Final Paper – Forensic Report

Helen Bramow, MA

Cybersecurity Department, Old Dominion University

CYSE 407: Digital Forensics

Prof. Bryan Bechard

April 18, 2024

Table of Contents

(Garrie, 2016)

Introduction:

On 3/20/24 at 12:00 p.m. EST, the prosecution requested CFI Forensic Investigation (Submitter #F300) to search for alleged contact evidence, both emails and sms/texts, between U.S. and Russian officials. The laptop owner refused to comply with questions and answers, was noncompliant with the investigation. However, he did provide passwords for both his cell phone and his laptop devices. CFI's forensic analysis was completed on the contact's laptop and cell phone following standard industry protocols and using standard industry digital forensic tools.

The suspect holds a high ranking US government official job, as a U.S. Senator, and his accomplice works at the Russian Embassy in Washington, D.C. The suspect's name is: Senator John B. Werner. He has access to classified and secret documents, which may have been traded to Red Ralph in exchange for monetary gain, i.e. profits. The investigative search includes the reference to the payment. CFI was hired to find any incriminating evidence on both the Senator's cell phone and his personal laptop, both of which are in custody.

Investigation Tools -

- **ProDiscovery** -
  Limitations - is an open sourced forensic tool, has less resources than others which are not open sourced. On incident response actions it is fast and allows for good baselines as to whether or not the device has been accessed. It is not as comprehensive as paid software like Encase, but still allows for tracking steps along the investigation. One con is there is not any documentation. It is lacking in some tools for analysis and also documentation. (Tullett, 2005)
- **Autopsy** -
  Limitations - another open sourced, digital forensic tool has less resources available than expensive other digital forensic tools, i.e., not open sourced. Compared against Encase or FTK both are expensive tools and are well known in courts for years, and have more resources than Autopsy. Supposedly, digital forensics tools that are more easily accepted in courts and utilized in cases like offer greater acceptance and also there may be less questions for expert witnesses. (Jaclaz, 2014) Another is process time because a large file with multiple ingests could take 24 hours, so running as a single user and only 1 or 2 ingests at once is recommended. (Nika, 2022) It won't work on Linux. (MostafaaSFX) Prior to v. 4.2.1, keyword searches were limited. ("Keyword Search", 2012-2022)
- **Dream Screens USB SIM Card Reader -**
  Limitations - Does not include Smart Card Data Software; does not work on iPhone because their data is not on the SIM.
  SIM Card Reader - reads micro and nano SIMs (multi-media SD TF MMC with adapters) and includes SIM recovery software. It also includes the software for text recover and edits of the SIM card. Also reads Smart Card but lacks the software as noted above; can recover deleted text/sms messages. ("Dreamscreens-Multi-Media-Adapters-Recovery-Software", 1996-2004)

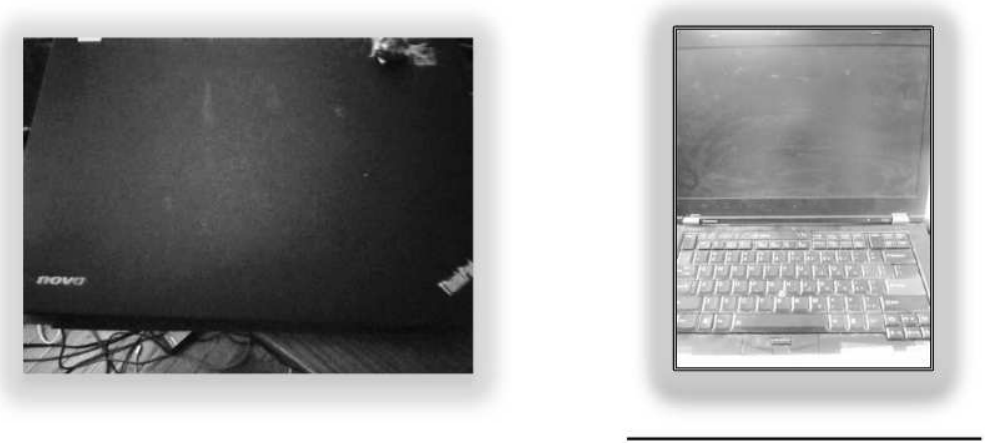
#1 Item Items for Examination: (*incl.: serial number, make and model*)
Cellular Device – Android, LG K20 Plus, network: AT&T, ; color - blue;
model # LG-TP260;
GOTA Serial # LGTP2604d4cg27a;
S/N 708CYRM208722;
OS - Android v. 7;
kernel - 3.18.3.1;
software v. TP26011|;
storage - 14.25 GB used, total - 32.00 GB; available - 17.75

