



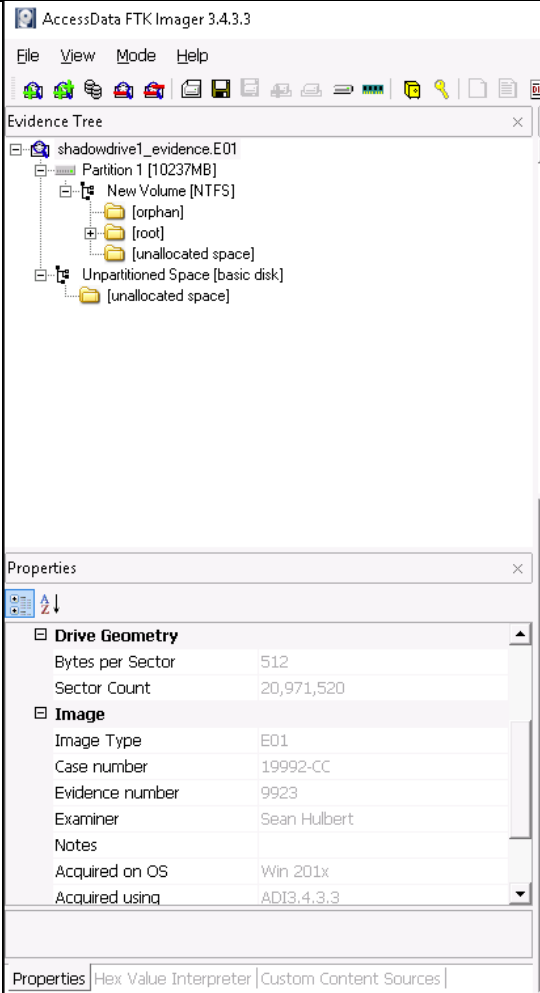
Analysis Notes – Do Not Disseminate

Initials XX = [Student Name]

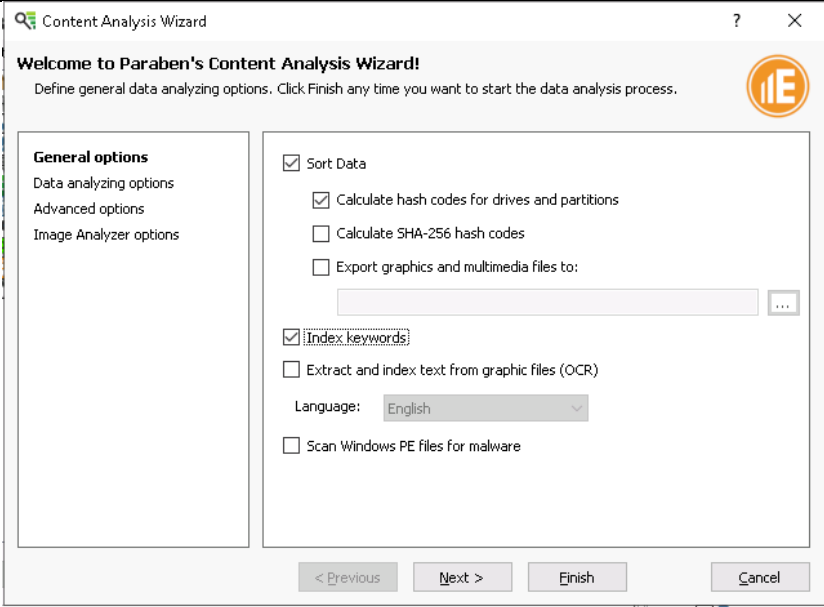
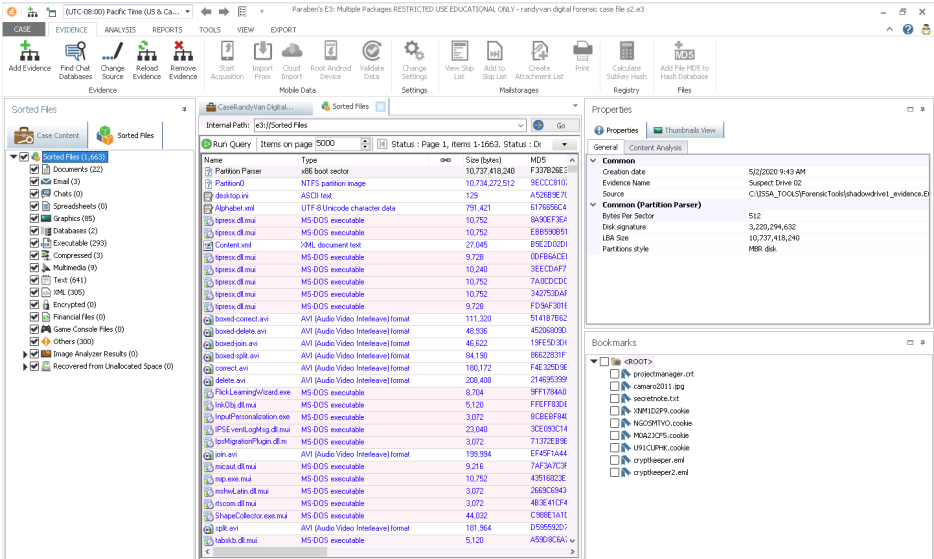
Dates	Initials	Specimen(s)	Notes
CART Equipment Used			
			<u>EXAM EQUIPMENT INFORMATION</u> The following workstation was used for analysis: <ul style="list-style-type: none">- Make: Apple- Model: MacBook Pro (15-inch, 2018)- Unique ID: C02XJ3J7JG6N- Label: Exam A
CART Request			
03/26/2020			CART exam Service Request ID 54321 submitted by Case Agent SA Austin Winters.
03/26/2020	RV	1B1	CART Service Request assigned to SA/FE Randy Van
05/02/2020	RV		<u>LEGAL AUTHORITY</u> <ul style="list-style-type: none">- Legal Authority was reviewed; Legal authority to proceed with the examination was a Search Warrant signed by Magistrate Judge Bryan Earl on 03/26/2020.
Evidence Inventory			
05/02/2020	RV	1B1	<u>RECEIPT OF EVIDENCE</u> Received the following evidence from case agent. Q numbers were assigned to each specimen: <ul style="list-style-type: none">- Q9923 shadowdrive1_evidence.E01 (1B1)
05/02/2020	RV	Q9923	<u>PRE-EXAMINATION HASH</u> <ul style="list-style-type: none">- The received images were copied to a shared area network(SAN) and were verified using FTK Imager version 3.4.3.3.- Once FTK Imager is opened, the evidence item would be added. Image File would be selected as the source and the image file would be found in PC>Local Disk(C:)> ISSA_TOOLS>ForensicTools>shadowdrive1_evidence.E01- After the image file is processed, the shadowdrive1_evidence.E01 file can be pre-verified. Q9923 shadowdrive1_evidence.E01 (1B1): Image Verification Results: Verification started: Sat May 02 08:12:43 2020 Verification finished: Sat May 02 08:15:53 2020 MD5 checksum: f337b26e312ea1282f8b93b6ce0ab271 : verified SHA1 checksum: c8b43e8d684d683d78bbb19fee82653ce31133ad : verified
05/02/2020	RV	Q9923	<u>HARDWARE GEOMETRY AND SYSTEM INFORMATION</u> FTK Imager was used to obtain the following Drive Geometry and Partition information for each item: The Drive Geometry and Partition section can be found by viewing Properties. Q9923



