Name: Teh Jia Xuan	Student ID: 32844700
Assignment 2 – IT Forensics 2023 Criminal Case	

Part A

Story 0: Design Question

1) Is the computer used by anyone else?
2) Is there any evidence of drug deals found on Ms Griffith's device?
3) Did you discover any interaction of individual named Jules with Ms Griffith?
4) Have you recovered any deleted files or suspicious conversations in Ms Griffith's device? If so, please provide details of your attempts
5) Did you find any evidence of money transfers from her device to the dark web vendors?

2) Forensically Sound Plan Design Forensic Tools

Preparation

I reviewed all relevant laws related to Ms.Griffth's case and rules for preserving evidences and analysis to be used in a court of law. I obtained the necessary legal authorisations to examine suspect's digital devices. Additionally, I have thoroughly read suspected case details that Ms.Griffth involved and determined chain of custody to handle evidence. Moreover, all forensic toolkits will be prepared according to the case. Lastly, a proper attire is worn.

Acquisition/Preservation

First, secure the scene and power source to prevent contamination of evidence and unauthorised personal access(Wahocho, 2023). Each piece of evidence will maintain chain of custody to track and document when, by whom and how it was collected and the purpose(NIST, n.d.). This ensures evidence's original condition is perfectly documented, which is vital in court of law. Moreover, it helps investigator track which area is investigated and which have not. Besides, write blocker is used to create forensic images of suspect's device to preserve data integrity(threatdotmedia, n.d.). During investigation, images will be hashed to ensure their integrity by confirming it outputs same value as the original(Microsoft, 2023). Furthermore, powered-on machines should be prioritised thus, live investigation will be conducted to examine components like memory, which have volatile data such as passwords and keys that can be lost upon shutdown. Additionally, the investigative process is time-consuming. Hence, the team works on multiple devices simultaneously, and members are assigned specific roles, like documenting and investigating(H-11, 2019). Not to mention, more time and resources will be allocated to high-priority items. Lastly, all images and data should be backup as a safeguard.

Examination/Analysis

Open-source tool

Open-source tools like autopsy are used to create images of relevant data in the evidence (sleuthkit, 2019). A write blocker is also used to prevent altering original data when creating forensic images(NIST, n.d.). Moreover, autopsy and FTKimager are used to analyse files, including recovering deleted files and obtaining metadata that is not accessible through normal file systems(CSS, n.d.). These tools enable me to reveal hidden information and trace back the timeline. Furthermore, autopsy is utilised to track suspect's online activity and use the cookies provided by autopsy to access the suspect's account. Additionally, I use keyword searching feature to search files that contain particular keywords to prevent overlook. Similarly, registry viewer is used to examine Windows registry files, allowing me to obtain critical information such as installed software and event logs, which can provide insights for examination. Besides, exiftool is used to extract metadata of images and video, including GPS coordinates, camera model etc(Harvey, 2023). I utilise this information to know locations of activity related to the drug case. Moreover, PECmd is used to extract metadata of executables from prefetch file(futurelearn, n.d.). This allows me to know when the file is executed and how often, which can identify applications that used to do malicious activities.

Paid tool

Paid FTK toolkits offer comprehensive investigative tool, like timeline analysis, which assists me in tracking user activity, including their online activities and identify any suspicious transactions or conversations(Forensic Focus, 2011). Paid FTK also offers advanced tools like live search, enabling me to query when the data is being analysed(96hz, 2011). This saves enormous time as I don't need to wait for analysis to complete. Moreover, we used Magnet DVR Examiner to analyse and recover CCTV footage for scrutinising suspects to identify suspicious actions(MagnetForensics, n.d.).

Tools

Tool	**Paid/Open-Source**	**Purpose**
FTK Imager	Open-Source	- Create image that is relevant to the case - Recover deleted files - Obtain metadata
PECmd	Open-Source	- Extract metadata from prefetch
Autopsy	Open-Source	- Track suspect activity - cookies for suspect's browsing website - Key searching to find relevant info -
Exiftool	Open-Source	- Extract metadata of image/video
Registry Viewer	Open-Source	- Examine window registry files
Write Blocker	Open-Source	- Preserve integrity when creating image
FTK toolkits	Paid	- Timeline analysis to track user online activity - Live search to query
Magnet DVR Examiner	Paid	- Recover CCTV footage - Analyse footage

Advantages and disadvantages of using free tools and license one

Advantage of licensed tools is they provide comprehensive forensic tools, making investigation process run smoothly and cracking cases effectively. Similarly, licensed ones ensure accurate and reliable results as they need to be used in court of law(ticktechtold, 2023). Additionally, licensed ones often update their tools to fix bugs and align with evolving technology. Disadvantage of licensed tools is expensive, which can be a constraint for small companies(IPL, n.d.). They often have complex features that require a trained employee to utilise(ticktechtold,2023).

