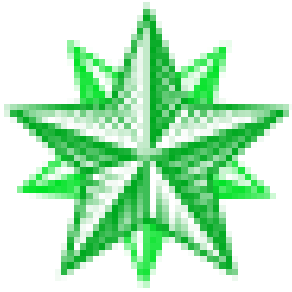
DIGITAL FORENSICS REPORT

Evidence Analysis in Case #5465448

Daniel Weinert
CSS-3752-01V
12/13/21



CyberDefenders LLC

Investigator:	Peter Hacx
	CTO
	X Corp
Digital Forensic Examiner:	Daniel Weinert
	Officer #064
	CyberDefenders LLC
Leading LEO:	Zoe Kallus
	Officer #064
	Metro Police
Subject:	Digital Forensics Report
	Case #5465448
Offences:	
	Network Intrusion
	Possible Breach of Pii
	Possible Breach of Financial Information
Data of Request:	10/15/2021
Date of Conclusion:	12/13/2021

Table of Contents

Abstract

Executive Summary

On September 22nd a break in occurred at X Corp headquarters, a single suspect tripped a silent alarm which alerted police and prompted the suspect to flee. A laptop and thumb drive were recovered from the scene and analyzed. We identified the owner of the laptop and now current suspect and the purpose which was to copy customer information from X Corp. All sensitive data that was stolen has been recovered and we do not believe there is a major risk to any more data breaches regarding this incident.

Case Background

According to the police report the break in occurred at X Corp headquarters on September 22nd, 2021, at 1:30am. A silent alarm was triggered around 2am which caused Officer Kallus from the Metro Police Department to respond. As soon as she arrived on scene, one suspect was seen fleeing the building, the officer started pursuit but failed when the suspect jumped into a parked car that was ready. A crime scene was then established at the X Corp offices and Metro Police CSI team started to gather evidence from the scene. They obtained an unknown laptop that was left plugged into the network and a thumb drive from the parking garage which the suspect presumably dropped during the pursuit.

IT Room #2101 (Crime Scene)

Police Report Case #5465448

OFFENSE/INCIDENT REPORT
INSTRUCTIONS ARE PRINTED SEPARATELY. IF ADDITIONAL SPACE IS NEEDED, USE REVERSE OF FORM; IDENTIFY ITEMS.

1. TYPE: [X] a. ORIGINAL [ ] b. CONTINUATION [ ] c. SUPPLEMENT OR FOLLOWUP
2. CODE NO.: 10-74 | 2a. SORT: | 3. TYPE OF OFFENSE OR INCIDENT: Burglary | 4. CASE CONTROL NUMBER: #5465448
5. BUILDING NUMBER: 01 | 6. ADDRESS: 25 E 16th Ave, Denver, CO 80202
7. NAME OF AGENCY/BUREAU: Metro Police | 8. AGENCY/BUREAU CODE: | 9. SPECIFIC LOCATION: IT Room #1201 | 10. LOCATION CODE:
11a. DATE OF OFFENSE/INCIDENT: 9/22/2021 | 11a. TIME OF OFFENSE/INCIDENT: 01:36 | 12. DAY: | 13a. DATE REPORTED: 9/22/2021 | 13b. TIME REPORTED: 02:05 | 14. DAY:
15. JURISDICTION (X): [ ] EXCLUSIVE [ ] CONCURRENT [ ] PARTIAL [ ] PROPRIETARY | 16. NO. OF DEMONSTRATORS: | 17. NO. EVACUATED: | a. TIME START: | b. TIME END:

18. PERSONS INVOLVED

ID CODE (a)	NAME AND ADDRESS (b)	AGE (c)	SEX (d)	RACE (e)	INJURY CODE (f)	TELEPHONE (g)
	Last Name, First, Middle Initial: Hacx, Peter		M			HOME
	Number, Street, Apt. No., City and State: CTO, point of contact for X Corp.					BUSINESS
	Last Name, First, Middle Initial					HOME
	Number, Street, Apt. No., City and State					BUSINESS

