

*M57 Jean*

*Digital Forensics Report*

*Παναγιώτης Κολλιόπουλος*

*July 24, 2023*

*Πρακτική στην Zelus IKE*

**Abstract**

Αυτό το report θα τεκμηριώσει τα ευρήματα μου από την εικόνα του σκληρού δίσκου του φορητού υπολογιστή που μας παρέιχε η άσκηση (1). Ο κύριος χρήστης του φορητού υπολογιστή είναι η Jean Jones, CFO της M57.biz. Η Jean κατηγορείται για διέρευση ευαίσθητων εταιρικών πληροφοριών σε έναν ανταγωνιστή μέσω email. Εξετάσαμε την εικόνα του σκληρού δίσκου χρησιμοποιώντας τα εργαλεία ανοιχτού κώδικα Autopsy και FTK Imager και επιβεβαίωσαμε ότι το εν λόγω αρχείο παραδόθηκε από την Jean σε λογαριασμό email εκτός του εταιρικού δικτύου. Το ερώτημα στη συνέχεια μεταβαίνει φυσικά στο αν η Jean γνώριζε ή όχι ότι διέρρεε δεδομένα. Αυτή η αναφορά θα δείξει ότι ενώ είναι πιθανό η Jean να ήταν συνένοχος στο έγκλημα, δεν υπάρχει καμία οριστική απόδειξη που να αποδεικνύει ότι είχε εγκληματική πρόθεση.

**Πληροφορίες**

Forensics Examiner: Παναγιώτης Κολλιόπουλος

Παράπτωμα: Corporate Data Exfiltration

Κατηγορούμενος: Jean Jones

**Γνωστικό υπόβαθρο (background)**

Η M57.biz είναι μια start-up με υπαλλήλους που εργάζονται κυρίως από τα σπίτια τους με καθημερινά chat sessions και τα περισσότερα έγγραφα ανταλλάσσονται μέσω email. Η Jean Jones, ο CFO για την M57.biz, είναι ύποπτη για διέρευση ευαίσθητων πληροφοριών των εργαζομένων σε έναν από τους ανταγωνιστές της M57.biz. Ένα υπολογιστικό φύλλο που περιέχει εμπιστευτικές πληροφορίες δημοσιεύτηκε ως συνημμένο στο φόρουμ «τεχνικής υποστήριξης» του ιστότοπου ενός ανταγωνιστή. Το υπολογιστικό φύλλο προήλθε από τον υπολογιστή της CFO Jean. Σε αυτήν την παρουσίαση θα καλύψω τις πρακτικές που χρησιμοποίησα για τη συλλογή δεδομένων για την υπόθεση, τα εργαλεία και τις μεθόδους που χρησιμοποίησα για την ανάλυση των δεδομένων, τις νομικές πτυχές που έπρεπε να λάβω υπόψη, την αλυσίδα αποδεικτικών στοιχείων (Chain of custody) και τα ευρήματά μου.

**Ερωτήσεις σχετικές με την υπόθεση:**

1. Πότε η Jean δημιούργησε το υπολογιστικό φύλλο?
2. Πως έφτασε από τον υπολογιστή της, στην ιστοσελίδα του ανταγωνιστή?
3. Ποιος άλλος είναι εμπλεκόμενος από την εταιρεία?

### Λογισμικό που χρησιμοποιήθηκε:



Autopsy 4.20.0

AccessData FTK Imager

Kernel Outlook PST Viewer

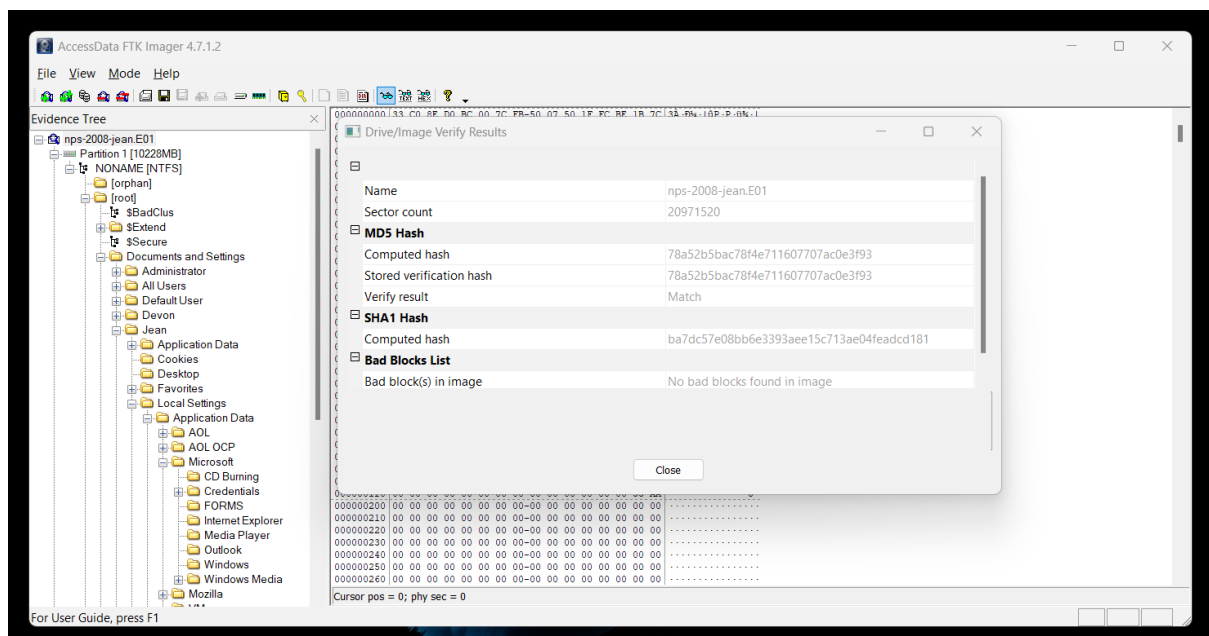
### Στοιχεία που συλλέχθηκαν

Είναι σημαντικό να σημειωθεί ότι δεν έκανα αντιγραφή (image) τον αρχικό σκληρό δίσκο, αλλά μου δόθηκε ένα αντίγραφο του δίσκου σε μορφή αρχείου Encase για ανάλυση.

 nps-2008-jean.E01	17/7/2023 5:38 μμ	Αρχείο E01	1.535.997 ...
 nps-2008-jean.E02	17/7/2023 5:36 μμ	Αρχείο E02	1.432.511 ...