Advantage of free tools is budget-friendly, which cuts down costs for companies (Hughes, 2007). Open-source free tools have public their code, hence users can verify the legitimacy and integrity of results(Hughes, 2007). Open-source tools have no license, thus they provide freedom for users to extend functionality. Additionally, open-source tools allow beginners to gain experience without external investment (InvestinTech, n.d.). Limitation of free tools is they might produce false results as they lack validation. Furthermore, free tools are not user-friendly, hence it requires experts to utilise them(CyberWritesTeam, 2021). Likewise, it lacked advanced features like live search, which caused slow progress in investigation. Similarly, free tools are often obtained from unofficial websites and may contain malware in softwares that could contaminate evidence(CyberWritesTeam, 2021).

In conclusion, we can balance utilizing paid and free tools. Free tools can be valuable for tasks like collecting data and file viewing, while paid tools use for tasks that emphasise integrity, like analysis and report. This ensures cost-effectiveness and quality of investigation.

License Tools

Advantage	Disadvantage
Comprehensive forensic tools	Expensive
Solve case effectively	Complex features, require training
Accurate and reliable	
Often updates to fix bugs and align with current technology	

Free Tools

Advantage	Disadvantage
Budget-friendly	Might produce false result
Open source code to Verify legitimacy and integrity of results	Not user friendly, requires expert to utilise
Allow beginners to gain experience without external investment	Lack advance features, causes slow progress
	Comes from unofficial website, It might contain malware in the software

Time Estimation (Assume suspect has 3 devices with 1 TB hard drive)

"*" Approximate Time

Item	Time Estimation (Hour)	Total (Hour)
Initial consultation	1.5 hours * (self estimation)	1.5
Collect data	1TB 3.5-4.5 hours (Computer Evidence Recovery, n.d.) 3.5 + 4.5 = 8 hours/2 = 4 hours* per hard drive	4 hours x 3 = 12 hours
Imaging data	1 TB 3 hours (Computer Evidence Recovery, n.d.)	3 hours x 3 = 9 hours
Analysis data	2-7 Days per hard drive (Computer Evidence Recovery, n.d.) 2+9 /2 = 4.5 days* 4.5 x 24 = 108 hours* per hard drive	108hours x 3 = 324 hours
Laboratory test (depends)	1 month (self estimation) 28 x 24 = 672 hours*	672 hours
Report	70-100 hours (Croft, 2021) 70 + 100 = 170/2 = 85 hours*	85 hours
Total		1,103.5 hours

Cost Estimation (Assume suspect has 3 devices with 1 TB hard drive)

"*" Representing approximate cost

Item	Cost Estimation (USD)	Total (USD)
Initial consultation fee	Fee per hour: $165-$350 Estimation = $165+$350 = $257.5* (Australia Data Recovery, n.d.)	$257.5 x 1.5 = $386.25
FTK toolkits Magnet DVR Examiner Overall Software	Perpetual license: $3,995 Yearly support: $1,119 (SC Media, 2016) License: $12,000 (Erminger, 2021) Software cost : $2,500 (self estimation)	$2,500
Daily rate	Daily rate: $2,100 (Elvidence, n.d.)	$2,100 x (1,103.5 / 24) = $ 96,556.25
Contract Fee	Contract: $5,000 (Elvidence, n.d.)	$5,000
Collect and preserve data	Collect per device: $1,275 (howelawfirm,n.d.)	$1,275 x 3 = $3,825
Imaging cost	Image per device: <500 GB $300 500 GB - 1 TB $500 1 TB - 2 TB $700 >2 TB $900 (USDF, 2019)	Total = 3 x $500= $1,500
Analysis cost	Analysis per device: <500 GB $1400 500 GB - 1 TB $1650 1 TB - 2 TB $1850 > 2 TB $2000 (USDF, 2019)	Total= 3 x $1,650= $4,950
Reports for legal review	Legal Review: $1,200 (howelawfirm, n.d.)	$1,200
Expert Witness	Expert review per hour: $475 (howelawfirm,n.d.)	$475

Transport fee	Fee: $500 (Self estimation)	$500
Forensic report and document	Report: $40,000 (Croft, 2021)	$40,000
Additional laboratory tests and research (Depends on situation)	Per hard drive/memory: $5,000-$20,000 (Sandra, 2022) Estimation = $20,000 + $5,000 = $25,000 / 2 = $12,500*	$12,500 x 3 = $37500
Total		$194,392.5

Reference

96hz. (n.d.). Live vs Index Search. Retrieved from, https://www.forensicfocus.com/forums/general/live-vs-index-search/#:~:text=In%20FTK%2C%20index%20search%2C%20searches,that%20as%20a%20live%20search.