19. VEHICLE

a. STATUS	b. YEAR	c. MAKE	d. MODEL	e. COLOR (Top/Bottom)	f. IDENTIFYING CHARACTERISTICS	i. VALUE
STOLEN / GOV'T / VANDALIZED / SUSPECT / PERSONAL / RECOVERED / IMPOUNDED BY ADMINISTRATION						

non-applicable

20. ITEMS TAKEN

a. NAME OF ITEM	b. QUANTITY	c. OWNERSHIP	d. BRAND NAME
		[ ] GOV'T [ ] PERSONAL	
e. SERIAL NO.	f. COLOR		g. MODEL
h. VALUE	i. UNUSUAL OR UNIQUE FEATURES		
j. PROPERTY WAS [ ] SECURRED [ ] UNSECURED	k. STATUS OF PROPERTY [ ] RECOVERED [ ] MISSING [ ] PARTIAL RECOVERY		VALUE RECOVERED
l. NAME OF ITEM	BRAND NAME		
p. SERIAL NO.	q. COLOR		r. MODEL
s. VALUE	t. UNUSUAL OR UNIQUE FEATURES		
u. PROPERTY WAS [ ] SECURRED [ ] UNSECURED	v. STATUS OF PROPERTY [ ] RECOVERED [ ] MISSING [ ] PARTIAL RECOVERY		VALUE RECOVERED

non-applicable

21. NARRATIVE (If additional space is needed, use blank sheet and attach.)

Objectives

There are multiple sub-objectives regarding the case that this digital forensic report will try to address to fulfill in order to get to the main objective. First is to determine the owner and purpose of the device that was found plugged into the network at the crime scene. Second is to determine if there was any sensitive data that was either stolen or changed. Third is to establish if the found thumb drive has any relevance to the case and if so, does it contain any sensitive data. These will help us get to the bottom of main objective which is to investigate if there was any data stolen whatsoever.

Evidence

Chain of Custody Form

EVIDENCE/PROPERTY CUSTODY DOCUMENT		TRACKING NUMBER CASE ID NUMBER #5465448
RECEIVING ACTIVITY	LOCATION	
NAME, GRADE AND TITLE OF PERSON FROM WHOM RECEIVED G OWNER G OTHER Mr. Hacx	ADDRESS (Including Zip Code) 25 E 16th Ave, Denver, CO 80202	
LOCATION FROM WHERE OBTAINED	REASON OBTAINED Investigation	DATE/TIME OBTAINED 9/22/2021 02:30

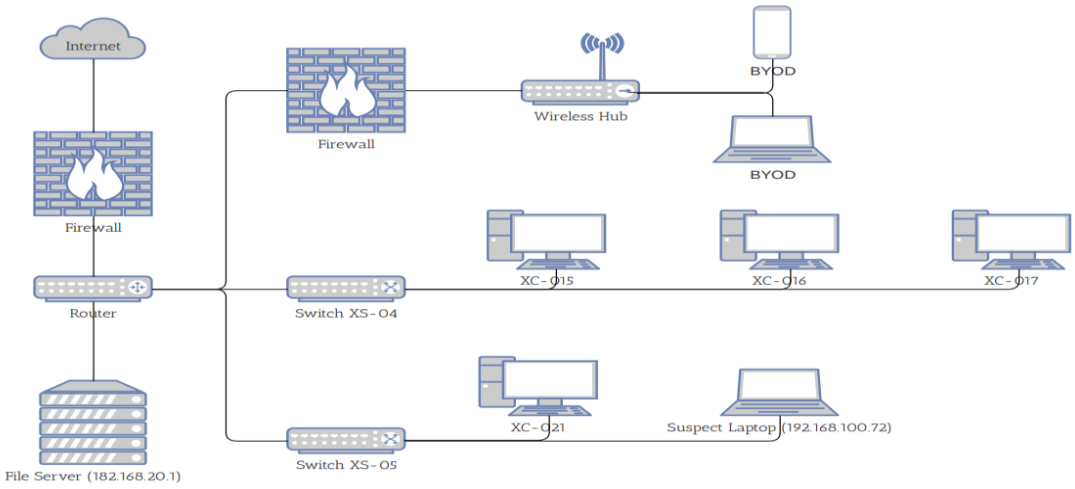
ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES (Include model, serial number, condition and unusual marks or scratches)
E-1	1	External Storage Device
E-2	1	Laptop
E-3	1	Cat 6 Ethernet cable

CHAIN OF CUSTODY

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
E-1,2,3	10/15/2021	SIGNATURE Zoe Kallus NAME, GRADE OR TITLE Officer	SIGNATURE Daniel Weinert NAME, GRADE OR TITLE CyberDefenders LLC	Digital Forensic Investigation by 3rd Party

Suspect Laptop

The laptop found at the scene has been identified as an Acer Aspire 5742 (S/N: LXPAU0Y00492806D392). It was found sitting on a desk with an active connection via an ethernet cable to a file server on the internal network. Officers closed the device and bagged it but haven't done anything else to it since we received it for forensic purposes. Below is a network diagram of how all devices where setup in the room when Police found it and they marked down the IPv4 address the laptop was assigned to.