### Legal Concerns

Ο νόμος περί ψηφιακών αποδεικτικών στοιχείων τείνει να περιβάλλει δύο βασικά ζητήματα: την αυθεντικότητα (authenticity) και την ακεραιότητα (integrity). Ο χειρισμός των αποδεικτικών στοιχείων έγινε έτσι ώστε να μην τροποποιηθούν από τον πρωτότυπο δίσκο. Εδώ έχουμε βοήθεια από το εργαλείο FTK Imager, το οποίο υπολογίζει τα MD5 hashes και μας διαβεβαιώνει ότι δεν έχει γίνει κάποια αλλοίωση των στοιχείων.



Για την έρευνα λοιπόν, δοκίμασα πέρα από αυτό το εργαλείο και το λογισμικό Autopsy για την ανάλυση της εικόνας του δίσκου. Αυτό το λογισμικό είναι εγγυημένο ότι δεν τροποποιεί τα περιεχόμενα της εικόνας με κανέναν τρόπο. Η ευκολία τροποποίησης των στοιχείων αποτελεί ανησυχία στον ψηφιακό κόσμο και η χρήση λογισμικού που μπορεί να ελέγξει την ορθότητα είναι σημαντική για τον ψηφιακό αναλυτή. Οι άλλες δύο νομικές πτυχές που πρέπει να λάβουμε υπόψη είναι η συνάφεια (relevance) και η αξιοπιστία (reliability). Σύμφωνα με όσα γνωρίζουμε, ψηφιακά αποδεικτικά στοιχεία είναι οποιαδήποτε αποδεικτική πληροφορία που αποθηκεύεται ή μεταδίδεται σε ψηφιακή μορφή και μπορεί να χρησιμοποιηθεί σε μια δικαστική υπόθεση. Πριν αποδεχτεί τα ψηφιακά αποδεικτικά στοιχεία, ένα δικαστήριο θα καθορίσει εάν αυτά είναι σχετικά, εάν είναι αυθεντικά, εάν είναι φήμες και εάν ένα αντίγραφο είναι αποδεκτό ή απαιτείται το πρωτότυπο. Μόλις αποδειχθεί ότι τα στοιχεία αυτά έχουν αυθεντικότητα, ακεραιότητα και είναι σχετικά, μπορούμε να ισχυριστούμε ότι μπορούν να βασιστούν στο δικαστήριο.

## Forensic examination of evidence and Analyzing the PST file

Όπως φαίνεται από το σενάριο, αυτή η υπόθεση περιστρέφεται γύρω από ένα σωρό email που στάλθηκαν προς και από τον υπολογιστή της Jean.

