Cyber Forensics Investigations

מרכז גרינברג, עמנואלית
20-02-2020
בית המשפט השלום
נתניה

הנדון: חוות דעת מומחה מתוקצבת- סייבר וראיות פורנזיות
תיק מח"ש מדינת ישראל נ' רמי מלכה/

1. שם המומחה: עו"ד דריר בוזגלו.

השכלה:

Microsoft Certified Professional (MCP) Certification – 2000

Microsoft Certified Solutions Expert (MCSE) Certification - 2002

Mobile Forensics Professional UFED Operations Certificate 2009

2005 – טכנאי PC ורשתות תקשורת, NESS.

2011 – EnCase Computer Forensics I.

2012 - EnCase Computer Forensics II.

2012 – לימודי משפטים תואר ראשון.

2014 – VMware workstation, IITC Interbit.

2017 - CSI - Cyber Security Intelligence, OMEGA.

2018 סייבר Network, JOHN BRYCE.

2. הסמכות:

קורס חקירות (משטרה).

קורס חיקור מחשבים מיומן (משטרה).

קורס מצלמות דיגיטאליות, JOHN BRYCE

שחזור ראיות דיגיטאליות IEF, EnCase, Axiom

3. ניסיון מקצועי בתחום חקירות במרחב הסייבר:

שירתתי במשטרת ישראל 28 שנים במגוון תפקידי שיטור. כ- 15 חשנים האחרונות, ביחידת חקירות סייבר של מחוז תל אביב. במרלך השירות לוויתי וניהלתי חקירות מסועפות, חלקי בארץ וחלקן חוצות גבולות. ערכתי חקירות טכנולוגיות לאיסוף ראיות דיגיטאליות, פורנזיות וחקירות פרונטאליות, הן במרחב האינטרנטי והן בחומרי מחשב, טלפונים, דיסקי זיכרון, מחשבים ושרתים.

כל הזכויות יהוצרים למסמך זה שייכות לדרור בוזגלו. חרייד ממסר לשימושו הבלעדי של רמי מלכה.
אין לפרסם, להעתיק, לרשרכ, לשכפל, ו/או לצטט חלקים מהמסמך ראי את המסמך במלואו ללא קבלת אישור מראש ובכתב.
מייל 050-5072717 , Email: drorbu76@gmail.com

אני מחתום מטה מבקשתי עיי רמי מלכה להוות דעתי המקצועית לעניין שבנדון. אני נותן חוות דעת זו במקום עדות בבית המשפט ומצהיר כי ידוע לי היטב, שלעניין הוראות החוק הפלילי בדבר עדות שקר בשבועה בבית חמשפט, דין חוות דעתי זו כשחיא חתומה על ידי כדין עדות בשבועה שנתתי בבית המשפט.

4. <u>המקורות לכתיבת חוות הדעת:</u>

4.1. דוחות בדיקה חומר מחשב ופלטים שהופק.

4.2. מסמכים מודפסים שמסרה המתלוננת.

4.3. עדויות, חקירות

4.4. פרוטוקולים דיוני בית המשפט.

4.5. כתב האישום כנגד הנאשם.

3. <u>נתבקשתי לחוות דעתי בסוגיות הבאות:</u>

5.1. מאיפה / מאיזה טלפון נשלחו הודעות ה – SMS?

5.2. האם בוצעה עריכה של ההודעות ה - WhatsApp שנמסרו למשטרה , לרבות מחיקה, שינוי או חוספה?

5.3. מה יכול היה מומחה מצדו של הנאשם לדעת , לו הייתה ניתנת לו הזדמנות לבדיק את המכשיר הנייד של המתלוננת?

5.4. ההודעות ה - WhatsApp שנמסרו למחיש מהמכשיר שמעולם לא היה בידי המשטרה. מה המשמעות של זה?

<u>להלן חוות הדעת:</u>

<u>הקדמה</u>

חוות הדעת התמקדה בשני מישורים עיקריים. האחד בדיקת הנייד של המתלוננת, השני הודעות ה - WhatsApp. איסוף ראיות דיגיטאליות מחייבת שימוש בכלים פורנזיים באופן מקצועי, וזאת על מנת לשמור על שכבות (METADATA) של הראיה בזמן האיסוף והחקירה, ולשמור על מקוריותה ואמינותה של הראיה שיבור הראיה במצב המקורי ותאפשר ביצוע בדיקות חוזרות, הן על ידי היחידה החוקרת והן על ידי הנאשם, באמצעות מומחים מטעמו הגשת ראיה מודפסת בלבד שמסרה המתלוננת מגיבוי שנעשה על ידה שוללת את האפשרות לבדוק את מקוריותה ו/או את אמינות תוכנה.