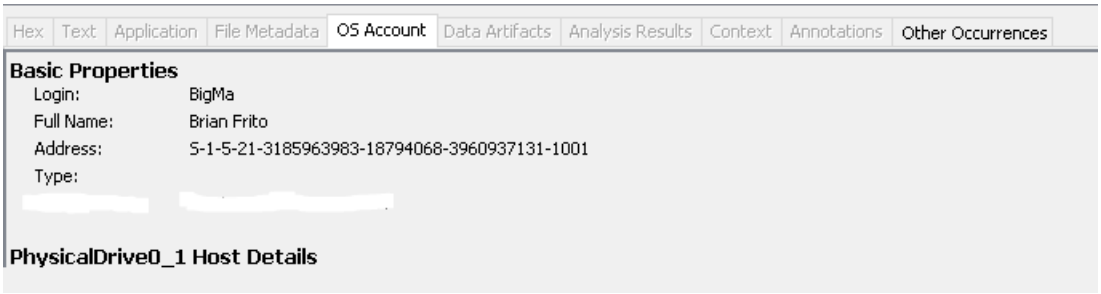
Dropped USB Thumb Drive

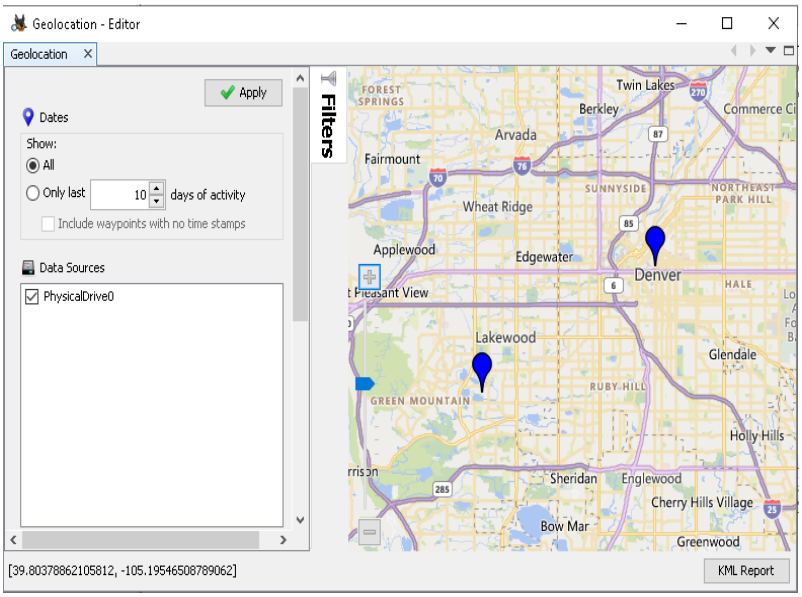
The dropped USB thumb drive has been identified as a 16GB PNY Thumb Drive. There seems to be nothing significant about the device, just a regular looking USB thumb drive. It only contained one file which will be discussed in the Analysis section.

Analysis

Analysis of Laptop

The laptop found at the scene was fully investigated and we ran a full spectrum autopsy analysis on it. First, we identified that the laptop is indeed not from X Corp but an unknown source. To figure out who that is we ran an analysis of the OS account on the device and matched the corresponding results to private information on the device to match the owner. We identified Brian Frito has the account holder of this device and shared all information we found about him with Officer Kallus.





Next up, an autopsy identified two GPS location that were made by the web browser in the last 24 hours on the day of the break in. The first one matches the location of the X Corp building and where the crime happened and the second is from a house in a neighborhood around 30 mins away which is presumably where the suspect was coming from. This map left shows the two points marked on the autopsy map.

Lastly on our analysis of the found laptop, we ran a keyword search regarding topics relevant to this investigation and we have identified a backed-up email thread log which very much relates to this case and seems to be the most significant peace of evidence we were able to find regarding what happened in this case.