M57 Jean 2 - Autopsy 4.20.0

Case View Tools Window Help

Listing Default Table Thumbnail Summary

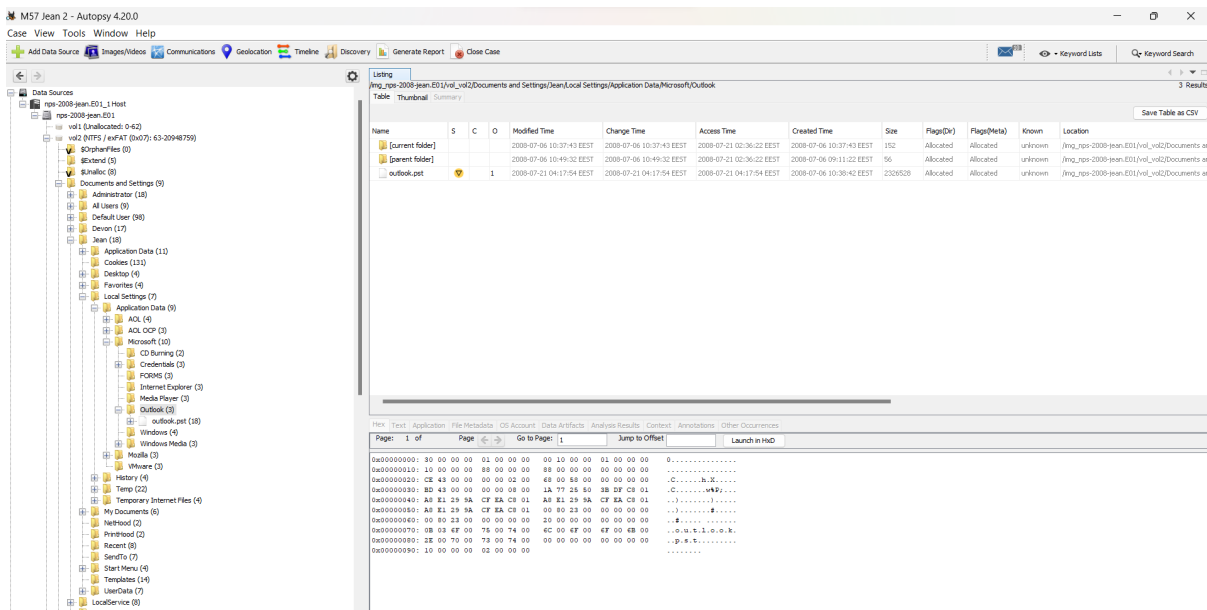
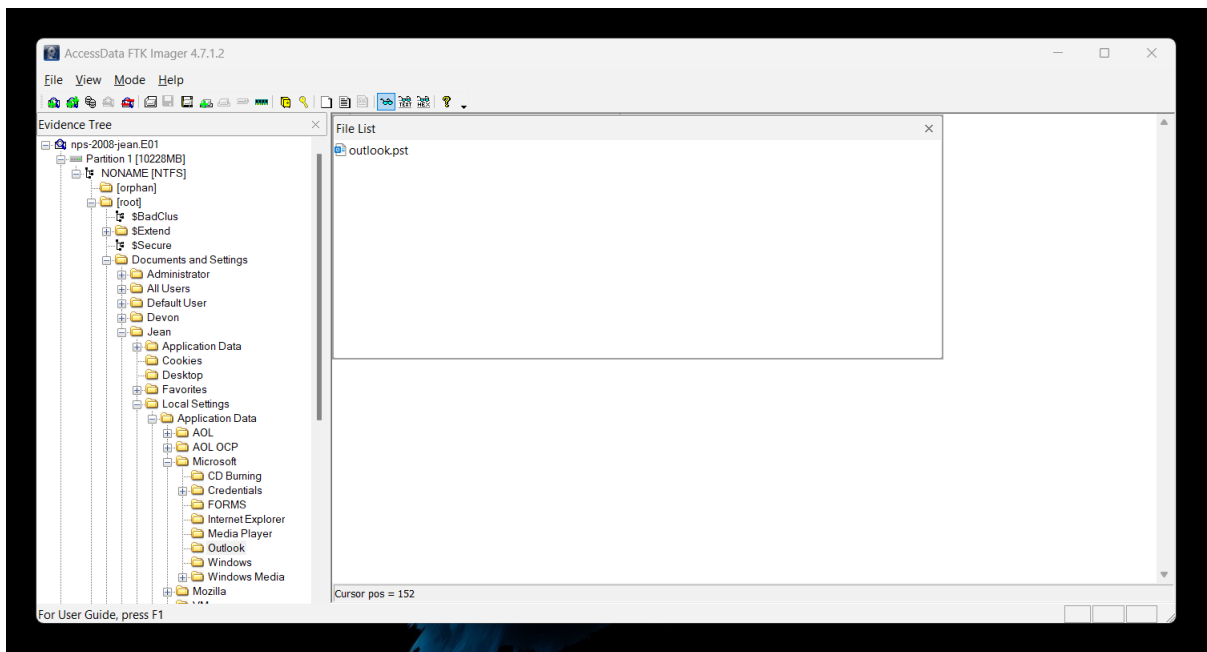
Source Name	S	C	O	E-Mail From	Subject	Date Received	Message (Plaintext)	Thread ID
outlook.pst				Microsoft Outlook-2000	Welcome to Microsoft Outlook-2000	2008-07-06 10:38:43 EEST	Welcome to Microsoft Outlook-2000 One Window to Your ...	0305d992-220e-4995-b4f1-43d2430eb84c
outlook.pst				Microsoft Outlook-2000	Welcome to Microsoft Outlook-2000	2008-07-06 10:39:00 EEST	Welcome to Microsoft Outlook-2000 One Window to Your ...	a82531a6-9079-4d81-94d2-34d20566914
outlook.pst				Jean User	test test test	2008-07-06 10:39:00 EEST	Do I have email now?	02c797d2-6f92-4078-9b79-838a6c376c57
outlook.pst				Jean User	test test test	2008-07-06 10:39:00 EEST	Do I have email now?	50c9379f-225c-470a-b478-696b7d5681d
outlook.pst				Jean User	let's try again	2008-07-06 10:40:00 EEST	Do I suck?	424af258-2c19-41f5-b6ba-d8f534d21a40
outlook.pst				Jean User	let's try again	2008-07-06 10:40:00 EEST	Do I suck?	2081a95c-feff-4a11-ba07-c41af3d862c2
outlook.pst				Jean User	test test test	2008-07-06 10:40:00 EEST	Do I have email now?	6cd30133-af58-47f5-8f6d-1a2d842e23f
outlook.pst				Jean User	let's try again	2008-07-06 10:40:00 EEST	Do I suck?	10419317-1d84-4463-906b-c2d47098620
outlook.pst				Jean User	test test test	2008-07-06 10:40:00 EEST	Do I have email now?	023b0a6c-7d81-4975-8b45-d8a6d6984985
outlook.pst				Jean User	let's try again	2008-07-06 10:40:00 EEST	Do I suck?	98c70d57-96d2-42d5-9e25-97f112d4e9f2
outlook.pst				Jean User	This is what I was talking about	2008-07-06 10:55:00 EEST	/living Home World U.S. Politics Crime Entertainment Hea...	84f1310e-6208-46d8-9a89-38a46308b3a
outlook.pst				Jean User	This is what I was talking about	2008-07-06 10:55:00 EEST	/living Home World U.S. Politics Crime Entertainment Hea...	58b24b0d-8cd1-444f-af41-190063208019
outlook.pst				jeand@07.baz	this is what I was talking about	2008-07-06 10:55:47 EEST	*Please note, the sender's email address has not been veri...	f13404c4-8a16-402e-bc94-25c39626608
outlook.pst				jeand@07.baz	this is what I was talking about	2008-07-06 10:55:47 EEST	*Please note, the sender's email address has not been veri...	937c4c57-182a-4994-6220-1a6d08f131ae
outlook.pst				Google Alerts	Click to confirm your Google Alert	2008-07-06 10:56:41 EEST	Google received a request to start sending Alerts for the s...	42d89391-a9ae-4d18-8c79-4b430d3f9f53
outlook.pst				Google Alerts	Click to confirm your Google Alert	2008-07-06 10:56:41 EEST	Google received a request to start sending Alerts for the s...	4a628a97-f6ac-46c8-a814-44c1202169fc
outlook.pst				Google Alerts	Click to confirm your Google Alert	2008-07-06 10:56:53 EEST	Google received a request to start sending Alerts for the s...	e4978765-7b79-42d9-931d-92d5c573a710
outlook.pst				Google Alerts	Click to confirm your Google Alert	2008-07-06 10:56:53 EEST	Google received a request to start sending Alerts for the s...	4a628a97-f6ac-46c8-a814-44c1202169fc

