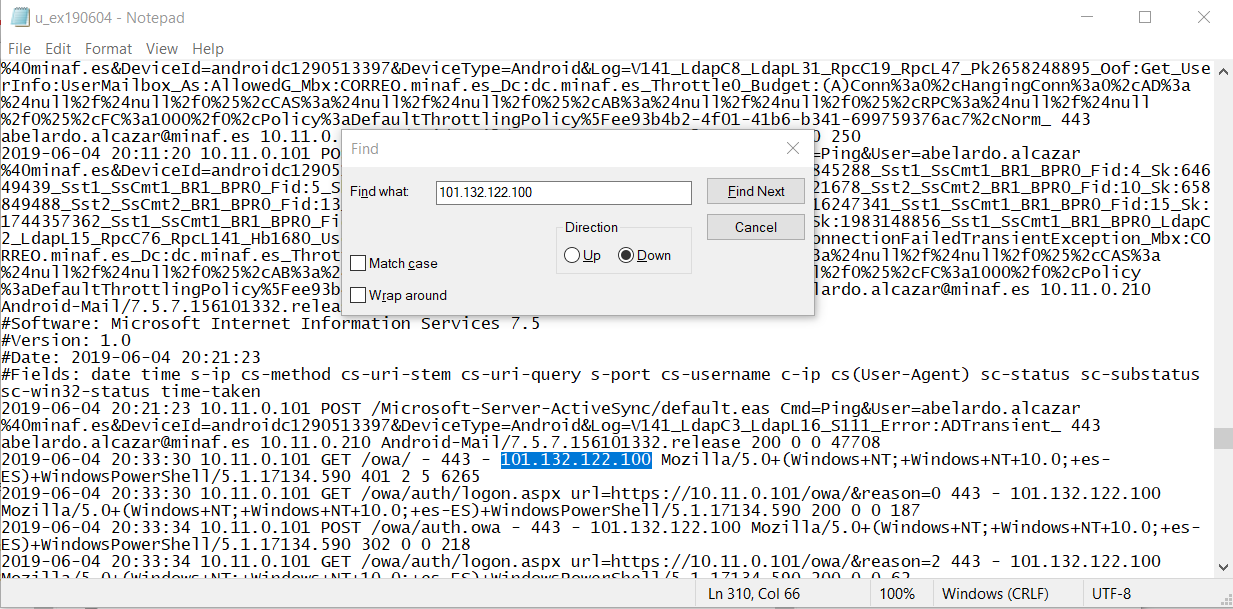
* Flag: inseclab{Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36}

1. **Challenge 18: Kẻ tấn công không phải bắt đầu tấn công vào hôm nay. Sau khi trả lời được các câu hỏi trước đó, vậy thì lần đầu tiên bạn nhìn thấy địa chỉ IP đó trong log của CAS Exchange là khi nào? Trả lời thời gian múi giờ UTC+0, định dạng YYYY-MM-DD HH:MM:SS.**

Từ các email chứa từ khoá “COBALTO” đã tìm được ở các câu trên, chúng ta tìm được địa chỉ IP của kẻ tấn công là 101.132.122.100. Thực hiện tìm kiếm địa chỉ IP này trong các file .log lần lượt theo thứ tự thời gian từ ngày 02/06 đến ngày 07/06.