Email Analysis

e: Craigslist - Job opportunity

From: Katey Holler <KateyKitten1@hotmail.com>
Sent: Sunday, September 12, 2021 5:54 PM
To: BigManBrian92@outlook.com <BigManBrian92@outlook.com>
Subject: Craigslist - Job opportunity

Hello Mr. Hacker,

I work for a financial company and would be interested in hiring your services. We are about to expand into a new sector and there is another firm in town which already expanded into that field. We were wondering if you could gain access to their network and take a little peep at their customer list for us that would be greatly appreciated, and you will be very nicely rewarded.

K.

From: Brian Frito <BigManBrian92@outlook.com>
Sent: Monday, September 13, 2021 3:36 PM
To: Katey Holler <KateyKitten1@hotmail.com>
Subject: Re: Craigslist - Job opportunity

Yes, I would be able to do this job. I would need to know the specifics of who the company is? What specific customer list do you need? and how much am I getting paid?

Hacker

From: Katey Holler <KateyKitten1@hotmail.com>
Sent: Monday, September 13, 2021 5:12 PM
To: Brian Frito <BigManBrian92@outlook.com>
Subject: Re: Craigslist - Job opportunity

Hacker,

Okay I am glad you can help us. The company is called X Corp and they are located 25 E 16th Ave. The customer list we are looking for is regarding their new high volatile securities program. Any customer list that contains customers with high shares of the new securities are interesting to us. Regarding your payment we are willing to pay $10,000

K.

From: Brian Frito <BigManBrian92@outlook.com>
Sent: Tuesday, September 14, 2021 2:41 AM
To: Katey Holler <KateyKitten1@hotmail.com>
Subject: Re: Craigslist - Job opportunity

Sounds good, I will accept that offer. I will need around 2 weeks or so. I will contact you when I have the information.

Katey Holler <KateyKitten1@hotmail.com>
Wed 09/15/2021 10:22 AM
To:

- Brian Frito <BigManBrian92@outlook.com>

Hacker,

Sounds good, we will have the payment ready.

K.

After the recovery and analysis of this email chain, we believe we have found the motive and structure of this case. The account email address that is receiving the first message in this thread (BigManBrian92@outlook.com) is the same one that the OS account of the laptop is registered too. The sending email address (KateyKitten1@hotmail.com) seems to belong to a Miss Katey Holler which according to Mr. Hacx is the CTO of a competing firm called Z Trading Inc. The conversation is relating to case and seems to be indicating that Miss Holler contacted Mr. Frito regarding hiring him to gain access to customer files of X Corp.

Analysis of USB Thumb Drive

After investigating and analyzing the thumb drive, we found nothing out of the ordinary with it and it seemed to only contain one file which was copied on to it just minutes before Officer Kallus arrived on scene. The file itself is a .cvs type and contained a list of customers and their private information. After talking to Mr. Hacx, we got permission to access that very same file server to check if the customers list recovered originated from that sever. First, we noticed that only about 27% of the customer list seems to be on the thumb drive, the last entry only contains half the information for the customer which might be an indication that the suspect was in the progress of copying the customer files when Officer Kallus arrived, the suspect must've abruptly stopped the copying process to flee. We found exactly 2,824 entries of individual customers on that file, a small snipped can be seen below. When we ran a hash checksum on each file set we found them to be identical and most likely a match.

Customer List:	MD5 Hash:	Check:
File Server	b119a9311aa67bec6daf502946f5	✓
Thumb Drive	b119a9311aa67bec6daf502946f5	✓