Analysis Results

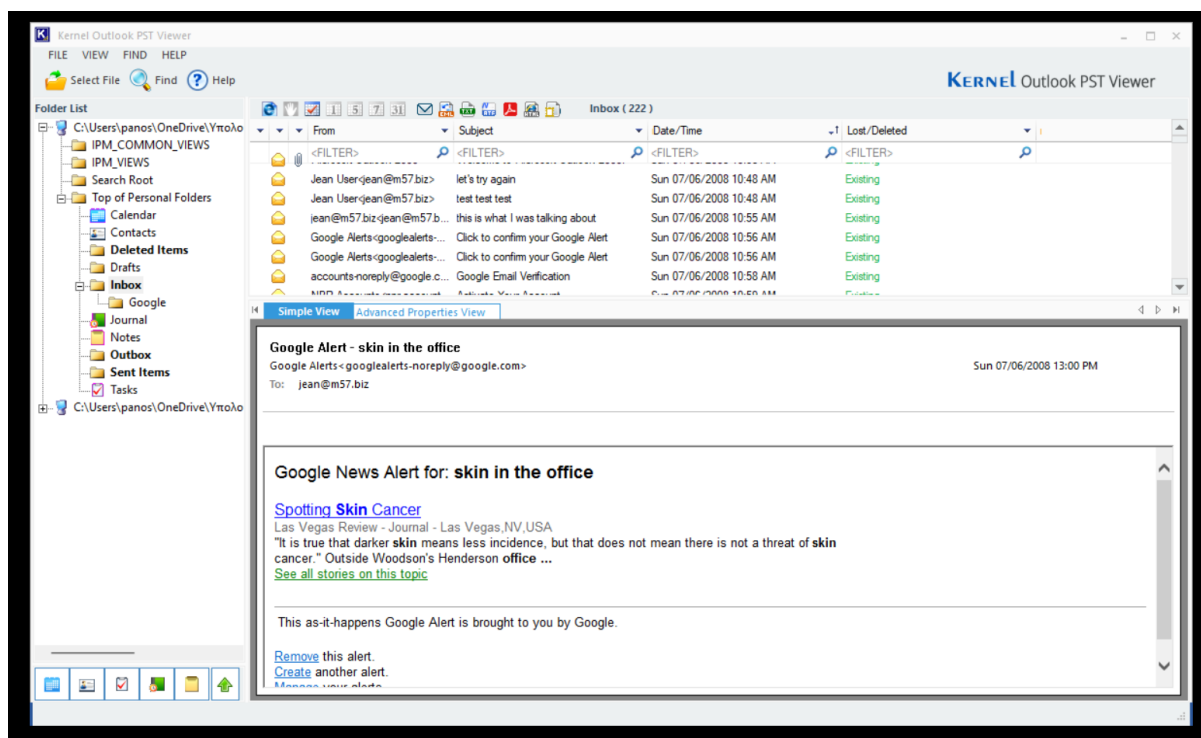
- Encryption Suspected (4)
- EXIF Metadata (86)
- Extension Mismatch Detected (46)
- Keyword Hits (1207)
- User Content Suspected (86)
- Web Categories (6)
- OS Accounts
- Tags
- Reports

Μετά από ανάλυση του δίσκου, γνωρίζουμε ότι η Jean χρησιμοποιούσε το Microsoft Outlook Express ως πρόγραμμα για το ηλεκτρονικό ταχυδρομείο της. Γνωρίζουμε ότι το Outlook Express αποθηκεύει τις λεπτομέρειες των email στον τοπικό δίσκο με τη μορφή Personal Storage Table (PST). Αυτό το αρχείο PST το εντοπίσαμε στο μονοπάτι:

/img\_nps-2008-jean.E01/vol\_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst

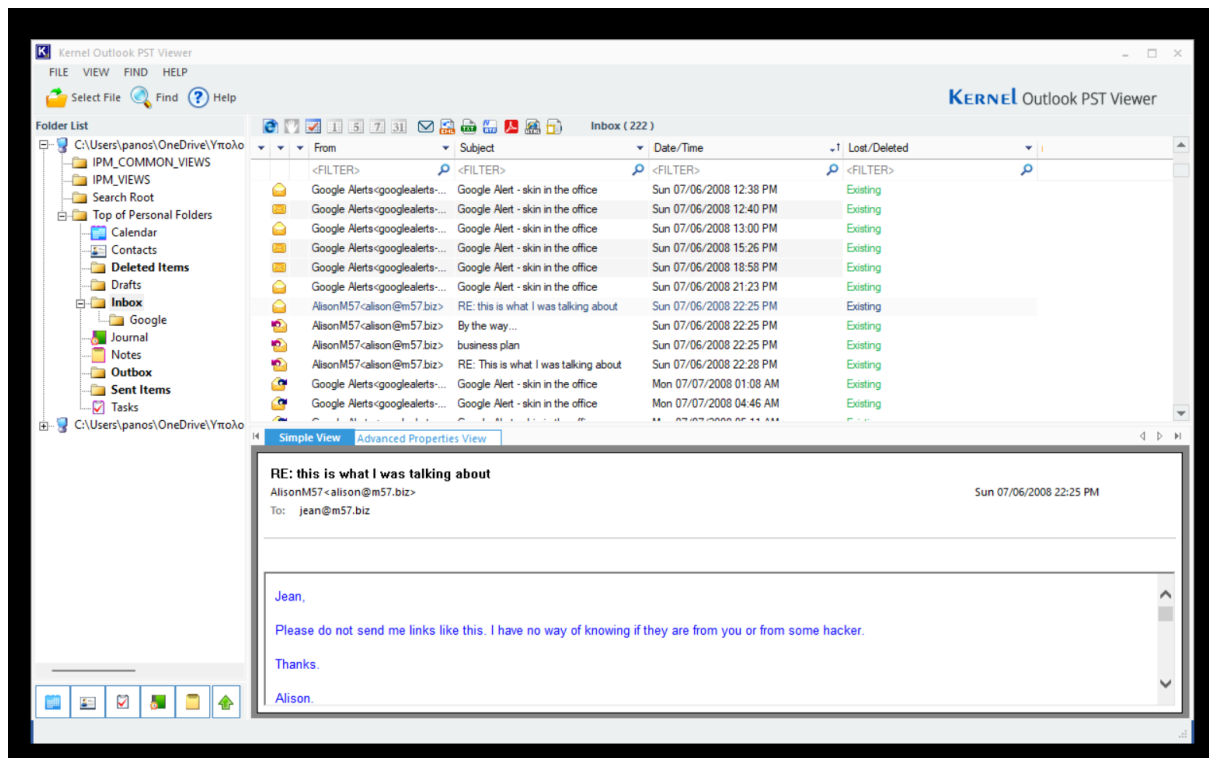


Δημιουργούμε ένα αντίγραφο αυτού του αρχείου PST για περαιτέρω ανάλυση κάνοντάς το εχροτί στον προορισμό που επιθυμούμε. Μετά από μια γρήγορη ματιά στα «Απεσταλμένα», μπορούμε να διαπιστώσουμε ότι το εν λόγω ευαίσθητο έγγραφο επισυνάπτεται ως μέρος ενός μηνύματος ηλεκτρονικού ταχυδρομείου. Εάν αυτό το αρχείο PST περιείχε μερικά μηνύματα, τότε αυτή η μέθοδος αναζήτησης μέσω των email για αποδεικτικά στοιχεία θα ήταν αρκετή. Ωστόσο, στην περίπτωση μας, το αρχείο PST περιέχει αρκετά email και είναι καλύτερο να χρησιμοποιήσουμε ένα εργαλείο στο οποίο μπορείς να διαχειριστείς ευκολότερα τα email, με αποτέλεσμα να διευκολύνει την ταχύτερη ανάλυση. Υπάρχουν πολλά διαθέσιμα εργαλεία που επιτρέπουν την προβολή των περιεχομένων των αρχείων PST στα Windows. Αποφάσισα να χρησιμοποιήσω το Kernel Outlook PST Viewer, το οποίο διαθέτει GUI και μπορεί να φορτώσει τα μηνύματα ακριβώς όπως θα τα βλέπαμε στο Outlook και έχει επίσης και την επιλογή ανάκτησης διαγραμμένων email.

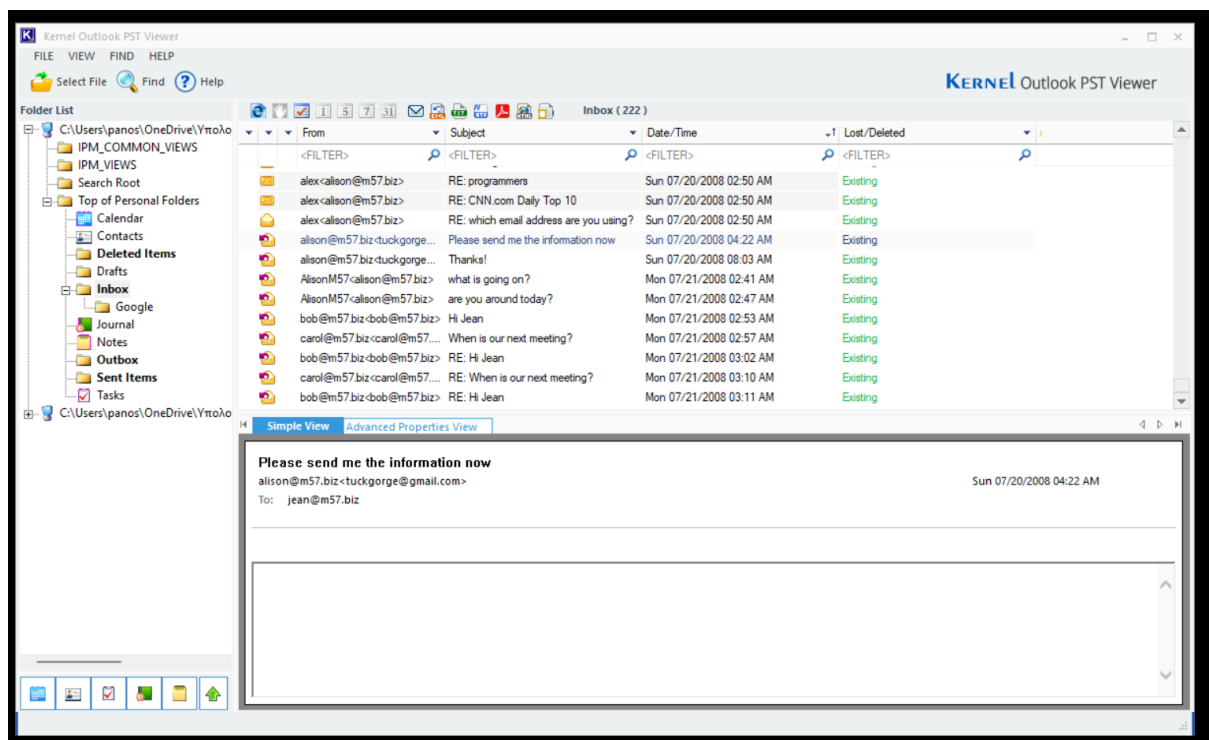


Τα πρώτα μηνύματα είναι από τον Jean που δοκιμάζει ότι το email της έχει ρυθμιστεί σωστά. Στη συνέχεια, υπάρχουν πολλά μηνύματα «Google Alert» που δεν σχετίζονται με την υπόθεση. Η πρόεδρος, Alison Smith, είχε βάλει στο email της στο όνομα «Alison57», όπως φαίνεται από τα μηνύματα που έλαβε από αυτήν στις 06/07/2008. Επίσης, στη συνέχεια, στις 21/07/2008, τα email που ελήφθησαν από την πραγματική Alison υποδηλώνουν επίσης ότι το email της έχει διαμορφωθεί στο όνομα 'Alison57'. Έτσι, η πρώτη μας διαίσθηση είναι ότι όλα τα άλλα email που έχουν τα ονόματα του "Alex" ή του "alison@m57.biz" είναι αυτά που στέλνει ο επιτιθέμενος προσποιούμενος την Alison.