כל הזכויות היוצרים למסמך זה שייכות לדרור בוזגלו. חוויו נמסרו לשימושו בלעדי של רמי מלכה
אין לפרסם, להציג, להעתיק, לשכפל, ואו לבצע כלשהם מהמסמך ואו את המסמך בכוליאו ללא קבלת אישור מראש ובכתב.
נייד: 050-5072717 , E-mail drorbuza@gmail.com

Cyber Forensics Investigations

6. <u>בדיקת המכשיר הסלולארי על ידי החוקרת</u>

הסלולארי של המתלוננת נפרק באמצעות מכשיר UFed והופק דוח המתאר את פרטי המכשיר ופרטי הבדיקה. בנוסף, דוח שערך החוקר, "דוח חדירה לחימר מחשב – בדיקת טלפון נייד", מתאר את פרטי המכשיר, סוג הפריקה ופרטים נוספים. בבדיקה של הדוחות הנ"ל עולים הדברים הבאים:

6.1. <u>מספר ז'ברזל IMEI</u> : המספר זיהוי של מכשיר הסלולארי שמסרה המתלוננת לא שלה בדוחות הפריקה של UFED. החוקר רשם בדוחות חתפיסה וחחדירה לחומר המחשב, את המספר הטירוני של המכשיר ולא את מספר הברזל, IMEI . לא ניתן לקשר בין המספר הסידורי שרשם החוקר לבין מספר הברזל, IMEI – 355236030922620 של המכשיר הסלילארי שנבדק כפי שעולה בדוח הפריקה

Phone Examination Report Properties

Selected Manufacturer:	Samsung GSM	
Selected Model:	GT-I9500 Galaxy S4	
Detected Manufacturer:	GT-I9500	
Detected Model:	GT-I9500	
Revision:	4.2.2 I9505XXUEMK6 sing mod 13921B8844	
IMEI:	355236030922620	**מספר ברזל**
ICCID:	8997250003003177477f	
MSISDN:	4250903003177477	
Extraction start date/time:	24/07/14 10:56:04	**משך זמן בפריקה**
Extraction end date/time:	24/07/14 10:57:50	
Phone Date/Time:	18/12/12 02:03:48 (GMT+2)	**שעון המכשיר בזמן הבדיקה**
Connection Type:	USB Cable	
UFED Version:	Software: 3.0.7.33 UFED , Full Image: 2.13.025 , Tiny Image: N/A	
UFED S/N:	6918780	

6.2. <u>בוצעה פריקה לוגית וקא פיזית</u> : משך הפריקה הקצר, כשתי דקות לערך, מעיד על פריקה לוגית ולא פיזית. פריקה לוגית היא פריקה חלקית של תכולת המכשיר המבדק, לעומת פריקה פיזית בה ניתן לקבל את מלוא התוכן האגור במכשיר, כגון : נתונים מחוקים, הודעות מחוקות, שכבות (METADATA) ועוד.

6.3. <u>תאריך ושעה</u> : במכשיר הסלולארי של המתלוננת שנבדק, התאריך והשעה נמצאו בהפרש של למעלה משנתיים לאחור, דבר שיכול להשפיע על ציר הזמן ותיעוד של הפעולות שבוצעו במכשיר, כגון - זמני קבלה והוצאה של שיחות, זמן של קבלה ושליחת הודעות - SMS , WhatsApp ועוד.

כל הזכויות היוצרים למסמך זה שייכות לדרור בוגלה. חל איסור מוחלט לשימוש בלעדי של רינה טלנה
אין לפרסם, לרצוץ, להעתיק, לשכפל, לראו לצטט חלקים מהמסמך ראו את המסמך במלואו ללא קבלת אישור מראש ובכתב.
נייד : 050-5073717 , Email drorbuz6@gmail.com

Cyber Forensics Investigations

6.4. כפי שעולה מטבלה זו, לא נוצעה הפקה של מלוא הנתונים של המכשיר הנבדק, וניתן לראות שבוצעה בחירה סלקטיבית של הנתונים, וזאת לאור דרישת צוות החקירה, כפי שעולה מדוח הבדיקה שערך החוקר.

Phone Examination Report Index

Contacts (207)	Selected
SMS - Text Messages (289)	Selected
Calepcar/Notes/Tasks	Not Selectec
Cell Logs	Not Selectec
MMS - Multimedia Messages (3)	Selected
Email Messages	Not Supported
Instant Messages	Not Supported
Images	Not Selected
Ringtones	Not Selected
Audio	Not Selected
Video	Not Selected
Database	Not Selected

7. חוזעות WhatsApp

7.1. המתלוננת מסרה בעדותה מסמכים מודפסים ובדס ההודעות ה - WhatsApp שלדבריה הם ביזה לבין הנאשם. המתלוננת היא זו שביצעה את יצוא ההודעות למייל שברשותה, ולאחר מכן הדפיסה ומסרה לחוקרת.