	CUSTOMERNAME	PHONE	ADDRESSLINE1	CITY	STATE	POSTALCO	COUNTRY	TERRITOR	CONTACTL	CONTACTF	DEALSIZE
2	Land of Toys Inc.	2125557818	897 Long Airport Avenue	NYC	NY	10022	USA	NA	Yu	Kwai	Small
3	Reims Collectables	26.47.1555	59 rue de l'Abbaye	Reims		51100	France	EMEA	Henriot	Paul	Small
4	Lyon Souveniers	+33 1 46 62 7555	27 rue du Colonel Pierre A	Paris		75508	France	EMEA	Da Cunha	Daniel	Medium
5	Toys4GrownUps.com	6265557265	78934 Hillside Dr.	Pasadena	CA	90003	USA	NA	Young	Julie	Medium
6	Corporate Gift Ideas Co.	6505551386	7734 Strong St.	San Franci	CA		USA	NA	Brown	Julie	Medium
7	Technics Stores Inc.	6505556809	9408 Furth Circle	Burlingam	CA	94217	USA	NA	Hirano	Juri	Medium
8	Daedalus Designs Imports	20.16.1555	184, chausse de Tournai	Lille		59000	France	EMEA	Rance	Martine	Small
9	Herkku Gifts	+47 2267 3215	Drammen 121, PR 744 Ser	Bergen		N 5804	Norway	EMEA	Oeztan	Veysel	Medium
10	Mini Wheels Co.	6505555787	5557 North Pendale Stree	San Franci	CA		USA	NA	Murphy	Julie	Small
11	Auto Canal Petit	(1) 47.55.6555	25, rue Lauriston	Paris		75016	France	EMEA	Perrier	Dominique	Medium
12	Australian Collectors, Co.	03 9520 4555	636 St Kilda Road	Melbourne	Victoria	3004	Australia	APAC	Ferguson	Peter	Medium
13	Vitachrome Inc.	2125551500	2678 Kingston Rd.	NYC	NY	10022	USA	NA	Frick	Michael	Small
14	Tekni Collectables Inc.	2015559350	7476 Moss Rd.	Newark	NJ	94019	USA	NA	Brown	William	Medium
15	Gift Depot Inc.	2035552570	25593 South Bay Ln.	Bridgewat	CT	97562	USA	NA	King	Julie	Medium
16	La Rochelle Gifts	40.67.8555	67, rue des Cinquante Ota	Nantes		44000	France	EMEA	Labrune	Janine	Medium
17	Marta's Replicas Co.	6175558555	39323 Spinnaker Dr.	Cambridge	MA	51247	USA	NA	Hernandez	Marta	Medium
18	Toys of Finland, Co.	90-224 8555	Keskuskatu 45	Helsinki		21240	Finland	EMEA	Karttunen	Matti	Small
19	Baane Mini Imports	07-98 9555	Erling Skakkes gate 78	Stavern		4110	Norway	EMEA	Bergulfsen	Jonas	Medium
20	Diecast Classics Inc.	2155551555	7586 Pompton St.	Allentown	PA	70267	USA	NA	Yu	Kyung	Medium
21	Land of Toys Inc.	2125557818	897 Long Airport Avenue	NYC	NY	10022	USA	NA	Yu	Kwai	Medium
22	Salzburg Collectables	6562-9555	Geislweg 14	Salzburg		5020	Austria	EMEA	Pipps	Georg	Large
23	Souveniers And Things Co.	+61 2 9495 8555	Monitor Money Building,	Chatswoo	NSW	2067	Australia	APAC	Huxley	Adrian	Small
24	La Rochelle Gifts	40.67.8555	67, rue des Cinquante Ota	Nantes		44000	France	EMEA	Labrune	Janine	Small
25	FunGiftIdeas.com	5085552555	1785 First Street	New Bedf	MA	50553	USA	NA	Benitez	Violeta	Medium
26	UK Collectables, Ltd.	(171) 555-2282	Berkeley Gardens 12 Bre	Liverpool		WX1 6LT	UK	EMEA	Devon	Elizabeth	Small
27	Euro Shopping Channel	(91) 555 94 44	C/ Moralzarzal, 86	Madrid		28034	Spain	EMEA	Freyre	Diego	Large

Conclusion

Outcome

CyberDefenders LLC was hired to help with digital forensics regarding this case. First, we were tasked to figure out who the device belongs to and who might've left it there. We identified the owner and presumed current user of the device as Brian Fritos. Next, we analyzed the thumb drive and determined it very much related to the case since we found customer files copied from the plugged-in laptop. We also discovered an email chain that is very relevant to the case and have forwarded that to the police. Regarding the risk of not having recovered all sensitive data, we rank this risk very low. We found no indication that the laptop copied and send information other than what is on that thumb drive, no digital or other connection was found on the device which could've been another file transfer.

Legal Matters

Since it does not seem likely any data was fully lost and all data that was stolen for a brief moment has been recovered, we do not think that any major legal action regarding data privacy is required, since the suspect did gain access to sensitive data for a while you will have to publicly announced the breach, but you won't have to contact individuals regarding their sensitive data.