Να σημειωθεί επίσης ότι δεν είναι δύσκολο για έναν εισβολέα να αποκτήσει το όνομα του email της Alison. Ωστόσο, ο επιτιθέμενος δεν μπήκε σε αυτόν τον κόπο και απλώς χρησιμοποίησε το όνομα "Alex" και πλαστοποίησε τη "διεύθυνση αποστολέα" στην πραγματική διεύθυνση email της Alison. Είναι πιθανό να σκέφτηκε ότι η «διεύθυνση αποστολέα» του alison@m57.biz θα ήταν αρκετή για να ψαρέψει την Jean, κάτι που όντως συνέβη. Επιπλέον, στις 06/07/2008, η Alison ζήτησε από τη Jean να μην της προωθεί συνδέσμους ανεπιθύμητης αλληλογραφίας καθώς δεν θα μπορούσε να καταλάβει αν τα email αυτά ήταν από την Jean ή από κάποιον χάκερ, οπότε καταλαβαίνουμε ότι τα email στις 20/07/2008 στάλθηκαν από τον επιτιθέμενο, αφού περιέχουν περιεχόμενο το οποίο είχε ζητήσει η Alison να μην της στέλνει η Jean.



Τέλος, παρατηρούμε αμέσως ότι 2 από αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου έχουν το "Return-Path" αλλαγμένο σε "tuckgorge@gmail.com", ώστε το έγγραφο να πάει κατευθείαν στον επιτιθέμενο.



### Ανάλυση Μεταδεδομένων (metadata) του Εγγράφου

Το έγγραφο είναι ένα φύλλο Excel που περιέχει εμπιστευτικά στοιχεία εργαζομένων όπως SSN, μισθοί και τμήματα.

ΕΙΔΟΠΟΙΗΣΗ Οι περισσότερες δυνατότητες είναι απενεργοποιημένες, επειδή το προϊόν του Office είναι ανενε					
A	B	C	D	E	F
M57.biz company					
Name		Position	Salary	SSN (for background check)	
Alison	Smith	President	\$140.000	103-44-3134	
Jean	Jones	CFO	\$120.000	432-34-6432	
Programmers:					
Bob	Blackman	Apps 1	90.000	493-46-3329	
Carol	Canfred	Apps 2	110.000	894-33-4560	
Dave	Daubert	Q&A	67.000	331-95-1020	
Emmy	Arlington	Entry Level	57.000	404-98-4079	
Marketing					
Gina	Tangers	Creative 1	80.000	980-97-3311	
Harris	Jenkins	G & C	105.000	887-33-5532	
BizDev					
Indy	Counterching	Outreach	240.000	123-45-6789	
Annual Salaries			\$1.009.000		
Benefits		30%	\$302.700		
Total Salaries + Benefits			\$1.311.700		
Monthly burn			#####		

Υπάρχουν διάφοροι τρόποι ανάλυσης των μεταδεδομένων (metadata) που είναι αποθηκευμένα σε αυτό το έγγραφο. Ο ευκολότερος τρόπος είναι να ανοίξουμε το έγγραφο στο MS Excel και να δούμε τις «Πληροφορίες».

Όπως είναι προφανές, το έγγραφο δημιουργήθηκε από την πρόεδρο, Alison Smith, στις 06/12/2008 στις 6:13 μ.μ. Το έγγραφο τροποποιήθηκε τελευταία φορά από την Jean στις 20/07/2008, την ημέρα της επίθεσης, στις 04:28 π.μ.

## Πληροφορίες

m57biz

OneDrive - Προσωπικό » Υπολογιστής » Digital Forensics Project

Κοινή χρήση

Αντιγραφή διαδρομής

Αντιγραφή τοπικής διαδρομής

Άνοιγμα θέσης αρχείου

Διαχείριση βιβλίου εργασίας

Διαχείριση βιβλίου εργασίας  
Υπάρχουν μη αποθηκευμένες αλλαγές.

Επιλογές προβολής του προγράμματος περιήγησης

Επιλογές προβολής του προγράμματος περιήγησης  
Επιλέξτε τα στοιχεία του βιβλίου εργασίας που θα είναι ορατά στους χρήστες όταν προβάλλεται στο Web.

Ιδιότητες

Μέγεθος285 KB

ΤίτλοςΠροσθήκη τίτλου

ΕτικέτεςΠροσθήκη ετικέτας

ΚατηγορίεςΠροσθήκη κατηγο...

Σχετικές ημερομηνίες

Τελευταία τροποποίηση20/7/2008 4:28 πμ

Δημιουργία12/6/2008 6:13 μμ

Τελευταία εκτύπωση

Σχετικά άτομα

Συντάκτης

Alison Smith  
Προσθήκη συντάκτη

Τελευταία τροποποίηση από

Jean User

Σχετικά έγγραφα

Άνοιγμα θέσης αρχείου

Εμφάνιση όλων των ιδιοτήτων

### Χρονοδιάγραμμα σημαντικών γεγονότων που σχετίζονται με τη διαρροή

Με βάση την ανάλυσή μας, μπορούμε τώρα να δημιουργήσουμε ένα χρονοδιάγραμμα σημαντικών γεγονότων που θα βοηθούσε στην κατανόηση του τρόπου με τον οποίο διέρρευσαν οι πληροφορίες.