7.2. בתהלך יצוא / גיבוי של הצ'אט מאפליקציית WhatsApp למייל נשלח קובץ TXT המכיל את התכתבויות, ואת המדיה במידה ונבחר.

7.3. קובץ TXT הינו קובץ גולמי הניתן בקלות, וללא כל מיומנות לבצוע עריכה, מחיקה, הוספה ושינוי של התכתובות. לא ניתן לדעת באופן סביר האם ההודעות שמסרה המתלוננת למחייש אכן משקפות את מה שנשלח או לא נשלח, מתנאשם למתלוננת או ההפך.

7.4. לא ניתן לקבוע באופן חד ערכי את מספר השילוח ו/או המקבל, לא ניתן לראות באיזה תאריך נשלחו ההודעות WhatsApp המודפסות שמסרה המתלוננת.

7.5. בהעדר קובץ יצוא הצ'אט TXT, ששלחה המתלוננת למייל, לא ניתן לבדוק את שכבות (METADATA) הקובץ ולקבל נתונים כגון : זמן יצירה, זמן שליחה ואם לא בוצעה עריכה של התכתובות

כל הזכויות הלוצרים למסמך זה שייכות לדרור בוגלה. רוזיה נמסר לעיעשוי הפעלדי ול רמי מלכה.
אין לפרסם, להעתיק, לשכפל, ולאי לצטט חלקים מהמסמך ולאו את חמסמך במלואו ללא הודעת אחשי. בכתב
Email: drorbug6@gmail.com , 050-5072717 - נייד

Cyber Forensics Investigations

8. <u>מסקנות</u>:

8.1. פריקה לוגית ולא פיזית, של המכשיר שמסרה המתלוננת, נספח 2

8.2 לא היה מקום להחזיר למתלוננת את המכשיר הסלולארי משלא עלה בידי החוקר לבצע תיעוד מלא או לכל היותר טאמן למקור, וזה מקום להשאיר את תנייד ברשות היחידה החוקרת, עד שימצא פתרון טכנולוגי לפריקה פורנזית של המכשיר. חחזרת המכשיר למתלוננת והצדר העונה מלא ונאמן למקור, מגעה מהנאשם לבצע בדיקה פורנזית עצמאית

8.3. הודעות SMS- מאחר ולא בוצעה פריקה פיזית של המכשיר הסלולארי, לא ניתי לראות באם היו הודעות SMS מחוקות במכשיר. לא ניתי לבדוק האם בוצע שינוי אי עריכה של הודעות SMS באופן מקומי במכשיר, וזאת בטרם נמסר למחייש.

8.4. הפרשי זמנים, לא ניתן משקל להפרשי הזמנים במכשיר הנבדק.

8.5. שרשרת ראייתית, מספר הברזל IMEI של המכשיר הנבדק לא נרשם בדות התפיסת, ולא בדות לבדיקה. למתלוננת היו שני טלפונים ניידים, ישן וחדש, יחעדר תיעוד של מספר ברזל IMEI על ידי החוקר ביום תפיסת המכשיר, הקשר על ההסנה מאיות טלפון הגיעו הודעות SMS ומאיות טלפון תגיעו הודעות ה-WhatsApp .

8.6. לא ביצעו ניסיונות נוספים לבדיקת הסלולארי של המתלוננת. בדוח יחדירה לחימר מחשב – בדיקת טלפון נייד", שערך רתוקר, נרשמה הערת על ידו, יבה צויין שנעשו ניסיונות לבדיקת תכתובות WhatsApp לבדיקה פיזית, אך לא היה ניתי לבצע. החוקר לא פרט מחם הניסיונות שביצע, באם פנה ליחידות מקבילות לקבלת סיוע או לתמיכה של חברת Cellebrite , שידוע כי ברשרה ישנה תמיכה בישראל ביעברית.

8.7. אציין כי בזמן הפריקה של המכשיר הסלולארי של המתלוננת, הייתה קיימת היאפשרות הטכנולוגית לבצע פריסה פיזית של המכשיר וזה עילה ממסמכים שונים שפרסמה חברת נספח 3

8.8. היה מקום לנסות דרכים אחרות לפריקה של המכשיר הסלולארי של המתלוננת כגון: גיבוי מהענן, Web WhatsApp והעברת של חשבון WhatsApp למכשיר אחר.