Analysis Notes – Do Not Disseminate

			
Examination			
05/02/2020	RV	Q9923	<p><u>PROCESSING</u></p> <p>Opened image associated with the shadowdrive1_evidence.E01 using Paraben's Electronic Evidence Examiner(E3) Bronze 2.2 Edition.</p> <ul style="list-style-type: none">- Add the evidence as an Image File and Auto detect the image.- The image can be found in PC>Local Disk(C:)>ISSA_TOOLS>ForensicTools>shadowdrive1_evidence.E01.- Open the content Analysis wizard and select Sort Data, Calculate hash codes for drives and partitions and Index Keywords.



			<div></div> <p>Q9923 shadowdrive1_evidence.E01 (1B1): Opened image using Paraben's Electronic Evidence Examiner(E3) Bronze 2.2 Edition.</p> <div></div>
05/02/2020	RV	Q9923	<p>DIRECTORY/FILE LISTING</p> <p>A directory file listing was generated using FTK Imager.</p>
Analysis			
05/02/2020	RV	Q9923	<p>ANALYSIS</p> <p>Analyzed image using Paraben's E3 to find and bookmark information about the case.</p> <ul style="list-style-type: none">- Personal Information about the suspect was found by performing a keyword search on the subject's name "Jamestown".- After performing the search a secretnote.txt was found and bookmarked. <ol style="list-style-type: none">1. Secretnote.txt – contains information personal information about the suspect that includes first and last name, birthdate, address, and credit