Computer Forensic Services. (n.d). Sydney Computer Forensic Services. Retrieved from, https://www.australiandatarecovery.com.au/computer-forensic-services

Computer Forensic Services. (n.d.). How Long Does A Forensic Exam Take? Retrieved from, https://www.computerpi.com/resources/how-long-does-a-forensic-exam-take/

Croft. (2021, July 21). How Much Does a Forensic Accounting Report Cost? Retrieved from, https://briferrier.com.au/news/how-much-does-a-forensic-accounting-report-cost

CSS. (n.d.). FTK Imager. Retrieved from, https://www.computersecuritystudent.com/FORENSICS/FTK/IMAGER/FTK_IMG_313/lesson4/index.html

Cyber Writes Team. (2021, November 8). Pros and Cons of Using Open-Source Software. Retrieved from, https://cybersecuritynews.com/pros-and-cons-of-using-open-source-software/

Elvidence. (n.d.). Rates. Retrieved from, https://www.elvidence.com.au/home/rates/

Erminger. (2022). Magnet Business Strategy and Pricing. Retrieved from, https://www.reddit.com/r/computerforensics/comments/v8rf82/magnet_business_strategy_and_pricing_cyber/

Forensic Focus. (2011, July 18). Timeline Analysis – A One Page Guide. Retrieved from, https://www.forensicfocus.com/articles/timeline-analysis-a-one-page-guide/

FutureLearn (n.d.). Prefetch Files. Retrieved from, https://www.futurelearn.com/info/courses/introduction-to-malware-investigations/0/steps/147875

H-11. (2019, July 30). 7 Time Saving Strategies for Investigators. Retrieved from, https://h11dfs.com/7-time-saving-strategies-for-investigators/

Harvery, Phil. (2023). Exiftool. Retrieved from, https://exiftool.org/exiftool_pod.html

Howelawfirm. (n.d.). Fees. Retrieved from, https://www.howelawfirm.com/fees/#F1

Hughes, A. (2007, January). Seven Uses of Open-Source Software for the Digital Forensic Lab. Retrieved from, https://www.ojp.gov/ncjrs/virtual-library/abstracts/seven-uses-open-source-software-digital-forensic-lab#:~:text=Some%20of%20the%20benefits%20of,which%20the%20data%20is%20viewed.

Investintech. (n.d.). Pros & Cons of Open Source in Business. Retrieved from, https://www.investintech.com/resources/blog/archives/7975-pros-cons-open-source-business.html

IPL. (n.d.). Advantages and Disadvantages Of Forensic Tools. Retrieved from, https://www.ipl.org/essay/Advantages-And-Disadvantages-Of-Forensic-Tools-FCQGHYXZ26#:~:text=The%20advantages%20of%20using%20forensic,can%20now%20be%20retrieved%20with

Magnet Forensics. (2022, March 7). How To Get Started with DVR Examiner. Retrieved from, https://www.magnetforensics.com/blog/how-to-get-started-with-dvr-examiner/?utm_source=Google&utm_medium=Search&utm_campaign=2023_Resource_Centre&gad=1&gclid=CjwKCAjwgZCoBhBnEiwAz35RwkjdpU5y04io30y_fWdbx3i59tq_nOZkQNMxCW7Kyg12f1OVNzmREBoC9YAQAvD_BwE

Microsoft. (2023, January 1). Ensuring Data Integrity with Hash Codes. Retrieved from, https://learn.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes

NIST. (n.d.). Chain of Custody. Retrieved from, https://csrc.nist.gov/glossary/term/chain_of_custody#:~:text=Definitions%3A,the%20purpose%20for%20the%20transfer.

Sandra. (2022). How much does a forensic analysis cost? Retrieved from, https://www.newzealandrabbitclub.net/how-much-does-a-forensic-analysis-cost/

SCMedia. (2016, October 3). AccessData Forensic Toolkit (FTK). Retrieved from, https://www.scmagazine.com/product-test/accessdata-forensic-toolkit-ftk

Sleuthkit. (n.d.). Autopsy User Documentation. Retrieved from, https://sleuthkit.org/autopsy/docs/user-docs/4.12.0/logical_imager_page.html#:~:text=To%20start%2C%20open%20Autopsy%20and,Tools%2D%3ECreate%20Logical%20Imager.&text=The%20normal%20use%20case%20is,once%20you%20finish%20the%20configuration.

ThreatDotMedia. (n.d.). What is a Write Blocker? A short definition of Write Blocker. Retrieved from, https://threat.media/definition/what-is-a-write-blocker/

Ticktechtold. (2023, March 8). 7 Advantages & Disadvantages of Digital Forensics [Pro Cons]. Retrieved from, https://www.ticktechtold.com/advantages-disadvantages-of-digital-forensics/

USDF. (2019). Flat Fee – Digital Forensic. Retrieved from, https://www.usdataforensics.com/digital-forensics-flat-fee

Wahocho, M. (2023, July 5). Why Is It Important To Secure The Scene Of The Accident? Retrieved from, https://www.hseblog.com/best-practices-for-securing-and-documenting-an-accident-scene/