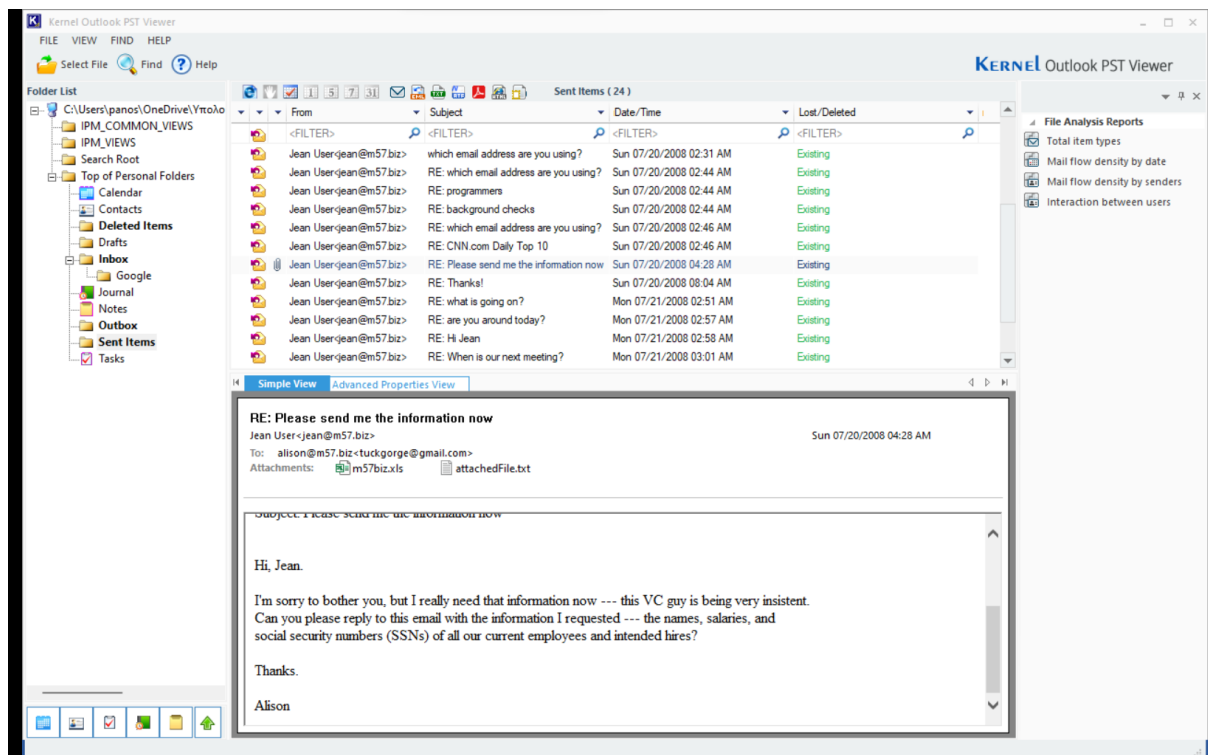
Ημερομηνία	Ώρα	Συμβάν
07/06/2008	22:25 μμ	Ο Jean έλαβε email από την Alison με το όνομα "Alison57".
07/20/2008	02:32 πμ	Ο επιτιθέμενος στέλνει το πρώτο email προσποιούμενος ότι είναι η Alison και ρωτά για "οικονομικά σχέδια", πιθανώς για να αποδείξει ψεύτικη ταυτότητα.
07/20/2008	02:32 πμ	Ο επιτιθέμενος στέλνει 4 συνεχόμενα email, πιθανώς για να αποσπάσει την προσοχή της Jean.



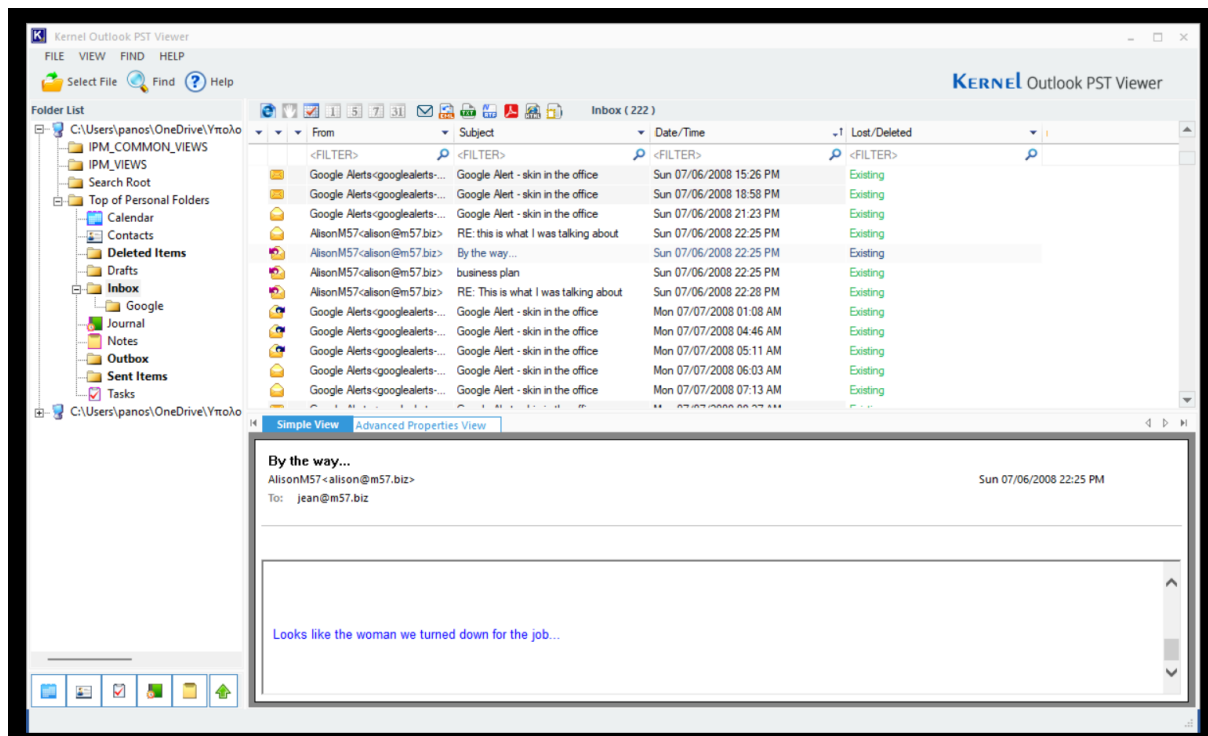
07/20/2008	02:33 πμ	Η Jean μπερδεμένη στέλνει email ρωτώντας για το email που χρησιμοποιεί η Alison.
07/20/2008	02:39 πμ	Ο επιτιθέμενος ζητά το έγγραφο σε ένα email με θέμα "background check".
07/20/2008	02:44 πμ	Η Jean επιβεβαιώνει ότι θα στείλει τις πληροφορίες που της ζητήθηκαν και απαντά με «Σίγουρα».
07/20/2008	04:22 πμ	Ο επιτιθέμενος ζητά ξανά το έγγραφο με τις πληροφορίες δείχνοντας επιμονή. Επίσης, η διαδρομή επιστροφής (return path) τροποποιήθηκε σε "tuckgorge@gmail.com".
07/20/2008	04:28 πμ	Η Jean τροποποιεί το έγγραφο XLS.
07/20/2008	04:28 πμ	Η Jean στέλνει το αρχείο XLS στον "tuckgorge@gmail.com".
07/20/2008	08:03 πμ	Ο επιτιθέμενος στέλνει ένα email για να ευχαριστήσει την Jean για την αποστολή των πληροφοριών.
07/21/2008	02:51 πμ	Η αληθινή Alison στέλνει ένα email στη Jean ρωτώντας τι κάνει.
07/21/2008	02:57 πμ	Η Alison στέλνει email στην Jean λέγοντάς της "κάτι περίεργο συμβαίνει".