- **Cell phone** – LG K20 front & back images


Figure 1 - LG K20 back


Figure 2 - LG K20 front

#2 Item Items for Examination: (*incl.: serial number, make and model*)
Personal Laptop Computer – Lenovo NB50 Thinkpad, NB-50, 64, 4 GB,
color - black
Intel Core i5-2520M
CPU 2.50 GHz,
77014D66-69F2-33334-96E2-2EE3BDG1F9CA,
type 4178-6UU
Serial #R9-N5KLP,
OS - Windows 7 Pro;
Storage - 123 GB out of 464 GB



Summary of Evidence Found

#1 Item Cell Phone -

- Text(s) confirming meeting on 2/15/2023 at lunch time, with phone number labelled "Red Ralph" in the contact list of contact's cell phone.

Figure 3 - LG K20 Contact List shows Red Ralph

Laptop - noted several email communications about meetings, including emails regarding the payment(s) for "consulting services" between contact and RedRalph@gmail.com.

----------original message----------

To: JW@gmail.com
From: RedRalph@gmail.com
Date: February 25, 2023
Subject: meeting re: consult services
Hello
Thank you again for meeting at lunch on Feb. 25th at the Russian House regarding your consulting services. Payment will be sent to you sometime tomorrow.

----------original message----------
To: RedRalph@gmail.com
From: JW@gmail.com
Date: February 19, 2023
Subject: meeting re: consult services
Hello. Yes that will be fine.
----------original message----------
To: JW@gmail.com
From: RedRalph@gmail.com
Date: February 18, 2023
Subject: RR meeting re: consult services
Hello.
Thank you for our lunch meeting on the 15th at the Russian House regarding your consulting services. We will need to schedule 1 more meeting then I will arrange payment for your services. Can you meet again on Feb. 24th, same time, at lunch time, 12:00 pm at the Russian House restaurant on 1800 Conn. Ave.?

Other Evidence on Laptop –
1. I noted several zip files (deleted) containing classified material; web logs show uploaded to a file sharing site. *Downloads unverified* - it is unclear whether they were downloaded, even though evidence shows they were uploaded.

#1 Item - Cellular Device –

- On 3/20/2024, at exactly 3:00 p.m. EST, I received a search warrant through the U.S. District Courts in Washington, D.C. downtown.
- A file is created, facts regarding the incident are noted, a search warrant is ordered, police attempt to get device passwords. Chain of custody begins to be recorded.
- I acquired: 1 - the search warrant, 2 - the evidence, kept safe and preserved, not comingled, using evidence bags in my kit.

Examination Steps:
1. Identify the devices used, in this case Sen. J. Werner's phone and laptop as noted above.
2. Wear gloves; bag up the evidence and label everything; keep original data/devices in safekeeping and locked; took pictures of the physical devices and scene. Labeled everything w case info, date and time collected, updated 'chain of custody' report, and used my evidence kit w/gloves, labels, etc.
3. Record the exact time, date, and pieces of evidence, as well as the pictures. Imaging - cloned the original data and worked with a copy.
4. The cell phone was on, but locked. Sen. Werner provided his password but no information otherwise. The SIM card was removed and inserted into Dream Screens SIM Card Reader to copy first.

---

5. The android mobile device was examined using Autopsy. First I set up the case in Autopsy which has a program for android. I started Autopsy, and opened a new case file called 'RedRalphRussian.'
6. Using digital forensic software Autopsy, searched for the data as evidence, first on the cell phone, then extract the data from the clone (forensic image), and also copied SIM. I mounted the cloned data. I placed the cell devices in evidence bag, labeled as stated above afterwards, to go to storage locker.
7. After entering the basic case info into Autopsy, I choose the 'ingest' modules. Autopsy has an ingest 'android analyzer' ingest module. The ingest modules I chose were: recent activity, file type identification, embedded file extractor, exit parser, extension mismatch detector, Android analyzer, interesting file identifier, PhotoRec carver and process unallocated space. This is the result:

Figure 4 - Autopsy Step #3 - https://www.digitalforensics.com/blog/articles/android-forensic-analysis-with-autopsy/

8. Search strings used: RedRalph, Red Ralph, Russian, Ralph, Red RedRalph@gmail.com. Searches were entered into a search list and results were saved ('x' box). Data sources can be checked and limited, but don't have to be limited and perhaps it's better if it isn't checked.
9. Search listings were also entered with: Red Ralph, Russian, Ralph, Red, RedRalph, RedRalph@gmail.com, and 202-930-8112 (Red Ralph's phone number at the Russian Embassy).
10. Graphic image search: Using the picture analyzer extracted EXIF data from the ingested images; then the images are a data source. Then they were searched, similar to the above search on files.
11. But there is also a file mismatch detector, and when the cached images are checked, there is one image that has a '0' in place of extension, but is an image file .png. It is clearly mismatched data! It should have an image extension (.jpg, .png, etc.) but it does not because it is really not a pic file but instead a Russian black market website. (Digital Forensics Corp, 2016)
12. Next, I checked for data that was on the phone, but some could have been transferred to the laptop, then deleted on the cell phone. So I searched for any deleted data on the phone too while working on it first.
13. I was looking for SMS/texts and email messages re: meetings, confirmations and payments for services with Red Ralph on the Android device. These did show up and were documented in the above paragraphs.

#1 Item - Cellular Device – Findings and Report

1. Noted on p. 4 - 5 above, evidence of meetings were found and screen shots are above, and confirmation of payment for consulting services to RedRalph@gmail.com from Sen. J. Werner on Sen. Werner's phone. Red Ralph was listed as a contact in Sen. Werner's phone in the contact listing also.
2. In emails, also noted on p. 4 above, there were email confirmations of meetings, and screen shots are also printed above.
3. The phone text or sms app, had a text confirmation of a lunch meeting at The Russian House restaurant, Washington, D.C. on 2/15/2023 sent to Red Ralph at his phone number 202-930-8112. It is clear that Red Ralph's phone number is at the Russian Embassy in Washington, D.C. and the restaurant meeting place for the two was at the Russian House restaurant on Connecticut Ave., N.W. Washington, D.C.

#2 Item - Personal Laptop Device

Examination Steps:

1. Senator's laptop was on when retrieved, and again the Senator supplied his password. Autopsy was used, with a write blocker to avoid changing the data. A copy was made of the device. Senator's laptop was on when retrieved, and again the Senator supplied his password. A copy was made of the device.
2. The extraction allowed me to review the data in the apps. As noted above on p. 5 - 6 there were several emails found on the laptop between RedRalph@gmail.com and the Senator concerning meetings and payment for services.
3. Search strings used: RedRalph, Red Ralph, RedRalph@gmail.com. Searches were entered into a search list and results were saved ('x' box). Data sources can be checked and limited, but don't have to be limited and perhaps it's better if it isn't checked.
4. Search listings were also entered with: Red Ralph, Russian, Ralph, RedRalph, RedRalph@gmail.com, and 202-930-8112 (Red Ralph's phone number at the Russian Embassy).
5. In addition to the emails found stated on p. 5 - 6, there were also some deleted zip files. Although they were uploaded to a website (another Russian black market website) and it was unverified whether they had been downloaded. So, the cycle remains incomplete, yet the upload is the evidence still. The information was classified.

#2 Item - Personal Laptop Device – Findings and Report

Findings and Report –

1. As sated in #5 above, there were both: deleted zip files with classified data found, as well as several meeting confirmation emails found.

Conclusion/Results–

1. There was neither any damage nor manipulation to either of the original devices, nor was either changed at all, in any way. They are still perfectly intact as at the beginning of the investigation.
2. Evidence found includes several emails and text messages indicating there were meetings, services rendered, and a payment made.

Hardware used -

1. Write Blocker
2. SIM card reader w/ USB cable - Dream Screens USB SIM Card Reader

Software used -

1. Autopsy
2. ProDiscover

Evidence -

#1 Item - Cellular Device -

- Evidence was found in the form(s) of the following: sms/text messages confirming meetings and payment between Sen. Werner and Red Ralph.