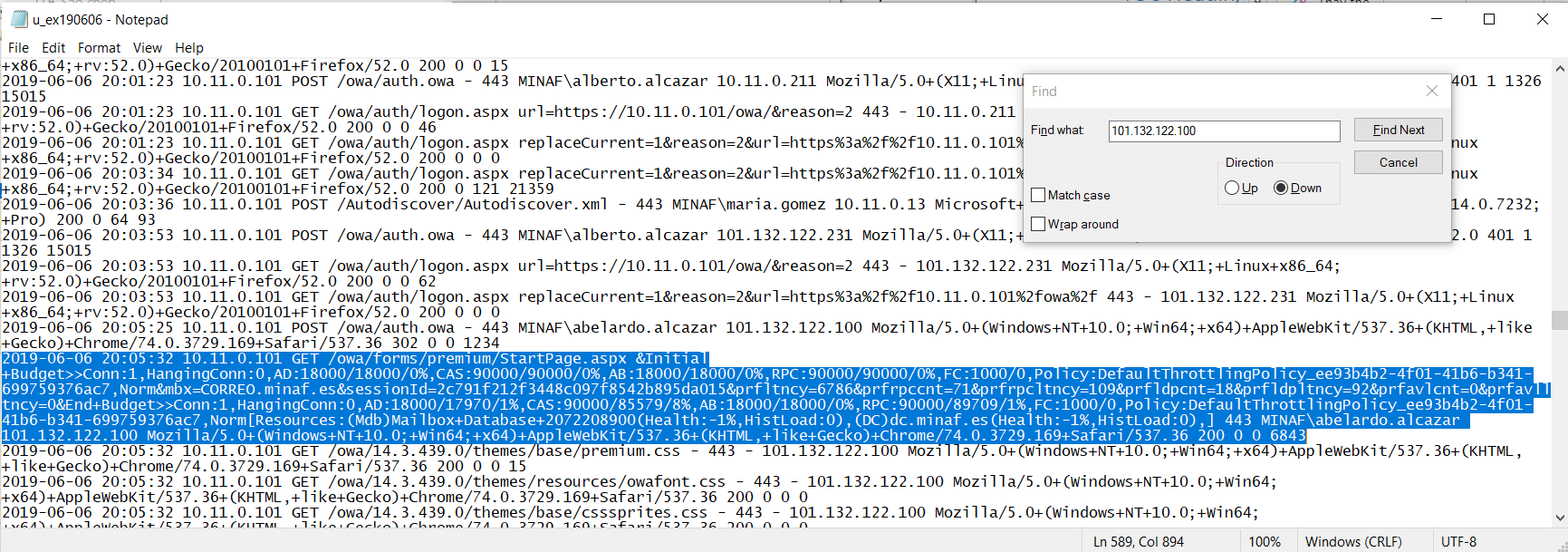
* Khi tìm đến ngày 04/06 thì tìm thấy địa chỉ IP.



* FLAG: inseclab{2019-06-04 20:33:30}

1. **Bằng một cách nào đó mà kẻ tấn công có được tài khoản của abelardo.alcazar. Bạn hãy cho biết lần đầu tiên mà kẻ tấn công đăng nhập thành công vào Exchange Server? Trả lời thời gian múi giờ UTC+0, định dạng YYYY-MMDD HH:MM:SS. (Lưu ý, chúng tôi định nghĩa “đăng nhập thành công” tính từ lúc gói tin đầu tiên được gửi đi sau khi chứng thực thành công)**

* Thực hiện tìm kiếm tiếp tục như yêu cầu 18, chúng ta có nhận xét là những yêu cầu đầu tiên được gửi đi có độ dài rất ngắn, nhưng từ ngày 06/06 lúc 20:05:32 xuất hiện yêu cầu có độ dài lớn hơn. Có thể suy luận là những yêu cầu đầu tiên mục đích để chứng thực nhưng không thành công, sau khi chứng thực thành công thì kẻ tấn công có thể thu thập được nhiều thông tin hơn. Hơn nữa, bắt đầu từ lúc này có thêm nội dung sessionId nên suy luận ở trên là đúng.



* FLAG: inseclab{2019-06-06 20:05:32}

1. **Kẻ tấn công đã thử rất nhiều cách để có thể vào được tài khoản**  
   **abelardo.alcazar… nhưng cuối cùng, các kỹ thuật cũ luôn thành công. Bạn hãy cho biết tên miền được sử dụng để lừa đảo Abelardo Alcazar**



* Abelardo có nhận được một bức thư, có lẽ là từ fedgolfmadrid, cung cấp thông tin về một giải đánh golf cũng như trang web để đăng kí. Và ông Abelardo không nghi ngờ gì, đã click vào đường link này, và bị tấn công.
* Kĩ thuật này gọi là phishing, là một kĩ thuật không có gì mới.
* FLAG: inseclab{http://www.federgolfmadrid.com}

1. **Với tất cả các chứng cứ thu thập được, ta có thể kết luận MINAF đã gặp phải cuộc tấn công có tên … (Gợi ý, chỉ 3 ký tự)**

Kẻ tấn công có thể giả mạo các quản lý hoặc nhân viên cấp cao trong tổ chức để tạo sự tin cậy và thúc đẩy hành động từ phía nạn nhân, yêu cầu chuyển khoản tiền từ các tài khoản doanh nghiệp hoặc quản lý tài chính sang các tài khoản ngân hàng được kiểm soát bởi kẻ tấn công. Các cuộc tấn công kiểu này gọi là BEC.

* FLAG: inseclab{BEC}

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)