8.9. בדיקה חזותית, לא בוצעה בדיקה בנייד שמסרה המתלוננת, באם מותקנת אפליקציית WhatsApp ואם אכן ישנן התכתובות בין הנאשם למתלוננת.

8.10. טלפון נייד נוסף, היה מקום לבקש מהמתלוננת את המכשיר הנייד הנוסף לפריקה ולא בדרך שנעשתה על ידיה.

8.11. טלפון נייד של הנאשם, באף אחת מחקירותיו של הנאשם, לא נתבקש למסור את הנייד שלו לבדיקה.

8.12. קובץ TXT , לא תועד הקובץ ששלחה המתלוננת לתיבת הדואר שלה. על מנת לבדוק שלא בוצעה עריכת.

דרור בוזגלו עו"ד
023713328

כל הזכויות היוצרים למסמך זה שייכות לדרור בוזגלו. חוייד נמסר לשימושו הבלעדי של רמי טלכה
אין להפיצו, לשכפל, לשנות, לשכפל ו/או לצטט חלקים מהמסמך ו/או את המסמך במלואו ללא קבלת אישור מראש ובכתב

נייד . 050-5072717 ; Email-drorbuzs@gmail.com

מועד ההגשה: **11:16 16/02/2020**
מספר תיק: **26185-11-14**
סוג בקשה: **מתן החלטה**
מספר אסמכתא למעקב: **1069056**

על המגיש לשמור את מספר האסמכתא לשם קבלת מידע אודותיו
המסמך הועבר לבדיקת מזכירות.

• אם יאושר, יתוייק בתיק ותאריך ההגשה התוקי יחושב לפי תאריך ההגשה בפועל ולא לפי תאריך האישור. כמו כן, יופק אישור שיוצג בתקיית תיק בייר.

• אם לא יאושר, תישלח למגיש הודעה על כך. המסמך שנדחה יוצג בתקיית תיק נייר

יונינה בלומנפלד, עו"ד – משרד עורכי דין
Yonina Blumenfeld, Law office
רחוב אלנבי 25 אי חיפה – 3326545 25A, Allenbi St, Haifa
טלי 04-8534240 , 04-8534239 Tel.
פקס. 04-8534150 Fax.
דואר אלקטרוני: shlomi_blumenfeld@yahoo.com E-mail:

יונינה בלומנפלד, עו"ד
שלומי בלומנפלד, עו"ד
רומי חן, עו"ד

Yonina Blumenfeld-Schechter, Adv.
Shlomi Blumenfeld, Adv.
Romi Chen Adv.

Haifa 16.2.26 חיפה,

בתשובה נא לציין
Ref ..... מס'

טופס העברת פקסימיליה

FAX NO :	04 8534150	מס' פקס
from :	שלומי בלומנפלד, עו"ד	מאת :
to:	שרית	אל :
fax to :	02-6761406	מס' פקס :
no. of pages incl this one	2	מס' העמודים המשודרים כולל זה

MESSAGE **ה ו ד ע ה**

הנדון : 26185-11-14

שרית היקרה שלחתי לך

שתעבירי להבאה לדיון

בכבוד רב,
ש. בלומנפלד, עו"ד

Transmission Log

Sunday, 2020-02-16 11:42

Date	Time	Type	Job #	Length	Speed	Fax Name/Number	Pgs	Status
2020-02-16	11:40	SCAN	20982	1:19	14400	Ministry of Justice	8	OK -- V.17 AM31

יעמינה בלומנפלד, עו"ד – מגדף עריכת דין
Yamina Blumenfeld, Law office
רח' אלנבי 25 חיפה – 3326545
St. Alenbi St, Haifa -3326545
טל' 04-8534240 , 04-8534230
Tel. 04-8534240 , 04-8534230
פקס: 8534150-04
Fax.no- 8534150
דואר אלקטרוני: E-mail:
shlomi_blumenfeld@yahoo.com

יעמינה בלומנפלד, עו"ד
שלומי בלומנפלד, עו"ד
רונית חן, עו"ד

Yoana Blumenfeld-Schechter, Adv.
Shlomi Blumenfeld, Adv.
Ronit Chen Adv.

Haifa 16.2.20 חיפה,

בהשיבה נא לציין
Ref .....

לכבוד משרד המשפטים

FAX NO :	02-6284150	מס' פקס
from :	שלומי בלומנפלד, עו"ד	מאת :
to:		אל :
fax to :	02-6284150	מס' פקס :
no. of pages incl this one	8	מס' העמודים המצורפים כולל זה

MESSAGE: הודעה

הנדון: 25185-11-19

שלום רב,

מצ"ב לשימוש מיידי

בכבוד רב,