Analysis Notes – Do Not Disseminate

			<p>card information that might be relevant to the credit card fraud case.</p> <ul style="list-style-type: none">- After searching through the emails in the sorted file section, two emails were found and bookmarked giving information about a possible fraud scheme and co-conspirators involved.2. Cryptkeeper.eml – This email gives the emails of Samuel Jamestown and outlines plans that suggest that the suspects have obtained keycodes and plan to get the access code of a women named Beth, so they can frame her. The email states that Samuel's code is in the email and the e-mail was signed off by a possible co-conspirator with the code name Skeleton Key.3. Cryptkeeper2.eml – this second e-mail confirmed that they have obtained Beth's access code and that the second part of Samuel's code can be found in a riddle provided the e-mail. The e-mail was signed off by another possible co-conspirator codenamed Diablo.- A keyword search was done to find and bookmark possible social media accounts.4. XNM1D2P9.cookie – a cookie giving information about a Facebook session. Facebook can possibly be used to as an another avenue to discuss further details of the fraud and can be used to find out more information about the suspect and the suspect's accomplices.5. NGOSMTVO.cookie – a cookie found giving information about a Twitter session. Twitter can possibly be used to as an another avenue to discuss further details of the fraud and can be used to find out more information about the suspect and the suspect's accomplices.6. MOA2JCF5.cookie – a cookie found giving information about a LinkedIn session. LinkedIn information can be used to find out information about the suspect's occupation.7. U91CUPHK.cookie - a cookie found giving information about a LinkedIn session. LinkedIn information can be used to find out information about the suspect's occupation.- Searching through image files evidence was found and bookmarked on the a suspected sports car and the suspect's possible occupation.8. Camaro2011.jpg – an image of a sports car that was possibly brought with the money obtained from the possible fraud scheme.9. Projectmanager.crt – this .crt extension was actually an image of a shirt describing what it's like being a project manager.
Derivative Evidence			
05/02/2020	RV	Q9923	REPORTING Generated report using Paraben's Electronic Evidence Examine(E3) Generate Report Wizard. Ensure that all cookies and case history is selected when generating the report.



Analysis Notes – Do Not Disseminate

		<div><div><div><div><div>Reports Wizard</div><div><div>General options</div><div>Select General options: report type, destination folder etc. Follow the wizard steps to define what information will be added to the report.</div><div><div><div>General options</div><div>Investigator's Information</div><div>Sorted files</div><div>Custom Report View</div><div>Summary and Conclusion</div><div>Logs & Supplementary files</div></div><div><div>Select the report type to be generated :</div><div><div><input type="radio"/> HTML Investigative Report</div><div>(example)</div><div>(all evidence)</div></div><div><input type="radio"/> Simple Text Report</div><div>(example)</div><div>(all evidence)</div></div><div><input type="radio"/> Simple RTF Report</div><div>(example)</div><div>(all evidence)</div></div><div><input type="radio"/> CSV Text Report</div><div>(example)</div><div>(all evidence)</div></div><div><input checked="" type="radio"/> HTML Evidence Summary Report</div><div>(example)</div><div>(all evidence)</div></div><div><input type="radio"/> HTML E-mail Message Report</div><div>(example)</div><div>(e-mail databases only)</div></div><div><input type="radio"/> Malware Scan Results Report</div><div>(example)</div><div>(malware scan results)</div></div><div><input type="radio"/> Mobile Evidence Timeline Report</div><div>(example)</div><div>(mobile cases only)</div></div> <div><input type="radio"/> Mobile Evidence PDF Report</div> <div>(example)</div> <div>(mobile cases only)</div>
--	--	---

☐ Mobile Excel Spreadsheet Report[\(example\)](#)

(mobile cases only)

☐ Mobile Data Review Report[\(example\)](#)[\(data included in report\)](#)☐ Include parsed embedded dataDestination folder :

Browse...

☒ Open report on finish☐ Save current wizard options as default

< Previous

Next >

Finish

Cancel

Reports Wizard

Logs and Supplementary files

Select case log options and supplementary files that will be added to the report.

General options

Investigator's Information

Sorted files

Custom Report View

Summary and Conclusion

Logs & Supplementary files

Case History options:

☒ Include Case History

☒ Export Case History to a file and add a link

Note: Case History can be very big. It is recommended to export it as a separate file.

Click the Add/Remove buttons to select files. Files are placed in the external folder and links to them are added to the report.

Add... Remove

< Previous

Next >

Finish

Cancel



Analysis Notes – Do Not Disseminate

Initials XX = [Student Name]

Post Examination Hash			
05/02/2020	RV	Q9923	<p><u>POST-EXAMINATION HASH</u></p> <p>FTK Imager version 3.4.3.3 was used to conduct a post-verification image.</p> <p>Q9923 shadowdrive1_evidence.E01 (1B1):</p> <p>Image Verification Results:</p> <p>Verification started: Sat May 02 19:42:02 2020</p> <p>Verification finished: Sat May 02 19:46:14 2020</p> <p>MD5 checksum: f337b26e312ea1282f8b93b6ce0ab271 : verified</p> <p>SHA1 checksum: c8b43e8d684d683d78bbb19fee82653ce31133ad : verified</p>
Disposition of Evidence			
05/02/2020	RV		Burned CD containing DE was entered into Evidence Control.
Archive Exam			
05/02/2020	RV		A backup tape was made of all case files and images, and entered into Evidence Control.
05/02/2020	RV		END OF EXAM