#2 Item - Personal Laptop Device -

- Evidence was found in the form of several email communications between Sen. Werner and Red Ralph. Again, these emails prove that there were meetings at the Russian House restaurant in Washington, D.C., and reference payment for services also. Evidence from laptop device is detailed on p. 5 - 6. Zip file containing uploaded classified documents also was found loaded to a Russian black market website also. Yet there was no evidence of downloads.

The evidence found on the Senator's personal laptop proves there was/were:

- several meetings together between both Senator John B. Werner and Red Russian at the Russian House restaurant in Washington, D.C.;
- an agreement between the two parties for 'services' provided and a monetary payment (referenced but not traced yet);
- confirmation that there was also a payment;
- an image file with a hidden Russian black market website on it also
- an upload of classified documents to a Russian black market website but no evidence when or if were downloaded.

Final Summary

- It is clear that the two parties met on several occasions, and there was a monetary payment for services, and the classified documents were uploaded to a Russian black market website.

Final Summary (cont'd.)

• The two suspects in this case are: Senator John B. Werner, a U.S. Senator and Red Ralph, who works at the Russian Embassy. Both suspects are located in Washington, D.C.

• It is clear from this evidence found that the suspect, Senator John B. Werner was carrying on meetings with Red Ralph at the Russian House restaurant. However, it is quite possible, but not probable that someone else could have been using both his identity and both of his devices and carried out these transactions.

• It is also clear that the two had an agreement to trade classified or secret government documents that Sen. Werner had access to, thereby making a exchange for a money in return.

• It is clear there was a payment, yet the complete money trail via banking systems has not yet been verified. It is not difficult with the dates and evidence presently to take this extra step.

• It is clear that such documents were in fact uploaded to a Russian black market website, however, it is unclear or unverified still if they were in fact downloaded.

References

"Dreamscreens-Multi-Media-Adapters-Recovery-Software". (1996-2004). Retrieved Apr. 14, 2024, from https://www.amazon.com/: https://www.amazon.com/Dreamscreens-Multi-Media-Adapters-Recovery-Software/dp/B09CFSHTQ3/ref=sr_1_3?dib=eyJ2IjoiMSJ9.Y9ekB-D0gPbzQr7qHYuL4alMYpR-lMx7kvlr70YNzCdG4ptZ0NUxAdMo-hj9tMj6McF_3YP7YcLWCnl1cRaYkIKETCObYnmK710X9ZoYMmwvNMQ9pPgfOLxhEv7f9LKcpcCwNcQ15C

"Keyword Search". (2012-2022). Retrieved Apr. 15, 2024, from https://www.sleuthkit.org/autopsy/docs/: https://www.sleuthkit.org/autopsy/docs/user-docs/4.20.0/ad_hoc_keyword_search_page.html#adhoc_limitations

Digital Forensics Corp. (2016, Apr. 5). *"Android forensic analysis with autopsy."*. Retrieved Apr. 14, 2024, from https://www.digitalforensics.com/blog/: https://www.digitalforensics.com/blog/articles/android-forensic-analysis-with-autopsy/

Garrie, D. (2016, Aug. 15). *"The Neutral Corner: Understanding a Digital Forensics Report"*. Retrieved Apr. 9, 2024, from https://www.thomsonreuters.com/: https://www.thomsonreuters.com/en-us/posts/legal/understanding-digital-forensics-report/

Jaclaz. (2014). *"Autopsy 3 the limitations."*. Retrieved Apr. 14, 2024, from https://www.forensicfocus.com/: https://www.forensicfocus.com/forums/general/autopsy-3-the-limitations/

MostafaaSFX. (n.d.). *"Sleuthkit autopsy issues"*. Retrieved Apr. 14, 2024, from https://github.com/sleuthkit/autopsy/issues?q=: https://github.com/sleuthkit/autopsy/issues?q=

Nika. (2022, Jun.). *"Large ingestion performance"*. Retrieved Apr. 14, 2024, from https://sleuthkit.discourse.group/: https://sleuthkit.discourse.group/t/large-ingestion-performance/3262/3

Tullett, J. (2005, Jul. 21). *"Review: ProDiscover Incident Response"*. Retrieved Apr. 14, 2024, from https://www.itnews.com.au/: https://www.itnews.com.au/feature/review-prodiscover-incident-response-65955