### Ανάλυση αιτίας διαρροής (exfiltration) του εγγράφου

Πώς λοιπόν το αρχείο κατέληξε στον ιστότοπο του ανταγωνιστή; Κατά πάσα πιθανότητα, ο εισβολέας έλαβε το email ID της Alison Smith από τον ιστότοπο του M57 και το χρησιμοποίησε για να στείλει ένα πλαστό email στην Jean ζητώντας τις εμπιστευτικές πληροφορίες.



Η Jean έπεσε στην παγίδα και τροποποίησε ένα έγγραφο XLS σύμφωνα με τις πληροφορίες που ζήτησε ο εισβολέας. Στα δύο τελευταία email προς την Jean, ο επιτιθέμενος τροποποίησε τη διαδρομή "Reply-To" για να λάβει την απάντηση της Jean στη διεύθυνσή του στο Gmail που ήταν tuckgorg@gmail.com. Αφού η Jean έστειλε το ευαίσθητο έγγραφο σε αυτή τη διεύθυνση, ο εισβολέας το δημοσιοποίησε επισυνάπτοντάς το στην ενότητα «σχόλια» του ιστότοπου ενός ανταγωνιστή. Ο επιτιθέμενος θα μπορούσε να είναι ένας δυσαρεστημένος πρώην υπάλληλος ή ένας υποψήφιος για θέση εργασίας που απορρίφθηκε από το M57. Σε ένα email στις 06/07/2008, η Alison αναφέρεται σε μια γυναίκα με τατουάζ την οποία η M57 απέρριψε για δουλειά.



Έχει κίνητρο να βλάψει την M57, αλλά χρειάζεται περαιτέρω έρευνα πριν μπορέσει να ειπωθεί οτιδήποτε για την ταυτότητα του δράστη.

### Συμπέρασμα

Αυτή η υπόθεση μας δίνει να καταλάβουμε τη σοβαρότητα της εκπαίδευσης σε θέματα ασφάλειας και της ευαισθητοποίησης των εργαζομένων σε μια εταιρεία. Δεν είναι σαφές εάν η M57 έλαβε μέτρα για την εκπαίδευση των εργαζομένων σχετικά με τις επιθέσεις phishing και τις πρακτικές ασφαλείας γενικότερα. Για κάποιον εκπαιδευμένο, υπήρχαν αρκετές ενδείξεις κατά τη διάρκεια της επίθεσης phishing που υποδηλώνουν κακόβουλες ενέργειες. Ωστόσο, η Jean τις παρέβλεψε απλώς και μόνο επειδή το email φαινόταν να έχει σταλεί από τη διεύθυνση email της Alison. Η επίθεση δεν ήταν πολύπλοκη και η διαρροή θα μπορούσε εύκολα να αποφευχθεί. Δεδομένου ότι ένας συγκεκριμένος υπάλληλος στοχοποιήθηκε σε αυτήν την περίπτωση, μπορούμε να πούμε ότι έχουμε spear phishing attack. Επίσης, καθώς ο οικονομικός διευθυντής (CFO) είναι ανώτερη θέση σε μια εταιρεία, μπορούμε επίσης να ονομάσουμε την επίθεση whaling.

### **Chain of custody**

17/07/2023 – Κατέβασμα αντίγραφου του δίσκου nrs-2008-jean.E01.

18/07/2023 – Άνοιγμα υπόθεσης στο Autopsy και φόρτωμα δίσκου για ανάλυση.

18/07/2023 – Πρόσβαση στα email της Jean

20/07/2023 – Αρχικά συμπεράσματα της ανάλυσης

24/07/2023 – Δημιουργία αναφοράς

31/07/2023 – Κλείσιμο υπόθεσης

### **Σχόλια από την χρήση των εργαλείων που δημιουργήθηκαν κατά την υλοποίηση της άσκησης:**

Autopsy:

- 1) Δεν κάνει disk imaging
- 2) Έχει πολλά modules, plugins (keyword search, web artifacts, email messages) που βοηθούν στην ανάλυση του δίσκου
- 3) Εύκολο στη χρήση UI
- 4) Αργεί να φορτώσει την ανάλυση των αρχείων του δίσκου (ingest modules), κολλάει σε κάποιο ποσοστό, με αποτέλεσμα να μην κάνει verify τον δίσκο

FTK imager:

- 1) Κάνει disk imaging
- 2) Εύκολο στη χρήση UI
- 3) Κάνει εύκολα verify το disk image υπολογίζοντας τα MD5 hashes
- 4) Λιγοστά plugins και modules για την ανάλυση του δίσκου

**Συμπέρασμα:** Κάθε εργαλείο έχει τα θετικά και τα αρνητικά του και θα χρησιμοποιούσαμε το καθένα ανάλογα με το τι μας ζητείται. Αν θέλουμε απλά να κάνουμε disk imaging και verify τον σκληρό, το FTK Imager είναι μια πολύ καλή επιλογή. Από την άλλη πλευρά αν μας απασχολεί περισσότερο η ανάλυση του δίσκου σε βάθος θα πηγαίναμε σίγουρα με το Autopsy για την πληθώρα των επιλογών που διαθέτει. Ίσως ο συνδυασμός τους να αποτελεί την καλύτερη πρακτική σε μια έρευνα digital forensics.

### **Βιβλιογραφία:**

1. [Best practices for writing a digital forensics report | Paliscope.com](#)
2. [Digital Forensic report- sample - With File HTML\\_redacted \(fliphtml5.com\)](#)
3. [Write a Forensic Report Step by Step \[Examples Inside\] \(salvationdata.com\)](#)
1. [2009 M57-Jean – Digital Corpora](#)